Majandus- ja infotehnoloogiaministri …… . a määrus nr …
„Ettevõtlus- ja infotehnoloogiaministri
16. detsembri 2022 määruse
nr 101 „Eesti infoturbestandard“ muutmine“
Lisa 2

Eesti infoturbestandard

Etalonturbe kataloog

E-ITS MOODULITE SISUKORD

ISMS: Turbehaldus

ISMS.1 Turbehaldus

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed infoturbe halduse süsteemi (ingl *Information Security Management System*, ISMS) rajamiseks ning täiustamiseks. Esitada juhised turbekontseptsiooni väljatöötamiseks.

1.2 Vastutus

Turbehalduse meetmete täitmise eest vastutab infoturbejuht.

Lisavastutajad

Organisatsiooni juhtkond, ülemus.

1.3 Piirangud

Moodul põhineb etalonturbe metoodikal ja Eesti Infoturbestandardi nõuete dokumendil (*Eesti Infoturbestandard Nõuded infoturbe halduse süsteemile*). Infoturbega seotud personalimeetmeid käsitletakse mooduligrupis ORP.2 *Personal*.

2 Ohud

2.1 Isikliku vastutuse puudumine turbeprotsessis

Kui organisatsiooni turbeprotsessis ei ole töökohustused piisava täpsusega määratud, puudub töötajal isiklik vastutus infoturbe tagamise eest. Töötajad enamasti väldivad lisakohustusi, mistõttu jäävad turvameetmed rakendamata.

2.2 Puudulik toetus organisatsiooni juhtkonnalt

Juhul, kui infoturbejuht ei kuulu organisatsiooni juhtkonda, on tal raske nõuda infoturbe meetmete rakendamist kõrgemal positsioonil olevatelt isikutelt. Töötajad ei täida infoturbe nõudeid, kui juhtkond ise eeskuju ei näita.

2.3 Ebapiisav kava infoturbe strateegia elluviimiseks

Turbekontseptsioonis sisalduvaid strateegilisi eesmärke võidakse pidada pelgalt kavatsuste deklaratsiooniks ja nende elluviimiseks ei eraldata piisavalt ressursse.

2.4 Ebaoptimaalsed investeeringud

Oludes, kus organisatsiooni juhtkond pole teadlik infoturbe tegelikust olukorrast, infoturbe tagamiseks piisavaid ressursse kas ei eraldata või ei kasutata neid parimal viisil. Puudused ressursside jaotamisel võivad põhjustada üleinvesteerimist ühes lõigus kui teistes lõikudes on ressursipuudus. Ülemäära kallite ja keerukate tehniliste turbelahendustega võib kaasneda uusi turvanõrkusi.

2.5 Turvameetmete rakendamata jätmine

Kui organisatsioon pole seadnud selgeid infoturbe eesmärke, saab infoturbe vajadust organisatsioonis tõlgendada mitmeti. Kui infoturvet ei peeta vajalikuks või piisavalt oluliseks, jäävad turvameetmed rakendamata.

2.6 Turbeprotsessi ajakohastamata jätmine

Kui organisatsioon pidevalt ei panusta turbeprotsessi läbivaatamisse ja parendamisse, siis organisatsiooni turvatase langeb või aegamööda asendub ohtliku näilise turvalisusega. Väheneb organisatsiooni vastupanuvõime uutele infoturbe ohtudele.

2.7 Seaduste ja lepingute mittetäitmine

Kui organisatsiooni töötajatel on puudulikud teadmised õigusaktidest, siis võidakse nende nõudeid tahtmatult rikkuda. Lepingutes sätestatud turvatingimuste mittetäitmine võib kaasa tuua leppetrahve või isegi lepingu lõpetamise ning ärisuhete katkestamise.

2.8 Äriprotsesside häirivad turvaintsidendid

Turvasündmus (mida sageli täiendab asjaolude halb kokkusattumus) võib vallandada turvaintsidendi, millel on organisatsiooni olulistele äriprotsessidele negatiivne mõju. Isegi kui turvaintsident ei saa avalikkusele teatavaks, võib see halvendada suhteid äripartnerite ja klientidega.

2.9 Ebamajanduslik ressursikasutus puuduliku turbehalduse tõttu

Turvatoodete ebaühtlase ja koordineerimata rakendamise korral kasutatakse raha ja tööjõudu ebaotstarbekalt. Puuduliku turbehalduse korral võivad organisatsioonile suurimat lisandväärtust toovad protsessid jääda piisava infoturbe investeeringuta.

3 Meetmed

3.1 Elutsükkel

Kavandamine

ISMS.1.M1 Infoturbe üldvastutuse võtmine juhtkonnatasemel

Evitus

ISMS.1.M2 Turvaeesmärgid ja turbe strateegia

ISMS.1.M3 Infoturvapoliitika

ISMS.1.M4 Infoturbejuhi määramine

ISMS.1.M5 Leping välise infoturbejuhi kasutamiseks

ISMS.1.M6 Infoturbekorralduse rajamine

ISMS.1.M7 Turvameetmete määramine

ISMS.1.M13 Turbeprotsessi dokumenteerimine

Käitus

ISMS.1.M8 Töötajate lõimimine turbeprotsessi

ISMS.1.M9 Infoturbe lõimimine organisatsiooniülestesse protsessidesse

ISMS.1.M10 Turbekontseptsioon

ISMS.1.M11 Infoturbe käigushoid

ISMS.1.M12 Infoturbearuanded juhtkonnale

ISMS.1.M15 Infoturberessursside ökonoomne kasutus

ISMS.1.M16 Täpsustavate turvapoliitikate väljatöötamine

Lisanduvad kõrgmeetmed

ISMS.1.M17 Kindlustuslepingute sõlmimine

3.2 Põhimeetmed

ISMS.1.M1 Infoturbe üldvastutuse võtmine juhtkonnatasemel [organisatsiooni juhtkond]

a. Organisatsiooni juhtkond võtab üldvastutuse organisatsiooni infoturbe eest. Juhtkonna kohustumus on kõigile asjaosalistele nähtav ja selgelt arusaadav.

b. Juhtkond algatab turbeprotsessi, juhib ja kontrollib protsessi ning on infoturbe korraldamisel eeskujuks.

c. Organisatsiooni juhtkond:

- määrab infoturbega seotud rollid ja ülesanded;
- tagab infoturbe töötajate pädevuse;
- tagab infoturbega seotud ülesannete täitmiseks vajalikud ressursid.

d. Organisatsiooni juhtkonda teavitatakse infoturbe olukorrast regulaarselt.

ISMS.1.M2 Turvaeesmärgid ja turbe strateegia [organisatsiooni juhtkond]

a. Arvestades organisatsiooni eesmärke, äriprotsesse ja muud olulist teavet, määrab organisatsiooni juhtkond turvaeesmärgid ja turbe strateegia.

b. Turvaeesmärgid ja turbe strateegia on dokumenteeritud. Eesmärgid on realistlikud, praktilised, põhjendatud ja arusaadavad.

c. Organisatsiooni juhtkond vaatab turbe strateegiat regulaarselt üle, tagamaks, et strateegia on endiselt sobiv ja ajakohane.

ISMS.1.M3 Infoturvapoliitika [organisatsiooni juhtkond]

a. Organisatsiooni juhtkond piiritleb üheselt ja selgelt infoturbe kaitseala.

b. Organisatsiooni juhtkond kinnitab ja kehtestab infoturvapoliitika (ingl *information security policy*).

c. Infoturvapoliitikas on kajastatud vähemalt järgmised aspektid:

- infoturbe tähtsus ning tähendus organisatsioonile;
- turbe strateegia põhielemendid;
- juhtkonna kohustumus;
- turbeprotsessi rakendamise korralduslikud alused;
- tulemuslikkuse hindamise põhimõtted.

d. Infoturvapoliitika seostab turvaeesmärgid organisatsiooni eesmärkidega arusaadaval ja iga töötajat motiveerival viisil.

e. Infoturvapoliitika tehakse teatavaks kõigile töötajatele ja organisatsiooni partneritele, vajadusel ka avalikkusele. Juurdepääs olulisele teabele võimaldatakse töötajatele ja partneritele üksnes pärast poliitika aktsepteerimist.
f. Infoturvapoliitikat ajakohastatakse regulaarselt (vähemalt kord aastas) või oluliste muudatuste puhul IT-süsteemides, organisatsiooni eesmärkides või turbe strateegias.

ISMS.1.M4 Infoturbejuhi määramine [organisatsiooni juhtkond]

a. Organisatsiooni juhtkond määrab infoturbe eest vastutava isiku - infoturbejuhi, kelle kohustused hõlmavad järgmist:
   - infoturbeprotsessi juhtimine ja koordineerimine;
   - juhtkonna toetamine infoturvapoliitika kehtestamisel;
   - turbekontseptsiooni(de) väljatöötamine ning koordineerimine;
   - infoturvapoliitika(te) ja -meetmete jõustamine;
   - turvameetmete rakendusplaani väljatöötamine, elluviimise algatamine ja kontrollimine;
   - juhtkonna pidev teavitamine infoturbe hetkeseisust;
   - infoturbe projektide koordineerimine;
   - infoturbeintsidentide menetlemine;
   - infoturbeteadlikkuse suurendamine, koolituste korraldamine.
b. Organisatsiooni juhtkond tagab infoturbejuhile tööks vajalikud tingimused ja ligipääsud teabele ning objektidele.
c. Infoturbejuhi erialane kvalifikatsioon on piisav ning infoturbejuhile on tagatud võimalused oma teadmiste täiendamiseks.
d. Infoturbejuhi kompetents ja isikuomadused lisaks erialastele oskustele on järgnevad:
   - organisatsiooni eesmärkide ja äriprotsesside tundmine;
   - koostöövõime, meeskonnatöö oskused;
   - iseseisvalt töötamise võime;
   - tahe ennast erialaselt täiendada;
   - enesekehtestamise oskus;
   - projektijuhtimise kogemus.
e. Infoturbejuht teeb oma ülesannete täitmisel koostööd andmekaitsespetsialisti ning väliste regulaatoritega.
f. Infoturbejuht on kaasatud IT projektidesse ning IT-süsteemide arendusprotsessi.

ISMS.1.M5 Leping välise infoturbejuhi kasutamiseks [organisatsiooni juhtkond]

a. Kui infoturbejuhi rolli ei saa täita oma töötajaga, siis hangitakse infoturbejuht teenusena väljastpoolt organisatsiooni.
b. Välisel infoturbejuhil on vajalik kvalifikatsioon.
c. Infoturbejuhi teenuseleping sisaldab infoturbejuhi tööülesandeid ning nendega seotud õigusi ja kohustusi. Sätestatud on vähemalt järgmised aspektid:
   - kvalifikatsiooninõuded;

- tööülesanded;
- minimaalsed ressursid ülesannete täitmiseks;
- teatamis- ja aruandlusahel, kontaktisikud;
- töökohad, tööruumid, kohaloleku- ja kättesaadavusajad;
- pääsuõigused;
- aruandluskohustus;
- koostöökohustus teenuse ostjaga.

d. Välise infoturbejuhiga on sõlmitud konfidentsiaalsusleping.

e. Infoturbejuhi teenuselepingus kajastatakse lepingulise suhte kogu elutsükkel, sealhulgas:
   - töid teostavate isikute asendamise kord;
   - huvide konflikti määratlus ja lahendusviisid;
   - lepingu rikkumise tagajärjed;
   - lepingulise suhte lõpetamise kord;
   - lepingu täitmisega seotud kulud.

ISMS.1.M6 Infoturbekorralduse rajamine [organisatsiooni juhtkond]

a. Organisatsiooni juhtkond kehtestab infoturbe korralduse organisatsioonis, määrab turvaeesmärkide saavutamiseks vajalikud rollid, tagab ressursid ning nimetab piisava kvalifikatsiooniga isikud nende rollide täitmiseks.

b. Infoturbe erinevate aspektide haldamiseks teevad koostööd:
   - infoturbejuht;
   - IT-juht;
   - äriüksuste juhid;
   - andmekaitsespetsialist.

c. Turbehalduse ülesanded on sõnastatud arusaadavalt, kohustused on selgelt määratud.

d. Kõigile olulist infoturbe rolli täitvatele isikutele on kehtestatud asendamise kord.

e. Infoturbekorralduse suhtlusteed on plaanitud, kirjeldatud, korraldatud ja teatavaks tehtud. Rollide kirjeldused sisaldavad, keda ja millises ulatuses tuleb infoturbe sündmustest teavitada.

f. Infoturbekorralduse sobivust ja toimivust kontrollitakse regulaarselt, vajadusel kohandatakse seda vastavalt muutunud tingimustele.

ISMS.1.M7 Turvameetmete määramine

a. Määratud on turvaeesmärkidest ja kaitsetarbest tulenevad turvameetmed, mis vastavad järgmistele põhinõuetele:
   - turvameetmete valik võtab arvesse toimivust, tõhusust ja majanduslikku otstarbekust;
   - meetmete valik on põhjendatud ning aluskaalutlusteni tagasijälitatav;
   - määratud on turvameetmete eest vastutavad isikud;
   - meetme rakendamise kirjeldus on esitatud turbeülesande täitmiseks vajaliku täpsusega.

b. Rakendatavad turvameetmed on süsteemselt dokumenteeritud, vajadusel meetme rakenduse kirjeldust ajakohastatakse.

c. Määratud, kuid rakendamata jäetud meetme puhul:

- on läbi viidud täiendav riskianalüüs, mis on aluseks juhtkonnale riski aktsepteerimise või mitteaktsepteerimise osas;
- on dokumenteeritud mitterakendamise põhjus ja asjaolud.

ISMS.1.M8 Töötajate lõimimine turbeprotsessi [ülemus]

a. Töötajad on kaasatud turbeprotsessi. Töötajad on teadlikud infoturbe ohtudest, tunnevad turvameetmeid ning oskavad neid tööülesannete täitmisel järgida.

b. Töötajatel on võimalik osaleda turvameetmete kavandamisel ja rakendamisel.

c. Enne turvapoliitika ja turvameetmete jõustamist selgitatakse töötajatele meetmete rakendamise vajalikkust.

d. Turvameetmete rakendamine mõjutab töötajate igapäevatööd võimalikult vähesel määral.

e. Töötajaid on teavitatud infoturvapoliitikate mittejärgimise ja turvameetmete eiramise võimalikest tagajärgedest.

ISMS.1.M9 Infoturbe lõimimine organisatsiooniülestesse protsessidesse [organisatsiooni juhtkond]

a. Infoturve on integreeritud kõigisse organisatsiooni äri- ja tugiprotsessidesse, äriprotsesside varadele infoturbe meetmete rakendamiseks on määratud vastutajad.

b. Infoturbe aspekte arvestatakse nii uute äriprotsesside juurutamisel kui olemasolevate äriprotsesside muutmisel.

c. Infoturbe haldus organisatsioonis on kooskõlas muude turvalisuse ja riskihaldusega seotud valdkondadega.

d. Infoturbejuht on alati ja vajalikul määral kaasatud infoturvet sisaldavate valdkondlike otsuste tegemisse.

ISMS.1.M10 Turbekontseptsioon

a. Infoturbe strateegia elluviimiseks ja infoturbe eesmärkide täitmiseks on välja töötatud turbekontseptsioon (ingl *security concept*). Turbekontseptsioon on turbeprotsessi alusdokument. Organisatsioonis võib olla samaaegselt mitu erinevat turbekontseptsiooni, mis rakenduvad organisatsiooni eri osadele.

b. Turbekontseptsiooni koostamisel arvestatakse infotehnoloogiast sõltuvaid äriprotsesse ja neid negatiivselt mõjutada võivaid riske.

c. Turbekontseptsioon määratleb vähemalt järgmist:

- kaitseala ja sellesse kuuluvad varad;
- kaitstavad äriprotsessid;
- äriprotsesside ja andmete kaitsetarve;
- turvameetmete modelleerimise protsess (sh meetmete prioriteedid ja teostusjärjekord, vt ISMS.1.M7 *Turvameetmete määramine*);
- riskianalüüsi läbiviimise korraldus;
- turbeprotsesside dokumenteerimise kohustus;

- infoturbe koolituste korraldus;
- infoturbe aruandluse korraldus.

d. Turbekontseptsioon arvestab asjakohaseid normdokumente ja õigusakte.

ISMS.1.M11 Infoturbe käigushoid

a. Turbeprotsessi, turbekontseptsiooni, infoturvapoliitika ja infoturbekorralduse toimivust, täielikkust ja ajakohasust kontrollitakse regulaarselt.

b. Regulaarseteks turvaläbivaatusteks on planeeritud, kes, millal, milliseid konkreetseid valdkondi ja turvameetmeid kontrollib. Läbivaatusi viivad läbi asjakohase kvalifikatsiooniga ning sõltumatud isikud.

c. Turvameetmeid ja turbekontseptsiooni vaadatakse üle lisaks regulaarsetele turvaläbivaatustele ka juhtumipõhiselt, kui:
   - lisandub uusi äriprotsesse, rakendusi ja IT-komponente;
   - tehakse olulisi taristumuudatusi;
   - viiakse läbi suuremaid korralduslikke muudatusi;
   - ohud oluliselt muutuvad;
   - ilmnevad olulised nõrkused või intsidendid.

d. Turvaläbivaatuse tulemused dokumenteeritakse ning lahknevuste põhjused selgitatakse. Läbivaatuse käigus ilmnenud puuduste parandusmeetmed dokumenteeritakse.

e. Leitud puudused kõrvaldatakse, vajadusel korrigeeritakse turvameetmeid või turbe kontseptsiooni.

f. Väliste kontrollijate puhul lepitakse kokku kohustused ja aruandlus ning sõlmitakse konfidentsiaalsuslepe.

ISMS.1.M12 Infoturbearuanded juhtkonnale [organisatsiooni juhtkond]

a. Juhtkonnale esitatakse regulaarselt aruandeid infoturbe olukorrast, eelkõige riskiseisu ning turbeprotsessi toimivuse ja tõhususe kohta.

b. Infoturbearuanne esitatakse lisaks sündmusepõhiselt, nt pärast turvaintsidenti või turbeprotsessi olulises punktis.

c. Juhtkonnale esitatavad aruanded sisaldavad olulist ja asjakohast teavet, probleeme, edusamme ja täiustamise võimalusi. Aruannetes sisalduvad ka parandusettepanekud koos prioriteetide ja hinnangutega realiseerimise aja ja töömahu kohta.

d. Juhtkonna otsused turvameetmete, jääkriskide ja turbeprotsesside muutmise kohta on jälitatavalt dokumenteeritud.

ISMS.1.M13 Turbeprotsessi dokumenteerimine

a. Turbeprotsessi protseduurid, olulised otsused ja tegevuste tulemused on dokumenteeritud. Kindlasti dokumenteeritakse järgmine:
   - aruanded juhtkonnale (vt ISMS.1.M12 *Infoturbearuanded juhtkonnale*);
   - turbeprotsessi korralduse dokumentatsioon;
   - turbetegevuste dokumentatsioon;
   - turvaintsidentide dokumentatsioon;

- tehniline dokumentatsioon (nt tehnilised juhendid, testimistulemid, rakenduste kasutusload);
- protsessijuhendid töötajatele.

b. On olemas reeglistik dokumentatsiooni koostamiseks, hoidmiseks ning dokumentatsiooni ajakohasuse ja konfidentsiaalsuse tagamiseks.

c. Olemasolevate dokumentide kehtivad versioonid on lugejate sihtgrupile kergesti kättesaadavad. Samade dokumentide eelmised versioonid on arhiveeritud ning kättesaadaval ühes kohas.

ISMS.1.M15 Infoturberessursside ökonoomne kasutus [organisatsiooni juhtkond]

a. Infoturberessursside kasutamisel arvestatakse majanduslikke aspekte. Turvameetmete ressursivajadus esitatakse numbriliselt.

b. Organisatsiooni juhtkond eraldab vajalikud infoturberessursid (raha, tööjõud, vahendid).

c. Infoturbe jaoks plaanitud ressursid on kättesaadavad õigeaegselt. Töötajatel on turbega seotud ülesannete täitmiseks piisavalt aega ja võimalusi.

d. Töökoormuse tippajal või eriülesannete täitmiseks saab kaasata lisatööjõudu.

3.4 Standardmeetmed

ISMS.1.M16 Täpsustavate turvapoliitikate väljatöötamine

a. Kitsama käsitlusalaga turvapoliitikad koostatakse vähemalt järgmistes valdkondades:
   - võrguhaldus;
   - tulemüüri haldus;
   - kahjurvaratõrje;
   - andmevarundus ja arhiveerimine;
   - e-post ja rühmatarkvara;
   - mobiilseadmete kasutamine;
   - teenuste väljasttellimine.

3.4 Kõrgmeetmed

ISMS.1.M17 Kindlustuslepingute sõlmimine (A)

a. Jääkriskide hindamise osana on hinnatud vajadus järgmiste kindlustusliikide järele:
   - tule ja loodusjõudude kahju kindlustus;
   - finantskahjude kindlustus;
   - varakindlustus;
   - õnnetusjuhtumikindlustus;
   - vastutuskindlustus;
   - tsiviilvastutuskindlustus.

b. Olemasolevate kindlustuslepingute otstarbekust ja toimivust kontrollitakse regulaarselt.

4 Lisateave

Lühend	Publikatsioon
[RT]	Vabariigi Valitsuse määrus „Infoturbe juhtimise süsteem“ , vastu võetud 15.03.2012, https://www.riigiteataja.ee/akt/119032012004?leiaKehtiv
[RIA]	IT-halduse raamdokumentide näidised, https://www.ria.ee/et/kuberturvalisus/iske/juhendid-ja-materjalid.html

ORP: Organisatsioon ja personal

ORP.1 Infoturbe korraldus

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed infoturbe korralduse sobitamiseks organisatsiooniga, infoturbe juhtimiseks ja käigushoiuks. Moodul reguleerib infoturbe protsesside haldust ja infoturbe rollide jaotust organisatsioonis.

1.2 Vastutus

„Infoturbe korraldus“ meetmete täitmise eest vastutab organisatsiooni juhtkond.

Lisavastutajad

Haldusosakond, tehnikatalitus, IT-talitus, infoturbejuht, töötaja.

1.3 Piirangud

Moodul käsitleb turbekorralduse üldmeetmeid. Täiendavad korraldusmeetmed esitatakse kitsama käsitlusalaga moodulites.

2 Ohud

2.1 Puuduvad või puudulikud eeskirjad

Kui infoturbe meetmeid ei ole kehtestatud või meetmete rakendamise juhised ei ole arusaadavalt dokumenteeritud, jäävad vajalikud turvameetmed sisuliselt rakendamata. Eeskirjade puudulikkus ja vastutajate puudumine võivad kaasa tuua suuri kahjusid. Seda eriti olukordade tõttu, mis nõuavad viivitamatut tegutsemist. Probleeme põhjustavad ka ajakohastamata, reaalseid olusid eiravad või arusaamatult esitatud eeskirjad.

2.2 Eeskirjade rikkumine

Kehtestatud eeskirjadest üleastumine töötaja poolt võib rikkuda teabe, äriprotsesside või IT-süsteemide konfidentsiaalsust, terviklust või käideldavust. Olenevalt teabe või süsteemide kaitsetarbest ja turvareeglite rikkujale antud pääsuõigustest võib kahju osutuda ulatuslikuks.

Nõuete järgimata jätmine andmetöötluses võib põhjustada andmekadu. Kui pääsuõiguste halduse protseduure ei järgita, võib see kaasa tuua volitamata juurdepääsu IT-süsteemidele.

2.3 Puuduvad, ebasobivad või ühildamatud töövahendid

Vajalike töövahendite puudumine ja rikutud või amortiseerunud töövahendid võivad organisatsiooni äriprotsesse märkimisväärselt takistada. Näiteks kaotab puhvertoiteallika (ingl uninterruptable power supply, UPS) aku aja jooksul osa oma mahutavusest ning ei suuda elektrikatkestuse puhul IT-seadmete elektrivarustust tagada. Töövahendi hankimisel võib uus töövahend osutuda olemasoleva vanema tehnoloogilise keskkonnaga ühildamatuks.

2.4 Ohud abi- ja välispersonali tõttu

Organisatsioonivälistelt isikutelt ei saa vaikimisi eeldada, et nad neile kättesaadavat teavet ja IT-vahendeid kasutaksid lähtudes organisatsioonis kehtestatud kordadest. Külastajad, koristajad ja muud välised töötajad võivad teabe turvalisust, äriprotsesse ja süsteeme mitmel viisil ohustada, alates tehniliste vahendite asjatundmatust kasutamisest ja IT-süsteemi võimaluste proovimisest kuni dokumentide ja IT-vahendite varguseni.

3 Meetmed

3.1 Elutsükkel

Kavandamine

ORP.1.M1 Kohustuste ja eeskirjade kehtestamine

ORP.1.M2 Teabe, rakenduste ja IT-komponentide eest vastutajate määramine

ORP1.M4 Tegevus- ja kontrollikohustuste lahusus

ORP.1.M16 IT-vahendite turvalise kasutamise eeskiri

Evitus

ORP.1.M8 Töövahendite ja seadmete haldus

Käitus

ORP.1.M3 Organisatsioonivälise isikute järelevalve või saatmine

ORP.1.M13 Kolimise turve

ORP.1.M15 Infoturbe kontaktisik

Lisanduvad kõrgmeetmed

ORP.1.M17 Nutitelefonide kaasas kandmise piiramine

3.2 Põhimeetmed

ORP.1.M1 Kohustuste ja eeskirjade kehtestamine

a. Organisatsioonis on määratud infoturbega seotud ülesanded ning kohustused.

b. Eeskirjadega kehtestatakse turbe korraldus vähemalt järgmistes valdkondades:

- varundus ja arhiveerimine;
- andmekandjate käitus;

- hoolde- ja remonditööd;
- andmekaitse;
- avariivalmendus.

c. Eeskirjad tehakse teatavaks kõigile töötajaile ning neid vaadatakse regulaarselt üle.

ORP.1.M2 Teabe, rakenduste ja IT-komponentide eest vastutajate määramine

a. Turvalisuse eest vastutajad on määratud kogu teabe ning kõigi äriprotsesside, rakenduste ja IT-komponentide osas.

b. Infoturbe meetmete rakendamise kohustused on selgelt sõnastatud ja määratud, meetmete rakendamist kontrollitakse regulaarselt.

c. Töötajad teavad, kes ja mil viisil infoturbe meetmete rakendamise eest vastutavad.

ORP.1.M3 Organisatsioonivälise isikute järelevalve või saatmine [töötaja, haldusosakond]

a. Organisatsioonivälised isikud liiguvad organisatsiooni ruumes koos töötajast saatjaga.

b. Väliste töötajate viibimine kõrgendatud kaitsetarbega aladel on lubatud ainult organisatsiooni töötaja otsesel järelevalvel.

c. Töötajaid on juhendatud mitte jätma väliseid isikuid organisatsiooni ruumidesse ilma järelevalveta.

ORP.1.M4 Tegevus- ja kontrollikohustuste lahusus

a. Organisatsioonis tagatakse infoturbe toimingu sooritaja ning toimingu kontrollija rollide lahusus ning neid rolle täidavad erinevad töötajad.

b. Tegevus- ja kontrollikohustuste lahusus kehtib ka töötaja asendamise korral.

ORP.1.M15 Infoturbe kontaktisik [infoturbejuht]

a. Organisatsioonis on turvaküsimuste lahendamiseks määratud isik(ud), kelle poole töötajad võivad kõikide infoturbe teemaliste küsimustega pöörduda.

b. Töötajaid julgustatakse turvaintsidendi kahtluse korral teavitama sellest kohe, vajaduse korral anonüümselt.

c. Infoturbe kontaktisik ja teavitamisteed on kõigile töötajatele teada või vajadusel kergesti leitavad.

3.3 Standardmeetmed

ORP.1.M8 Töövahendite ja seadmete haldus [IT-talitus, haldusosakond]

a. Organisatsioonis on ülevaade kõigist töövahenditest ja seadmetest, mis võivad infoturbe olukorda mõjutada. Lisaks IT-süsteemide ja tööstusautomaatika komponentidele kuuluvad seadmete hulka ka esemevõrgu (ingl *Internet of Things* – IoT) seadmed.

b. Töövahendite ja seadmete hankimisel arvestatakse nende ühilduvust ja turvalisust. Võimalusel testitakse uusi seadmeid enne nende soetamist.

c. Töövahendid ja seadmed (ka nende kulumaterjalid, seonduv tarkvara, andmekandjad jms) võetakse arvele (nt varade registris).

d. Töövahendite ja seadmete turvaliseks kasutuselt kõrvaldamiseks on koostatud juhendid ja soetatud vajalikud vahendid (nt dokumendipurusti). Andmekandjad kõrvaldatakse vastavalt moodulile CON.6. *Andmete kustutus ja hävitamine.*

ORP.1.M13 Kolimise turve [IT-haldus, tehnikatalitus, haldusosakond]

a. Enne plaanitud kolimist töötatakse välja või ajakohastatakse kolimisplaan, kus muuhulgas määratletakse töötajate kohustused.

b. Töötajaid teavitatakse turvameetmetest, mida on vaja järgida kolimise eel, ajal ja järel.

c. Enne kolimist varundatakse andmed ja märgistatakse ümberpaigutatavad varad.

d. Kolimise käigus rakendatakse juurdepääsu kontrolle, väline personal liigub lähtekohas ja sihtkohas ainult organisatsiooni töötaja saatel.

e. Pärast kolimist kontrollitakse, kas kolimisel transporditud seadmed jm varad on täielikult, kahjustusteta ning muutmata kujul kohale jõudnud.

f. Enne töötajate tööle asumist uude kohta luuakse vajalik taristu, paigaldatakse ning testitakse IT- ja automaatikaseadmed ning veendutakse kasutajakontode toimimises.

ORP.1.M16 IT-vahendite turvalise kasutamise eeskiri [infoturbejuht, kasutaja]

a. Organisatsioonis on kehtestatud IT-vahendite turvalise kasutamise eeskiri.

b. IT-vahendite turvalise kasutamise eeskiri sisaldab vähemalt järgmist:
   - organisatsiooni turvaeesmärgid;
   - olulised mõisted ja nende selgitused;
   - infoturbe rollid ja tööülesanded;
   - infoturbe kontaktid ja teavitusteed;
   - rakendatavad turvameetmed.

c. IT-vahendite turvalise kasutamise eeskiri on kõikidele töötajatele teatavaks tehtud ning on vajadusel kergesti leitav (nt siseveebist).

d. Uus töötaja kinnitab enne IT-vahendite kasutuselevõttu kirjalikult, et on eeskirjaga tutvunud.

e. IT- vahendite turvalise kasutamise eeskirja vaadatakse üle perioodiliselt ning pärast oluliste muudatuste tegemist IT-süsteemides.

3.4 Kõrgmeetmed

ORP.1.M17 Nutitelefonide kaasas kandmise piiramine [haldusosakond, infoturbejuht] (C)

a. Mobiiltelefonide kaasa võtmine konfidentsiaalsetele koosolekutele ja kõrget konfidentsiaalsustaset eeldavatele töökohtadele on keelatud.

b. Vajadusel kasutatakse turvaalale sisenejate mobiilsideseadmete avastamiseks detektorseadet.

ORP.2 Personal

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed personaliosakonnale ja juhtidele, et oma töötajad ning välised töötajad tegutseks organisatsiooni turvaeesmärke silmas pidades.

1.2 Vastutus

„Personal“ meetmete täitmise eest vastutab personaliosakond.

Lisavastutajad

IT-talitus, ülemus.

1.3 Piirangud

Moodulis käsitletavad meetmed on üldised. Konkreetse funktsiooniga seotud personalimeetmed esitatakse asjakohastes moodulites.

2 Ohud

2.1 Personali piisamatus

Vajaliku hulga ja nõutava kvalifikatsiooniga personali piisamatus viib selleni, et ettenähtud tööülesandeid ei ole võimalik õigeaegselt ja terviklikult täita. Suureneb hooletusest tehtud vigade arv.

2.2 Nõuete puudulik tundmine

Kui infoturbe meetmeid ei ole kehtestatud või meetmete rakendamise juhised ei ole arusaadavalt dokumenteeritud, jäävad vajalikud turvameetmed sisuliselt rakendamata. Kui kehtestatud poliitikaid ja eeskirju pole kõigile töötajatele tutvustatud, siis ei saa ka eeldada, et kõik töötajad neid järgiksid.

2.3 Hooletus andmete kasutamisel

Organisatsioonis määratud korralduslikke ja/või tehnilisi turvameetmeteid võidakse isiklikust mugavusest või muretusest tingituna ignoreerida või neist mööda minna. Sotsiaalvõrkudes ja töökeskkonnas samade paroolide kasutamine võib viia IT-süsteemide kuritarvitamiseni parooli äraarvamise kaudu. IT-seadmete ja tarkvara manipuleerimine või väärkasutamine võib kaasa tuua tundlike andmete lekkimise või IT-süsteemide kahjustumise. Olenevalt teabe või süsteemide kaitsetarbest ja pääsuõiguste ulatusest võib kehtestatud eeskirjade eiramine kaasa tuua ulatusliku kahju.

2.4 Ebapiisav töötajate kvalifikatsioon

Paljud igapäevased IT-probleemid ja intsidendid on põhjustatud asjaolust, et töötajad ei oma antud töö tegemiseks piisavat kvalifikatsiooni või on töötajate koolitus olnud ebapiisav. Aegunud teadmiste ja puuduliku arvutioskuse tõttu ei pruugita infoturbe rikkeid tähele panna ega normaalsest erinevale tarkvara käitumisele õigeaegselt tähelepanu juhtida. Teist töötajat asendav isik võib jätta tööprotsessis olulise tegevuse tegemata või teha seda valesti. See võib põhjustada IT-süsteemis töös tõrkeid või tekitada infoturbe intsidendi.

3 Meetmed

3.1 Elutsükkel

Kavandamine

ORP.2.M1 Uue töötaja sisseelamise kord

ORP.2.M2 Töötaja lahkumise protseduur

ORP.2.M14 Tööülesannete ja kohustuste kehtestamine

Käitus

ORP.2.M3 Töötaja asendamise kord

ORP.2.M4 Asendamise kord välise töötaja puhul

ORP.2.M5 Konfidentsiaalsusleping väliste töötajate kasutamisel

ORP.2.M7 Kandidaadi usaldusväärsuse kontrollimine

ORP.2.M15 Piisava kvalifikatsiooniga töötajad

Lisanduvad kõrgmeetmed

ORP.2.M11 Turvakultuuri analüüs

ORP.2.M13 Taustakontroll

3.2 Põhimeetmed

ORP.2.M1 Uue töötaja sisseelamise kord [ülemus]

a. Uute töötajate sisseelamise kord sisaldab infoturbe nõuete, tavade ja tegevusjuhiste tutvustamist.

b. On koostatud kontroll-loend, mis sisaldab kõiki uue töötaja töö alustamiseks vajalikke tegevusi.

c. Töötajatele selgitatakse igapäevaseid tööprotseduure, infoturvameetmeid ning nende mõju äriprotsessile ja töökeskkonnale.

d. Uuele töötajale on määratud sisseelamise perioodiks kontaktisik (mentor), kes aitab teda kõigis ettetulevates küsimustes.

ORP.2.M2 Töötaja lahkumise protseduur [ülemus, IT-talitus]

a. Enne töötaja lahkumist või üleviimist teisele ametikohale koolitatakse välja tema tööülesannete jätkaja. Soovitatavalt teeb seda lahkuv töötaja. Kui tööülesandeid ei saa otse üle anda, on uue töötaja jaoks loodud üksikasjalik tööülesannete juhend.

b. Lahkuv töötaja annab organisatsioonile üle kõik töösuhte ajal saadud dokumendid, võtmed ja seadmed, samuti töötõendi ning pääsukaardid.

c. Endise töötaja pääsuõigused IT-süsteemides suletakse õigeaegselt.

d. Töötaja üleviimisel teisele ametikohale kohandatakse töötaja pääsuõigused ja tema käes olevate organisatsiooni varade valik vastavaks muutunud tööülesannetega.

e. Enne töölt lahkumist juhitakse selgesõnaliselt veel kord töötaja tähelepanu konfidentsiaalsuskohustusele ja võimaliku huvide konflikti ärahoidmisele.

f. Töötaja lahkumisest teavitatakse asjakohaseid töötajaid, sealhulgas turvapersonali.

g. Vajadusel ajakohastatakse eriolukorra- jm tegevuskavad, kuhu lahkuv töötaja või teisele ametikohale üleviidav töötaja oli kaasatud.

h. Tegevuste koordineerimiseks töötaja lahkumise korral kasutatakse sarnaselt töölevõtmisele asjakohast kontroll-loendit.

ORP.2.M3 Töötaja asendamise kord [ülemus]

a. Juhtkond on koostanud töötaja asendamise korra ja loonud eeldused selle järgimiseks. Asendamise kord eksisteerib tööülesannetele kõigis olulistes äriprotsessides.

b. Töötaja asendamise korras kirjeldatakse ülesannete jaotus töötaja asendamisel.

c. Asendaja nimetamisel veendutakse, et tal on olemas asendamiseks vajalikud teadmised. Vajadusel asendajat koolitatakse ja tööprotseduurid dokumenteeritakse sellise täpsusega, et ka vähemate teadmistega isik saaks asendamisega hakkama.

d. Kui erandjuhul ei saa konkreetsele töötajale pädevat asendajat määrata ega koolitada, otsustatakse, kas saab töötaja asendamiseks kasutada organisatsioonivälist tööjõudu.

ORP.2.M4 Asendamise kord välise töötaja puhul

a. Kui töötaja asendamiseks kasutatakse välist töötajat, siis kohustub ta täitma organisatsiooni poliitikaid ja sise-eeskirju sarnaselt organisatsiooni töötajatega.

b. Lühiajaliselt või ühekordselt kaasatud välist töötajat käsitletakse külastajana, keda kaitsevajadusega alas üksinda ei jäeta.

c. Pikemaks ajaks värvatud väliseid töötajaid õpetatakse ja koolitatakse tööülesandeid täitma sarnaselt organisatsiooni töötajatega. Ka välistele töötajatele kehtib töötaja asendamise kord (vt ORP.2.M3 *Töötaja asendamise kord*).

d. Töölt lahkumise korral annab väline töötaja oma töö tulemi üle ja tema juurdepääsuõigused suletakse sarnaselt organisatsiooni oma töötajaga.

ORP.2.M5 Konfidentsiaalsusleping väliste töötajate kasutamisel

a. Organisatsioonivälise isikuga sõlmitakse kirjalik konfidentsiaalsusleping enne, kui talle antakse juurdepääs konfidentsiaalsele teabele.

b. Konfidentsiaalsuslepingus on määratud vähemalt järgmine:

- millist teavet käsitletakse konfidentsiaalsena;
- millised nõuded kehtivad konfidentsiaalse teabe kasutamisel ja edastamisel;
- kui kaua konfidentsiaalsusleping kehtib;
- kuidas reguleeritakse teabe omandiõigusi;
- millised on lepingu rikkumise tagajärjed.

ORP.2.M14 Tööülesannete ja kohustuste kehtestamine [ülemus]

a. Kõik töötajad on selgesõnaliselt kohustunud järgima asjakohaseid õigusakte, organisatsiooni poliitikaid ja sise-eeskirju.

b. Töötaja tööülesanded ja kohustused on dokumenteeritud ja neid on töötajale tutvustatud. Töötajad kinnitavad nõuete järgimist, allkirjastades vastava kontroll-loetelu.

c. Töötajad teavad, et töötamise käigus saadav teave on ette nähtud ainult organisatsioonisiseseks kasutamiseks, kui see ei ole teisiti tähistatud.

d. Töötajad on kohustatud organisatsiooni varasid ja andmeid kaitsma ka pärast tööaega ja väljaspool organisatsiooni territooriumi.

ORP.2.M15 Piisava kvalifikatsiooniga töötajad [ülemus]

a. Töötajad saavad regulaarselt tegevusalale vastavat koolitust ja täiendõpet.

b. Töötajate täiendõpet soositakse ja töötajaid motiveeritakse ennast pidevalt arendama.

c. Uute töötajate otsimisel on nõutav haridus, kvalifikatsioon ja oskused selgelt kirjeldatud.

d. Töötajate vastavust ametikohale ja vastava ametikohale vajaliku kvalifikatsiooni kirjelduste õigsust kontrollitakse perioodiliselt.

3.3 Standardmeetmed

ORP.2.M7 Kandidaadi usaldusväärsuse kontrollimine

a. Personalivalikul osalejad kontrollivad enne töölevõtmist nõuetekohase hoolsusega kandidaadi esitatud andmete tõepärasust.

b. Eriti hoolikalt kontrollitakse esitatud elulookirjelduse täielikkust, usutavust ja õigsust. Olulisi fakte kontrollitakse täiendavate tõendite küsimise ja esitamise teel.

3.4 Kõrgmeetmed

ORP.2.M11 Turvakultuuri analüüs (C-I-A)

a. Turvameetmete rakendamisel arvestatakse organisatsiooni töötajaid, nende tausta, teadmisi ning IT-süsteemide kasutamise kogemusi. Turvalisust parandatakse analüüsides töötajate turvakäitumist.

b. Turvaintsidentide toimivaks ja tõhusaks käsitlemiseks soodustatakse usalduslikku ja avatud suhtluskultuuri, mis võimaldab turvaintsidentidest kohe teatada ja neile lahendused leida.

c. Suurema organisatsiooni korral analüüsitakse, kas turvakultuuri võivad mõjutada riikidevahelised, piirkondlikud või üksustevahelised kultuurilised erinevused.

ORP.2.M13 Töötaja taustakontroll (C-I-A)

a. Suure kaitsetarbega valdkondades tehakse lisaks töötajate usaldatavuse põhikontrollile (vt ORP.2.M7 *Töötajate usaldatavuse kontrollimine*) seadusega lubatud piires täiendav taustakontroll, nt küsides kinnitust kriminaalkaristatuse puudumise kohta.

b. Teatud ametikohtadele kandideerimine ja ametikohal töötamine on lubatud ainult juhul, kui töötaja on taotlenud kehtiva seadusandluse kohase riigisaladusele juurdepääsu loa.

ORP.3 Infoturbe teadlikkuse tõstmine ja koolitus

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed töötajate turvateadlikkuse tõstmiseks ja töötajate koolitusplaani koostamiseks, arvestades organisatsiooni spetsiifikat ja töötajatele vajalikke teadmisi ja oskusi.

1.2 Vastutus

Infoturbe teadlikkuse tõstmise ja koolituse meetmete täitmise eest vastutab infoturbejuht.

Lisavastutajad

Personaliosakond, IT-talitus, organisatsiooni juhtkond, ülemus.

1.3 Piirangud

Moodul ORP.3 *Infoturbe teadlikkuse tõstmine ja koolitus* käsitleb infoturbe valdkonda. Muudel teemadel kavandab, plaanib ja viib koolitusi läbi organisatsiooni personaliosakond või koolituste koordinaator.

2 Ohud

2.1 Turvanõuete puudulik tundmine

Turvaintsidendi põhjuseks on sageli turvanõuete järgimata jätmine. Nõuete puuduliku tundmise tulemusena tekkinud turvanõrkused võivad ohustada töödeldava teabe konfidentsiaalsust, käideldavust ja terviklust.

2.2 Puudulik infoturvateadlikkus

Kui töötajad ei ole infoturbe meetmetest piisavalt teadlikud, kannatab organisatsiooni turvakultuur ja turvaeesmärkide täitmine. Töötajad ei suuda luua konkreetseid seoseid oma töökeskkonnaga, sest neile ei ole selgitatud turvameetmete olulisust.

2.3 Teadvustuse ja koolituse vähene tulemuslikkus

Teadvustus- ja koolitustegevuse vähese tulemuslikkuse põhjusteks on juhtkonna puudulik toetus, koolituse ebaselged eesmärgid, puudused koolituste läbiviimisel või ressursside vähesus. Kui organisatsioon töötajate teadlikkuse suurendamist ja koolitamist piisavalt ei tähtsusta, siis võib vähene turvateadlikkus otseselt takistada tööülesannete täitmist.

2.4 Puudlik koolitus turvafunktsioonide alal

Sageli ei rakenda töötajad organisatsioonis kasutusele võetud turvarakendusi ja -funktsioone oskamatuse tõttu. Puudulik teadmine turvafunktsioonidest võib põhjustada tarkvara kasutusvigu ja seisakuid. Väärkasutuse mõju võib oluliste IT-süsteemide korral olla märkimisväärne.

2.5 Avastamata jäänud turvasündmused

IT- ja automaatikakomponentide igapäevases töös võib esineda palju häireid ja rikkeid. Piisamatu koolituse tõttu ei suuda töötajad turvaintsidentidel ja tehnilistel riketel vahet teha, turvaintsidentidele ei reageerita ja nõrkused jäävad parandamata. See võib pärssida äriprotsesse, tekitada rahalist kahju või tuua kaasa õigusaktidest tulenevaid sanktsioone.

2.6 Turvameetmete eiramine

Töötaja hooletuse või kiirustamine tõttu on oht, et konfidentsiaalsed dokumendid jäävad avatuna lauale, uksed jäävad lukustamata, aknad jäävad avatuks või arvutiekraan lukustamata.

2.7 Hooletus teabe töötlemisel

Kui organisatsioonis kehtestatud turvameetmeid eiratakse, näiteks paroole kuvari peale kleebitud sedelile kirjutades, siis muutuvad ka parimad tehnilised turvameetmed ebatõhusaks. Kui konfidentsiaalse teabega dokumendid jäetakse printerisse või visatakse prügikasti, millele igaüks ligi pääseb, ei ole failide krüpteerimisest kõvakettal kasu.

2.8 Infoturbe puudulik omaksvõtmine

Organisatsioonis võidakse infoturbenõudeid mitte omaks võtta ega tajuda turvameetmete rakendamise olulisust. Mitteomaksvõtmine võib näiteks olla tingitud organisatsioonikultuurist („nii on meil alati olnud“) või juhtkonna eeskuju puudumisest. Töötajate vastuseis turvameetmetele võib tekkida ka ebamõistlike või ülepingutatud turvanõuete tõttu.

2.9 Suhtlusrünne

Suhtlusründe (ingl *social engineering*) tulemusel võib ründaja saada teabele või IT-süsteemidele lubamatu juurdepääsu, luues kontakte telefoni, e-posti või sotsiaalvõrgu kaudu

ning kasutades ära inimeste abivalmidust. Kui töötaja sellist ründeviisi piisaval määral ei tunne, siis osavalt suheldes suunatakse töötaja toimima lubamatul viisil. Suhtlusründe tulemusena võib ründaja hankida konfidentsiaalset teavet, levitada kahjurtarkvara või koguni sundida töötajat väidetavale äripartnerile raha üle kandma.

3 Meetmed

3.1 Elutsükkel

Kavandamine

ORP.3.M1 Juhtkonna teadlikkuse suurendamine infoturbe alal

ORP.3.M3 Infotehnoloogia turvalise kasutamise juhendamine

ORP.3.M4 Infoturbe teadvustus- ja koolitusplaan

Käitus

ORP.3.M6 Infoturbe teadvustus- ja koolitusmeetmete kavandamine ja rakendamine

ORP.3.M7 Infoturbe halduse meetodeid käsitlevad koolitused

Parendamine ja täiustamine

ORP.3.M8 Õpitulemuste mõõtmine ja hindamine

Lisanduvad kõrgmeetmed

ORP.3.M9 Ohustatud isikute ja organisatsioonide erikoolitus

3.2 Põhimeetmed

ORP.3.M1 Juhtkonna teadlikkuse suurendamine infoturbe alal [ülemus, organisatsiooni juhtkond]

a. Juhtkonda teavitatakse regulaarselt infoturbe riskidest, nendega seotud võimalikest kahjudest ja mõjust äriprotsessile.

b. Juhtkond on teadlik õigusaktidega kehtestatud infoturbenõuetest.

c. Juhtkond on kursis infoturbe rakendamise praktikatega teistes sarnastes organisatsioonides ning infoturbe protsesside sertifitseerimise võimalustega.

d. Organisatsiooni juhtkond toetab töötajatele korraldatavaid turvalisuse tõstmise kampaaniaid ning muude koolitusmeetmete rakendamist.

e. Juhtivtöötajad näitavad infoturbes eeskuju, järgides turvameetmeid ise ja juhtides teiste töötajate tähelepanu meetmetest kinnipidamise vajalikkusele.

ORP.3.M3 Infotehnoloogia turvalise kasutamise juhendamine [ülemus, personaliosakond, IT-talitus]

a. Töötajad on läbinud küberhügieeni baasteadmise koolituse ja tõendanud oma teadmisi vastava testi sooritamisega.

b. Töötajatele ja organisatsioonivälistele kasutajatele on selgitatud, kuidas IT-, tööstusautomaatika- ja esemevõrgu komponente turvaliselt kasutada ja millised on kasutamisega seotud õigused ja kohustused.

c. Organisatsioon on koostanud eeskirjad IT-, tööstusautomaatika ja esemevõrgu komponentide turvaliseks kasutamiseks. Eeskirjad on arusaadavad ja ajakohased, kohustuste selgeks määratlemiseks on need kinnitatud juhtkonnas.

d. Eeskirjade või kasutusjuhiste muutmisel tagatakse, et muudatused tehakse kasutajatele teatavaks.

3.3 Standardmeetmed

ORP.3.M4 Infoturbe teadvustus- ja koolitusplaan

a. Töötajate teadlikkuse suurendamiseks on välja töötatud ja juhtkonna poolt kinnitatud infoturbe teadvustus- ja koolitusplaan.

b. Infoturbe teadvustus- ja koolitusplaanide koostamisel võetakse arvesse konkreetsete sihtrühmade vajadusi. Ühte sihtrühma koondatakse sarnase erialatausta, teadmiste või ülesannetega töötajad. Praktikas moodustatakse sihtrühmi ka struktuuriüksuste alusel.

c. Infoturbe teadvustus- ja koolitusprogrammi ajakohasust kontrollitakse regulaarselt, vajaduste muutumise korral koolitusprogrammi kohandatakse või täiustatakse.

ORP.3.M6 Infoturbe teadvustus- ja koolitusmeetmete kavandamine ja rakendamine

a. Töötajate infoturbe koolituse kavandamisel lähtutakse töötajate tööülesannetest ja vastutusalast. Koolituse sisu on piisav kehtivate turvanõuete ja -meetmete rakendamiseks.

b. Kõik töötajad on läbinud oma tööülesannetele ja vastutusalale vastava infoturbe koolituse.

ORP.3.M7 Infoturbe halduse meetodeid käsitlevad koolitused

a. Infoturbe eest vastutavad isikud on läbinud infoturbe halduse ja infoturbe standardi rakendamise koolituse.

b. Infoturbe halduse koolitused peavad sisaldama näiteid ja praktilisi harjutusi, sh elulisi näiteid infoturbe standardi rakendamisest.

ORP.3.M8 Õpitulemuste mõõtmine ja hindamine [personaliosakond]

a. Infoturbe valdkonna õpitulemusi mõõdetakse ja hinnatakse sihtrühmapõhiselt, et teha kindlaks, millisel määral on infoturbe teadvustus- ja koolitusplaanis ettenähtud eesmärgid saavutatud (vt ORP.3.M4 *Infoturbe teadvustus- ja koolitusplaan*).

b. Õpitulemuste hindamisel mõõdetakse nii teadvustus- ja koolitusplaani kvalitatiivseid kui kvantitatiivseid aspekte, kasutades selleks koolituste hindamislehti, koolituse lõputeste, töötajate küsitlusi või perioodilisi teadmiste kontrolle (nt RIA Kübertest, https://www.ria.ee/kuberturvalisus/kuberruumi-analuus-ja-ennetus/kubertest).

c. Personaliosakond teeb koolituse sisu ja efektiivsuse hindamisel koostööd infoturbejuhi, andmekaitsespetsialisti, töökeskkonnavoliniku, tuleohutuse eest vastutava isiku ja teiste oluliste võtmeisikutega.

d. Õpitulemuste mõõtmise tulemusi arvestatakse infoturbe teadvustus- ja koolitusplaani muutmisel ja täiustamisel.

3.4 Kõrgmeetmed

ORP.3.M9 Ohustatud isikute ja organisatsioonide erikoolitus (C-I-A)

a. Eriti ohustatud isikud (nt kriitilise funktsiooni täitjad) ning eriti turvatundlike organisatsioonide töötajad on läbinud põhjaliku koolituse ohtude, ohu realiseerumise korral tegutsemise ja ettevaatusmeetmete kohta.
b. Õppematerjalide kinnistamise meetmed valitakse sobivalt organisatsiooni kultuuri ja suurusega, näiteks võib korraldada töötajatele simulatsiooniõppuseid pingeolukorras tegutsemise harjutamiseks.

4 Lisateave

4.1 Näide sihtrühmadele määratud koolitusmoodulitest.

X-ga tähistatakse seda, et konkreetset moodulit soovitatakse asjakohasele rollile. Numbriga 0 tähistatakse valikulisi koolitusmooduleid, mille korral otsustatakse mooduli valimine igal üksikjuhul eraldi.

Moodul 1. Infoturbe alused

Moodul 2. Infoturve töötamiskohal

Moodul 3. Seadused ja eeskirjad

Moodul 4. Organisatsiooni infoturbe kontseptsioon

Moodul 5. Riskihaldus

Moodul 6. Infoturbe haldus

Moodul 7. IT-süsteemid

Moodul 8. Tegevusala

Moodul 9. Turvameetmete tehniline teostus

Moodul 10. Avariivalmendus / eriolukorra tegevuskava

Moodul 11. Uued suundumused IT-valdkonnas

Moodul 12. Infoturbe äriline külg

Moodul 13. Taristu turve

Moodul → funktsioon ↓	1	2	3	4	5	6	7	8	9	10	11	12	13
Ülemus	X	X	X	X							O	X	
Turbehaldus	X	X	X	X	X	X	X	X	X	X	X	X	X
Andmekaitsespetsialist	X	X	X	X							X	O	
Taristu eest vastutav isik	X	X	X	X	X	O				X			X
Kasutaja	X	X											

Süsteemiülem	X	X		X	X		X	X	X	X	X		O

Tabel. Soovitatavad koolitusmoodulid funktsioonide järgi

Selles näites kuuluvad moodulid 1 ja 2 kõigi töötajate baaskoolitussse ning need peavad teadlikkuse suurendamise meetmetega täpselt kokku sobima. Muud moodulid näitavad, milliseid valdkondi koolitatakse sihtgrupi tööülesannetest olenevalt.

ORP.4 Identiteedi- ja õiguste haldus

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed identiteedi- ja õiguste halduse korraldamiseks. Nii kasutajad kui IT-komponendid peaksid saama juurdepääsu üksnes vajalikele IT-ressurssidele ja informatsioonile.

1.2 Vastutus

Identiteedi- ja õiguste halduse meetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Kasutaja, infoturbejuht, organisatsiooni juhtkond.

1.3 Piirangud

Identiteedi- ja õiguste halduse meetmed IT-süsteemi komponentides, operatsioonisüsteemides või kataloogiteenustes esitatakse vastavates moodulites (nt SYS.1.3 *Linuxi ja Unixi server*, SYS.1.2.2 *Windows Server 2012*; APP.2.1 *Kataloogiteenus üldiselt*, APP2.2 *Active Directory*).

2 Ohud

2.1 Identiteedihalduse protsesside puudumine või puudulikkus

Kui identiteedi- ja õiguste halduse protsessid on puudulikud või kui protseduure ei järgita, ei saa vastutav süsteemiülem personalimuudatuste kohta piisavat teavet. Selle tulemusena võib lahkunud töötaja kasutajakonto jääda sulgemata ja ta võib edaspidigi tundlikule teabele või pilvrakendustele juurde pääseda. Samuti võivad teise osakonda siirdunud töötajal säilida tema endised õigused.

2.2 Kasutaja õiguste keskse peatamise võimaluse puudumine

Töötajal võib erinevatesse IT-süsteemidesse juurdepääsuks olla mitmeid kasutajakontosid. Kui IT-süsteemide juurdepääsudest puudub keskne ülevaade, siis ei saa süsteemiülemad ründe või paroolivarguse korral töötaja kõiki õigusi kohe peatada. Samuti võib töötaja lahkumisel jääda mõni juurdepääs sulgemata.

2.3 Pääsuõiguste puudulik haldamine

Kui eri struktuuriüksustes vastutavad õiguste andmise eest erinevad isikud ja pääsuõiguste haldus on halvasti korraldatud, võib pääsuõiguste saamine osutuda põhjendamatult

keeruliseks või vastupidi, on tehtud liiga lihtsaks. Ühel juhul võivad puuduvad õigused takistada igapäevatööd, teisel võib mittevajalik pääsuõigus tekitada turvariski.

3 Meetmed

3.1 Elutsükkel

Kavandamine

ORP.4.M1 Kasutajakontode halduse eeskiri
ORP.4.M2 Õiguste andmine, muutmine ja tühistamine
ORP.4.M3 Kasutajate õiguste dokumenteerimine
ORP.4.M4 Kohustuste jaotamine ja kohustuste lahusus
ORP.4.M8 Paroolide kasutamise kord
ORP.4. M11 Paroolide lähtestamine ja muutmine
ORP.4.M12 IT-süsteemide ja rakenduste autentimiskord
ORP.4.M13 Sobivate autentimismehhanismide valimine
ORP.4.M22 Parooli kvaliteedinõuete kehtestamine
ORP.4.M23 Nõuded paroole töötlevatele IT-süsteemidele

Evitus

ORP.4.M5 Füüsilise ligipääsu haldamine
ORP.4.M6 IT-vahenditele juurdepääsu haldamine
ORP.4.M7 Andmetele juurdepääsu haldamine
ORP.4.M16 IT-süsteemidele juurdepääsu reguleerimine
ORP.4.M17 Sobiv identiteedi- ja õiguste halduse süsteem

Käitus

ORP.4.M9 Tuvastamine ja autentimine
ORP.4.M10 Eeliskontode kaitsmine
ORP.4.M14 Kasutajakontode kasutamise kontrollimine
ORP.4.M15 Identiteedi- ja õiguste halduse protseduurid
ORP.4.M18 Keskse autentimisteenuse kasutamine
ORP.4.M19 Töötajate juhendamine autentimisprotseduuride ja -mehhanismide kasutamisel

Lisanduvad kõrgmeetmed

ORP.4.M20 Identiteedi- ja õiguste halduse süsteemi avariivalmendus
ORP.4.M21 Mitmikautentimine
ORP.4.M24 Nelja silma põhimõtte rakendamine IT-halduses

3.2 Põhimeetmed

ORP.4.M1 Kasutajakontode halduse eeskiri [infoturbejuht]

a. Organisatsioon on koostanud ja kinnitanud kasutajakontode halduse eeskirja.

b. Kasutajakonto määratakse identideedipõhiselt, kasutajakonto on seotud konkreetse kasutajaga.

c. IT-süsteemi standardseades määratud isikustamata haldus- ja külaliskontod, mida reaalselt ei kasutata, desaktiveeritakse või kustutatakse.

d. Kasutajakontod, mida ei ole kaua aega kasutatud, desaktiveeritakse.

e. Kasutajarühmad määratakse rollipõhiselt.

ORP.4.M2 Õiguste andmine, muutmine ja tühistamine

a. IT-süsteemi kasutajakonto luuakse ja pääsuõigused antakse üksnes tööalase vajaduse alusel, kasutades minimaalsuse põhimõtet.

b. Muudatuste korral personali koosseisus tühistatakse pääsuõigused, mida enam ei vajata.

c. Mittevajalike kasutajakontode kustutamine on lubatud ainult erandjuhtudel ning ainult siis kui samade kasutajatunnuste taaskasutamine ei tekita probleeme identiteedihaldusega (nt AD/LDAP teenust kasutavates süsteemides).

d. Õigused määratakse vastavalt kasutaja rollile.

e. Tavapärasest suuremaid õigusi antakse töötajatele ülemuse taotluse alusel ning pärast vajadust kinnitavate ja täpsustavate põhjenduse esitamist.

ORP.4.M3 Kasutajate õiguste dokumenteerimine

a. Kasutajakontod, moodustatud kasutajarühmad ja õiguste profiilid dokumenteeritakse.

b. Kasutajakontode, moodustatud kasutajarühmade ja õiguseprofiilide dokumentatsiooni ajakohasust ja vastavust kasutaja tööülesannete ning infoturbe nõuetega kontrollitakse regulaarselt.

c. Kasutajate õiguste dokumentatsioon on kaitstud lubamatu andmepääsu eest.

d. Elektroonilisel kujul talletatav kasutajate õiguste dokumentatsioon varundatakse vastavalt varundusprotseduurile.

ORP.4.M4 Kohustuste jaotamine ja kohustuste lahusus [organisatsiooni juhtkond]

a. Organisatsioon on määranud kohustused ja tööülesanded, kus infotehnoloogia kasutamine on vajalik.

b. On määratud, milliseid kohustusi või tööülesandeid ei saa täita sama isik.

c. Tööülesandeid määrates järgitakse kohustuste lahususe põhimõtteid, tööülesannete omavahelisi rollikonflikte arvestatakse täiendavate kontrollide kehtestamisel.

ORP.4.M5 Füüsilise ligipääsu haldamine [haldusosakond]

a. Organisatsioon on määranud töötaja kohustuste ja tööülesannete täitmiseks vajalikud füüsilise ligipääsu õigused.

b. Sissepääsuvahendina kasutatavate pääsmike (ingl *security token*) väljaandmine või kehtetuks muutmine dokumenteeritakse.

c. Kõiki füüsilise ligipääsu õigusega isikuid juhendatakse sissepääsuvahendeid õigesti kasutama.

d. Isiku pikema äraoleku korral tema ligipääsuõigused ajutiselt peatatakse.

ORP.4.M6 IT-vahenditele juurdepääsu haldamine

a. Organisatsioon on määranud töötaja kohustuste ja tööülesannete täitmiseks vajalikud IT-vahendite juurdepääsuõigused.

b. Juurdepääsuvahendina kasutatavate kiipkaartide vm pääsmike väljaandmine või kehtetuks muutmine dokumenteeritakse.

c. Kõiki juurdepääsuõigusega isikuid juhendatakse juurdepääsuvahendeid õigesti kasutama.

d. Isiku pikema äraoleku korral tema juurdepääsuõigused ajutiselt peatatakse.

ORP.4.M7 Andmetele juurdepääsu haldamine [infoturbejuht]

a. Organisatsioon on määranud isiku kohustuste ja tööülesannete täitmiseks vajalikud andmete juurdepääsuõigused.

b. Kui andmetele juurdepääsuks kasutatakse pääsmikku, siis selle väljaandmine või kehtetuks muutmine dokumenteeritakse.

c. Kõiki andmepääsuõigusega isikuid juhendatakse juurdepääsuvahendeid õigesti kasutama.

d. Isiku pikema äraoleku korral andmetele juurdepääs ajutiselt peatatakse.

ORP.4.M8 Paroolide kasutamise kord [kasutaja, infoturbejuht]

a. Organisatsioonis on kehtestatud paroolide kasutamise kord (vt ka ORP.4.M22 *Parooli kvaliteedinõuete kehtestamine* ja ORP.4.M23 *Nõuded paroole töötlevatele IT-süsteemidele*).

b. Paroolide kasutamise kord sätestab selgelt kasutaja kohustuse hoida paroole teiste eest salajas.

c. Paroole muudetakse regulaarselt, mõistliku ajavahemiku järel.

d. Kui on kahtlus, et volitamata isikud on parooli teada saanud, muudetakse parool koheselt.

e. On keelatud kasutada paroole, mis on hõlpsasti äraarvatavad või mis on välja toodud avaldatud enimkasutatud paroolide nimekirjades.

f. Sama parooli ei tohi kasutada rohkem kui üks kord.

g. Iga IT-süsteemi või rakenduse jaoks kasutatakse erinevat parooli.

h. Parooli talletamine kirjalikult on lubatud ainult erandjuhtudel, neid hoitakse turvalises asukohas.

i. Elektroonilise paroolihalduri kasutamine on lubatud ainult juhul, kui paroolihalduri kasutamiseks on läbi viidud turvaanalüüs ja kasutus on infoturbejuhiga kooskõlastatud. Eriti ettevaatlik tuleb olla paroolihaldurite puhul, mis sünkroniseerivad andmeid kolmanda osapoole pilveteenusega.

j. Kui IT-süsteemides saab kehtestada parooli keerukusreegleid, tuleb keerukusreeglid jõustada.

k. Kui IT-süsteem seda võimaldab, kasutatakse ainult parooliga autentimise asemel mitmikautentimist.

ORP.4.M9 Tuvastamine ja autentimine

a. Juurdepääs kõigile IT-süsteemidele ja teenustele on kaitstud kasutajate (sh ka teised IT-süsteemid) tuvastamise ja autentimisega.

b. Parooliga juurdepääsuvahendi kasutamisel muudetakse parool juurdepääsuvahendi esmakordsel kasutamisel.

ORP.4.M22 Parooli kvaliteedinõuete kehtestamine [infoturbejuht, kasutaja]

a. Nõuded parooli kvaliteedile on kehtestatud arvestades IT-süsteemide kaitsetarvet ja kasutajate profiili.

b. Parool peab olema piisavalt keerukas, et parooli ei saaks ära arvata.

c. Soovitatav on kasutada vähemalt 12 tähemärgi pikkuseid paroole.

d. Parool ei tohi olla nii keeruline, et kasutaja ei suuda seda regulaarse kasutuse puhul mõistlike pingutustega meelde jätta.

ORP.4.M23 Nõuded paroole töötlevatele IT-süsteemidele

a. IT-süsteemis või rakenduses ei talletata paroole avateksti kujul.

b. Võrgustatud IT-süsteemide ja rakenduste paroole edastatakse ainult krüpteeritult. See meede kehtib ka sisevõrgus kasutatavate rakenduste puhul.

c. IT-süsteemi või rakenduse nõutud paroolivahetusel on alati konkreetne põhjus.

d. IT-süsteemi või rakenduse standardsete kasutaja- ja süsteemikontode paroolid on muudetud esimesel võimalusel. Vaikeparoolid asendatakse piisavalt tugevate paroolidega, vaikimisi sisselogimissseaded muudetakse.

e. Edutu sisselogimiskatse puhul ei tohi IT- süsteem anda vihjet, kas vale on parool või kasutajanimi.

3.3 Standardmeetmed

ORP.4.M10 Eeliskontode kaitsmine

a. Eeliskontode (ingl *privileged account*) kaitseks väliste ründajate eest ja õiguste volitamatu laiendamise eest kasutatakse mitmikautentimist (ingl *multifactor authentication*).

ORP.4.M11 Paroolide lähtestamine ja muutmine

a. Paroolide lähtestamiseks või muutmiseks on organisatsioonis kehtestatud piisavalt turvalised protseduurid.

b. Paroolide lähtestamise ja muutmisega seotud tugipersonal on asjakohaselt koolitatud.

c. Suurema kaitsetarbe puhuks on olemas tegevuskava parooli turvaliseks muutmiseks ja edastamiseks ilma tugipersonali osaluseta.

ORP.4.M12 IT-süsteemide ja rakenduste autentimiskord [infoturbejuht]

a. Organisatsioonis on iga IT-süsteemi ja rakenduse jaoks määratud autentimisnõuded ja kehtestatud autentimiskord.

b. Autentimisandmeid hoitakse krüpteerituna.

c. Autentimisandmeid edastatakse üle andmesidevõrkude krüpteeritult.

ORP.4.M13 Sobivate autentimismehhanismide valimine [infoturbejuht]

a. Organisatsioonis kasutatakse kaitsetarbele vastavaid tuvastus- ja autentimismehhanisme.

b. IT-süsteemide või rakenduste autentimisandmeid kaitstakse kogu nende töötlemise ajal volitamata juurdepääsu, muutmise ja hävitamise eest.

c. Pärast ebaõnnestunud sisselogimiskatseid suurendab IT-süsteem või rakendus ajavahemikku, mille möödudes on lubatud teha uus sisselogimine.

d. IT-süsteemis või rakenduses on võimalik määrata ebaõnnestunud sisselogimiskatsete arv, pärast mida IT-süsteemi või rakenduse kasutajakonto lukustatakse.

ORP.4.M14 Kasutajakontode kasutuse kontrollimine

a. Regulaarselt kontrollitakse, kas IT-süsteemide kasutajad kasutavad oma kasutajakontot ning logivad end pärast ülesande täitmist alati süsteemist välja.

b. IT-süsteemi sisenemine teise füüsilise kasutaja kasutajanimega on rangelt keelatud.

ORP.4.M15 Identiteedi- ja õiguste halduse protseduurid

a. Organisatsioonis on koostatud ja rakendatud protseduurid:

- pääsupoliitikate haldamiseks;
- kasutajakontode ja kasutajarühmade haldamiseks;
- õiguste profiilide ja kasutajarollide haldamiseks.

ORP.4.M16 IT-süsteemidele juurdepääsu reguleerimine

a. IT-süsteemidele juurdepääsu andmisel lähtutakse kehtestatud pääsupoliitikatest.

b. Kasutatakse töötaja ülesannetele vastavaid standardseid õiguste profiile.

c. Iga IT-süsteemi juurdepääsude haldamiseks on kehtestatud protseduurid.

d. Kasutajale lubatakse juurdepääs IT-süsteemidele ja teenustele pärast kasutaja tuvastamist ja autentimist.

ORP.4.M17 Sobiv identiteedi- ja õiguste halduse süsteem [infoturbejuht]

a. Identiteedi- ja pääsuõiguste halduse süsteem:

- on sobitatud organisatsiooni ja selle äriprotsessidega ning vastab nende kaitsetarbele:
- vastab organisatsioonis kehtivatele pääsuhalduse nõuetele;
- võimaldab ellu viia kohustuste lahususe põhimõtet.

b. Identiteedi- ja pääsuõiguste halduse süsteemi kaitstakse siseste ja väliste rünnete eest.

ORP.4.M18 Keskse autentimisteenuse kasutamine [infoturbejuht]

a. Ühtse identiteedi- ja õiguste halduse rakendamiseks kasutatakse keskset ainulogimisega autentimisteenust (ingl *single sign-on access*).

b. Enne teenuse kasutuselevõttu on kavandatud ja dokumenteeritud keskse autentimisteenuse turvanõuded.

ORP.4.M19 Töötajate juhendamine autentimisprotseduuride ja -mehhanismide kasutamisel [kasutaja, IT-talitus]

a. Töötajatele tutvustatakse autentimise korda ja juhendatakse, kuidas autentimisprotseduure õigesti kasutada.

b. Autentimiseks on koostatud kõigile töötajaile arusaadavad juhised.

3.4 Kõrgmeetmed

ORP.4.M20 Identiteedi- ja õiguste halduse süsteemi avariivalmendus [organisatsiooni juhtkond, infoturbejuht](C-I-A)

a. Talitluspidevuse tagamiseks tuvastatakse identiteedi- ja õiguste halduse süsteemi turvakriitilisus äriprotsesside vaates ning kontrollitakse identiteedi- ja õiguste halduse süsteemi avariiolukorraks valmisolekut.

b. Avariiolukordade puhul tegutsemiseks on koostatud kasutajaõiguste erikontseptsioon ja määratud avariiolukorras rakendatavad õiguseprofiilid vastavalt töötajate hädaolukorras teistsuguseks muutuvatele kohustustele.

ORP.4.M21 Mitmikautentimine [IT-talitus] (C)

a. Suure kaitsetarbe korral kasutakse autentimiseks turvalist mitmikautentimist, nt ID-kaardi või tookeni (ingl *token*) abil.

ORP.4.M24 Nelja silma põhimõtte rakendamine IT-halduses [IT-talitus] (C)

a. Suure kaitsetarbega haldustegevuste läbiviimiseks kasutatakse kahte administraatorit.

b. Mitmikautentimise korral on autentimisvahendid administraatorite vahel jagatud. Ainult parooli kasutamise puhul on parool jagatud kaheks osaks, millest kumbki administraator teab ainult oma osa.

ORP.5 Vastavusehaldus (nõuete haldus)

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed organisatsiooni eesmärkidel, õigusaktidel, lepingutel ja poliitikatel põhinevate turvanõuete kehtestamiseks ja järgimiseks.

1.2 Vastutus

Vastavusehalduse meetmete täitmise eest vastutab vastavushaldur.

Lisavastutajad

Infoturbejuht, organisatsiooni juhtkond, haldusosakond, ülemus.

1.3 Piirangud

Selles moodulis käsitletakse infoturbe vastavusehaldust üldiselt, konkreetseid valdkonnakohaseid õigusakte ja üksikuid lepinguid meetmetes ei käsitleta.

2 Ohud

2.1 Seaduse- või lepingusätete rikkumine

Infoturvameetmete puuduliku rakendamise tulemusena võidakse kas kogemata või tahtlikult rikkuda seaduse- või lepingusätteid.

2.2 Teabe lubamatu avaldamine

Kui töötaja eirab kehtestatud turvanõudeid, võib konfidentsiaalne teave lekkida.

2.3 Suhtluspartneri identiteedi puudulik kontrollimine

Suhtlemisel e-kanalite vahendusel jäetakse suhtluspartneri identiteedi samasus enamasti tuvastamata. Seda kas peetakse ebaviisakaks või on see tehniliselt keerukas. Alusetult eeldatakse, et vestluse või e-kirja sisu on konfidentsiaalne ning et teave ei satu valedesse kätesse.

2.4 Siseteabe kogemata avaldamine

Teabe edastamisel, nt telefoni teel või irdmäluseadme ning e-kirja vahendusel, võib juhtuda, et peale soovitud teabe avaldatakse kogemata ka midagi soovimatut. Kui töötaja kasutab pilvteenust hooletult, võib ta tahtmatult lekitada konfidentsiaalset teavet.

3 Meetmed

3.1 Elutsükkel

Kavandamine

ORP.5.M1 Õiguslike raamtingimuste piiritlemine

ORP.5.M4 Vastavusehalduse kavandamine ja korraldamine

Käitus

ORP.5.M2 Õiguslike raamtingimuste järgimine

ORP.5.M5 Erandite haldus

Parendamine ja täiustamine

ORP.5.M8 Vastavusehalduse regulaarne läbivaatus

Lisanduvad kõrgmeetmed

ORP.5.M9 Teabe tagantjärele muutmise kaitse

ORP.5.M10 Informatsiooni turvamärgendus

ORP.5.M11 Krüptograafia õiguslike kitsenduste väljaselgitamine

3.2 Põhimeetmed

ORP.5.M1 Õiguslike raamtingimuste piiritlemine [haldusosakond, ülemus, organisatsiooni juhtkond]

a. Organisatsioonis on välja töötatud protsess kõigi turbehaldusele mõju avaldavate õigusaktide, lepingute ja muude nõuete väljaselgitamiseks. Asjakohased nõuded dokumenteeritakse.

b. Tuvastatud õiguslikke raamtingimusi võetakse arvesse äriprotsesside, rakenduste ja IT-süsteemide kavandamisel ning IT-komponentide hankimisel.

c. Õiguslikke raamtingimusi kontrollitakse ja dokumenteeritud nõudeid uuendatakse regulaarselt.

d. Õigusaktidest tulenevaid erinõudeid arvestatakse eriti järgmistes valdkondades:

- isikuandmete kaitse;
- ärisaladuse kaitse;
- intellektuaalomandi kaitse;
- krüptograafia kasutamine;
- IT-süsteemide logimine ja seire;
- andmete pikaajaline säilitamine;
- tegutsemine eriolukorras.

ORP.5.M2 Õiguslike raamtingimuste järgimine [ülemus, haldusosakond, organisatsiooni juhtkond]

a. Äriprotsesside kujundamisel või IT-süsteemide väljatöötamisel arvestatakse õiguslikest raamtingimustest tulenevaid infoturbe nõudeid juba kavandamise ja disaini etappides.

b. Õigusaktide nõuete järgimise üldvastutus on organisatsiooni juhtkonnal.

c. Õiguslike raamtingimuste järgimise ja õigusaktide nõuete täitmise eest vastutavad konkreetsed, kinnitatud tööülesannetega töötajad.

d. Mittevastavuste kõrvaldamiseks rakendatakse sobivaid meetmeid.

3.3 Standardmeetmed

ORP.5.M4 Vastavusehalduse kavandamine ja korraldus [organisatsiooni juhtkond]

a. Iga konkreetse valdkonna õigusaktide nõuetest ülevaate tagamiseks on määratud vastutavad isikud ja nende vastavusehalduse ülesanded.

b. Vastavusnõuetest tehakse sihtrühmadele struktureeritud kokkuvõtted.

c. Vastavusnõuetest tulenevad täiendavad infoturvameetmed integreeritakse eeskirjadesse ja kordadesse koostöös infoturbejuhiga.

d. Vastavusehalduse infoturvameetmete rakendamist kontrollitakse regulaarselt.

ORP.5.M5 Erandite haldus [infoturbejuht]

a. Erandjuhtudel võib turvapoliitika järgimises teha mööndusi. Erandite tegemine turvapoliitikast põhjendatakse ja viiakse läbi riskihindamine.

b. Erandid kooskõlastatakse juhtkonnaga, kõigist eranditest säilitatakse ülevaade.

c. Tähtajaliste erandite puhul kontrollitakse regulaarselt erandite jätkuvat vajadust.

ORP.5.M8 Vastavusehalduse regulaarne läbivaatus

a. Vastavushalduse ning sellest tulenevate meetmete tõhususe ja toimivuse läbivaatust tehakse regulaarselt (vt DER.3.1 *Auditid ja läbivaatused*).

b. Regulaarsel läbivaatusel kontrollitakse töökorralduse ja äriprotsesside vastavust muutuvatele vastavusehalduse nõuetele.

3.4 Kõrgmeetmed

Moodulis kõrgmeetmed puuduvad.

CON: Kontseptsioonid ja metoodikad

CON.1 Krüptokontseptsioon

1 Kirjeldus

1.1 Eesmärk

Esitada krüptograafiliste vahendite kasutamise korralduslikud meetmed ning juhised krüptokontseptsiooni koostamiseks.

1.2 Vastutus

Krüptokontseptsiooni meetmete täitmise eest vastutab infoturbejuht.

Lisavastutajad

Vastutav spetsialist, IT-talitus.

1.3 Piirangud

Krüptograafiliste vahendite (krüptograafilist funktsiooni täitev riist- või tarkvaraüksus) käitamisega seotud IT protseduurid esitatakse mooduligrupis OPS.1.1 *IT-põhitööd*. Üksikute rakenduste või IT-süsteemide kaitsmist krüptograafia abil kirjeldatakse vastavate rakenduste moodulites.

2 Ohud

2.1 Puudulik võtmehaldus

Puuduliku võtmehalduse tulemusena võib paljastuda konfidentsiaalne teave. Kui protsessijuhendi puudumise tõttu on krüpteeritud andmed ja krüptovõtmed ekslikult paigutatud samale andmekandjale, saavad sümmeetrilise krüptoprotseduuri korral kõik andmekandjale või sidekanalile juurdepääsu omavad isikud andmeid dekrüpteerida.

Puudulik võtmehaldus võib ohustada andmete käideldavust, nt kui krüptovõtme või sertifikaadi kehtivusaeg on läbi saanud ja krüptovahendeid ei ole õigeaegselt uuendatud.

2.2 Õiguslike raamtingimuste rikkumine krüptomoodulite rakendamisel

Õiguslikud raamtingimused krüptograafiliste vahendite rakendamisel võivad riigiti erineda. Mõnes riigis ei tohi krüptomooduleid (ingl *cryptographic module*) ilma riikliku loata kasutusele võtta või on riigis piiratud suure murdmiskindlusega krüptograafiaga toodete eksport. Kui andmekaitse regulatsioon nõuab isikuandmete kaitseks selliste krüptograafiliste protseduuride kasutamist, mida teise riigi seadused ei toeta, muutub andmekaitse subjektide vaheline andmevahetus võimatuks.

2.3 Andmete konfidentsiaalsuse või tervikluse kadu kasutamisvigade tõttu

Kui organisatsioon võtab kasutusele krüptograafilise vahendi, mille kasutamine on liiga keerukas või see ei ole intuitiivne, võivad kasutajad krüptograafiliste vahendite kasutamisest loobuda ja selle asemel edastada andmeid avateksti kujul. See võimaldab ründajatel pealt kuulata edastatavaid andmeid.

2.4 Krüptograafilise vahendi tarkvaravead või turvanõrkused

Krüptomehhanismide turvalisust võivad vähendada nõrkused või vead krüptograafiliste vahendite tarkvaras. Näiteks võivad krüptomooduli poolt genereeritud juhuarvud olla prognoositavad, mistõttu juhuarvuga seotud krüptovõtme rekonstrueerimine lihtsustub oluliselt. Krüptograafilist funktsiooni täitva riist- või tarkvara turvanõrkusi saab ründaja ära kasutada elutähtsate süsteemide manipuleerimiseks ja andmete volitamata muutmiseks.

2.5 Krüptomooduli tõrge

Tehniliste defektide, elektrikatkestuste või tahtliku hävitamise tõttu võib tekkida tõrge riistvaralises krüptomoodulis. Seetõttu pole krüpteeritud andmeid niikaua võimalik kasutada kuni asendatakse dekrüpteerimiseks vajalik riistvara. Organisatsiooni ärikriitilised protsessid võivad seiskuda.

2.6 Ebaturvalised krüptograafilised vahendid

Ebaturvaliste või aegunud krüptoalgoritmide murdmiseks ei ole tarvis kalleid ressursse. Isegi kui organisatsioonisiseselt kasutatakse üksnes turvalisi ja sertifitseeritud tooteid, võib teabevahetus osutuda murtavaks juhul, kui organisatsioonivälise suhtluspartner ajakohaseid krüptograafilisi vahendeid ei kasuta.

2.7 Viga krüpteeritud andmetes või krüptovõtmes

Kui pärast andmete krüpteerimist krüptogrammi muudetakse, ei ole krüpteeritud teksti võimalik dekrüpteerida. Ainuüksi ühe biti vahetumine krüptovõtmes muudab krüpteeritud andmete dekrüpteerimise võimatuks. Kui andmetest ei ole tehtud varukoopiat, muutuvad kõik andmed kättesaamatuks.

2.8 Krüptovõtme paljastamine

Krüptomehhanismi turvalisus oleneb sellest, kas krüptovõtmed jäävad konfidentsiaalseks. Ründaja proovib enamasti tuvastada kasutatud võtit. Teades võtit ja krüptomehhanismi, on ründajal võimalik andmed dekrüpteerida. Selleks võib ründaja üritada taastada krüptovõtit kasutatud seadme mälutõmmisest (ingl *memory dump*), otsida seda konfiguratsioonifailidest või andmete varukoopiatest. Krüpteeritud kõvaketta korral võib ründaja kõvaketta dekrüpteerimiseks paigaldada klaviatuuri ja arvuti vahele paroolile juurdepääsu saamiseks klahvilogeri (ingl *keylogger*).

2.9 Võltsitud sertifikaat

Sertifikaate kasutatakse avaliku krüptovõtme konkreetse isiku privaatvõtmega sidumiseks, mis on omakorda krüptograafiliselt kaitstud digitaalsignatuuri abil. Kui sertifikaat on võltsitud, seotakse digitaalsignatuurid sertifikaadis nimetatud isikuga vääralt või krüpteeritakse ja edastatakse andmed ebaturvalise võtmega.

3 Meetmed

3.1 Elutsükkel

Kavandamine

CON.1.M1 Krüptomehhanismide kasutuselevõtu kavandamine

CON.1.M9 Krüptograafiliste vahendite valikukriteeriumite kehtestamine

Käitus

CON.1.M2 Andmete turvalisuse tagamine krüptomehhanismide kasutamisel

CON.1.M4 Turvaline võtmehaldus

CON.1.M10 Krüptokontseptsioon

CON.1.M15 Reageerimine krüptomehhanismide nõrgenemisele

CON.1.M19 Kasutatavate krüptograafiliste vahendite loend

Kõrvaldamine

CON.1.M5 Krüptovõtmete turvaline kustutus ja hävitamine

Lisanduvad kõrgmeetmed

CON.1.M11 Krüptograafiliste funktsioonidega riistvara testimine

CON.1.M16 Riistvaraliste krüptomoodulite füüsiline turve

CON.1.M17 Kiirguseturbe meetmed

CON.1.M18 Krüptograafiliste funktsioonidega riistvara asendus

CON.1.M20 Krüptograafiliste funktsioonidega riist- ja tarkvara manipuleerimise tuvastamine

3.2 Põhimeetmed

CON.1.M1 Krüptomehhanismide kasutuselevõtu kavandamine [vastutav spetsialist]

a. Krüptomehhamismide valimisel eelistatakse sõltumatutes uuringutes heakskiidetud krüptoalgoritme, mida on põhjalikult kontrollitud ja mis on teadaolevate turvanõrkusteta.

b. Krüptograafilises vahendis kasutatakse hetkel soovitatavaid võtmepikkusi.

c. Võtme pikkuse määramisel arvestatakse selle sobivust krüptovõtme plaanitud kasutusajaga. Pikemate kasutusaegade puhul on soovitatav võtme pikkust suurendada.

CON.1.M2 Andmete turvalisuse tagamine krüptomehhanismide kasutamisel [IT-talitus]

a. Krüpteeritud andmete varundamisel on krüptovõtmed kaitstud lubamatu juurdepääsu eest.

b. Pika kasutuskestusega krüptovõtmeid hoitakse väljaspool kasutatavat IT-süsteemi paiknevas võrguühenduseta asukohas.

c. Krüpteeritud andmete pikaajalisel säilitamisel on tagatud andmetele juurdepääs. Krüpteerimiseks kasutatud krüptoalgoritmide ja võtmepikkuste vastavust hetkel soovitavatele väärtustele kontrollitakse regulaarselt.

d. Kasutusest võetud krüptograafilised vahendid on arhiveeritud ning vastav riist- ja tarkvarakonfiguratsioon on varundatud.

CON.1.M4 Turvaline võtmehaldus

a. Krüptograafiliste vahendite krüptovõtmete halduseks on kehtestatud sobiv võtmehaldussüsteem ja loodud turvaline keskkond.

b. Võtmehaldussüsteem käsitleb krüptovõtmete tervikluse ja autentsuse säilitamist kogu võtme elutsükli (võtmete loomine, säilitamine, uuendamine, hävitamine) vältel.

c. Krüptovõtmete loomisel on kasutatud sobivat võtmegeneraatorit ja turvalist keskkonda.
d. Kolmandate poolte genereeritud võtmete kasutamisel kontrollitakse võtmeandmete päritolu ja terviklust. Kontrollimatu võtmehoidlaga krüptograafilisi vahendeid ei kasutata.
e. Krüptograafiliste vahendite vaikevõtmed (va avaliku võtme sertifikaadid) on asendatud.
f. Võimalusel kasutatakse krüptovõtit ainult üheks kasutusotstarbeks. Krüpteerimiseks ja signatuuride moodustamiseks kasutatakse erinevaid võtmeid.
g. Salajased võtmed (ingl *secret key*) on kaitstud volitamata juurdepääsu eest ja nende transpordil kasutatakse turvalisi edastuskanaleid.
h. Krüptovõtmeid muudetakse vastavalt IT-süsteemi nõuetele ja fikseeritud sagedusega.
i. Salajaste võtmete ja privaatvõtmete (ingl *private key*) avalikuks tuleku puhuks on loodud protseduurid intsidendi käsitlemiseks.

3.3 Standardmeetmed

CON.1.M5 Krüptovõtmete turvaline kustutus ja hävitamine [IT-talitus]

a. Kasutusest võetud krüptovõtmed ja sertifikaadid kustutatakse turvaliselt ja hävitatakse.
b. Krüptovõtmete turvalise kustutuse ja hävitamise protseduurid on dokumenteeritud krüptokontseptsioonis.

CON.1.M9 Krüptograafiliste vahendite valikukriteeriumite kehtestamine [vastutav spetsialist]

a. Enne krüptograafiliste vahendi valimist määratakse, millistele nõuetele peab toode vastama. Seejuures pööratakse tähelepanu järgmistele aspektidele:
   - funktsionaalsus;
   - koostalitlusvõime;
   - majanduslik otstarbekus;
   - töö- ja tõrkekindlus;
   - tehnilised aspektid;
   - personali- ja korralduslikud aspektid;
   - kasutatavad krüptomehhanismid, -algoritmid ja võtmepikkused;
   - andmekaitse nõuded;
   - õiguslikud raamtingimused (sh rahvusvahelised õiguslikud aspektid).
b. Kasutusotstarbe ja käituskoha alusel otsustatakse, kas on vajalik kasutada ainult sertifitseeritud krüptovahendeid.

CON.1.M10 Krüptokontseptsioon

a. Organisatsiooni krüptokontseptsiooni loomisel on lähtutud organisatsiooni üldisest turvapoliitikast. Krüptokontseptsioon esitab kasutatavate krüptomehhanismide ja krüptograafiliste vahendite tehnilised ja korralduslikud nõuded.
b. Krüptokontseptsioonis on sätestatud vähemalt järgmine:
   - vastutus krüptograafiliste vahendite eest;
   - krüptograafiliste vahendite turvaline konfigureerimine ja nõutavad tehnilised parameetrid;

- krüptograafiliste vahendite testimine;
- krüptograafiliste vahendite turvaline kasutamine;
- krüptograafiliste vahendite turvaline haldus;
- krüptovõtmete haldus (sh võtmete turvaline varundamine);
- krüptograafiliste vahendite asendamine;

krüptograafiliste vahendite turvaline kustutus ja hävitamine.

c. Krüptograafiliste vahendite kasutajatele on koostatud õppematerjalid, tegevusjuhised ning loodud teavitusteed probleemidest ja turvasündmustest teavitamiseks.

d. Asjassepuutuvad töötajad järgivad tegevusjuhiseid.

e. Krüptokontseptsiooni täitmist kontrollitakse regulaarselt. Kontrollitulemused dokumenteeritakse. Vajadusel krüptokontseptsioon ajakohastatakse.

CON.1.M15 Reageerimine krüptomehhanismide nõrgenemisele

a. Usaldusväärsetele allikatele tuginedes kontrollib organisatsioon vähemalt korra aastas kõigi kasutatavate krüptograafiliste vahendite, meetodite ja parameetrite ajakohasust ja turvalisust.

b. Krüptomehhanismi turvanõrkuste ilmnemiseks on koostatud protseduur, mis taastab krüptomehhanismi nõutava turvataseme või asendab nõrgenenud krüptograafilise vahendi sobiva alternatiiviga.

CON.1.M19 Kasutatavate krüptograafiliste vahendite loend [IT-talitus]

a. Organisatsioon on loonud kasutatavate krüptograafiliste vahendite (sh krüptograafiliste funktsioonidega riist- ja tarkvara) loendi. Loend sisaldab vähemalt järgmist:
   - IT-süsteemid, mis antud krüptograafilist vahendit kasutavad;
   - krüptograafilise vahendi kasutamise eesmärk (nt arvuti kõvaketta krüpteerimine);
   - krüptograafilised meetodid ja krüptomehhanismid;
   - krüptograafilise vahendi turvaparameetrid (nt võtme pikkus).

3.4 Kõrgmeetmed

CON.1.M11 Krüptograafiliste funktsioonidega riistvara testimine (C-I) [IT-talitus]

a. Krüptograafiliste funktsioonidega riistvara kasutuselevõtu eel luuakse uued krüptovõtmed ja kontrollitakse, kas krüptograafilised funktsioonid toimivad ootuspäraselt.

b. Krüptograafiliste funktsioonidega riistvara testimisprotseduurid on kirjeldatud krüptokontseptsioonis.

c. IT-süsteemi muudatuste järgselt testitakse kasutavate krüptograafiliste funktsioonide toimivust.

d. Krüptograafiliste funktsioonidega riistvara konfiguratsiooni õigsust kontrollitakse regulaarselt.

e. Võimalusel kasutatakse krüptograafiliste funktsioonidega riistvara, mis võimaldab läbi viia eneseteste.

CON.1.M16 Riistvaraliste krüptomoodulite füüsiline turve (C-I) [IT-talitus]

a. On rakendatud meetmed krüptograafiliste funktsioonidega riistvarale volitamata füüsilise juurdepääsu tõkestamiseks.

CON.1.M17 Kiirguseturbe meetmed (C) [IT-talitus]

a. Lähtuvalt teabe konfidentsiaalsusvajadusest võetakse kiirguseturbe parendamiseks kasutusele täiendavad meetmed.

b. Kiirguseturbe meetmed ja meetmete rakendamise lävendid on dokumenteeritud krüptokontseptsioonis.

CON.1.M18 Krüptograafiliste funktsioonidega riistvara asendus (C-I-A) [IT-talitus]

a. Krüptograafiliste funktsioonidega riistvara asendamiseks on olemas asendusriistvara, nt piisav varu mitmikautentimiseks kasutatavaid riistvaralisi krüptopääsmikke (ingl *cryptographic token*).

b. On olemas krüptograafiliste funktsioonidega riistvara asendamist kirjeldavad juhendid.

CON.1.M20 Krüptograafiliste funktsioonidega riist- ja tarkvara manipuleerimise tuvastamine (C-I)

a. Kasutusele võetud krüptomooduleid ei saa märkamatult välja lülitada ega ignoreerida.

b. Krüptograafilisi funktsioone täitvate riist- või tarkvaraüksuste toimimist seiratakse võimalike manipuleerimiskatsete tuvastamiseks.

4 Lisateave

Lühend	Publikatsioon
[BSI]	BSI TR-02102-1 „Cryptographic Mechanisms Recommendations and Key Lengths“ https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf?__blob=publicationFile&v=6

CON.2 Isikuandmete kaitse

1 Kirjeldus

1.1 Eesmärk

Esitada organisatsioonile meetmed füüsiliste isikute (andmesubjektide) põhiõiguste kaitseks isikuandmete töötlemisel.

Turvameetmete rakendamine äriprotsesside kaitseks tagab andmeid töötleva organisatsiooni turvalisuse, kuid see ei pruugi ilma täiendavaid meetmeid rakendamata olla piisav füüsiliste isikute (andmesubjektide) kaitsmiseks isikuandmete väärkasutuse eest.

1.2 Vastutus

Isikuandmete kaitse meetmete rakendamise eest vastutab organisatsiooni juhtkond.

Lisavastutajad

IT-talitus, infoturbejuht, testija, personaliosakond, andmekaitsespetsialist.

1.2 Piirangud

Õigusaktidest tulenevate andmekaitsenormide, sh isikuandmete töötlemise põhimõtete järgimine on andmetöötleja kohustus.

Andmekaitsespetsialisti ülesandeks on analüüsida ja kontrollida isikuandmete töötlemise toimingute õiguspärasust organisatsioonis, andes talle seoses tema kohustustega nõu ja soovitusi. Sel põhjusel ei ole andmekaitse spetsialisti tegevusi vastutajana järgnevates moodulites välja toodud.

Moodulis esitatavaid meetmeid rakendatakse isikuandmeid salvestatavatele ja talletavatele sihtobjektidele.

Täiendavalt tuleb isikuandmete kaitseks rakendada asjakohaseid meetmeid järgnevatest moodulitest:

- ORP.2 *Personal*
- ORP.4 *Identideedi- ja õiguste haldus*
- ORP.5 *Vastavusehaldus (nõuete haldus)*
- CON.1 *Krüptokontseptsioon*
- CON.3 *Andmevarunduse kontseptsioon*
- CON.6 *Andmete kustutus ja hävitamine*
- CON.8 *Tarkvaraarendus*
- CON.9 *Teabevahetus*
- OPS.1.1.3 *Paiga- ja muudatusehaldus*
- OPS.1.1.4 *Kaitse kahjurprogrammide eest*
- OPS.1.1.5 *Logimine*
- OPS.1.1.6 *Tarkvara testimine ja kasutuselevõtt*
- OPS.1.2.2 *Arhiveerimine*
- OPS.2.2 *Pilvteenuste kasutamine*
- OPS.2.3 *Väljasttellimine*
- OPS.3.2 *Teenuseandja infoturve*
- DER.1 *Turvaintsidentide avastamine*
- DER.2.1 *Turvaintsidentide käsitlus*
- DER.3.1 *Auditid ja läbivaatused*
- NET.3.2 *Tulemüür*
- NET.3.3 *Virtuaalne privaatvõrk (VPN)*

2 Ohud

2.1 Andmekaitseregulatsioonide eiramine

Euroopa Liidu isikuandmete kaitse üldmäärus (ingl General Data Protection Regulation, GDPR), isikuandmete kaitse seadus ning teatud juhtudel ka muud seadusandlikud aktid esitavad nõuded isikuandmete töötlemisele. Regulatsiooni eesmärk on füüsiliste isikute (andmesubjektide) õiguseid kaitsta.

Oht füüsilistele isikutele tekib, kui organisatsioon eirab andmekaitsenõudeid, nt töödeldes andmeid eesmärgita või suuremas ulatuses kui on eesmärgi täitmiseks vajalik, õigusliku aluseta, läbipaistmatult, turvameetmeid rakendamata või ilma andmesubjekti sekkumisvõimaluseta. Lisaks organisatsiooni poolt isikutele tekitatud kahjude hüvitamisele on isikuandmete kaitse üldmäärusest tulenevalt võimalik andmekaitsenõuete rikkujat trahvida kuni 20 000 000 euro ulatuses või ettevõtja puhul kuni 4% tema eelneva majandusaasta ülemaailmsest aastasest kogukäibest, olenevalt sellest, kumb on suurem.

2.2 Puudulikud andmetöötlusprotseduurid

Andmete väärkasutamise oht kasvab, kui organisatsioonis puuduvad protseduurid IT-süsteemidele ja andmetele õiguspärase juurdepääsu tagamiseks või kui töötajatel on juurdepääs isikuandmetele, mida ei ole konkreetsete tööülesannete täitmiseks vaja.

Kui andmete kasutamist ei kontrollita või kui andmete töötluse faktid ei ole logide ega dokumentatsiooni abil tõendatavad, võib suureneda andmete väärkasutamine.

Kui andmetöötlusjuhendid ei sätesta, kuidas ja millises ulatuses organisatsiooni töötajad tohivad isikuandmeid vaadata, muuta või edastada, võib töötaja selge ja üheselt mõistetava juhendi puudumise tõttu isikuandmete töötlemise käigus eksida.

2.3 Puudulikud ressursid

Kui organisatsioon hindab isikuandmete kaitsevajadust liiga madalaks ja ei eralda isikuandmete kaitseks piisavalt tööjõudu, vahendeid jm vajalikke ressursse, jäävad isikuandmete kaitse korralduslikud ja tehnilised meetmed kas osaliselt või täielikult rakendamata. Tulemus ei pruugi tagada isikuandmete piisavat kaitset, seadusest tulenevad nõuded jäävad täitmata.

Ressursside puuduse põhjuseks on tihtipeale organisatsiooni juhtkonna ükskõiksus või teadmatus andmekaitsereeglite ja andmekaitse vajalikkuse osas.

2.4 Puudulik privaatsus

Isikuandmete töötlemine võib riivata andmesubjekti õigust perekonna- ja eraelu puutumatusele.

Eriti intensiivne riive võib tekkida, kui töödeldakse eriliigilisi isikuandmeid ehk isikuandmeid, mis paljastavad rassilist ja etnilist päritolu, poliitilisi vaateid, religioosseid või maailmavaatelisi tõekspidamisi ning ametiühingusse kuulumist, samuti geneetilisi andmeid, andmeid tervise, seksuaalelu ning biomeetria kohta.

Puudulik privaatsus tähendab isikuandmete töötlemist, millega seotud tegevused või tegevusetus, rakendamisest tulenevad tagajärjed, sealhulgas kõrgendatud oht isikuandmetega seotud rikkumise toimepanemisele, põhjustavad andmesubjekti perekonna- ja eraelu puutumatuse riive. Näiteks on õigusrikkumine inimese andmete vaatamine andmekogus ilma selleks tegevuseks õiguslikku alust omamata.

2.5 Isikuandmete konfidentsiaalsuse kadu

Isikuandmete töötlemisel on alati oht, et andmed satuvad volitamata isikute kätte. See võib juhtuda näiteks andmebaasi turvalisuse rikkumise, häkkerite rünnaku või füüsilise andmekandja kaotamise tõttu. Andmelekete tagajärjel võidakse isikuandmeid kuritarvitada, need võivad saada aluseks isiku identiteedivargusele või muudele ebaseaduslikele, isiku enesemääramise õigusi kahjustavatele tegevustele.

2.6 Ebatäpsete andmete töötlemine

Isikuandmete töötlemisel on oht, et andmed muutuvad ebatäpseks, ebaõigeks või aegunuks. See võib juhtuda inimese enda eksimuste või IT-süsteemis tekkivate vigade tõttu. Andmete masstöötlusel on selliseid vigu väga keeruline tuvastada. Isiku kohta käivate ekslike andmete töötlemine võib viia ebaõigete otsuste tegemiseni ja võib mõjutada inimeste õigusi, vabadusi ja huve.

2.7 Andmetöötleja mainekahju

Töötajate, klientide või partnerite isikuandmete lekkimine organisatsiooni enda süül võib organisatsiooni mainet tugevasti kahjustada. Kliendid võivad loobuda lepingutest, mis on organisatsiooniga sõlmitud ning see avaldub käibe vähenemisest tuleneva rahalise kahjuna. Töötajad ja partnerid kaotavad organisatsiooni vastu usalduse.

3 Meetmed

3.1 Elutsükkel

Kavandamine

CON.2.M1 Isikuandmete kaitse kavandamine

CON.2.M2 Andmekaitsespetsialisti (andmekaitseametniku) määramine

CON.2.M3 Isikuandmete töötluse kaardistamine

Evitus

CON.2.M4 Andmekaitsepoliitika ja andmekaitsejuhiste väljatöötamine

CON.2.M7 Andmekaitsetingimuste dokumenteerimine

Käitus

CON.2.M5 Organisatsiooni töötajate teadlikkuse tõstmine

CON.2.M6 Isikuandmete töötlemise õigus- ja eesmärgipärasuse ning minimaalsuse tagamine

CON.2.M8 Andmesubjekti õiguste tagamine

CON.2.M9 Isikuandmete pseudonüümimine ja anonüümimine

CON.2.M10 Isikuandmetele juurdepääsu piiramine

CON.2.M11 Isikuandmete korrakohane säilitamine

CON.2.M12 Isikuandmete kaitse tehniliste meetmete rakendamine

CON.2.M13 Andmekaitsealased mõjuhinnangud

CON.2.M14 Volitatud töötlejate haldus

CON.2.M15 Isikuandmete turvaline krüpteerimine

CON.2.M16 Isikuandmete säilitamise eeskiri

CON.2.M17 Keskne pääsuhalduse süsteem

CON.2.M18 Isikuandmete töötlemise turve

CON.2.M19 Andmetöötluse toimingute logimine

CON.2.M20 Andmetöötluse asukohtade füüsiline turvalisus

CON.2.M21 Võrguturbe tagamine

CON.2.M22 Lõimitud andmekaitse ja vaikimisi andmekaitse põhimõtete rakendamine rakendustes

CON.2.M23 Isikuandmeid sisaldavate rakenduste testimine

CON.2.M24 Privaatsusseadistused veebilehtedel

CON.2.M25 Isikuandmete kustutamine töötaja lahkumisel

CON.2.M26 Andmekaitseauditi läbiviimine

Lisanduvad kõrgmeetmed

CON.2.M27 Tähtajalised juurdepääsuõigused

CON.2.M28 Isikuandmete töötlemise automaatseire

CON.2.M29 Juurdepääsupiirangute klassifikaator

CON.2.M30 Isikuandmete automaatne tuvastamine

CON.2.M31 Digitaalsete õiguste halduse süsteem

3.2 Põhimeetmed

CON.2.M1 Isikuandmete kaitse kavandamine

a. Organisatsioonis on analüüsitud töödeldavate isikuandmete asukohti, liike ja kaitsetarvet.

b. Organisatsioon on kaardistanud ning dokumenteerinud seadusandlusest ning kolmandate pooltega sõlmitud lepingutest tulenevad andmekaitsenõuded.

c. Organisatsioon on tuvastanud isikuandmete kaitse meetmete rakendamise kohustuse ja määranud isikuandmete kaitse meetmete eest vastutajad.

CON.2.M2 Andmekaitsespetsialisti (andmekaitseametniku) määramine

a. Organisatsiooni juhtkond on määranud andmekaitsespetsialisti, kui isikuandmete kaitse üldmääruse (IKÜM) artikkel 37 seda nõuab.

b. Organisatsioon tagab, et andmekaitsespetsialist saab oma teadmisi regulaarselt uuendada (koolitused) ning võimaluse olla kursis andmekaitse-alaste arengute ja sündmustega.

c. Organisatsioon tagab andmekaitsespetsialisti nõuetekohase ja õigeaegse kaasamise kõikidesse isikuandmete kaitsega seotud küsimustesse.

CON.2.M3 Isikuandmete töötluse kaardistamine

a. Organisatsioon on kaardistanud isikuandmete töötlemise kogu andmete elutsükli ulatuses.

b. Kaardistamise tulemused on dokumenteeritud isikuandmete töötlemise ülevaates.

CON.2.M4 Andmekaitsepoliitika ja andmekaitsejuhiste väljatöötamine

a. Organisatsioon on välja töötanud ja kehtestanud andmekaitsepoliitika ja andmekaitsejuhised.

b. Andmekaitsepoliitikas on kirjeldatud isikuandmetele juurdepääsu andmise ning andmete kogumise, töötlemise, säilitamise ja kustutamise põhimõtted.

c. Andmekaitsepoliitika sätestab organisatsiooni töötajate vastutuse isikuandmete kaitse tagamisel.

d. Andmekaitsejuhised sisaldavad organisatsiooni töötajatele suunatud tegevusjuhiseid isikuandmete turvalisust mõjutavate intsidentidele ja andmesubjektide pöördumistele reageerimiseks.

CON.2.M5 Organisatsiooni töötajate teadlikkuse tõstmine [andmekaitsespetsialist, infoturbejuht, personaliosakond]

a. Organisatsioon korraldab regulaarselt andmekaitsealaseid koolitusi, kaasates selleks vajadusel ka väliseid eksperte.

b. Organisatsioon viib läbi küberhügieeni koolitusi (nt ekraaniluku kasutamine arvuti juurest lahkudes).

c. Organisatsiooni töötajate teadmisi kontrollitakse regulaarsete testidega, mis sisaldavad andmekaitsealaseid küsimusi ja tüüpjuhtumite lahendamist.

CON.2.M6 Isikuandmete töötlemise õigus- ja eesmärgipärasuse ning minimaalsuse tagamine

a. Organisatsioon töötleb isikuandmeid ainult IKÜM artikkel 6 sätestatud õigusliku aluse olemasolul.

b. Organisatsioon töötleb isikuandmeid ainult kindlaksmääratud eesmärkidel ning ulatuses, mis on nende eesmärkide täitmiseks vajalik.

CON.2.M7 Andmekaitsetingimuste dokumenteerimine

a. Organisatsioon on koostanud andmekaitsetingimused vastavalt isikuandmete kaitse üldmääruse artiklitele 5 lg 1 p. a ja lg 2, 12-22 ning pp. 39, 58-72.

b. Andmekaitsetingimused on töötajatele ja teistele andmesubjektidele arusaadavad ja vajadusel kergesti kättesaadavad.

CON.2.M8 Andmesubjekti õiguste tagamine

a. Organisatsioon tagab, et andmesubjektide IKÜM-st tulenevaid õigusi on IT-süsteemides tehniliselt võimalik rakendada.

b. Andmesubjektidele antakse selget ja arusaadavat teavet nende õiguste kohta.

c. Õiguste rakendamine on andmesubjekti jaoks lihtne.

CON.2.M9 Isikuandmete pseudonüümimine ja anonüümimine

a. Organisatsioon minimeerib isikuandmete töötlemisel isikuga otseselt või kaudselt seostatavate andmete kasutamist.

b. Võimalusel isikuandmed pseudonüümitakse (meetod, kus isikuandmed asendatakse andmete töötlemisel unikaalse identifikaatori või koodiga, mis ei võimalda isikut otseselt tuvastada) või anonüümitakse (meetod, mille käigus isikuandmeid muudetakse sellisel viisil, et neid ei ole võimalik enam konkreetse isikuga seostada ei otseselt ega kaudselt).

c. Statistilises andmetetöötluses kasutatakse võimalusel ainult anonüümitud isikuandmeid.

CON.2.M10 Isikuandmetele juurdepääsu piiramine [IT-talitus]

a. Isikuandmetele juurdepääsu andmisel lähtutakse minimaalsuse printsiibist, st töötajale antakse juurdepääs ainult sellele osale IT-süsteemist ja andmetest, mis töötajal on tööülesannete täitmiseks vajalik.

b. Juurdepääsu piiramine hõlmab nii füüsilise juurdepääsu kui pääsuõiguste piiramist.

CON.2.M11 Isikuandmete korrakohane säilitamine

a. Organisatsioon on määranud säilitustähtajad kõikidele säilitavatele isikuandmetele.

b. Säilitamise eesmärk ja säilitustähtajad on kooskõlas asjakohaste õigusaktidega.

c. Organisatsioon säilitab isikuandmeid ainult nii kaua, kui see on vajalik säilitamise eesmärgi saavutamiseks.

d. Kui säilitamise eesmärk on täidetud või kui isikuandmed ei ole enam vajalikud, korraldab organisatsioon nende isikuandmete turvalise hävitamise.

CON.2.M12 Isikuandmete kaitse tehniliste meetmete rakendamine [IT-talitus]

a. Organisatsioon on isikuandmetele volitamata juurdepääsu takistamiseks võtnud IT-süsteemides kasutusele turvalised autentimismeetodid (vt ORP4 *Identiteedi- ja õiguste haldus*).

b. Organisatsioon on võrguliikluse kaitseks paigaldanud tulemüüri ja piiranud mittevajaliku võrguliikluse (vt NET.3.2 *Tulemüür*).

c. Isikuandmete töötlemisel (sh. nende saatmisel) organisatsioon krüpteerib isikuandmed, kui see on asjakohane.

d. Isikuandmete töötluse tegevused ja asjaolud logitakse (vt OPS 1.1.5 *Logimine*).

e. Isikuandmete varundamine toimub regulaarselt. Varukoopiaid säilitatakse varundatavatest andmetest eemal asuvas asukohas. (vt CON.3 *Andmevarunduse kontseptsioon*).

f. Organisatsioon kontrollib ja testib regulaarselt isikuandmete töötlemisel tehniliste meetmete rakendamist, et veenduda nende tõhususes, turvalisuses ning vastavuses isikuandmete kaitse üldmääruse ja käesoleva standardiga.

3.3 Standardmeetmed

CON.2.M13 Andmekaitsealased mõjuhinnangud

a. Organisatsioon on läbi viinud andmekaitsealase mõjuhinnangu, kui see on isikuandmete kaitse üldmääruse artiklist 35 tulenevalt nõutud. Andmekaitsespetsialist on mõjuhinnangu koostamisel nõustavas rollis.

b. Andmekaitsespetsialist või organisatsiooni juhtkond on koostanud mõjuhinnangu läbiviimise juhendi, mille alusel oskavad mõjuhinnangut läbi viia ka ilma eelneva põhjaliku ettevalmistuseta töötajad.

CON.2.M14 Volitatud töötlejate haldus

a. Organisatsioon on volitatud töötlejatega sõlminud isikuandmete kaitse üldmääruse artiklile 28 vastavad andmetöötluslepingud;

b. Organisatsioon on kontrollinud, et volitatud töötlejad rakendavad nõutavaid turvameetmeid isikuandmete töötlemisel ja järgivad isikuandmete töötlemise põhimõtteid.

c. Organisatsioon on valinud volitatud töötlejaid hoolikalt, tehes põhjalikke taustauuringuid ja veendudes nende pädevuses ning kogemustes andmekaitse valdkonnas.

d. Organisatsioon on volitatud töötlejate kaasamisel vaadanud üle nende andmekaitsetingimused, protseduurid ja turvameetmed ning on veendunud, et need vastavad isikuandmete kaitse üldmääruses sätestatud nõuetele.

e. Organisatsioon kontrollib volitatud töötlejate tegevuse vastavust isikuandmete kaitse üldmääruses sätestatud nõuetele. Vastav audit viiakse läbi minimaalselt kord nelja aasta jooksul ja seda võib teha koos üldise andmekaitseauditiga.

f. Isikuandmete kaitse nõuete muutumisel veendub organisatsioon, et volitatud töötlejad oleksid muudatustest teadlikud ning sõlmitud andmetöötluslepingud vastaksid uutele nõuetele. Vajadusel andmetöötluslepingud uuendatakse.

CON.2.M15 Isikuandmete turvaline krüpteerimine [IT-talitus]

a. Organisatsioon on juurutanud turvalise võtmehaldusprotseduuri ning kasutab isikuandmete turvalisuse tagamiseks tugevat ja usaldusväärset krüpteerimisalgoritmi.

b. Organisatsioon tagab, et asjakohasel juhul toimub krüpteerimine juba andmete kogumise või edastamise ajal.

c. Organisatsioon tagab, et krüpteeritud isikuandmete dekrüpteerimise võimalus oleks rangelt piiratud vaid selleks volitatud isikutele.

d. Organisatsiooni töötajaid peab koolitama ja teavitama krüpteerimise parimate tavade teemal ja tagama, et töötajad oskavad krüptovahendeid isikuandmete kaitseks korrektselt kasutada.

CON.2.M16 Isikuandmete säilitamise eeskiri

a. Organisatsioon on koostanud eeskirja, mis kirjeldab, kuidas ja kui kaua erinevaid isikuandmeid säilitatakse ning kuidas toimub isikuandmete hävitamine.

b. Eeskiri sisaldab säilitusperioode kõigile varundatud või arhiveeritud isikuandmetele.

c. Organisatsioon kasutab säilitamistähtaegade jälgimiseks automaatseid teavitusi või automaatset kustutamist.

d. Organisatsioon auditeerib andmete säilitamise tähtaegade järgimist regulaarselt.

CON.2.M17 Keskne pääsuhalduse süsteem [IT-talitus]

a. Organisatsioon kasutab keskset pääsuhalduste süsteemi, mille abil organisatsioon haldab töötajate juurdepääsu isikuandmetele.

b. Organisatsioon logib töötajate tegevusi, et tuvastada isikuandmete väärkasutamist, kiirendada reageerimist turvasündmustele ning vähendada andmelekke riski.

c. Organisatsioon korraldab juurdepääsuõiguste ülevaatuse vähemalt kord aastas. Liigsed pääsuõigused eemaldatakse.

CON.2.M18 Isikuandmete töötlemise turve [IT-talitus, infoturbejuht]

a. Organisatsioon kasutab tundlikele isikuandmetele juurdepääsu andmisel mitmikautentimist (ingl *multifactor authentication*), eesmärgiga tagada ainult volitatud isikute juurdepääs.

b. Kaugtöötamiseks on organisatsioonis kasutusel virtuaalne privaatvõrk (ingl *virtual private network*, VPN). VPN tagab turvalise ja krüpteeritud ühenduse organisatsiooni

sisevõrguga, võimaldades töötajatel turvaliselt juurde pääseda isikuandmetele väljastpoolt organisatsiooni võrku.

c. Tundliku teabe kaitsmiseks kõrvaliste pilkude eest kasutatakse ekraanifiltrit. Ekraanifilter on olemas pidevalt sülearvutiga kaugtööd tegevatel töötajatel.

CON.2.M19 Andmetöötluse toimingute logimine [IT-talitus]

a. Kõik isikuandmete töötlemise toimingud logitakse.

b. Andmetöötluse logid sisaldavad järgmist:

- kes isikuandmeid töötles;
- millal isikuandmeid töödeldi;
- mis isikuandmeid töödeldi;
- milliseid toiminguid isikuandmetega tehti (toimingute all peetakse silmas kõiki andmetöötluse vorme sh. vaatamised, muutmised, allalaadimised, kustutamised).

c. Kui andmetöötluses on kaasatud kolmandaid osapooli (sh. volitatud, kaasvastutavaid töötlejaid), siis lepitakse kokku selged rollid andmetöötluslogide talletamiseks ja juurdepääsuks.

d. Andmetöötluslogidele on rakendatud automaatne logianalüsaator, mis aitab tuvastada võimalikke andmekaitsealaseid rikkumisi.

e. Organisatsioon on kehtestanud protseduuri andmetöötluslogide ülevaatamiseks. Andmetöötluslogisid kontrollitakse regulaarselt ning vajadusel juhtumipõhiselt.

f. Andmetöötluslogisid säilitatakse minimaalsuse ja eesmärgipärasuse põhimõtteid silmas pidades. Eelkõige on oluline, et andmetöötluslogisid ei säilitataks ebamõistlikult kaua, kuid siiski piisavalt kaua, et saaks tuvastada võimalikke rikkumisi.

g. Andmetöötluslogidele on sätestatud säilitamistähtajad, mille lõppedes need kustutatakse automaatselt.

CON.2.M20 Andmetöötluse asukohtade füüsiline turvalisus

a. Organisatsioon on isikuandmete turvaliseks töötlemiseks ja säilitamiseks määranud piiratud pääsuga alad (näiteks lukustatud ruumid või serveriruumid).

b. Organisatsioon on kehtestanud ruumidele juurdepääsu reeglid ja rakendanud selle jõustamiseks tehnilised juurdepääsu- ja valvesüsteemid (nt elektrooniline lukustussüsteem, uksekaart, biomeetriline autentimine, valvekaamerad).

c. Organisatsioon viib regulaarselt läbi ülevaatusi füüsiliste turvameetmete efektiivsuse hindamiseks (sh. uste ja lukkude seisukorra kontrolli, valvesüsteemide testimist, videoseire toimimise kontrolli, uksekaardi logide kontrolli jne).

d. Organisatsioon on koostanud protseduurid külaliste haldamiseks, kes sisenevad organisatsiooni aladele, kus töödeldakse isikuandmeid. See hõlmab nii külaliste registreerimist, külastuste eelnevat kooskõlastamist, külaliste juhendamist organisatsiooni reeglite osas ning külastaja saatmist (st. külastaja liigub organisatsioonis ainult koos organisatsiooni töötajast saatjaga).

CON.2.M21 Võrguturbe tagamine [IT-talitus]

a. Organisatsioon kasutab võrgurünnete ja isikuandmetega tehtavate ebaharilike tegevuste tuvastamiseks ja ennetamiseks sissetungituvastuse ja -tõrje süsteeme (IDS, IPS).

b. Isikuandmete saatmiseks üle avaliku võrgu kasutatakse turvalisi, krüpteeritud protokolle.

CON.2.M22 Lõimitud andmekaitse ja vaikimisi andmekaitse põhimõtete rakendamine rakendustes

a. Rakendustes, mis põhinevad isikuandmete töötlemisel või mille käigus töödeldakse isikuandmeid, arvestatakse lõimitud andmekaitse (ingl *data protection by design*) ja vaikimisi andmekaitse (ingl *data protection by default*) põhimõtteid juba rakenduse valimise ja väljatöötamise kavandamise etappides.

b. Rakendustele kehtestatud andmekaitsenõuete täitmist järgitakse ja kontrollitakse rakenduse kogu eluea vältel.

c. Rakendustes kasutatakse ainult töötlemise eesmärgi täitmiseks vajalikke isikuandmeid.

CON.2.M23 Isikuandmeid sisaldavate rakenduste testimine [testija]

a. Organisatsioon on koostanud põhimõtted rakenduste testimise läbiviimiseks, milles keelatakse isikuandmete avaldamine, volitamata juurdepääs isikuandmetele ning piiratakse testijate tegevust isikuandmetega seotud süsteemides. Testimise all peetakse silmas nii rakenduste kasutuselevõtueelset testimist kui rakenduse läbistustestimisi turvanõrkuste avastamiseks.

b. Testimise läbiviimiseks on sõlmitud lepingud, mis selgitavad testimise ulatust, eesmärke ja testimisel lubatud tegevusi. Eesmärk on tagada vastutuse selgus ning kaitsta isikuandmete konfidentsiaalsust ja privaatsust.

c. Enne testimise läbiviimist tehakse kindlaks testimiseks hädavajalikud isikuandmed, võimalusel need andmed anonüümitakse või pseudonüümitakse.

d. Võimalusel antakse testijatele IT-süsteemi regulaarsest kasutajast piiratumad õigused. Testijal on juurdepääs ainult neile ressurssidele, mis on vajalikud testimise läbiviimiseks.

e. Organisatsioon tagab, et pärast testimise lõppu kõik testijate poolt talletatud isikuandmed turvaliselt kustutatakse. Selleks sõlmitakse vastavad lepingud (sh. andmetöötlusleping).

f. Pärast testimist teostab organisatsioon järelkontrolli, et hinnata andmekaitse ja turvameetmete tõhusust.

CON.2.M24 Privaatsusseadistused veebilehtedel

a. Organisatsiooni veebilehel kasutatavad küpsised (ingl *cookie*) ja jälgimisvahendid on kooskõlas isikuandmete kaitse üldmääruse ja teiste asjakohaste regulatsioonidega.

b. Veebilehe külastajatele on kasutavate küpsiste ja jälgimisvahendite kohta antud selge ja üheselt mõistetav teave. Kui on nõutud, küsitakse küpsiste kasutamiseks veebilehe külastajalt nõusolekut.

c. Veebilehe külastajatel on võimalik kontrollida ja hallata oma küpsiste eelistusi.

d. Organisatsioon on veebilehel avalikustanud andmekaitsetingimused, mis kirjeldavad, milliseid isikuandmeid kogutakse (sh. küpsised), kuidas neid töödeldakse, millistel eesmärkidel, kaua säilitatakse ja kuidas privaatsust kaitstakse. Täiendavate andmekaitsetingimuste elementide koostamisel tuleb lähtuda isikuandmete kaitse üldmääruse artiklitest 12-22.

e. Organisatsioon rakendab veebilehtedel isikuandmete kaitseks turvameetmeid.

f. Organisatsioon rakendab isikuandmeid sisaldaval veebilehel turvalist andmeedastusprotokolli HTTPS.

g. Veebilehe või võrguühenduse kaitseks kasutavate kolmandate osapoolte teenuste (näiteks: Google Analytics, Matomo, CloudFare) kasutamine on andmekaitsetingimustes välja toodud.

h. Organisatsioon on teinud kõik selleks, et volitatud töötlejad rakendaksid isikuandmete kaitseks asjakohaseid turvameetmeid.

CON.2.M25 Isikuandmete kustutamine töötaja lahkumisel [personaliosakond]

a. Organisatsioon on kehtestanud eeskirjad isikuandmete käitlemiseks ja kustutamiseks arvutitöökohtadel.

b. Eeskiri sisaldab sätteid lahkuva töötaja võimaluste kohta saada kätte oma isiklikud dokumendid (sh. isikuandmed), mida ta on tööandja IT-süsteemides hoiustanud. Eeskiri võiks näiteks sätestada, et töötaja hoiab oma isikuandmeid ja isiklikke dokumente ainult selleks markeeritud kaustas.

c. Eeskiri hõlmab lahkuva töötaja andmetest organisatsioonile vajalike andmete kättesaamist (nt e-postkastist organisatsiooni jaoks oluliste kirjade või dokumentide kättesaamine).

d. Töötaja organisatsioonist lahkumisel kustutatakse talle personaalseks kasutuseks antavatelt seadmetelt ja andmekandjatelt (sh irdandmekandjad) isikuandmed.

e. Lahkunud töötaja isikuandmeid hoiab organisatsioon alles seadusandlusest tulenevas mahus ning sätestatud säilitustähtaja jooksul.

CON.2.M26 Andmekaitseauditi läbiviimine

a. Organisatsioon viib läbi regulaarseid sõltumatuid läbivaatusi või auditeid, et hinnata organisatsiooni isikuandmete kaitse tegelikku olukorda ning tuvastada võimalikud riskid ja puudused.

b. Andmekaitseaudit viiakse läbi vähemalt kord nelja aasta jooksul.

3.3 Kõrgmeetmed

CON.2.M27 Tähtajalised juurdepääsuõigused (C)

a. Organisatsioon rakendab tähtajalisi juurdepääsuõigusi, et tagada juurdepääsuõiguste õiguspärasus ning vähendada isikuandmete volitamata töötlemise riski.

b. Juurdepääsuõiguste tähtaegade määramisel lähtutakse minimaalsuse printsiibist, eelkõige seetõttu, et organisatsiooni töötajad võivad vahetuda ja see meede aitab vältida organisatsioonist lahkunud töötajate juurdepääsu isikuandmetele.

CON.2.M28 Isikuandmete töötlemise automaatseire (C)

a. Organisatsioon kasutab automaatset isikuandmete töötlemise seiresüsteemi, mis tuvastab isikuandmed, mida soovitakse organisatsioonist välja saata, saadab selle kohta volitatud isikutele teavituse ja vajadusel blokeerib isikuandmete saatmise.

b. Teavituse saabudes hinnatakse, kas isikuandmete saatmine on õiguspärane ja vajalik.

CON.2.M29 Juurdepääsupiirangute klassifikaatorite süsteem (C)

a. Organisatsioon (avalikus sektoris) rakendab juurdepääsupiirangute klassifikaatorite süsteemi, mis hõlbustab dokumentidele avaliku teabe seadusest tuleneva juurdepääsupiirangu määramist vastavalt dokumendi sisule.

b. Juurdepääsupiirangute klassifikaatorite süsteem suudab muuhulgas automaatselt tuvastada, kas dokumentides sisaldub isikuandmeid või peaks dokument olema konfidentsiaalne mõnel muul põhjusel.

CON.2.M30 Isikuandmete automaatne tuvastamine (C)

a. Organisatsioon kasutab automaatset süsteemi, mis suudab tuvastada organisatsiooni võrguliikluses ja infosüsteemides isikuandmeid (sh IKÜM mõistes eriliiki isikuandmeid) ning neid klassifitseerida ilma kasutaja sekkumiseta.

b. Eriliiki andmete asukohad on automaatselt kaardistatud. Organisatsioon on rakendatud eriliiki isikuandmete kaitseks tugevdatud turvameetmed.

CON.2.M31 Digitaalsete õiguste halduse süsteem (C-I-A)

a. Organisatsioon on privaatsfuse tagamiseks kasutusele võtnud digitaalsete õiguste halduse süsteemi, mis võimaldab erinevatele kaustadele, IT-süsteemidele ja dokumentidele määrata rangelt vajaduspõhiseid õigusi. Näiteks on võimalik määrata, et teatud töötajad saavad dokumenti ainult vaadata ja muutmine (sh. allalaadimine) nõuab täiendavaid õigusi.

4 Lisateave

Lühend	**Publikatsioon**
[IKÜM]	Isikuandmete kaitse üldmäärus https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A02016R0679-20160504
[IKS]	Isikuandmete kaitse seadus https://www.riigiteataja.ee/akt/104012019011?leiaKehtiv
[AKI]	Isikuandmete töötleja üldjuhend (2018, uuendatud 2019) https://www.aki.ee/sites/default/files/dokumendid/isikuandmete_tootleja_uldjuhend.pdf
[ISO27701]	ISO/IEC 27701:2019 „Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines“
[CNIL]	Mõjuhinnangute läbiviimiseks loodud tarkvara https://www.cnil.fr/en/privacy-impact-assessment-pia

CON.3 Andmevarunduse kontseptsioon

1 Kirjeldus

1.1 Eesmärk

Esitada juhised organisatsiooni andmevarunduse kontseptsiooni koostamiseks ja rakendamiseks andmete kaitseks.

1.2 Vastutus

Andmevarunduse kontseptsiooni meetmete täitmise eest vastutab infoturbejuht.

Lisavastutajad

IT-talitus, vastutav spetsialist, töötaja.

1.3 Piirangud

Elektrooniliste dokumentide pikaajalise talletamise hoiu- ja hooldusmeetmed on esitatud moodulis OPS.1.2.2 *Arhiveerimine*. Süsteemi- ja rakendusspetsiifilised logimismeetmed on esitatud asjakohastes moodulites, nt SYS.1.1 *Server üldiselt,* APP.3.2 *Veebiserver* ja NET.3.2 *Tulemüür*.

Andmete kustutamisel ja varukoopiate hävitamisel lähtutakse moodulist CON.6 *Andmete kustutus ja hävitamine*.

2 Ohud

2.1 Andmevarunduse puudumine

Andmevarunduse puudumisel võib andmekadu (nt kahjurvara, tehniliste tõrgete või tulekahju tõttu) organisatsioonile kaasa tuua korvamatut kahju.

2.2 Taaste testimise puudumine

Kui andmete varukoopiast taastamiseks ei viida läbi regulaarseid taasteteste, puudub kindlus, et andmed on tegeliku taastevajaduse korral ja kokkulepitud aja jooksul taastatavad.

2.3 Varukoopiate andmekandjate ebaturvaline säilitus

Kui varukoopiaid sisaldavaid andmekandjaid hoitakse ebaturvalises kohas, võib ründaja andmekandjaile juurde pääseda, andmeid varastada või manipuleerida. Varunduseks kasutatavad andmekandjad võivad sobimatute hoiu- ja keskkonnatingimuste tõttu muutuda kasutuskõlbmatuks.

2.4 Dokumentatsiooni puudumine või puudulikkus

Kui varundusprotseduure ei dokumenteerita või seda tehakse puudulikult, võib taastamine oodatust kauem aega võtta või ebaõnnestuda.

2.5 Õigusaktide nõuete eiramine

Kui andmevarundusel ei järgita õigusaktide nõudeid, võib pärast andmetega toimunud intsidenti (andmevargus, andmete hävimine) järgneda trahv või kahjunõue.

2.6 Ebaturvaline pilvteenuse tarnija

Kui organisatsioon varundab andmeid pilves, võib ründaja juurde pääseda varukoopiatele. Pilve varundatud andmeid ei pruugi saada piisavalt kiiresti taastada.

2.7 Andmekandja salvestusmahu piisamatus

Kui andmekandjatel ei ole piisavalt salvestusmahtu, võib ühel hetkel andmevarundus seiskuda. Varundustarkvara võib automaatselt üle kirjutada vanemad ja võib-olla veel vajalikud andmevarundused.

2.8 Andmevarunduse kontseptsiooni puudulikkus

Kui varundusprotseduuride jaoks ei ole koostatud andmevarunduskontseptsiooni või kontseptsioonist ei peeta kinni (nt varundatakse andmeid liiga harva või on andmete reaalne taasteaeg suurem kui organisatsioonis kokku lepitud), on andmete taastamine raskendatud.

Piisavalt kaitsmata varukoopiad võimaldavad ründajal saada väheste pingutustega oma valdusesse kõik organisatsiooni jaoks olulised andmed.

Kui varundatud andmed on krüpteeritud, aga koos andmetega on kaotsi läinud ka andmetega koos talletatud dekrüpteerimiseks vajalik võti, osutub taastamine võimatuks.

2.9 Andmete salvestuskiiruse piisamatus

Varundatava andmemahu lisandumisel pikeneb andmete varundamiseks kuluv aeg. Halvimal juhul võib enne andmete plaanipärase varundamise lõppemist juba käivituda järgmine andmevarundus. See võib kaasa tuua erinevaid probleeme, nt käsiloleva andmevarundusprotsessi pooleli jäämist või varundussüsteemi koormuse kasvu, kuna korraga töötab mitu andmevarundusprotsessi.

2.10 Lunavara rünne

Lunavara (ingl *ransomware*) on kahjurvara erivorm, mis krüpteerib nakatunud IT-süsteemide andmed. Seejärel nõuavad ründajad ohvrilt andmete dekrüpteerimiseks lunaraha maksmist. Kui andmetest ei ole tehtud varukoopiat, lähevad krüpteeritud andmed kaotsi või neid saab tagasi ainult nõutud lunaraha eest. Kuid isegi pärast lunaraha maksmist pole mingit garantiid, et andmed tagasi saadakse.

Paljud lunavaravormid otsivad kõiki kirjutusjuurdepääsuga võrgukettaid. Seega lunavara ei mõjuta mitte ainult algselt nakatunud IT-süsteemi, vaid kõiki salvestuskohti, millele IT-süsteemidel on juurdepääs. Kui varukoopiaid sisaldavad andmekandjaid piisavalt ei kaitsta, võib lunavararünne mõjutada otseselt ka varukoopiate käideldavust.

3 Meetmed

3.1 Elutsükkel

Kavandamine

CON.3.M1 Andmevarunduse mõjurite piiritlemine

CON.3.M2 Andmevarunduseeskiri

CON.3.M4 Andmevarundusplaanid

CON.3.M6 Andmevarunduse kontseptsioon

Soetamine

CON.3.M7 Sobiva andmevarundussüsteemi soetamine

Evitus

CON.3.M9 Tingimuste tagamine kaugvarunduseks

Käitus

CON.3.M5 Regulaarne andmevarundus

CON.3.M12 Varunduseks kasutatavate andmekandjate turvaline säilitus

CON.3.M14 Varukoopiate turve

CON.3.M15 Varunduse regulaarne testimine

Lisanduvad kõrgmeetmed

CON.3.M13 Krüptograafia rakendamine andmevarundusel

3.2 Põhimeetmed

CON.3.M1 Andmevarunduse mõjurite piiritlemine [vastutav spetsialist, IT-talitus]

a. IT-süsteemide ja vajadusel ka olulise tähtsusega üksikute IT-rakenduste jaoks on koostatud varundatavate andmete register ja määratud andmevarunduse mõjurid. Andmevarunduse mõjurite määramisel osalevad IT-süsteemide ja IT-rakenduste äripoole omanikud.

b. Andmevarunduse mõjuritena on määratud vähemalt järgnev:
   - varundatavate andmete koosseis;
   - varundatavate andmete käideldavus-, terviklus-, ja konfidentsiaalsusnõuded;
   - seadusandlusest tulenevad nõuded;
   - vajalik andmemaht;
   - andmete säilitusaeg;
   - nõutav varunduse sagedus;
   - lubatav taasteaeg;
   - nõuded andmete kustutamiseks ja andmekandjate hävitamiseks.

c. Vajaliku andmemahu hindamisel arvestatakse eeldatava andmemahu suurenemisega tulevikus.

d. Varunduse sagedus määratakse andmete muudatuste ja lisanduste sageduse ja maksimaalse lubatava andmekao hinnangu alusel.

e. Varundavate andmete lubatav taasteaeg määratakse tuginedes IT-süsteemi maksimaalselt talutavale seisuajale (ingl *maximum tolerable downtime*, MTD).

f. Varundatud andmetele kehtivad samad konfidentsiaalsusnõuded kui andmetele töösüsteemis.

g. Andmevarunduse mõjurid on dokumenteeritud. Uute nõuete lisandumisel või olemasolevate nõuete muutumisel uuendatakse dokumentatsiooni.

CON.3.M2 Andmevarunduseeskiri [vastutav spetsialist, IT-talitus]

a. IT-talitus koostab andmevarunduse protseduure sisaldava andmevarunduseeskirja.

b. Andmevarunduseeskirja koostamisel arvestatakse andmevarunduse mõjuritega (CON.3.1 *Andmevarunduse mõjurite piiritlemine*).

c. Andmevarunduseeskiri sisaldab iga IT-süsteemi ja andmestiku kohta vähemalt järgmist:
   - andmevarunduse tüüp;
   - varundusviis ja andmekandja;
   - protseduurid andmete varundamiseks ja taastamiseks;
   - varundussagedus ja hetk;
   - säilituskoht;
   - andmekandjate transpordi- ja hoiutingimused;
   - säilitusajad;
   - vastutused varunduse rakendamise eest.
d. Andmed varundatakse käiduandmetest eraldi paiknevale andmekandjale.
e. Suurema kaitsevajadusega andmekandjad on sisevõrgu või IT-süsteemiga ühendatud ainult andmete varundamise või taastamise ajal.
f. Virtuaaltaristu olemasolul määratakse, millises ulatuses toetutakse serveri hetktõmmistel (ingl *snapshot*) põhinevale andmevarundusele.

CON.3.M4 Andmevarundusplaanid

a. On koostatud andmevarundusplaanid erinevate andme- ja tarkvaratüüpide varundamiseks.
b. Andmevarundusplaanides kirjeldatud varunduse ja andmetaaste põhimõtted, sealhulgas:
   - riist- ja tarkvara, mida varundamisel kasutatakse;
   - riist- ja tarkvara konfiguratsioon;
   - andmete varundamise ja taastamise järjekord;
   - säilitavate andmete põlvkondade arv.
c. Andmevarundusplaanid arvestavad vähemalt järgmist:
   - soetatud või omatarkvara varundatakse täieliku varundusega ühe andmete põlvena;
   - süsteemiandmed varundatakse vähemalt kord kuus ühe andmete põlvena;
   - rakendusandmed varundatakse vähemalt kord nädalas täieliku varundusega ja säilitatakse vähemalt kolm andmete põlve;
   - logiandmed varundatakse vähemalt kord kuus täieliku varundusega ja säilitatakse vähemalt kolm andmete põlve.

CON.3.M5 Regulaarne andmevarundus [IT-talitus, töötaja]

a. Andmeid varundatakse andmevarundusplaanis ja andmevarunduseeskirjas toodud regulaarsusega.
b. Töötajaid teavitatakse andmevarunduse korraldusest.
c. Andmevarunduse protsessiga seotud töötajaid teavad, millised on nende ülesanded.
d. Töötajad täidavad neile määratud andmevarunduse ülesandeid.

CON.3.M12 Varunduseks kasutatavate andmekandjate turvaline säilitus [IT-talitus]

a. Varunduseks kasutatavaid andmekandjaid hoitakse lähtesüsteemist eraldi asuvas hoiustuskohas.

b. Samas hoones hoiustamise puhul asuvad varundatud andmed tuletõkkega eraldatud hooneosas.
c. Hoiukoha keskkonnatingimused on sobivad andmekandjate pikaajaliseks säilitamiseks.
d. Andmete turvaline säilitus on tagatud vähemalt nõutud andmesäilitustähtaegade ulatuses.

CON.3.M14 Varukoopiate turve [IT-talitus]

a. Varunduseks kasutatavaid andmekandjaid kaitstakse lubamatu juurdepääsu eest.
b. Juurdepääs andmekandjatele on üksnes selleks volitatud isikutel.
c. Varunduseks kasutatavad andmekandjad on kaitstud lubamatu ülekirjutamise eest.
d. Varunduse andmekandjatele antakse kirjutusõigus ainult andmete varundamiseks või autoriseeritud haldustoimingute läbiviimiseks.

CON.3.M15 Varunduse regulaarne testimine [IT-talitus]

a. Andmevarunduse toimimist ja varundatud andmete taastamist testitakse regulaarselt.
b. Andmete taastamine jääb ajaliselt lubatava taasteaja piiresse ja toimub veatult.

3.3 Standardmeetmed

CON.3.M6 Andmevarunduse kontseptsioon [vastutav spetsialist, IT-talitus]

a. On koostatud andmevarunduse kontseptsioon, mis on kooskõlas organisatsiooni ärijätkuvusplaaniga (ingl *business continuity plan*, BCP) ja lubatava andmete kaoga peale taastamist (ingl *recovery point objective*, RPO).
b. Andmevarunduse kontseptsiooni väljatöötamisel on arvestatud kõigi oluliste IT-süsteemide ja rakendustega ning andmevarunduse mõjuritega.
c. Andmevarunduse kontseptsioon on vastutajatega kooskõlastatud.
d. Töötajad tunnevad andmevarunduse kontseptsiooni vähemalt tööülesannete täitmiseks vajalikul määral.
e. Andmevarunduse kontseptsioon ja sellega seonduvad dokumendid on turvaliselt varundatud ja kasutatavad ka juhul, kui olulised IT-süsteemid (sh dokumendihaldussüsteem) ei ole juurdepääsetavad.
f. Andmevarunduse kontseptsiooni rakendamist kontrollitakse regulaarselt.

CON.3.M7 Sobiva andmevarundussüsteemi soetamine [IT-talitus]

a. Enne andmevarundussüsteemi hankimist on koostatud andmevarundussüsteemi valiku kriteeriumid.
b. Andmevarundussüsteem vastab järgmistele andmevarunduse kontseptsioonist tulenevatele nõuetele:
    - tuvastab vale või vigase andmekandja;
    - töötab raskusteta olemasoleva riistvaraga;
    - võimaldab automaatset ajastust;
    - võimaldab ühele või mitmele kasutajale automaatteadete saatmist;
    - võimaldab andmekandja turvet parooliga või krüpteerimisega;
    - võimaldab andmete tihendust (ingl *compression*);

- võimaldab andmeid andmeloendite alusel kategoriseerida;
- võimaldab andmeid valida loomis- või muutmisaja alusel;
- suudab teha täisvarundust (ingl *full backup*) ja inkrementvarundust (ingl *incremental backup*);
- võimaldab automaatselt võrrelda varukoopiat originaaliga;
- võimaldab taastada andmeid algsesse või valitud asukohta;
- lubab samanimeliste failide taastet.

CON.3.M9 Tingimuste tagamine kaugvarunduseks [IT-talitus]

a. Välise salvestuskoha kasutamisel võrgustatud andmevarunduseks (ingl *online backup*) sõlmitakse teenusekvaliteedi tagamiseks teenusetasemelepe (ingl *service level agreement*, SLA) ja lepitakse kokku andmete füüsiline asukoht.

b. Varukoopiatele juurdepääs võimalik ainult turvalise autentimisega.

c. Varukoopias sisalduvad andmed on krüpteeritud nii varunduskohas kui andmete ülekandmisel.

d. Võrguühenduse kvaliteet võimaldab varundada ja taastada andmeid lubatavate varundus- ja taasteaegade piires.

3.4 Kõrgmeetmed

CON.3.M13 Krüptograafia rakendamine andmevarundusel (C-I) [IT-talitus]

a. Varundatavad andmed on andmete konfidentsiaalsuse ja tervikluse tagamiseks krüpteeritud.

b. Krüptomehhanismi valikul on arvestatud, et andmed oleks taastatavad ka pikema aja möödumisel.

c. Krüptovõtmete kaitse ja säilimine tagatakse turvalise võtmehalduse protseduuridega (vt CON.1.M2 *Andmevarundus krüptovahendi kasutamisel*).

4 Lisateave

Andmevarunduse kontseptsiooni tüüpsisukord

1. Määratlused
   g. Rakendusandmed, süsteemiandmed, tarkvara, logiandmed
   h. Täielik varundus, inkrementvarundus
2. Ohud
   - Organisatsiooni sõltuvus andmete seisust
   - Tüüpilised ohud (koolitamatus, ühiskasutus, viirused, häkkerid, toitekatkestus, kettarike)
   - Kahjude põhjused ja kahjujuhtumid organisatsioonis
3. Mõjurid IT-süsteemide haaval
   - Varundatavate andmete spetsifikatsioon
   - IT-rakenduse ja andmete käideldavusnõuded
   - Ressursid andmete taasteks, sh varukoopia puudumisel
   - Andmemahud
   - Muutumismahud
   - Säilitusajad

- Andmete konfidentsiaalsustarve
- Andmete terviklustarve
- IT kasutaja oskused ja andmetöötlusspetsiifilised võimed

4. Andmevarundusplaan IT-süsteemide haaval

Määrangud andmeliikide järgi ja taasteprotseduurid:

- Varundusviis
- Varunduse sagedus ja aeg
- Põlvkondade arv
- Andmekandja
- Vastutus andmevarunduse eest
- Varuandmete säilituskoht
- Nõuded andmevarundusarhiivile
- Edastus ja transport
- Taasteajad
- Varundusarhiveerimise tingimused
    - Lepingu sõlmimine (välise arhiivi puhul)
    - Varundustsükkel
    - Andmete kataloog
    - Varuandmete kustutus
    - Tarbetute andmekandjate hävitamine
    - Lugemisseadmete töövõime tagamine

5. Varunduse minimaalkontseptsioon
6. Töötajate kohustumus andmevarunduse alal
7. Taasteharjutused

CON.6 Andmete kustutus ja hävitamine

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed andmete turvaliseks kustutamiseks ning juhised andmete hävitamise eeskirjade koostamiseks.

1.2 Vastutus

Andmete kustutuse ja hävitamise meetmete täitmise eest vastutab infoturbejuht.

Lisavastutajad

Andmekaitsespetsialist, vastutav spetsialist, IT-talitus, töötaja, haldusosakond.

1.3 Piirangud

Moodul hõlmab üksnes kustutuse ja hävitamise üldisi korralduslikke nõudeid. Kustutuse ja hävitamisega on seotud moodulid CON.3 *Andmevarunduse kontseptsioon*, OPS 1.2.2 *Arhiveerimine, CON.9 Teabevahetus*

2 Ohud

2.1 Kustutuse ja hävitamise eeskirja puudumine või puudulik dokumenteerimine

Kui töötajaid ei ole juhendatud andmeid turvaliselt kustutama, võib andmekandjatele jääda alles loetaval kujul andmeid. Kasutuselt kõrvaldatud andmekandjad ja IT-süsteemid ei pruugi olla enam organisatsiooni kontrolli all, sellisel juhul on andmelekke oht veelgi suurem. Tundlikud andmed võivad andmekandjalt sattuda kolmandate isikute kätte. Hooletuse tõttu isikuandmete lekitamine võib tuua organisatsioonile kaasa olulise mainekahju ja rahatrahvi.

2.2 Konfidentsiaalsuse kadu andmekandjate jäätkteabe tõttu

Enamikes failsüsteemides ei hävita lihtsa kustutusfunktsiooni kasutamine kasutaja poolt kustutamiseks märgitud faile. Failisüsteemi haldusteabest kustutatakse üksnes failiviited ja failiga seotud andmeruum märgitakse vabaks. Andmeruumi tegelik sisu andmekandjal aga säilib ja seda saab sobivate vahendite abil taastada.

Arvuti saalefailid (ingl swap file) ja ajutiste failide kataloogid võivad muuhulgas sisaldada konfidentsiaalseid andmeid (nt paroolid ja krüptovõtmed) ja rakenduste tööfaile (nt. sirvimisajalugu). Saalefailide ja ajutiste failide sisu on võimalik lugeda, kui krüpteerimata kõvaketas eemaldada ja paigaldada teise IT-seadmesse.

2.3 Ebausaldusväärse kõrvaldusteenuse kasutamine

Kui andmekandjate turvaline kustutamine või hävitamine (sh ka paberdokumentide hävitamine) on usaldatud välisele teenuseandjale, võib teenuseandja hooletus põhjustada andmekandjate varguse kas otse teenuseandja ruumidest või hävitamiseelsest kogumispunktidest.

Andmekandjalt kustutamata jäänud või mittetäielikult kustutatud konfidentsiaalsed andmed (nt eriliiki isikuandmed) võivad sattuda volitamata isikute kätte ka juhul kui kõrvaldusteenuse tarnija ei ole kasutanud vahendeid või protseduure, mis tagavad andmete täieliku kustutamise.

2.4 Defektsete andmekandjate väär käsitlemine

Kui tavakasutajal ei õnnestu enam andmekandjalt andmeid laadida, ei tähenda see veel seda, et andmed on andmekandjalt lõplikult hävinud. Kui sellised defektsed andmekandjad visatakse tavalisse prügikasti, võivad need sattuda ründaja kätte, kellel õnnestub spetsiaalsete vahendite abil andmed osaliselt või tervenisti taastada.

Kui defektne andmekandja tagastatakse tarnijale või arvutipoodi, asendatakse see tavaliselt garantiikorras uue andmekandjaga. Tihti jäetakse tagastatud andmekandjatelt andmed turvaliselt kustutamata või andmekandja hävitamata, mistõttu eksisteerib oht, et andmed võivad sattuda volitamata isikute kätte.

3 Meetmed

3.1 Elutsükkel

Kavandamine

CON.6.M1 Andmete kustutuse ja hävitamise kord

CON.6.M2 Kaitset vajavate töövahendite ja andmekandjate turvaline kasutuselt kõrvaldamine

CON.6.M4 Protseduurid andmekandjate turvaliseks hävitamiseks

CON.6.M11 Andmekandjate hävitamise tellimine väliselt teenuseandjalt

Evitus

CON.6.M8 Andmete kustutuse juhised töötajatele

CON.6.M12 Protseduurid andmete turvaliseks kustutuseks

CON.6.M13 Defektsete andmekandjate hävitamise juhised

Lisanduvad kõrgmeetmed

CON.6.M14 Andmekandjate turvalise hävitamise täiendavad juhised

3.2 Põhimeetmed

CON.6.M1 Andmete kustutuse ja hävitamise kord [haldusosakond, vastutav spetsialist, andmekaitsespetsialist, IT-talitus]

a. Organisatsioon on kehtestanud andmete kustutuse ja hävitamise korra.

b. Iga allüksus määrab, milliseid tööalaseid andmeid ja millistel tingimustel kustutatakse või kasutuselt kõrvaldatakse.

c. Andmete minimaalsete ja maksimaalsete säilitustähtaegade määramisel järgitakse seadusandlusest tulenevaid nõudeid. Isikuandmete säilitamise ja kustutuse protseduurid on kooskõlastatud andmekaitsespetsialistiga.

d. On määratud andmete kustutuse ja hävitamise eest vastutajad, vajadusel kasutatakse spetsiaalset välisteenust.

CON.6.M2 Kaitset vajavate töövahendite ja andmekandjate turvaline kasutuselt kõrvaldamine

a. Enne andmekandjate ja töövahendite kasutuselt kõrvaldamist kustutatakse või hävitatakse turvaliselt nendes sisalduvad andmed.

b. Andmekandjate kasutuselt kõrvaldamisel järgitakse kehtestatud eeskirju ja juhiseid (vt CON.6.M12 *Protseduurid andmete turvaliseks kustutuseks*.

c. Andmekandjate ja töövahendite kõrvaldamiseks on loodud organisatsiooni territooriumile kõrvaliste isikute juurdepääsu eest kaitstud kogumiskohad.

CON.6.M11 Andmekandjate hävitamise tellimine väliselt teenuseandjalt [hankeosakond]

a. Väliste teenuseandjate osalusel toimuv andmekandjate kõrvaldamise ja hävitamise protseduur on turvaline ja arusaadav. Kasutatakse sobivaid ja turvalisi hävitus- või kustutusvahendeid.

b. Hävitamise väljasttellimisel hoitakse hävitamisele kuuluvaid andmekandjaid kuni äraviimiseni organisatsiooni territooriumil, kaitstuna lubamatu juurdepääsu eest.

c. Andmekandjate äravedu turvatakse lähtuvalt andmete kaitsetarbest.

d. Kõrvaldamise ja hävitamise eest vastutavaid väliseid ettevõtteid kontrollitakse ettenähtud nõuetele vastavuse osas regulaarselt.

e. Teenusetarnijale ja selle personalile kohandatakse moodulis OPS.2.3 *Väljasttellimine* kirjeldatud põhimeetmeid.

CON.6.M12 Protseduurid andmete turvaliseks kustutuseks

a. Tulenevalt andmekandja tüübist ja andmete kaitsetarbest rakendatakse andmete kustutusel järgnevaid protseduure:
   - kui ülekirjutataval andmekandjal pole andmed krüpteeritud, kirjutatakse andmekandjad mitmekordselt ja täies ulatuses üle, kasutades juhuslike andmete generaatorit (nt PRNG Stream).
   - kui andmed andmekandjal on krüpteeritud, hävitatakse krüptovõtmed. Krüptovõtmete hävitamine toimub krüptokontseptsioonis kirjeldatud protseduurireeglite kohaselt.

b. Nutitelefonide ja teiste nutiseadmete andmete kustutamiseks lähtestatakse seadmed tehaseseadetesse ning teostatakse esmane alglaadimine ja -seadistus.

c. Nutivõrgu (IoT) seadmed lähtestatakse tehaseseadetesse, kõik seadmes talletatud pääsuandmed kirjutatakse üle või kustutatakse.

d. IT-seadmetesse integreeritud andmekandjate sisu kustutatakse kasutades seadme vastavat funktsionaalsust.

3.3 Standardmeetmed

CON.6.M4 Protseduurid andmekandjate turvaliseks hävitamiseks

a. Enne andmekandjate hävitamist kontrollitakse, kas andmekandjalt on võimalik andmed tõhusalt ja turvaliselt kustutada (vt. CON.6.M12 *Protseduurid andmete turvaliseks kustutuseks*).

b. Kasutusel olevate andmekandjate hävitamiseks on koostatud sobivad protseduurid. Erinevat tüüpi andmekandjate hävitamisel kasutatakse selleks sobivaid vahendeid.

c. Vastutavad töötajad on teadlikud, mis protseduuri ja mis vahendeid tuleb andmekandja hävitamiseks kasutada.

d. Regulaarselt kontrollitakse, kas hävitusprotseduurid ja -vahendid vastavad hetke tehnoloogiatasemele ja kas need on endiselt piisavalt turvalised.

CON.6.M8 Andmete kustutuse juhised töötajatele [töötaja, IT-talitus, andmekaitsespetsialist]

a. On koostatud andmete kustutuse ja hävitamise kirjalikud juhised, mis hõlmavad kõiki andmekandjaid, rakendusi, IT-süsteeme ja muid teavet sisaldada võivaid töövahendeid (nt nutiseadmed).

b. Andmete kustutuse ja hävitamise juhised tehakse teatavaks kõigile töötajatele. Regulaarselt ja pisteliselt kontrollitakse, kas töötajad juhiseid järgivad.

c. Teabe kustutuse ja hävitamise juhiseid ajakohastatakse vastavalt vajadusele.

CON.6.M13 Defektsete andmekandjate hävitamise juhised

a. Kui andmeid pole andmekandja defekti tõttu võimalik andmekandjalt turvaliselt kustutada, hävitatakse andmekandja füüsiliselt.

b. Erikokkuleppel teenuseandjaga (nt andmekandja paranduse teostajaga) võib andmekandja hävitamise läbi viia ka teenuseandja. Teenuseandja peab sellisel juhul järgima kõiki andmekandja turvalise hävitamise nõudeid.

3.4 Kõrgmeetmed

CON.6.M14 Andmekandjate turvalise hävitamise täiendavad juhised (C)

a. Andmekandjate hävitamine toimub tõendatult vastavuses tunnustatud valdkondlike normide või standarditega (nt ISO/IEC 21964).

4 Lisateave

Lühend	Publikatsioon
[ISO 21964]	ISO/IEC 21964 „Information technology – Destruction of data carriers“
[NIST]	NIST Special Publication 800-88 „Guidelines for Media Sanitization“

CON.7 Välislähetuste infoturve

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed digitaalsete andmete ja paberkandjal oleva teabe turvalisuse tagamiseks töötaja välislähetusel viibimisel ning abistada vastutavaid isikuid välislähetuste turvameetmete kehtestamisel. Moodulis käsitletakse spetsiifiliselt välisreisidel ametitööks vajalikke protseduurilisi, tehnilisi ja korralduslikke meetmeid.

1.2 Vastutus

Välislähetuste infoturbe meetmete täitmise eest vastutab infoturbejuht.

Lisavastutajad

Kasutaja, IT-talitus, personaliosakond.

1.3 Piirangud

Moodulis ei käsitleta lokaalseid IT-süsteeme, mille turvameetmed on kirjeldatud mooduligruppides NET *Võrgud ja side,* SYS *IT-süsteemid* ja APP *Rakendused.* Klientarvuti turbe teemasid üldisemalt käsitletakse moodulites SYS.2.1 *Klientarvuti üldiselt*, NET.3.3 *Virtuaalne privaatvõrk (VPN)* ja SYS.3.2.2 *Mobiilseadmete haldus (MDM)*.

2 Ohud

2.1 Teabe pealtkuulamine ja luuramine / Majandusspionaaž

Võõrastes ruumides ja IT-keskkondades võidakse vestlusi, telefonikõnesid või andmeedastust pealt kuulata.

Välisriigis reisides võib tekkida olukord, kus kõrvaline isik saab töötaja mobiilseadmele füüsilise juurdepääsu. Ründaja võib seadme sisu märkamatult kopeerida, andmeid lugeda või neid manipuleerida.

Teatud riikidesse reisimisel võidakse nõuda sülearvutisse ja muudesse kaasaskantavatesse IT-seadmetesse salvestatud andmete läbivaatust. Seejuures on oht, et konfidentsiaalseid andmeid või isikuandmeid mitte üksnes ei vaadata, vaid ka kopeeritakse ja salvestatakse.

Majandusspionaaži eesmärgil võib ründaja ära kasutada töötaja mobiilseadmesse integreeritud kaameraid ja mikrofone.

2.2 Kaitset vajava teabe avaldamine ja väärkasutus (elektrooniline ja füüsiline)

Välislähetusel võib kergesti juhtuda, et ametireisija jätab konfidentsiaalsed paber- või digitaalkujul dokumendid avaliku kasutusega ruumi või hotellituppa.

Kasutaja lõppseadmeid võib ohustada tundmatute IT-süsteemide ja raadiovõrkudega ühendamine. Arvutis kasutatavad võõrad andmekandjad võivad sisaldada kahjurprogramme.

2.3 Identiteedi teesklus

Ründaja võib teeselda teise inimese identiteeti, seda nii füüsilises kui digitaalses suhtluses (teeskluse, võltsimise, kaaperduse, vahendusründe vms abil). Välismaiseid äripartnereid ei tunne töötaja sageli isiklikult. Seetõttu võib töötaja pimesi usaldada inimest, kes taustainfot teades ennast teise isikuna esitleb.

2.4 Turvateadlikkuse puudumine ja hooletus teabega tegelemisel

Andmekandjad võivad ajutiselt jääda järelevalveta, näiteks nõupidamise vaheajal nõupidamisruumi või reisijakupeesse.

Töötajad võivad kingitusena vastu võetud andmekandjad mõtlematult ühendada oma sülearvutiga.

Ühissõidukis või näiteks ärilõuna ajal on võimalik ärikriitilistel teemadel peetavat vestlust pealt kuulata.

2.5 Kohalike õigusaktide või eeskirjade rikkumine

Sihtkohariigi õigusaktid ja regulatsioon (nt andmekaitse, teavitamiskohustused, vastutus, kolmandate juurdepääs) ei ole välisreisil viibivale töötajale sageli teada, seetõttu riigis kehtestatud nõudeid ei täideta.

2.6 Sundimine, väljapressimine, inimröövi ja korruptsioon

Reisivate isikute füüsilist turvalisust võidakse välisreisidel rikkuda, kasutades sundimist, väljapressimist või inimröövi. Ründe sihtmärgiks on sageli tippjuhtkond.

Poliitilistest, ideoloogilistest või majanduslikest eesmärkidest lähtuv ründaja võib pakkuda konfidentsiaalse teabe eest raha või muid hüvesid.

2.7 Teave lubamatust allikast / väljamõeldis

Välisriigis töötamise ajal on võimalik reisivale isikule tema petmiseks esitada valet ja manipuleeritud teavet. See võib mõjutada ärilisi otsuseid ja äriprotsesside toimimist.

2.8 Seadmete, andmekandjate ja dokumentide vargus või kaotamine

Mobiilsed seadmed või dokumendid võivad kaotsi minna või neid võidakse varastada, mistõttu satub ohtu ka neis sisalduv tundlik teave.

3 Meetmed

3.1 Elutsükkel

Kavandamine

CON.7.M1 Välislähetuste turbe eeskiri

CON.7.M3 Riigispetsiifiliste õigusaktide, reisi- ja keskkonnatingimuste väljaselgitamine

Evitus

CON.7.M2 Töötajate teadlikkuse suurendamine

CON.7.M10 Mobiilsete IT-seadmete ja andmekandjate krüpteerimine

CON.7.M11 Varguskaitsevahendid

CON.7.M14 E-posti turve

Käitus

CON.7.M4 Ekraanifiltri kasutamine

CON.7.M5 Ekraaniluku kasutamine

CON.7.M7 Turvaline kaugjuurdepääs

CON.7.M8 Avalike raadiokohtvõrkude turvaline kasutamine

CON.7.M9 Andmekandjate turvaline käitlus

CON.7.M12 Kaitset vajavate materjalide ja dokumentide turvaline hävitamine

CON.7.M13 Andmete ja andmekandjate turvaline kaasavõtmine

Avariivalmendus

CON.7.M6 Õigeaegne intsidendist teatamine

Lisanduvad kõrgmeetmed

CON.7.M15 Mobiilsete IT-seadmete kiirguseturve

CON.7.M16 Tervikluse kaitse meetodid ja vahendid

CON.7.M17 Spetsialiseeritud reisiseadmed

CON.7.M18 Pääsuõiguste kitsendamine välismaareiside ajaks

3.2 Põhimeetmed

CON.7.M1 Välislähetuste infoturbe eeskiri

a. Infoturbe nõuded välisriigis viibimisel on kehtestatud välislähetuste infoturbe eeskirjas.

b. Välislähetuste infoturbe eeskirjas käsitletakse vähemalt järgmist:

- teabe turvalisuse olemus välisreisil, turbe eesmärgid ja käsitlusala;
- juhtkonna, infoturbejuhi ja reisiva töötaja vastutus;
- IT-süsteemi kaotuse, varguse või teabelekke käsitlus;
- töötajate teadlikkuse suurendamine ja koolitus;
- IT-seadmete kaitse (nt krüpteerimine, viirusetõrje, automaatne lukustus);
- andmete ja andmekandjate kaitse;

- andmete ja andmekandjate või dokumentide turvaline kustutus;
- side ja andmevahetuse turve;
- andmete kaasavõtmise ja kogumise õigused;
- 24/7 kasutajatugi küsimuste esitamiseks ja intsidentide lahendamiseks.

c. Mobiilseid IT-seadmeid kasutavatele, välislähetustel käivatele töötajatele koostatakse infoturbe aspekte käsitlev teabeleht.

CON.7.M2 Töötajate teadlikkuse suurendamine

a. Töötajatele on välislähetuste infoturbe eeskirja tutvustatud.

b. Töötajatele tunnevad ja järgivad infotehnoloogia vastutustundliku kasutamise reegleid välisreisidel, sh:
   - kinnitamata riist- ja tarkvara kasutamise keeld;
   - suhtlus oma organisatsiooni ja äripartneritega;
   - ettevaatlikkus pakutavate kingituste vastuvõtmisel;
   - digitaalmälu sisaldavate kingituste kasutamise keeld;
   - paroolide ja juurdepääsupiirangute kasutamine;
   - ebaturvalise võrgu kasutamise keeld.

c. Töötajad viiakse kurssi sihtkoha õigusaktide ja keskkonnatingimustega, sh:
   - sihtriigispetsiifilised õigusnormid;
   - riigispetsiifilised reisi- ja keskkonnatingimused;
   - nõuanded turvaliseks käitumiseks.

CON.7.M3 Riigispetsiifiliste õigusaktide, reisi- ja keskkonnatingimuste väljaselgitamine [personaliosakond]

a. Enne reisi algust tutvutakse riigikohaste õigusaktide ja kliimatingimustega ja koostatakse töötajatele vastav infomaterjal.

b. Organisatsioon hindab sihtkoha riski- ja turvataset ning keskkonnatingimusi ning otsustab täiendavate kaitsemeetmete vajaduse (nt töötajate vaktsineerimine).

c. Organisatsioon töötab välja ja rakendab meetmed seadmete kaitsmiseks keerulistes reisi- ja keskkonnatingimustes.

CON.7.M4 Ekraanifiltri kasutamine [kasutaja]

a. Mobiilse IT-seadme ekraanil kuvatava teabe kaitseks kasutatakse kogu ekraani katvat ekraanifiltrit.

CON.7.M5 Ekraaniluku kasutamine [kasutaja]

a. Seadmetel kasutatakse turvalist, pääsukoodi või parooliga kaitstud ekraanilukku.

b. Ekraanilukk rakendub lühikese kasutuspausi korral automaatselt. Piisav lukustusviivitus sülearvutitele ja nutiseadmetele on määratud välislähetuste infoturbe eeskirjas.

CON.7.M6 Õigeaegne intsidendist teatamine [kasutaja]

a. Töötajad teavitavad organsatsiooni IT-seadme või andmekandja kaotusest või vargusest esimesel võimalusel, kokkulepitud teavituskanalite ja kontaktisikute kaudu.

b. Hinnatakse IT-seadme või andmekandja kaotuse mõju ja rakendatakse sobivaid meetmeid:
   - muudetakse seadme juurdepääsu seadistus;
   - teavitatakse konfidentsiaalse teabe kaotamisest võimalikke riskiosalisi;
   - blokeeritakse mõjutatud kasutajakontod ja VPN-ühendused;
   - vastava funktsionaalsuse olemasolul kaugblokeeritakse ja/või lähtestatakse seade;
   - kaotatu leidmise korral kontrollitakse, kas seda on manipuleeritud.

CON.7.M7 Turvaline kaugjuurdepääs [IT-talitus, kasutaja]

a. Organisatsiooni võrku ühendumiseks luuakse välisreisil viibivatele töötajatele eelseadistatud VPN-iga ja turvalise autentimismehhanismiga kaugjuurdepääsu võimalus.
b. Kaugjuurdepääsu võimalusega IT-seadmeid kasutavad üksnes selleks volitatud isikud.
c. Kaugjuurdepääsuga seadmetes on tarkvara, eelkõige veebirakendused, ajakohastatud ja turvaliselt konfigureeritud.
d. Mobiilsetesse IT-seadmetesse on paigaldatud kitsendavalt seadistatud personaaltulemüür.

CON.7.M8 Avalike raadiokohtvõrkude turvaline kasutamine [kasutaja]

a. Avalikus raadiokohtvõrgus kasutatakse virtuaalset privaatvõrku (ingl *virtual private network*, VPN) või sellega võrreldavaid turvamehhanisme (vt NET.3.3 *Virtuaalne privaatvõrk (VPN)*, CON.7.M7 *Turvaline kaugjuurdepääs*).
b. Avalike raadiokohtvõrkude kasutamisel järgitakse reegleid WLAN-võrgu pääsupunktide turvaliseks kasutamiseks (vt. NET.2.2 *Raadiokohtvõrgu kasutamine.* INF.9 *Mobiiltöökoht*).

CON.7.M9 Andmekandjate turvaline käitlus [kasutaja]

a. Enne mobiilsete andmekandjate kasutamist kontrollitakse, et need ei oleks kahjurvaraga nakatatud.
b. Edasiantavate andmekandjate puhul on veendutud, et neil ei ole tundlikku teavet.
c. Andmekandja kõrvaldamisel kustutatakse andmed andmekandjalt, arvestades järgmist:
   - andmekandja tühjendatakse täielikult, erinevalt tavalisest kustutusest kustutatakse lisaks andmeviitadele ka viidatavad andmed.
   - krüpteeritud andmete kustutamisel kustutatakse turvaliselt ka krüptovõtmed;
   - mälupulgal või muul pooljuhtkandjal kustutatakse andmed vähemalt kahe ülekirjutusega.

CON.7.M10 Mobiilsete IT-seadmete ja andmekandjate krüpteerimine [kasutaja, IT-talitus]

a. Tundliku teabe kaitseks on mobiilsed IT-seadmed ja andmekandjad organisatsioonis kehtestatud korra kohaselt krüpteeritud.
b. Krüptovõtmeid hoitakse krüpteeritud seadmest eraldi.
c. Andmete krüpteerimisel arvestatakse välisriigi õigusnorme.

CON.7.M12 Kaitset vajavate materjalide ja dokumentide turvaline hävitamine [kasutaja]

a. Töötajad on välisriigis viibides kohustatud tarbetud andmekandjad või dokumendid nende äraviskamise asemel turvaliselt hävitama.

b. Kui reisil olles puuduvad turvalise hävituse võimalused või kui on tegemist eriti tundlikku teavet sisaldavate dokumentide või andmekandjatega, hoitakse need tagasipöördumiseni alles ja seejärel hävitatakse turvalisel viisil.

c. Võõraste andmehävitusseadmete (paberipurusti) kasutamisel kontrollitakse kasutuselt kõrvaldamise õnnestumist.

3.3 Standardmeetmed

CON.7.M11 Varguskaitsevahendid [kasutaja]

a. Mobiilsete IT-seadmete kaitseks rakendatakse varguskaitsevahendeid (nt mehhaanilist või elektroonilist lukustust).

b. Varguskaitsevahendite soetamine ja kasutamine on kooskõlas organisatsiooni turvapoliitikatega ja majanduslikult põhjendatud.

CON.7.M13 Andmete ja andmekandjate turvaline kaasavõtmine [kasutaja]

a. Enne reisi algust kustutatakse või eemaldatakse kaasavõetavatest IT-seadmetest tarbetud andmed (vt CON.7 M9 *Andmekandjate turvaline käitlus*).

b. Töötaja on teadlik, mis andmekandjaid tohib välisreisidele kaasa võtta ja milliste turvameetmetega peab seejuures arvestama.

c. Andmete kaitsetarbe määrangust tulenevalt võib andmete välisriiki kaasavõtmiseks kehtestada täiendavaid nõudeid (vt CON.7.M10 *Mobiilsete IT-seadmete ja andmekandjate krüpteerimine*).

d. IT seadmete transpordil rakendatakse järgmisi meetmeid:

- seadmeid transporditakse mitte pagasina, vaid käsipagasis;
- välditakse järelevalveta jätmist ja unustamist;
- seadmed kaitstakse paroolidega, kaitsetarbega andmed krüpteeritakse;
- omatakse ülevaadet seadmete hetkeasukohast.

CON.7.M14 E-posti turve [kasutaja, IT-talitus]

a. E-posti lahenduse turvalisuse tagamiseks kasutatakse otspunktkrüpteeringut.

b. Välditakse organisatsiooni e-posti kasutamist avalikes arvutites (nt hotellides või internetikohvikutes).

3.4 Kõrgmeetmed

CON.7.M15 Mobiilsete IT-seadmete kiirguseturve (C)

a. Väga suure kaitsetarbe korral kasutatakse juhtmega ühendatavaid välisseadmeid.

b. Kasutatakse seadmeid, mille kiirguseturvalisus on sertifitseeritud.

CON.7.M16 Tervikluse kaitse meetodid ja vahendid (I) [kasutaja]

a. Andmete edastamisel kasutatakse andmete tervikluse tagamiseks kontrollkoodide (nt CRC) võrdlemist.

b. Tundliku teabe tervikluse säilitamiseks kasutatakse digitaalsignatuure ja ajatempleid.

CON.7.M17 Spetsialiseeritud reisiseadmed (C-I-A) [IT-talitus]

a. Välislähetustel kasutatakse selleks otstarbeks eelkonfigureeritud seadmeid.

b. Reisimiseks ettevalmistatud seadmes on vastavalt minimaalsuspõhimõttele võimalik kasutada üksnes vajalikke funktsioone.

CON.7.M18 Pääsuõiguste kitsendamine välismaareiside ajaks (C-I) [IT-talitus]

a. Välisriigis asuvale töötajale tagatakse igapäevase töö jaoks vajalikud pääsuõigused. Liigsed pääsuõigused reisi kestel peatatakse, vajadusel piiratakse ajutiselt töötaja juurdepääs sisevõrgule.

b. Välisriigis viibimise aja jooksul piiratakse kasutajakeskkonnas võimalusi kasutada funktsioone ja käivitada toiminguid, mis ei ole kasutaja ülesannete täitmiseks vajalikud (nt skriptide käivitamine).

CON.8 Tarkvaraarendus

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed organisatsiooni tellitud või organisatsioonis arendatava tarkvaralahenduse infoturbe haldamiseks ja tarkvara turvalisuse tagamiseks. Moodulis olevad meetmed on kasutatavad nii projektipõhise tarkvara erilahenduse loomiseks kui aastaid kasutusel olnud pärandtarkvara pidevaks kohandamiseks.

1.2 Vastutus

Tarkvaraarenduse meetmete täitmise eest vastutab vastutav spetsialist.

Lisavastutajad

Arendaja, IT-talitus, testija, haldusosakond.

1.3 Piirangud

Moodul käsitleb tarkvaraarenduse infoturvet tellija/teostaja koostöö vaatest ega anna terviklikku ülevaadet kogu tarkvaraarenduse protsessist. Meetmed täiendavad moodulis APP.7 *Tellimustarkvara arendus* esitatud tellijapoolset vaadet tarkvaraarenduse infoturbe nõuetele ja turvariskide vähendamisele. Seadusandlusest tulenevad nõudeid tarkvaraarendusele käsitletakse moodulis ORP.5 *Vastavusehaldus (nõuete haldus).* Tarkvaramuudatuste haldust käsitletakse moodulis OPS.1.1.3 *Paiga- ja muudatusehaldus*. Tarkvara vastuvõtmist ja käidukeskkonda paigaldamist käsitletakse moodulis OPS.1.1.6 *Tarkvara testimine ja kasutuselevõtt*. Kui kavandatav tarkvara sisaldab andmete krüpteerimist, arvestatakse täiendavate meetmetega moodulist CON.1 *Krüptokontseptsioon*.

2 Ohud

2.1 Ebasobiv tarkvaraarendusmetoodika

Tarkvaraarendusmetoodika sätestab arendusprotsessi käigus läbiviidavad tegevused, sealhulgas formuleerib arendusprojekti etapid, nende järjestuse ja tingimused, mille täitmisel liigutakse edasi järgmisesse etappi. Ebasobiv tarkvaraarendusmetoodika mõjutab kogu arendusprotsessi toimimist, kui projekti olulised infoturbe aspektid jäävad piisava tähelepanuta ja vastupidi, liiga palju väärtuslikku projektiaega kulub ebaoluliste detailide peale. Seetõttu kannatab projekti efektiivsus ja üldine kvaliteet. Kui oluline infoturbe funktsionaalsus on jäänud tarkvaratootest välja või selle toimimist pole piisavalt testitud, ei pruugi arendatav tarkvara vastata püstitatud infoturbe nõuetele.

2.2 Ebasobiva tarkvaraarenduskeskkonna valimine

Kui tarkvaraarenduskeskkonna valikul on jäetud arvestamata vajalik funktsionaalsus ja nõutavad laiendusvõimalused, tekib arendusetapis tõsiseid probleeme kui vajalik funktsionaalsus arenduskeskkonnas puudub või see ei vasta esitatud nõuetele.

Kui iga arendaja võib ise valida endale sobiva arenduskeskkonna ja harjumuspärased arendusvahendid, võib tekkida ühilduvusprobleeme tarkvara erinevate moodulite ühendamisel või tarkvara kompileerimisel. Samuti võivad vähem testitud arenduskeskkonnad või -tööriistad sisaldada vigu või nõrkusi, mille tagajärjel tekkinud koodivigu on hilisemas arendusfaasis väga keeruline parandada.

2.3 Ebapiisav kvaliteedihaldus

Ebapiisav kvaliteedihaldus (ingl *quality assurance*) võib kaasa tuua arendusprojekti venimise üle lõpptähtaja või halvemal juhul nurjata terve projekti. Kui tarkvaraarenduses puudub pidev seire tarkvara lubamatu manipuleerimise või arendusprotsessi tervikliku ja piisava turvalisuse üle, võib tarkvaratootesse sisse jääda olulisi turvanõrkusi. Tihti on nii, et kvaliteedihaldust suudetakse rakendada organisatsioonisisestele tarkvaraarendusprojektidele, kuid välise teenuseandja poolt tehtud arendustööd samal tasemel ei hinnata.

2.4 Puuduv või puudulik dokumentatsioon

Kui tarkvaraarenduses kasutatav töödokumentatsioon on disainikavandite tasemel ja ei sisalda vajalikku detailsust, jäävad tarkvaravead õigeaegselt avastamata. Puudulik dokumentatsioon takistab oluliselt hilisemate tarkvaramuudatuste või edasiarenduste kavandamist ja läbiviimist. Vähene dokumenteeritus muudab keeruliseks tarkvara hoolduse ja haldamise protseduurid pärast tarkvara juurutamist. Halduse käigus võib administraator teadmatusest teha vea, mis võib halvemal juhul põhjustada andmekao või katkestuse tarkvaraga seotud äriprotsessis.

2.5 Ebapiisav arenduskeskkonna turve

Ebaturvaline ja juurdepääsupiiranguteta arenduskeskkond võimaldab tarkvara manipuleerida. Arendaja või väliste volitamata isikute poolt tehtud volitamata tarkvaramuudatusi on hiljem raske tuvastada. Kui pole tagantjärele tuvastatav, kes ja millal midagi tarkvarakoodis muutis, pole võimalik ründajat tabada.

Kui lähtekood pole volitamata muudatuste eest kaitstud ja samal ajal puudub ka versioonihaldus, on ründajal võimalik lähtekood kas osaliselt või täielikult hävitada. Samasuguse mõjuga võib olla arendaja inimlik eksimus või tehniline rike. Lähtekoodis tehtud muudatuste taastamine juhul, kui puudub värskelt tehtud varukoopia, on äärmiselt töömahukas ning võib tekitada uusi vigu.

2.6 Tarkvara kavandamise vead

Mida rohkem funktsionaalsust tarkvara sisaldab, seda keerukamaks muutub tarkvara lähtekoodi haldamine. Kui tarkvara ei tugine läbimõeldud tarkvaraarhitektuuril, on hiljem tarkvaratoodet keeruline muuta. On oht, et kõiki teadaolevaid turvanõrkusi ei suudeta parandada piisavalt kiiresti.

Pärandtarkvara (ingl *legacy software*) ei olnud algselt mõeldud kasutamiseks ega disainitud töötamaks tänapäevaste riistvara- ja operatsioonisüsteemidega. Seetõttu tuleb selliseid süsteeme pidevalt kohandada, kuid kõiki turvanõrkusi sellistes tarkvaratoodetes on äärmiselt keeruline kõrvaldada.

2.7 Puudulikud tarkvara testimis- ja vastuvõtuprotseduurid

Kui tarkvara enne käidukeskkonnas kasutuselevõttu piisavalt ei testita või kui puuduvad korrektsed tarkvara vastuvõtmise ja kinnitamise protseduurid, võib vastu võetud tarkvara sisaldada turvanõrkusi ja vigu tarkvara funktsionaalsuses. Sellised vead võivad käidukeskkonnas mõjutada ka teiste IT-süsteemide toimimist, millega antud tarkvaratoode on liidestatud.

Kui arenduse käigus on testimata jäänud infoturbe funktsionaalsus, võib juhtuda, et antud funktsionaalsus vastu võetud lõpptootes ei toimi. Tulemuseks on, et tarkvara ei vasta püstitatud infoturbe nõuetele. Eksisteerib oht, et andmetele on juurdepääs volitamata isikutel ning andmeid saab manipuleerida, hävitada või lekitada.

2.8 Tootmiskeskkonna andmete kasutamine tarkvara testimisel

Kui arendus- või testkeskkondades kasutatakse reaalseid, tootmiskeskkonnast võetud andmeid, on võimalik, et konfidentsiaalsetele andmetele saavad juurdepääsu volitamata isikud. Oluline kahju võib tekkida anonüümimata isikuandmete kasutamisest testkeskkonnas.

Kui testimist tehakse otse tootmiskeskkonnas, võib testimisel tehtud operatsioonid või tarkvara vea tõttu põhjustatud muutus, mida ei õnnestu tagasi võtta (nt andmetabeli sisu muutmine) mõjutada andmete terviklust erinevate andmebaaside vahel.

3 Meetmed

3.1 Elutsükkel

Kavandamine

CON.8.M1 Tarkvaraarenduse rollide ja vastutuste määramine

CON.8.M2 Sobiva tarkvaraarendusmetoodika valimine

CON.8.M3 Sobiva tarkvaraarenduskeskkonna valimine

CON.8.M11 Tarkvaraarenduste läbiviimise korra koostamine

Evitus

CON.8.M14 Tarkvaraarendajate infoturbealane koolitus

CON.8.M21 Tarkvara riskide kaalutlemine

CON.8.M22 Turvaline tarkvaraarhitektuur

Käitus

CON.8.M5 Turvaline süsteemi kavandamine

CON.8.M6 Usaldusväärsetest allikatest pärinevate tarkvarateekide kasutamine

CON.8.M7 Tarkvara testimine tarkvaraarenduse käigus

CON.8.M8 Tarkvaramuudatuste, paikade ja uuendite turvaline paigaldamine

CON.8.M10 Lähtekoodi versioonihaldus

CON.8.M12 Detailne tarkvara dokumentatsioon

CON.8.M16 Tarkvaraarenduse järelevalve

CON.8.M20 Väliste tarkvarakomponentide kontrollimine

Lisanduvad kõrgmeetmed

CON.8.M17 Usalduväärsete arendusvahendite valimine

CON.8.M18 Regulaarsed arenduskeskkonna turvaauditid

CON.8.M19 Arenduskeskkonna tervikluskontrollid

3.2 Põhimeetmed

CON.8.M2 Sobiva tarkvaraarendusmetoodika valimine

a. Tarkvaraarenduseks on valitud sobiv tarkvaraarendusmetoodika ja metoodikale vastav protsessimudel.

b. Projektiplaani koostamisel ja elluviimisel on järgitud valitud tarkvaraarendusmetoodikat.

c. Tarkvaraarenduse protsessimudel sisaldab infoturbe nõudeid. Arendusprotsessi käigus on infoturbe nõuetega arvestatud.

d. Töötajad on läbinud tarkvaraarendusmetoodika rakendamise koolituse.

CON.8.M3 Sobiva tarkvaraarenduskeskkonna valimine

a. Enne tarkvaraarenduskeskkonna valimist on dokumenteeritud nõuded, millele tarkvaraarenduskeskkond ja -tööriistad peavad vastama ning määratud tööriistade valikukriteeriumid. Nõuded on kinnitanud tarkvaraarenduse eest vastutav töötaja.

b. Kasutusele võetud tarkvaraarenduskeskkond vastab kehtestatud nõuetele.

CON.8.M5 Turvaline süsteemi kavandamine

a. Arenduses oleva tarkvara puhul on arvestatud järgmisi turvalise süsteemide kavandamise (ingl *system design*) reegleid:

- andmete sisestamisel kontrollitakse ja valideeritakse andmed enne nende edasist töötlemist IT-süsteemis;
- klient-server rakenduste puhul tehakse andmete lõplik valideerimine ja kinnitamine alati serveris;
- tarkvara tüüpseadistus ja parameetrite vaikeväärtused võimaldavad tarkvara turvaliselt kasutada;
- tarkvarakomponendi vea või tõrke puhul ei muutu kättesaadavaks kaitset vajavad andmed;
- tarkvara vajab kasutamiseks võimalikult vähe süsteemiprivileege;
- kaitset vajavate andmete edastamisel ja talletamisel kasutatakse krüptokontseptsioonile (vt CON.1 *Krüptokontseptsioon*) vastavaid krüptoprotsesse ja –tooteid;

- kasutatakse turvalisi ja usaldusväärseid ning kaitsetarbele vastavaid kasutajate autentimise ja pääsuõiguste andmise mehhanisme;
- autentimiseks kasutatavatest salasõnadest tohib tarkvaras talletada ainult turvalisi parooliräsisid (ingl *password hash*);
- infoturbe sündmused logitakse tarkvaras tõendusväärtusega ja kujul, mis võimaldab sündmusi vajadusel tagantjärele analüüsida;
- käidukeskkonnas toimimiseks mittevajalik teave (nt liigsed kommentaarid) on tarkvara programmikoodist ja konfiguratsioonifailidest eemaldatud.

b. Süsteemide kavandamise reeglid on dokumenteeritud. Tarkvaraarendajad on kehtestatud süsteemi kavandamise reeglitest teadlikud.

c. Süsteemi kavandamise reeglitest kinnipidamist kontrollitakse tarkvara arendusprotsessi käigus ja enne tarkvara kasutuseks kinnitamist.

CON.8.M6 Usaldusväärsetest allikatest pärinevate tarkvarateekide kasutamine

a. Enne väliste tarkvarateekide arendusprotsessis käitamist kontrollitakse kasutatud allikate usaldusväärsust ja teekide terviklust.

CON.8.M7 Tarkvara testimine tarkvaraarenduse käigus [testija, arendaja]

a. Tarkvara testimine ja koodi läbivaatus (ingl *code review*) viiakse läbi enne tellijapoolset tarkvara vastuvõtutestimist (ingl *acceptance test*) ja kasutamiseks kinnitamist.

b. Tarkvara testimise ja koodi läbivaatuse protsessi on kaasatud tellija või tellija esindaja.

c. Juba arenduse käigus testitakse tarkvara vastavust funktsionaalsetele nõuetele (nõuded, mida tarkvara peab täitma, ingl *functional requirements*) ja mittefunktsionaalsetele nõuetele (nõuded, millele tarkvara peab vastama, ingl *non-functional requirements*).

d. Arenduse käigus testitakse tarkvara käitumist vigaste ja lubatavatest sisendväärtustest erinevate sisendväärtuste ning andmetüüpide korral (ingl *negative testing*).

e. Testimisel kasutatav testandmestik on hoolikalt valitud ja kaitstud volitamata muudatuste eest.

f. Võimalusel kasutatakse tarkvara testimiseks automaatseid töövahendeid (nt koodianalüsaatorit).

g. Tarkvara testimine viiakse läbi arendus- ja testkeskkondades, mis on käidukeskkonnast (ingl p*roduction environment*) eraldatud.

h. Tarkvaraarenduse käigus testitakse, kas tarkvarale esitatud nõuded on asjakohased ja õigesti dimensioneeritud.

CON.8.M8 Tarkvaramuudatuste, paikade ja uuendite turvaline paigaldamine [arendaja]

a. Tarkvara turvakriitilised paigad ja uuendid töötab arendaja välja ja need edastatakse tellijale ilma viivituseta.

b. Pärast välistes tarkvarateekides tehtud turvakriitilisi muudatusi teostab arendaja tarkvaras vajalikud muudatused ja edastab tellijale vastavad paigad.

c. Tarkvaramuudatusi, paiku ja uuendeid kaitstakse volitamata muudatuste eest installipaketi kontrollkoodi (ingl *checksum*) või digiallkirja abil.

CON.8.M10 Lähtekoodi versioonihaldus

a. Tarkvara lähtekoodi (ingl *source code*) turvalisuse tagamiseks ja koodimuudatuste haldamiseks on rakendatud sobivad versioonihalduse tööriistad.

b. Koodis tehtud muudatused salvestatakse versioonihalduse käigus eraldi versioonina. Vajadusel on võimalik tehtud muudatusi tagasi võtta (taastada muudatuse-eelne lähtekoodi versioon).

c. Andmevarunduse kontseptsioon arvestab tarkvara versiooni muutusi. Enne ja pärast uue tarkvaraversiooni paigaldamist varundatakse tarkvaras kasutatavad andmed.

CON.8.M20 Väliste tarkvarakomponentide kontrollimine

a. Kõik välised tarkvarakomponendid (sh teegid), mille turvalisuses ei saa olla täielikult kindel, läbivad enne kasutuselevõttu turvatestimise.

b. Võimalike tarkvarakonfliktide ärahoidmiseks testitakse kõiki väliseid tarkvarakomponente enne nende esmakordset rakendamist.

c. Väliste tarkvarakomponentide tervikluse tagamiseks kontrollitakse komponentide kontrollkoode ja/või digitaalseid sertifikaate.

d. Tarkvara arendamisel kasutatakse väliste tarkvarakomponentide viimaseid heakskiidetud versioone, aegunud tarkvarakomponente ei kasutata.

3.3 Standardmeetmed

CON.8.M1 Tarkvaraarenduse rollide ja vastutuste määramine [haldusosakond]

a. Organisatsioonis on määratud tarkvara arendusprotsessi juhtimise üldine vastutaja.

b. Organisatsioonis on määratud vastutajad järgmiste tarkvaraarenduse tegevuste eest:
   - nõuete koostamine, nõuetehaldus ja muudatuste haldus;
   - tarkvara kavandamine ja tarkvara arhitektuur;
   - tarkvaraarenduse infoturve;
   - spetsiifilised tarkvaraarenduse tegevused (nt testimine).

c. Iga tarkvaraarendusprojekti raames on määratud arendusprojekti infoturbe eest vastutav isik.

CON.8.M11 Tarkvaraarenduste läbiviimise korra koostamine

a. Organisatsioon on kehtestanud tarkvaraarenduste läbiviimise korra. Kord sisaldab antud moodulis käsitletud meetmeid, mis vastavad organisatsiooni spetsiifikale.

b. Tarkvaraarenduse läbiviimise korda rakendatakse kõikide tarkvaraarenduste puhul.

c. Välistele arendajatele on tarkvaraarenduste läbiviimise korra järgimine lepinguline kohustus.

d. Tarkvaraarenduste läbiviimise korda ajakohastatakse vastavalt vajadusele.

CON.8.M12 Detailne tarkvara dokumentatsioon

a. Tarkvaratoote kohta on olemas üksikasjalik ja põhjalik dokumentatsioon.

b. Tarkvara dokumentatsioon hõlmab vähemalt järgmist:
   - tarkvara funktsionaalsuse kirjeldust;
   - kasutusjuhendeid tarkvara kasutajatele;

- tarkvaraarhitektuuri kirjeldust ja jooniseid;
- tarkvara liidestuste spetsifikatsioone;
- tarkvarateekide dokumentatsiooni;
- kasutatud krüptomehhanismide spetsifikatsiooni;
- tarkvara installimise, seadistamise ja haldamise juhendeid tarkvara haldajatele.

c. Tarkvara dokumentatsiooni detailsus on piisav, et nõutava tasemega tehniline ekspert suudaks dokumentatsioonile tuginedes tarkvaratoote halduse ja arendamise üle võtta.

d. Valitud tarkvaraarendusmetoodika ja protsessimudel sisaldab tarkvara dokumentatsiooni loomist ja selle pidevat ajakohastamist.

CON.8.M14 Tarkvaraarendajate infoturbealane koolitus

a. Tarkvaraarendajatel on infoturbealased baasteadmised ja nad on kursis infoturbe üldiste trendidega.

b. Tarkvaraarendajad on läbinud organisatsioonispetsiifilise koolituse, milles käsitletakse vähemalt järgmist:

- tarkvara nõuete (sh infoturbe nõuete) analüüs;
- projektijuhtimine üldiselt ja eriti tarkvaraarenduses;
- riskijuhtimine ning ohtude modelleerimine tarkvaraarenduses;
- tarkvaraarenduse kvaliteedijuhtimine ja kvaliteedi tagamine;
- tarkvaraarendusmeetodid ja protsessimudelid;
- tarkvaraarhitektuur;
- tarkvara testimine;
- tarkvara muudatuste juhtimine;
- infoturbe nõuded organisatsioonis ja valdkondlikud turbeaspektid.

CON.8.M16 Tarkvaraarenduse järelevalve

a. Tarkvaraarenduse juhtimiseks on välja töötatud valitud tarkvaraarendusmetoodikaga sobiv projektijuhtimismudel. Projektijuhtimismudeli üheks osaks on arendusprojektide järelevalve funktsioon.

b. Tarkvaraarenduse järelevalve teostajatel on piisav kvalifikatsioon tarkvara elutsükli kõikide etappide hindamiseks.

c. Tarkvaraarenduse projektijuhtimismudel on kooskõlas organisatsiooniülese riskijuhtimissüsteemiga.

d. Arendusprojektidele on määratud kvaliteedieesmärgid.

CON.8.M21 Tarkvara riskide kaalutlemine

a. Tarkvaratoote arendamise esimeses etapis on läbi viidud tarkvara riskide kaalutlemine.

b. Tarkvara riskide kaalutlemisel lähtutakse tarkvara kasutava organisatsiooni kaitsetarbest, tarkvara nõuetekataloogist ja tarkvara toimimise kontekstist.

c. Tarkvara riskide kaalutlemise käigus koostatakse võimalikud ohustsenaariumid, tuvastatakse nendega seotud riskid, hinnatakse ohtude realiseerumise tõenäosust ja võimalikku mõju.

CON.8.M22 Turvaline tarkvaraarhitektuur

a. Tarkvaraarhitektuuri valimisel on arvestatud tarkvara nõuetekataloogiga ja riskide kaalutlemise tulemustega.
b. Tarkvaraarhitektuur võimaldab tarkvara loomisel turvalise süsteemi kavandamise põhimõtete (vt CON.8.M5 *Turvaline süsteemi kavandamine*) rakendamist.
c. Võimalusel arvestatakse tarkvara väljatöötamisel tarkvara vastavust tulevikustandarditele ja vastupidavust uutele võimalikele ründemeetoditele.
d. Valitud tarkvaraarhitektuur võimaldab ka tulevikus tarkvara hõlpsasti hooldada ja edasi arendada.

3.4 Kõrgmeetmed

CON.8.M17 Usalduväärsete arendusvahendite valimine (C-I-A)

a. Tarkvara arendamisel kasutatakse ainult vajalikke ja tõestatud turvaomadustega arendustööriistu.
b. Arenduses kasutatava riistvara- ja tarkvaratootjate vastavus infoturbe nõuetele on kontrollitav.

CON.8.M18 Regulaarsed arenduskeskkonna turvaauditid (C-I-A)

a. Tarkvara arendus- ja testkeskkonna turvameetmete rakendamise hindamiseks viiakse läbi regulaarseid turvaauditeid.

CON.8.M19 Arenduskeskkonna tervikluskontrollid (I) [IT-talitus]

a. Arenduskeskkonna tervikluse tagamiseks ja manipuleerimise vältimiseks kasutatakse sobivaid krüptoprotsesse (nt failide kontrollsummasid).
b. Terviklushäirete kiireks tuvastamiseks on väärpositiivsete (ingl *false positive*) häireteadete hulk viidud võimalikult väikseks.

4 Lisateave

Lühend	Publikatsioon
[ISO 25000]	ISO/IEC 25000:2014 „ Systems and Software Quality Requirements and Evaluation – Guide to SQuaRE“
[ISO 25001]	ISO/IEC 25001:2014 „Planning and management“
[ISO 25010]	ISO/IEC 25010:2011 „System and software quality models“
[NIST 800-160]	National Institute of Standards and Technologie, NIST 800-160 „Systems Security Engineering, Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems“

CON.9 Teabevahetus

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed IT-süsteemide ja väliste poolte vaheliseks turvaliseks teabevahetuseks.

1.2 Vastutus

Andmevahetuse mooduli meetmete täitmise eest vastutab infoturbejuht.

Lisavastutajad

Kasutaja, vastutav spetsialist, haldusosakond.

1.3 Piirangud

Võrguühenduste turvet käsitletakse mooduligrupis NET. Irdandmekandjate kasutamiseks andmete edastuseks käsitletakse moodulis SYS.4.5 *Irdandmekandjad*.

2 Ohud

2.1 Teabe puudumine ettenähtud ajal

Teabe puudumine ettenähtud ajal võib oluliselt kahjustada äriprotsesse või põhjustada väärate juhtimisotsuste vastuvõtmist. Kui andmeid ei suudeta õigeaegselt töödelda või neid otsuste tegemiseks ette valmistada, jäävad ärieesmärgid täitmata.

Andmevahetusprotsessis võivad tekkida häired, samuti võib protsess katkeda tehnilistel põhjustel. Andmeseanssi võidakse põhjendamatult edasi lükata, andmete edastus võib võtta oodatust rohkem aega. Andmeliideste ja riistvara tõrked võivad põhjustada andmevahetuse täieliku katkemise.

2.2 Teabe volitamata avalikustamine

Teabevahetusel võivad andmed ja seeläbi ja konfidentsiaalne teave sattuda valedesse kätesse või ei jõua teave soovitud adressaadini. Teabe vastuvõtja võimalused teabe volitamata avalikustamist ära hoida on piiratud. Teabe väärkasutamise oht on suurem, kui teabevahetuse osapooled pole sõlminud konfidentsiaalsuslepingut.

2.3 Väära või sisemise teabe edastamine

Kui kasutajad ei ole piisavalt koolitatud või nad ei ole teabe edasiandmisel piisavalt tähelepanelikud, võib tundlik teave saada kättesaadavaks volitamata isikutele. Kui andmekandja antakse edasi ilma andmekandjale eelnevalt salvestatud andmeid turvaliselt kustutamata, on sellised näiliselt kustutatud andmed saajale juurdepääsetavad.

Samuti võib juhtuda, et konfidentsiaalsed dokumendid saadetakse kogemata valele vastuvõtjale või on saadetavas kirjas jäänud sisemiseks kasutuseks mõeldud kommentaarid kustutamata.

2.4 Andmete lubamatu kopeerimine või muutmine

Kui andmete või andmekandja edasisaatmisel kasutatakse ebaturvalisi kanaleid, on võimalik andmeid nende edastamise ajal märkamatult kopeerida. Ründaja võib suhtlust pealt kuulata ka andmevahetuseks kasutatavas sidevõrgus. Kui ründajal on ligipääs, saab ta andmeid edastamise ajal ka muuta, manipuleerida või lisada andmetele pahavara.

2.5 Ebapiisavate krüptovahendite kasutamine

Kui krüpteerimiseks valitakse kergesti äraarvatav võti või kui krüptovõtme saatmiseks suhtluspartnerile ei kasutata turvalisi kanaleid, võivad konfidentsiaalsed andmed lekkida.

3 Nõuded

3.1 Elutsükkel

Kavandamine

CON.9.M1 Lubatavate teabevahetuspartnerite määramine

CON.9.M2 Teabevahetuse kord

Evitus

CON.9.M3 Teabevahetuse koolitus töötajatele

CON.9.M4 Välise teabevahetuse lepped

Käitus

CON.9.M5 Jääkteabe kõrvaldamine failidest enne edasiandmist

CON.9.M6 Saatja ja saaja IT-süsteemide ühilduvuse kontroll

CON.9.M7 Edasiantavate andmete varundamine

CON.9.M8 Krüpteerimine ja digitaalsignatuurid

Lisanduvad kõrgmeetmed

CON.9.M9 Konfidentsiaalsuslepingu sõlmimine

3.2 Põhimeetmed

CON.9.M1 Lubatavate teabevahetuspartnerite määramine [haldusosakond, kasutaja]

a. Organisatsioon on määranud, mis teavet ja millistele partneritele ja mis andmevahetuskanalite kaudu on lubatud edastada.

b. Enne info edastamist välisele partnerile veendutakse vastuvõtja õigustes seda teavet vastu võtta ja edasi töödelda.

c. Teabe saajat teavitatakse, milleks ja kuidas seda teavet tohib kasutada.

CON.9.M2 Teabevahetuse kord [haldusosakond, kasutaja]

a. Organisatsioon on kehtestanud kõiki suulise ja elektroonilise teabevahetuse vorme hõlmava teabevahetuse korra.

b. Organisatsioon on kehtestanud teabe kaitsetarbe määramise juhised ja kaitsetarbele vastavad meetmed teabe kaitsmiseks.

c. Enne konfidentsiaalse teabe edastamist teavitatakse teabevahetuspartnerit, et teave on mõeldud kasutamiseks ainult edastamisel ettenähtud eesmärgil.

d. Organisatsioon on määranud, milliste andmevahetuskanalite ja -keskkondade kasutamine ei ole lubatud.

CON.9.M3 Teabevahetuse koolitus töötajatele [vastutav spetsialist]

a. Töötajad tunnevad teabevahetuse eeskirja ja oskavad konfidentsiaalset ning sisemiseks kasutamiseks mõeldud teavet käidelda.

b. Töötajad on teadlikud, millist teavet, millal, kus ja kuidas on lubatud edastada.

c. Töötajad läbinud koolituse andmete kaitsmiseks IT-vahendite abil (nt krüpteerimine või kontrollkoodide kasutamine).

3.3 Standardmeetmed

CON.9.M4 Välise teabevahetuse lepped [haldusosakond]

a. Regulaarseks teabevahetuseks väliste partneritega on kokku lepitud järgmised tingimused:

- kas ja millist teavet tuleb kaitsta;
- millised on teabevahetusteed;
- konfidentsiaalsusnõuded (vt ka CON.9.M9 *Konfidentsiaalsuslepingu sõlmimine*);
- nõutav turvatase ja kuidas seda tõendatakse;
- tegutsemine turvaintsidentide korral;
- vaidluste lahendamise kord;
- õiguslikud raamtingimused.

b. On kokku lepitud teabevahetuse korraldus olukorras, kui tavapärane suhtlus on häiritud.

CON.9.M5 Jääkteabe kõrvaldamine failidest enne edasiandmist [kasutaja]

a. Kasutajaid on jääkteabe kõrvaldamise vajadustest ja viisidest teavitatud. Kasutajad on läbinud vastava koolituse.

b. Enne failide edastamist kontrollitakse, kas failid ei sisalda avaldamisele mittekuuluvat jääkteavet, nagu kommentaarid, muudatuste ajalugu või liigsed metaandmed.

c. Tuvastatud jääkteave kustutatakse, vajadusel muudetakse selleks failivormingut.

d. Jääkteabe puudumist edastatud failides kontrollitakse pisteliselt.

CON.9.M6 Saatja ja saaja IT-süsteemide ühilduvuse kontroll

a. Enne andmekandja saatmist kontrollitakse saatja ja saaja IT-süsteemide ja -toodete ühilduvust järgnevas:

- seadmete füüsiline kokkusobivus;
- kasutatav märgikood (nt ASCII);
- operatsioonisüsteem ja failisüsteemi vormingud;
- rakendustarkvara;
- turvatarkvara ja turvaparameetrid.

b. Lahknevused kõrvaldatakse andmete konverteerimisega ja/või andmekandja asendamisega.

CON.9.M7 Edasiantavate andmete varundamine [kasutaja]

a. Kui edasiantavad andmed asuvad üksnes andmekandjal ning andmeid ei saa taastada muudest andmeallikatest, tehakse andmekandjast ajutine varukoopia.

CON.9.M8 Krüpteerimine ja digitaalsignatuurid [kasutaja]

a. Võimalusel krüpteeritakse konfidentsiaalne teave enne selle edastamist.

b. Suure terviklustarbega teavet kaitstakse digitaalsignatuuriga.

c. Andmete krüpteerimiseks valitakse kaitsetarbele vastav, nii saatjale kui ka saajale sobiv krüptomehhanism.

3.4 Kõrgmeetmed

CON.9.M9 Konfidentsiaalsuslepingu sõlmimine (C) [haldusosakond, kasutaja]

a. Konfidentsiaalse teabe edastuseks on selle saajaga sõlmitud leping, mis määrab:

- milline teave on konfidentsiaalne ja kui kaua;
- kellel on lubatud juurdepääs konfidentsiaalsele teabele;
- kuidas konfidentsiaalset teavet on lubatud hoida;
- millised on omandiõigused teabele ja saaja õigused teavet kasutada;
- millised on konfidentsiaalsuslepingu rikkumise tagajärjed.

CON.10 Veebirakenduste arendus

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed turvaliste dünaamiliste (muutuva sisuga) veebirakenduste arendamiseks ning veebirakendustes töödeldavate andmete kaitsmiseks.

1.2 Vastutus

Veebirakenduste arendamise meetmete täitmise eest vastutab arendaja.

Lisavastutajad

Antud moodulis lisavastutajad puuduvad.

1.3 Piirangud

Veebirakenduste turvalise kasutamisega seotud meetmed on kirjeldatud moodulis APP.3.1 *Veebirakendused.* Turvalise tarkvaraarenduse üldmeetmed on kirjeldatud moodulis CON.8 *Tarkvaraarendus*.

2 Ohud

2.1 Puudulik autentimine ja kasutusõiguste andmine

Kui ründajal õnnestub veebirakenduse autentimisest mööda hiilida, saab ta veebirakendust volitamata kasutada. Kui veebirakendus sisaldab tundlikke andmeid, võib see organisatsioonile kaasa tuua ulatusliku finants- ja mainekahju. Kui ründajal õnnestub veebirakendusse sisse logida veebirakenduses laiendatud kasutusõigusi omava kasutajana, avaneb tal andmete varastamiseks, manipuleerimiseks või kustutamiseks veelgi rohkem võimalusi.

Kui veebirakenduse kasutajaõiguste andmine, volitamine ja ressursside jagamine on ebaturvaliselt kavandatud ja puudulikult realiseeritud, võib veebirakenduse kasutaja (ning kasutajana esinev ründaja) saada volitamata juurdepääsu turvakriitilistele andmetele.

2.2 Puudulik sisendite ja väljundite valideerimine

Kui veebirakenduses töödeldakse manipuleeritud sisendandmeid, ei pruugita seda õigeaegselt märgata. Ründajal võimalik sisendandmeid manipuleerides veebirakenduse kaitsemehhanismidest mööda pääseda ja käivitada käske otse süsteemi või andmebaasi tasandil. Kui andmeid enne väljastamist ei kontrollita, võib andmetes sisalduv kahjurkood (nt kahjuliku toimega Javascript'i käsud) levida seotud IT-süsteemidesse.

2.3 Veebirakenduse puuduv või puudulik tõrkehaldus

Tihti jäävad väiksemad anomaaliad veebirakenduse töös registreerimata ja nendega ei tegeleta. Kui veebirakenduse töös esinevaid tõrkeid ja vigu õigeaegselt ei avastata ja nende kõrvaldamisega ei tegeleta, võib see probleemi kasvades hakata mõjutama rakenduse tööd või muuta rakenduse kasutajatele kättesaamatuks. Veebirakenduse viga võib kaasa tuua suuremahulise andmekao. Viga vahemällu salvestatud andmetes võib mõjutada andmete terviklust. Vigane turvamehhanism võib põhjustada volitamata juurdepääsu andmetele.

2.4 Puudulik turvasündmuste logimine

Veebirakenduse turvasündmuste ebapiisaval logimisel ei ole võimalik hiljem turvasündmusi tuvastada ja nende tekkepõhjuseid välja selgitada. Kuna intsidendi põhjus jääb välja selgitamata, on raskendatud meetmete rakendamine sarnaste intsidentide ärahoidmiseks tulevikus.

Kui rakenduses esinevaid vigu ja võimalikule ründele viitavaid konfiguratsioonimuudatusi ei logita, võivad need jääda märkamata.

2.5 Tundliku taustainfo avaldamine veebirakenduses

Teatud päringutele veebiserveri ja veebirakenduse poolt vastuseks väljastatavad andmed võivad sisaldada ründajale vajalikku teavet veebiserveri, operatsioonisüsteemi ja tarkvara versiooni ja konfiguratsiooni kohta. Ründaja saab IT-komponentide teadaolevaid nõrkusi ära kasutada veebirakenduse sihtründe (ingl *targeted attack*) plaanimiseks.

2.6 Automaatsete ründevahendite kasutamine

Ründaja võib veebirakenduse töö tõkestamiseks või andmetele juurdepääsu saamiseks lasta automaatselt genereerida suure hulga korduvaid päringuid, mida veebirakendus peab suutma töödelda. Veebirakenduse vastu suunatud teenusetõkestusrünne (ingl *denial-of-service attack*) võib tekitada veebirakenduse ülekoormuse ja muuta rakenduse kasutajaile kättesaamatuks. Ründevahendi poolt genereeritud korduvate sisselogimiskatsete abil on võimalik püüda ära arvata rakenduse kasutajanimede (kui rakendus annab selle kohta tagasisidet) ja salasõnade kombinatsioone ehk korralda jõurünnet (ingl *brute-force attack*) või koostada kehtivate kasutajanimede loendeid.

2.7 Puudulik seansihaldus

Puuduliku seansihalduse puhul saab ründaja ilma pääsuõigusi omamata kaaperdada teise kasutaja poolt algatatud seansi. Kui ründajal õnnestub kindlaks teha rakenduses laialdasi õigusi omava eeliskasutaja seansiidentifikaator (ingl *session ID*), on tal võimalik lubatud kasutajana tegutseda. Seansipette (ingl *session fixation*) korral laseb ründaja kõigepealt veebirakendusel määrata seansiidentifikaatori ja seejärel edastatakse see mõnele volitatud kasutajale (nt e-posti lingiga). Kui volitatud kasutaja kasutab seda linki ja veebirakenduses

end ründaja edastatud seansiidentifikaatoriga autendib, saab ründaja veebirakendust temale teadaolevaks saanud seansiidentifikaatoriga seansi ning volitatud kasutaja õiguste piires kasutada.

3 Meetmed

3.1 Elutsükkel

Kavandamine

CON.10.M11 Veebirakenduse turvaline tarkvaraarhitektuur

CON.10.M9 Kaitse SQL-süsti eest

Evitus

CON.10.M1 Turvaline autentimine veebirakenduses

CON.10.M2 Veebirakenduse juurdepääsu reguleerimine

CON.10.M4 Veebirakenduse sisu kasutamise piiramine

CON.10.M5 Andmete üleslaadimise piiramine

CON.10.M6 Kaitse veebirakenduste volitamata automaatse kasutamise eest

CON.10.M14 Veebirakenduste turvaline HTTP-konfiguratsioon

CON.10.M16 Mitmikautentimise kasutamine

Käitus

CON.10.M3 Turvaline seansihaldus

CON.10.M7 Konfidentsiaalsete andmete kaitse

CON.10.M8 Sisendite valideerimine ja väljundite kodeerimine

CON.10.M10 Tundliku taustainfo avaldamise piiramine

CON.10.M12 Oluliste muudatuste kinnitamine

CON.10.M13 Veebirakenduse tõrketöötlus

CON.10.M15 Päringuvõltsingu takistamine

Lisanduvad kõrgmeetmed

CON.10.M17 Ressursside blokeerimise takistamine

CON.10.M18 Tundlike andmete krüptograafiline turve

3.2 Põhimeetmed

CON.10.M1 Turvaline autentimine veebirakenduses

a. Veebirakenduse sisule juurdepääs võimaldatakse ainult kasutaja autentimise kaudu ning on reguleeritud turvaliste ja asjakohaste autentimismeetoditega.

b. Valitud autentimismeetodid on asjakohased ja turvalised ning nende valik on dokumenteeritud.

c. Võimaluse korral on autentimiseks kasutusel tsentraalselt hallatavad autentimiskomponendid (näiteks riigi autentimisteenus TARA).

d. Kasutaja autentimisandmeid on lubatud veebirakenduses salvestada ainult pärast kaasnevate riskide kaalumist ja teadvustamist. Kasutajalt nõutakse enne oma autentimisandmete salvestamist riskidega tutvumist ja üheselt mõistetavat („opt-in“) nõusolekut.
e. Veebirakenduses on määratud ebaõnnestunud logimiskatsete lubatud arv. Pärast selle ületamist rakendatakse täiendavaid turvaprotseduure (nt tõkestatakse kasutaja juurdepääs määratud ajaks).

CON.10.M2 Veebirakenduse juurdepääsu reguleerimine

a. Kasutaja pääsuõigused on vajadusekohaselt piiratud.
b. Õiguste mehhanism tagab, et kasutajad saavad teha üksnes oma õigustega lubatud toiminguid.
c. Kasutajate pääsuõigusi hallatakse tsentraalses ja usaldusväärses IT-süsteemis.
d. Pääsuõiguste süsteemi vea korral veebirakendusele juurdepääs keelatakse.
e. Pääsu reguleerimine hõlmab lisaks rakenduse ressurssidele ja funktsioonidele ka URL-kutseid ja objektiviiteid.

CON.10.M3 Turvaline seansihaldus

a. Seansiidentifikaatorite (ingl *session ID*) loomisel, edastamisel ja klientarvutisse salvestamisel on tagatud seansiidentifikaatorite turvalisus.
b. Seansiidentifikaatorid genereeritakse juhuslikkuse põhimõttel ja piisava entroopiaga. Võimalusel kasutatakse veebirakenduse taristu seansiidentifikaatorite genereerimise funktsiooni. Selleks on veebirakenduse taristu turvaliselt konfigureeritud.
c. Veebirakendus võimaldab kasutajatel pooleliolevat seanssi kontrollitult ja üheselt mõistetavalt lõpetada. Pärast kasutaja uut sisselogimist asendatakse seansiidentifikaator uuega.
d. Seansi kestusele on määratud ülempiir. Mitteaktiivsed seansid lõpetatakse pärast määratud jõudeolekuaega automaatselt.
e. Pärast seansi lõppemist kustutatakse kõik seansiandmed nii serveri kui kliendi poolel.

CON.10.M4 Veebirakenduse sisu kasutamise piiramine

a. Veebirakendus väljastab kasutajatele üksnes ettenähtud ja lubatavaid andmeid ja sisu.
b. Veebirakendusest edasisuunamise sihtkohad asuvad usaldusväärses domeenis.
c. Edasisuunamise funktsionaalsus kasutajatele on veebirakenduses piiratud.
d. Kasutaja lahkumisel usaldatavast domeenist kasutajat informeeritakse.

CON.10.M5 Andmete üleslaadimise piiramine

a. Kasutaja saab salvestada faile ainult ettemääratud viisil.
b. Kasutaja ei saa veebirakenduses seadistatud andmesalvestuse asukohta muuta.
c. Veebirakenduse failide üleslaadimise funktsioon on piiratud.

CON.10.M6 Kaitse veebirakenduste volitamata automaatse kasutamise eest

a. Veebirakendus on kaitstud automatiseeritud juurdepääsu eest.
b. Turvamehhanismide rakendamisel on arvestatud, et turvamehhanismid ei piiraks volitatud kasutajate toiminguid ülemäära.

c. Veebirakenduse RSS-söödete (ingl *RSS feed*) või teiste automatiseeritud funktsioonide olemasolul arvestatakse neid turvamehhanismide seadistamisel.

CON.10.M7 Konfidentsiaalsete andmete kaitse

a. Klientarvutist serverisse edastatakse andmeid ainult HTTP meetodiga POST.

b. Klientarvutisse ei salvestata ega ajutiselt puhverdata tundlikke andmeid.

c. Vormidel olevaid konfidentsiaalseid andmeid ei hoita brauseris avateksti kujul.

d. Veebirakenduse pääsuandmeid on serveris kaitstud piisavalt tugeva krüpteeringuga. Autentimisandmetest hoitakse serveris ainult parooli „soolatud“ räsi (ingl *salted hash*).

e. Veebirakenduse lähtekoodi kaitstakse lubamatu juurdepääsu eest.

CON.10.M8 Sisendite valideerimine ja väljundite kodeerimine

a. Veebirakendusse edastatud sisendandmeid käsitletakse potentsiaalselt ohtlike andmetena, mida peab enne edasist töötlust filtreerima ja valideerima.

b. Kõiki sisendandmeid, sh sekundaarandmeid (nt seansiidentifikaatorid) valideeritakse serveris asuvas usaldusväärses IT-süsteemis.

c. Vigaseid sisestusi ei töödelda võimaluse korral automaatselt. Kui seda ei saa vältida, muudetakse sisendandmed turvaliseks.

d. Ohtlikud sümbolid varjestatakse viisil, et nende edasine interpreteerimine või käivitamine sihtsüsteemis osutuks võimatuks.

CON.10.M9 Kaitse SQL-süsti eest

a. SQL-süsti (ingl *SQL injection*) välistamiseks edastatakse andmed veebirakendusest andmebaasisüsteemi (DBMS) salvestatud protseduuride (ingl *stored procedures*) või SQL-valmislausetega.

b. Kui salvestatud protseduure ega SQL-valmislauseid ei saa kasutada, siis kaitstakse SQL-päringuid muul viisil.

CON.10.M10 Tundliku taustainfo avaldamise piiramine

a. Veebilehed ja veebirakenduste vastusteated ei sisaldada informatsiooni, mis ründajat abistaks turvamehhanismidest mööda hiilida. Selleks tagatakse, et:

- edastatakse üksnes neutraalseid veateateid;
- ei paljastata turbega seotud kommentaare ega toote- või versiooniandmeid;
- turvadokumentatsioonile on võimalik üksnes piiratud juurdepääs;
- ebavajalikke faile kustutatakse regulaarselt;
- väliste otsingumootoritega kasutatakse veebirakendust ettenähtud viisil;
- välditakse teabe jagamist salvestusteede kohta;
- veebirakenduse konfiguratsioonifailid ei asu veebisaidi juurkataloogis.

3.3 Standardmeetmed

CON.10.M11 Veebirakenduse turvaline tarkvaraarhitektuur

a. Veebirakenduse tarkvaraarhitektuur koos kõikide komponentide ja sõltuvustega on dokumenteeritud. Tarkvaraarhitektuuri dokumentatsiooni uuendatakse ja kohandatakse vastavalt vajadusele.

b. Veebirakenduse arendamisel lähtutakse kinnitatud tarkvaraarhitektuuri dokumentatsioonist. Dokumentatsiooni detailsus on piisav arendajatel tekkivate küsimuste lahendamiseks.

c. Tarkvaraarhitektuuri dokumentatsioonis on välja toodud ka rakendusevälised, kuid rakenduse tööks vajatavad komponendid.

d. Tarkvaraarhitektuuri kavandamisel on arvestatud, milliste komponentide jaoks milliseid turvamehhanisme rakendatakse, kuidas veebirakendus on olemasolevasse taristusse integreeritud ning milliseid krüpteerimisfunktsioone ja -protseduure kasutatakse.

CON.10.M12 Oluliste muudatuste kinnitamine

a. Enne oluliste muudatuse tegemist veebirakenduses nõutakse kasutaja kinnitust, mis on realiseeritud kasutaja salasõna uuesti sisestamisega. Mitmikautentimise (*ingl multifactor authentication*) puhul piisab täiendava autentimisteguri sisestamisest.

b. Kui salasõna uuesti sisestamist tegevuse kinnitamiseks ei saa rakendada, kasutatakse mõnda muud autentimismeetodit.

c. Kasutajaid teavitatakse toimunud muudatustest veebirakendusevälise sidekanali kaudu.

CON.10.M13 Veebirakenduse tõrketöötlus

a. Veebirakenduse töö ajal tekkinud tõrgete lahendamisel säilitatakse veebirakenduse terviklus.

b. Veebirakendus logib kõik tekkinud veateated.

c. Tõrke tõttu pooleli jäänud toiming katkestatakse ja juurdepääs ressurssidele tõkestatakse.

d. Eelnevalt reserveeritud veebirakenduse ressursid vabastatakse tõrketöötluse käigus.

e. Võimaluse korral teostab tõrketöötluse veebirakendus ise.

CON.10.M14 Veebirakenduste turvaline HTTP-konfiguratsioon

a. Kaitseks klõpsurööv-rünnete (ingl *clickjacking*) ja skriptisüsti (ingl *cross-site scripting*) eest on veebirakenduses määratud sobivad HTTP-vastusepäise sätted (nt X-FRAME-OPTIONS: *deny*).

b. Veebirakendus kasutab vähemalt järgmisi HTTP-päiseid:
   - Content-Security-Policy (CSP);
   - Strict-Transport-Security (HSTS);
   - Content-Type;
   - X-Content-Type-Options;
   - Cache-Control.

c. Veebirakendus on HTTP-päistega seadistatud sedavõrd päringuid piiravaks kui võimalik.

d. Küpsistele (ingl *cookie*) on määratud atribuudid *secure*, *SameSite* ja *httponly*.

CON.10.M15 Päringuvõltsingu takistamine

a. Veebirakendus toetab päringuvõltsingu (ingl *cross-site request forgery*) takistamise turvamehhanisme, mis eristavad kasutaja kavatsetud ja korralisi veebilehepäringuid soovimatutest päringutest või volituseta käskudest.
b. Kontrollitakse, kas kaitstud ressurssidele ja funktsioonidele juurde pääsemiseks on lisaks seansiidentifikaatorile vaja mingit lisanduvat volitustõendit.
c. Kasutaja kavatsetud päringu tõendamiseks kontrollitakse täiendavalt HTTP-päringu autentsust.

CON.10.M16 Mitmikautentimise kasutamine

a. Võimalusel rakendatakse veebirakenduse kasutajate autentimisel mitmikautentimist.

3.4 Kõrgmeetmed

CON.10.M17 Ressursside blokeerimise takistamine (A)

a. Ummistusrünnete (ingl *denial-of-service attack*) ärahoidmiseks välditakse ressursimahukaid tüüptoiminguid.
b. Kui ressursimahukaid tüüptoiminguid ei saa välistada, rakendatakse nende kaitseks spetsiaalseid turvameetmeid.
c. Jälgitakse ja ollakse valmis võimalikuks veebirakenduse logide ületäitumiseks.

CON.10.M18 Tundlike andmete krüptograafiline turve (C-I)

a. Veebirakenduse tundlikud andmed on kaitstud piisavat kaitset pakkuvate krüptomehhanismidega.

OPS.1: Oma käidutööd

OPS.1.1: IT-põhitööd

OPS.1.1.1 IT-haldus üldiselt

1 Kirjeldus

1.1 Eesmärk

Kehtestada infoturbe meetmed lahutamatu osana kõigis IT-halduse põhiaspektides (IT-varade haldamine, IT-hanked, IT käitamine, muudatuste haldus, seire, intsidentide haldus ja IT kasutusest kõrvaldamine).

1.2 Vastutus

IT-halduse meetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Lisavastutajad puuduvad.

1.3 Piirangud

Moodul käsitleb IT-halduse valdkonnaüleseid infoturbe aspekte. IT-haldus ei keskendu ainult infotehnoloogiale, vaid selle turvalisele integreerimisele organisatsiooni äriprotsessidesse. Moodul ei asenda IT-halduse parimaid tavasid koondavaid raamistikke, nt ITIL (Information Technology Infrastructure Library) või standardeid (ISO 20000 Infotehnoloogia.Teenusehaldus).

IT-halduse valdkondlikke turvameetmeid käsitletakse mooduligrupi OPS.1.1 IT-põhitööd järgnevates moodulites, eelkõige moodulites OPS.1.1.2 *IT-süsteemide haldus*, OPS.1.1.3 *Paiga- ja muudatusehaldus* ja OPS.1.1.7 *Süsteemihaldus*.

Võrguhalduse meetmed kirjeldatakse moodulis NET.1.2 *Võrguhaldus.* Pääsuõiguste haldust käsitletakse moodulis ORP.4 *Identiteedi- ja õiguste haldus* ning IT-süsteemide kaughaldust moodulis OPS.1.2.5 *Kaughooldus.*

Andmete varundamist ja arhiveerimist käsitletakse moodulites CON.3 *Andmevarunduse kontseptsioon* ja OPS.1.2.2 *Arhiveerimine*.

IT-halduse aspekte erandlikes olukordades toimetulekuks käsitletakse moodulites DER.1 *Turvaintsidentide avastamine*, DER.2.1 *Turvaintsidentide käsitlus* ja DER.2.3 *Ulatuslike turvaintsidentide lahendamine*.

Kolmandate poolte haldusülesannete täitmist käsitlevad moodulid OPS.2.3 *Väljasttellimine* ja OPS.3.2 *Teenuseandja infoturve*.

Antud moodul ei käsitle DevOps metoodika eriaspekte ega infoturbe meetmete rakendamist IT projektide läbiviimisel.

2 Ohud

2.1 Kvalifitseeritud tööjõu puudumine

IT-halduse sujuvast toimimisest sõltub organisatsiooni äriprotsesside toimimine. Kvalifitseeritud töötajate puudumisel võib katkeda IT-halduse protsesside järjepidevus, pikenevad ooteajad ja sagenevad IT-töötajate inimlikest eksimustest tingitud vead.

Tööjõu puudus nõrgendab oluliselt IT-halduse infoturbe aspekte. Näiteks ei ole võimalik töötajate vähesuses tõttu korraldada piisavat seiret ja tegevuslogide analüüsi.

Vajaliku oskusteabe koondumine ainult mõnede töötajate valdusesse tekitab sõltuvuse üksikutest inimesest. Võtmeisiku lahkumise korral tekivad probleemid IT-süsteemide käideldavuse tagamisel.

2.2 IT-halduse dokumentatsiooni puudulikkus

IT- halduse protseduuride läbiviimine ebapiisavatele, vananenud või volitamata muudetud protsessijuhenditele tuginedes võib põhjustada katkestusi IT-süsteemide töös, andmete lekkimist või tervikluse kadu. Ka toimunud intsidentide tagajärgede likvideerimine võtab oluliselt rohkem aega, sest puuduvad detailsed tegevusjuhised IT-süsteemide ja seonduvate andmete taastamiseks.

Kui IT-haldusesse on kaasatud väliseid osapooled, võib puudulik tegevuste juhtimine põhjustada tundliku teabe lekkimist.

2.3 Piiratud ressursid IT-halduses

Kui puuduvad vajalikud tööriistad IT-halduse protsesside läbiviimiseks ja automatiseerimiseks, kannatab IT-halduse kvaliteet ja efektiivsus ja seeläbi organisatsiooni äriprotsesside toimimine. Tõrgete kõrvaldamiseks kuluv aeg pikeneb, töötajad on tegevuses äriprotsesside parendamise asemel „tulekahjude kustutamisega“.

Ressursside puudumisel ei ole võimalik luua taristut käidukeskkonnas tehtavate muudatuste testimiseks ja IT-haldusprotsesside parendamiseks.

2.4 Eelisõiguste või konfidentsiaalse teabe kuritarvitus

IT-halduri eelisõigustega kasutajakonto kuritarvitamise teel on võimalik ligi pääseda konfidentsiaalsele teabele ja manipuleerida ärikriitilisi andmeid. Volitamata isikud võivad eeliskontole ligi pääseda läbi halduri vastu suunatud kalastamis- (ingl *phishing*) või suhtlusrünnete (ingl *social engineering*).

Kui IT-halduri organisatsioonist lahkumisel ei suleta tema kontosid või ei muudeta sisselogimisandmeid, võib ta jätkata IT-süsteemidesse sisselogimist, seades niiviisi ohtu IT-süsteemide turvalisuse.

Konfidentsiaalse teabe lekke võib põhjustada ka IT-halduri inimlik eksimus, näiteks kui ta jätab laokile oma pääsukaardi või väljatrükitud IT-süsteemi konfiguratsiooniandmed.

2.5 Volitamata juurdepääs IT-seadmetele

Kui IT-halduseks kasutavatele arvutitele või IT-seadmetele pääsevad ligi volitamata isikud (nt asuvad seadmed lukustamata ruumis), eksisteerib oht, et neid seadmeid kasutatakse erinevate IT-süsteemide vastu suunatud rünnete algatamiseks. Oht on suurem, kui IT-halduse jaoks vajalikud kasutajakontod ja andmesideliidesed on nõrgalt kaitstud, näiteks nõuavad ainult parooli sisestamist.

2.6 IT-haldustoimingute salgamine või võltsimine

Kui IT-haldur esitab haldustoimingute kohta valeinformatsiooni (nt salgab, et oluline protseduur jäi tegemata), võib see ohustada IT-süsteemi käideldavust ja IT-süsteemis olevate andmete turvalisust.

Kui IT-haldurile saadetakse valeinformatsiooni (nt manipuleeritud e-kirjaga) süsteemi oleku või edasiste tegevuste kohta, võib ta tegelikku olukorda valesti hinnata ja käivitada protseduure, mis muudavad IT-süsteemi kasutajale kättesaamatuks või ohustavad IT-süsteemi turvalisust muul viisil.

2.7 Haldustoimingute tegemata jätmine

Kui IT-halduse toiminguid ei viida läbi vastavalt kehtestatud nõuetele ja protsessijuhenditele, võib kahjustuda IT-süsteemide käideldavus ja terviklus.

Sageli jäetakse IT-komponentide soetamisel arvestamata nende hilisem hooldus- ja haldusvajadus. IT-komponendid võivad asuda kohtades, kus neile ligipääs on raskendatud või pole kasutusele võetud haldamiseks vajalikke haldusliideseid.

Samuti võib IT-süsteemide turvalisus ohtu sattuda kui IT-halduse toiminguid viiakse läbi hoolimatult või ebakorrektselt.

3 Meetmed

3.1 Elutsükkel

Kavandamine

OPS.1.1.1.M1 IT-halduse ülesannete ja kohustuste määramine

OPS.1.1.1.M2 IT-halduse rollide ja kasutusõiguste määratlemine

OPS.1.1.1.M3 IT-halduse juhendite koostamine

OPS.1.1.1.M4 IT-halduseks vajalike ressursside tagamine

Evitus

OPS.1.1.1.M11 Teenusetasemelepete sõlmimine

OPS.1.1.1.M12 IT-halduse protsesside määratlemine

OPS.1.1.1.M14 IT-halduse kavandamine IT-komponentide soetamisel

OPS.1.1.1.M15 IT-halduse tööriistade turvaline soetamine ja kasutamine

Käitus

OPS.1.1.1.M5 Turvaliste tüüpkonfiguratsioonide määratlemine

OPS.1.1.1.M6 Keskne IT-varade haldus

OPS.1.1.1.M7 Turvalised IT-halduse protseduurid

OPS.1.1.1.M8 IT-halduse regulaarne kontrollimine

OPS.1.1.1.M9 IT-halduse regulaarne seire

OPS.1.1.1.M10 IT-komponentide turvanõrkuste loend

OPS.1.1.1.M13 IT-halduse tööriistade ja dokumentatsiooni turve

OPS.1.1.1.M16 IT-halduse personali väljaõpe

OPS.1.1.1.M18 Väliste teenuseandjate kasutamine IT-halduses

OPS.1.1.1.M19 IT-komponentide regulaarne hooldus

OPS.1.1.1.M20 IT-komponentide turvanõrkuste seire

Avariivalmendus

OPS.1.1.1.M17 IT-halduse korraldamine avariiolukorras

Lisanduvad kõrgmeetmed

OPS.1.1.1.M21 IT-halduse tööriistade kasutamise seire

OPS.1.1.1.M22 Automatiseeritud turvatestimine

OPS.1.1.1.M23 IT-komponentide läbistustestimine

OPS.1.1.1.M24 IT-halduse protseduuride detailne logimine

OPS.1.1.1.M25 IT-halduse tööriistade autonoomsuse tagamine

OPS.1.1.1.M26 IT-komponentide ennetav hooldus

3.2 Põhimeetmed

OPS.1.1.1.M1 IT-halduse ülesannete ja kohustuste määramine

a. Kõikide IT-komponentide puhul on määratletud vajalikud IT-halduse toimingud.
b. On määratud IT-komponentide halduse eest vastutavad IT-haldurid.
c. Organisatsioon on määranud IT-halduse suhtluskanalid ja kinnitanud organisatsiooniüksuste vahelise aruandluse, sh suhtluskanalid intsidentide eskaleerimiseks.

OPS.1.1.1.M2 IT-halduse rollide ja kasutusõiguste määratlemine

a. IT-komponentidele on määratud komponendi halduseks kasutatavad rollid ja halduseks vajalikud õigused ja volitused.
b. On loodud IT-halduse rollikontseptsioon, millega eraldatakse IT-halduseks kasutatavad rollid igapäevase IT-tavakasutaja rollidest.
c. Igapäevaste IT-tegevuste jaoks ei kasutata IT-halduri õigustega kasutajakontot.
d. Ühiskasutuses olevaid kasutajakontosid on lubatud luua ja kasutada ainult põhjendatud erandjuhtudel.
e. Rollide ja halduskontode pääsuõiguste asjakohasust kontrollitakse perioodiliselt. IT-halduse rolle, kontosid ja pääsuõigusi uuendatakse vastavalt vajadusele.
f. Lahkunud töötajate kasutajakontod eemaldatakse IT-komponentidest esimesel võimalusel.
g. IT-komponendi kasutusest kõrvaldamisel kustutatakse sellega seotud rollid ja halduskontod.

3.3 Standardmeetmed

OPS.1.1.1.M3 IT-halduse juhendite koostamine

a. Käitatavate IT-komponentide haldustööd on kirjeldatud IT-halduse juhendites.
b. IT halduse juhendites käsitletakse vähemalt järgmist:
    - hallatava IT-komponendi andmed;
    - vajalikud haldusvahendid ja -tööriistad;
    - IT-komponendi konfiguratsioon;
    - konfiguratsioonis sisalduvate turvaseadistuste kohandused;
    - IT-halduse rollid ja kontod;
    - IT-komponentide testimine;
    - seire, logimine ja automaatteavitused;
    - andmete varundamine ja taasteplaanid;
    - IT-intsidentide käsitlemise kord;
    - regulaarsed ja plaanivälised haldustegevused.
c. IT halduse juhendid on volitatud isikutele igal ajal kättesaadavad.
d. IT-halduse juhendite aja- ja asjakohasust kontrollitakse perioodiliselt. Juhendeid uuendatakse vastavalt vajadusele.

OPS.1.1.1.M4 IT-halduseks vajalike ressursside tagamine

a. Piisavate ressursside leidmiseks on analüüsitud IT-halduse toimingute mahtu, vajalikke ressursse, tööjõudu ja oskusteavet.

b. IT-halduseks on olemas piisaval hulgal vajaliku oskusteabega töötajaid. Personaliressursi kavandamisel on arvestatud reserviga, mis on vajalik lühiajaliste töölt eemalolekute ja ajutiste suurema personalivajadusega perioodide kompenseerimiseks.

c. IT-halduseks on olemas piisaval hulgal materiaalseid ressursse.

d. Ressursivajadusi hinnatakse perioodiliselt. IT-halduse ressursse kohandatakse vastavalt ärivajadustele ja kehtivatele nõuetele.

OPS.1.1.1.M5 Turvaliste tüüpkonfiguratsioonide määratlemine

a. IT-halduse juhendites on koostatud ja dokumenteeritud tüüpsete IT-komponentide tugevdatud turvet sisaldavad tüüpkonfiguratsioonid.

b. Virtualiseeritud IT-platvormides, milles käitatakse teisi IT-komponente, on välja töötatud ja rakendatud kõigile IT-komponentidele sobivad turvaseadistused.

c. IT-komponentide konfiguratsioonid vastavad organisatsiooni turvanõuetele ning arvestavad tootjapoolseid soovitusi komponentide turvaliseks seadistuseks.

d. Tüüpkonfiguratsioone testitakse enne nende juurutamist käidukeskkonnas (ingl *operational environment*).

e. Tüüpkonfiguratsioonide aja- ja asjakohasust kontrollitakse regulaarselt. Tüüpkonfiguratsioone muudetakse vastavalt tehnoloogilise keskkonna ja riskihinnangute muutumisele.

f. Tüüpkonfiguratsioonid sisaldavad versiooninumbrit ning teostatud muudatusi kirjeldavat muutelugu.

OPS.1.1.1.M6 Keskne IT-varade haldus

a. IT-halduse protseduurid sisaldavad olemasolevatest IT-varadest ülevaate saamist ja varade perioodilise inventuuri läbiviimist.

b. Kõik käidukeskkonda paigaldatud, testimiseks kasutatavad ning varus olevad IT-komponendid on registreeritud varade keskset haldust võimaldavas varahaldussüsteemis.

c. Varahaldussüsteemis on andmed ka olemasolevate, kuid kasutusest maha võetud IT-varade kohta.

OPS.1.1.1.M7 Turvalised IT-halduse protseduurid

a. IT-halduse protseduuridele on kehtestatud kvaliteedinõuded ning on määratud kriteeriumid IT-halduse toimingute nõuetele vastavuse mõõtmiseks.

b. IT-komponente testitakse enne nende käidukeskkonda paigaldamist ning pärast oluliste muudatuste rakendamist. Vajalikud testid ja nende läbiviimise kord on kirjeldatud IT-halduse juhendites.

c. IT-talitusel on valmisolek kasutatavate IT-komponentide asendamiseks varukomponentidega. Selleks on olemas vajalikud ressursid ja tarnelepingud.

d. IT-halduse käigus tehtud tööd on sobival ja arusaadaval viisil dokumenteeritud. Soovitatav on kasutada selleks spetsiaalset tarkvara, nt IT Helpdeski rakendust.

e. Süstemaatiliselt jälgitakse IT-halduse protseduuride kvaliteeti ning kasutajate rahulolu.

f. Süstemaatiliselt kontrollitakse teenusetasemelepete (ingl *service level agreement*, SLA) ning tegevuslepete (ingl *operational level agreement*, OLA) järgimist.

OPS.1.1.1.M8 IT-halduse regulaarne kontrollimine

a. Regulaarselt kontrollitakse, kas:
   - IT-halduse protseduure kohaldatakse kõikidele käidukeskkonna IT-komponentidele;
   - IT-komponentide konfiguratsioonid vastavad ettenähtud tüüpkonfiguratsioonidele;
   - IT-halduse protsess on integreeritud kõikidesse organisatsiooni äriprotsessidesse.

OPS.1.1.1.M9 IT-halduse regulaarne seire

a. IT-komponentide seiret teostatakse keskse, IT-talituse juhtkonnas kinnitatud seireplaani alusel.
b. Olulistele IT-komponentide parameetritele on määratud lävendid, millest hälbimine käivitab IT-haldurite automaatse teavituse.
c. IT-talitus on IT-halduse seire tulemustest teavitamiseks määranud suhtluskanalid, määratlenud aruandluse sisu ning koostanud avariiolukordadest teavitamise korra.
d. Seireandmete põhjal on võimalik jälgida IT-komponentide hetkeolukorda ning oluliste parameetrite muutumist ajas. Seiretulemused on üheks sisendiks IT-süsteemides tehtavate muudatuste kavandamiseks.
e. Seireandmeid edastatakse ainult turvaliste sidekanalite kaudu.
f. IT-süsteemide kaetust IT-halduse seireplaaniga kontrollitakse perioodiliselt. IT-halduse seireplaani ajakohastatakse vastavalt vajadusele.

OPS.1.1.1.M10 IT-komponentide turvanõrkuste loend

a. IT-komponentide teadaolevad turvanõrkused registreeritakse keskses turvanõrkuste loendis.
b. Turvanõrkuste loendi pidamine ja turvanõrkuste käsitlus on osa IT-halduse protsessist.
c. Turvanõrkuste käsitluse käigus dokumenteeritakse:
   - kas eksisteerib turvauuend, mis parandaks IT-komponendi teadaoleva turvanõrkuse;
   - mis ajaks on IT-komponendi turbepaik paigaldatud;
   - kas IT-komponent tuleb turvanõrkuste tõttu kasutusest kõrvaldada ja/või asendada;
   - kuidas toimub IT-komponendi eraldamine juhul kui IT-komponendi uuendamine või asendamine pole võimalik.

OPS.1.1.1.M11 Teenusetasemelepete sõlmimine

a. IT-talitus on sõlminud oma klientidega IT-komponentide kaitsetarvet arvestavad teenusetasemelepped (ingl *service level agreement*, SLA) või tegevuslepped (*operational level agreement*, OLA).
b. Teenusetasemelepete tingimuste määramisel on arvestatud organisatsiooniüksuste ja äriprotsesside sõltuvusi IT-komponendi toimimisest ning äriprotsesside kaitsetarvet.
c. Teenusetasemelepetes määratletud rolle ja vastavaid kohustusi täidetakse.

OPS.1.1.1.M12 IT-halduse protsesside määratlemine

a. IT-talitus on määratlenud ja kinnitanud IT-halduse protsessid.

b. Iga IT-halduse protsessi kohta on kirjeldatud:
   - protsessi algataja ja protsessis osalejad;
   - protsessis sisalduvad IT-halduse tegevused;
   - liidestused (sh sisendid ja väljundid) teiste IT-halduse protsesside või äriprotsessidega;
c. IT-talituse töötajad tunnevad IT-halduse protsesse ja järgivad tööprotseduure.
d. IT- halduse protsessi läbimise tõestusmaterjalid dokumenteeritakse. Üksikute protsessietappide läbimist logitakse vastavalt vajadusele.
e. On loodud tegevusjuhised olukordadeks, mis väljuvad tüüpsete IT-halduse protsesside raamest. Dokumenteeritud on vähemalt:
   - tegevusjuhend juhuks, kui IT-halduse protsessi pole võimalik läbi viia;
   - juhised veaolukorra ja protsessi tahtliku manipuleerimise korral tegutsemiseks.

OPS.1.1.1.M13 IT-halduse tööriistade ja dokumentatsiooni turve

a. IT-halduses kasutatavatele seadmetele, tööriistadele ja juhenditele on juurdepääs ainult volitatud IT-talituse töötajatel.
b. IT-halduseks vajalikud ressursid ja dokumentatsioon on volitatud isikutele vajadusel kättesaadavad.
c. Kui IT-halduse toiminguid tehakse otse käidukeskkonnas (ingl *operational environment*), edastatakse tundlikke andmeid ainult turvaliste protokollide kaudu.
d. IT- halduse tööriistade kasutamist seiratakse ja neile kohandatakse paigahaldust (vt OPS.1.1.3 *Paiga- ja muudatusehaldus*).

OPS.1.1.1.M14 IT-halduse kavandamine IT-komponentide soetamisel

a. IT-süsteemide kavandamisel ja IT-komponentide hankimisel on arvestatud nende toimimise tagamiseks vajalike IT-haldustööde mahtu ning organisatsiooni IT-halduse protsessidest tulenevaid nõudeid.
b. IT-haldusvajaduse analüüsis on arvestatud kavandavate IT-süsteemide keerukust (ingl *complexity*).

OPS.1.1.1.M15 IT-halduse tööriistade turvaline soetamine ja kasutamine

a. IT-halduse ressursside kavandamisel ning haldustööriistade soetamisel ja kasutamisel lähtutakse IT-komponentide halduse reaalsest vajadusest.
b. IT-halduse protsessid ja vajalikud ressursid on organisatsiooni kõigi äriüksustega kooskõlastatud.
c. IT-halduse võrk on asutuse teistest võrkudest vähemalt loogiliselt eraldatud (vt NET.1.1 *Võrgu arhitektuur ja lahendus*). Ressursside täiendav segmentimine otsustatakse, lähtudes IT-halduse tööriistade funktsionaalsetest sõltuvustest, infoturvapoliitikast ja andmete kaitsetarbest.

OPS.1.1.1.M16 IT-halduse personali väljaõpe

a. IT-halduse töötajate koolitusplaani koostamisel arvestatakse, et IT-komponendi haldamiseks vajalikud oskused ja kvalifikatsioon oleks mitmel töötajal.
b. Koolitustel käsitletavad teemad katavad vähemalt järgmist:
   - tüüpkonfiguratsioonid ja infoturbe tugevdamine (ingl *hardening*);

- kasutatavate IT-komponentide ja haldustööriistade spetsiifilised turvaseaded;
- haldustööriistade tüüpsed veaolukorrad ja nende lahendamine;
- IT-halduse protsesside vahelised seosed ja liidestused.

c. Uute IT-komponentide soetamisel kavandatakse koolitused asjakohaste IT-halduse protseduuride omandamiseks.

OPS.1.1.1.M17 IT-halduse korraldamine avariiolukorras

a. On määratletud tingimused, mille täitumisel rakendub IT-halduses avarii korral tegutsemise kord.

b. IT-süsteemide pikaajalise katkestuse või avarii korral tegutsemiseks on koostatud IT-halduse avariiteatmik.

c. IT-halduse avariiteatmik määratleb, millised IT-komponendid on vajalikud organisatsiooni toimimiseks minimaalsel lubataval tasemel ning milliste IT-komponentide tugi tagatakse eelisjärjekorras.

d. Avarii korral tegutsemise juhised sisaldavad vähemalt järgmist:

- toibumisplaanid (ingl *disaster recovery plan*) avariiolukorrast väljumiseks;
- IT-komponentide taastamise juhised;
- tegevusjuhised kriitiliste äriprotsesside pikaajalise katkestuse mõju leevendamiseks.

OPS.1.1.1.M18 Väliste teenuseandjate kasutamine IT-halduses

a. IT-haldusega seotud väliste teenuseandjate tegevus on reguleeritud lepingute ja teenusetasemelepetega (SLA).

b. Teenuseandjaga on kokku lepitud suhtluskanalid ja teenuse üksikasjalik sisu. Eriti oluline on see siis kui kitsas teenusevaldkonnas kasutatakse mitmeid teenuseandjaid.

c. Teenuseandja tegevused fikseeritakse. Teenuseandja tegevuste vastavust kokkulepitule kontrollitakse regulaarselt.

OPS.1.1.1.M19 IT-komponentide regulaarne hooldus

a. IT-komponente hooldatakse regulaarselt. Teostatud hooldus- ja parendustööd dokumenteeritakse.

b. On määratud IT-komponendi hoolduse eest vastutavad isikud.

c. Hooldustööde läbiviimisel arvestatakse kehtestatud infoturbe nõudeid.

d. Väliste hooldusspetsialistide tööd on eelnevalt asjaosalistega kooskõlastatud. On määratud kontaktisik, kes kolmandate poolte hooldustegevusi koordineerib ning vajadusel kontrollib ja kinnitab tööde läbiviimise.

OPS.1.1.1.M20 IT-komponentide turvanõrkuste seire

a. IT-haldurid jälgivad ja analüüsivad regulaarselt infot kasutatavate IT-komponentide teadaolevate nõrkuste ning turvapaikade väljalaske kohta.

b. IT-komponente testitakse turvanõrkuste olemasolu suhtes. Iga IT-komponendi jaoks on määratud sobiv testimise ulatus, sügavus ja metoodika. Testimisel tuvastatud turvanõrkused registreeritakse.

c. Teadaolevad riistvara, operatsioonisüsteemide ja rakenduste nõrkused parandatakse esimesel võimalusel. Kui nõrkuse parandamiseks ei ole tootja väljastanud turvapaika, kasutatakse IT-süsteemi kaitseks täiendavaid turvameetmeid.

d. Ilma tootjapoolse toeta ja teadaolevate turvanõrkustega riistvara, operatsioonisüsteemid, rakendused ja teenused kõrvaldatakse kasutusest.

3.4 Kõrgmeetmed

OPS.1.1.1.M21 IT-halduse tööriistade kasutamise seire (C-I-A)

a. IT-komponentide haldustööriistade kasutamist jälgitakse organisatsiooniüleste turvaseire vahenditega.

b. Turvasündmuste reaalajaliseks ja keskseks tuvastamiseks on IT-halduse tööriistad integreeritud automatiseeritud sissetungituvastuse süsteemi (ingl *intrusion detection system*, IDS) seireandmestikuga.

OPS.1.1.1.M22 Automatiseeritud turvatestimine (C-I-A)

a. Turvanõrkuste avastamiseks testitakse IT-komponente regulaarselt automatiseeritud testimistööriistadega.

b. Nõrkuseotsingu (ingl *vulnerability scanning*) tulemused logitakse automaatselt ning need on kättesaadavad teistele asjakohastele tööriistadele.

c. Kriitilise turvanõrkuse avastamisel saadetakse volitatud töötajatele automaatteavitus.

OPS.1.1.1.M23 IT-komponentide läbistustestimine (C-I-A)

a. Organisatsiooniülese turvatestimise kontseptsiooni alusel viiakse läbi IT-komponentide regulaarset läbistustestimist (ingl *penetration testing*).

OPS.1.1.1.M24 IT-halduse protseduuride detailne logimine (C-I-A)

a. Kõik IT-halduse protseduurid logitakse jälgitavalt ja tõendatavalt.

OPS.1.1.1.M25 IT-halduse tööriistade autonoomsuse tagamine (C-I-A)

a. IT-halduse tööriistu on võimalik kasutada ka võrguühenduse katkestuse või mõne muu välise mõjutuse korral.

b. IT-halduse tööriistade omavahelised sõltuvused on võimalikult minimeeritud. Tööriistade konfigureerimisel välditakse olukordi, mille puhul ühe tööriista rike põhjustab häireid teise tööriista toimimises.

OPS.1.1.1.M26 IT-komponentide ennetav hooldus (I-A)

a. IT-komponentide hooldused plaanitakse ja viiakse läbi vähendatud ajavahemike järel, ennetades sellega võimalike tõrgete teket.

4 Lisateave

Lühend	**Publikatsioon**
[ITIL]	The Information Technology Infrastructure Library (ITIL) framework, https://www.axelos.com/certifications/itil-service-management
[ISO]	EVS-ISO/IEC 20000, Infotehnoloogia.Teenusehaldus

OPS.1.1.2 IT-süsteemide haldus

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed IT-süsteemide ja võrkude turvaliseks halduseks. IT-süsteemide haldamiseks on vaja IT-süsteemis eeliskontot. Haldustoimingute tulemusena võib muutuda hallatavate IT-komponentide konfiguratsioon.

1.2 Vastutus

IT-süsteemide halduse meetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Personaliosakond.

1.3 Piirangud

Moodulis on esitatud IT-süsteemide halduse üldmeetmed. Pääsuõiguste haldust käsitletakse moodulis ORP.4 *Identiteedi- ja õiguste haldus*, muudatuste haldust käsitletakse moodulis OPS.1.1.3 *Paiga-ja muudatusehaldus*. IT-süsteemide kaughaldust käsitletakse moodulis OPS.1.2.5 *Kaughooldus.*

IT-halduse turvet aitavad tagada meetmed moodulitest NET.1.2 *Võrguhaldus* ja OPS.1.1.7 *Süsteemihaldus*.

Kolmandate poolte haldusülesannete täitmist käsitlevad moodulid OPS.2.3 *Väljasttellimine* ja OPS.3.2 *Teenuseandja infoturve*. IT-süsteemide haldust veaolukorras käsitletakse mooduligrupis DER.2 *Turvaintsidentide haldus.*

IT-halduse korraldamise üldiseid aspekte käsitletakse moodulis OPS.1.1.1 *IT-haldus üldiselt*.

2 Ohud

2.1 Kohustuste reguleerimatusest tingitud probleemid

Kui IT-süsteemide halduse ülesanded (nt kavandamise, installimise, dokumenteerimise, paigahalduse või järelevalve osas) pole selgelt määratud või kui IT-süsteemide halduse kord ei ole töötajatele teada või arusaadav, võivad turbe jaoks olulised tegevused jääda ellu viimata

2.2 Puudulik dokumentatsioon

Kui dokumenteeritud teave IT-komponentide kohta ei vasta tegelikule olukorrale, on raskendatud haldustoimingute korrektne plaanimine ja teostus. Eelnevad konfiguratsioonimuudatused võivad kaotsi minna. Haldustööde käigus ilmnenud ootamatud asjaolud võivad oluliselt pikendada toimingute läbiviimise aega. Halvemal juhul võib väär konfiguratsioon põhjustada turvaintsidendi.

2.3 Eeliskasutaja õiguste kuritarvitus

Dokumentidele ja andmebaasis asuvatele andmetele juurdepääsu omavad isikud võivad oma suuremaid õigusi enda või kõrvaliste isikute huvides ära kasutada. Kui organisatsioonist lahkunud IT-halduril on jäänud kasutajaõigused korrektselt eemaldamata, võib ta tehtud

eksimust kuritarvitada. IT-haldurit võidakse andmetele juurdepääsu saamise nimel survestada või muul viisil mõjutada.

2.4 Tundliku teabe leke

Kui IT-süsteemidega seotud tundlik teave (nt IT-komponentidele juurdepääsuinfo või IT-komponentide konfiguratsioonid) ei ole piisavalt kaitstud, võib teave sattuda volitamata isikute kätte, kellel on võimalus seda manipuleerida või kasutada organisatsiooni IT-süsteemide vastu suunatud rünnete kavandamiseks.

2.5 Pädevuse puudumine

Sageli on keerulise IT-süsteemi haldamise oskused ja vajalikud teadmised ainult ühel IT-halduril. Kui talle ei ole vastava väljaõppega asendajat, võib IT-halduri lahkumise korral tekkida probleeme IT-süsteemi nõuetekohase ja turvalise töö tagamisega. Probleeme IT-süsteemide halduses võib põhjustada ka pädevate töötajate haigestumine või ette kavandamata töölt eemalviibimine.

2.6 Haldusvahendite ebapiisav kaitse

Rünnet IT-süsteemile lihtsustavad IT-halduri poolt IT-süsteemi konfigureerimisel tehtud hooletusvead. IT-süsteemi kaitseks mõeldud turvameetmed võivad jääda rakendamata IT halduri mugavuse või mõne muu põhjuse tõttu. Näiteks kasutatakse IT-halduseks samu tekstiredaktoreid või SSH-kliente, mida kasutatakse ka teiste tööülesannete tarbeks. Vähene turvateadlikkus, haldurite ajanappus ja protseduuride puudumine loovad nõrkusi, mida ründaja saab kergelt ära kasutada.

2.7 IT-süsteemi halduse vead

IT-süsteemi haldustoimingute läbiviimisel ei saa kunagi välistada IT-halduri tehtud inimlikku eksimust. Nt võib IT-haldur omavahel segi ajada lahtiolevad konsooliaknad ja sisestada vale käsurea. Vigasel haldustoimingul võivad olla kaugeleulatuvad negatiivsed tagajärjed.

2.8 IT-süsteemide töö häirimine

Haldustoimingute läbiviimine mõjutab tavaliselt IT-süsteemide tööd. Kui IT-süsteemide halduse toiminguid tehes ei arvestata nende mõju samaaegsele IT-süsteemide kasutamisele ja toiminguid ei ajastata töövälisele ajale, võidakse äriprotsessi olulisel määral häirida.

3 Meetmed

3.1 Elutsükkel

Kavandamine

OPS.1.1.2.M2 IT-haldurite asendamise kord

OPS.1.1.2.M7 IT-halduri kohustuste määramine

OPS.1.1.2.M21 IT-süsteemide halduse rollide määramine

OPS.1.1.2.M23 IT-süsteemide halduse rollide ja kasutajaõiguste määramise põhimõtted

OPS.1.1.2.M27 Alternatiivlahendus kesksele IT-süsteemide halduse tööriistale

Evitus

OPS.1.1.2.M5 IT-süsteemide halduse toimingute tõendamine

OPS.1.1.2.M16 Halduspääsu tehniline eraldamine

Käitus

OPS.1.1.2.M4 IT-haldurina töötamise lõpetamine

OPS.1.1.2.M6 Halduskontode turve

OPS.1.1.2.M8 Rakenduste haldus

OPS.1.1.2.M11 Haldustegevuste dokumenteerimine

OPS.1.1.2.M22 IT-süsteemide halduse eraldamine tavatöödest

OPS.1.1.2.M24 IT-süsteemide halduse toimingute kontrollimine

OPS.1.1.2.M25 IT-süsteemide halduse toimingute läbiviimise ajastamine

OPS.1.1.2.M26 IT-komponentide konfiguratsiooni varundamine

OPS.1.1.2.M28 IT-süsteemide haldustoimingute logimine

Lisanduvad kõrgmeetmed

OPS.1.1.2.M17 IT-haldurite nelja silma põhimõte

OPS.1.1.2.M18 Haldustoimingute täielik logimine

OPS.1.1.2.M19 Kõrgkäideldavuse tagamine

OPS.1.1.2.M29 IT-halduse tööriistade toimimise seire

OPS.1.1.2.M30 IT-halduse süsteemide integreerimine turvateabe halduse süsteemiga

3.2 Põhimeetmed

OPS.1.1.2.M2 IT-haldurite asendamise kord

a. IT-süsteemide halduritele on määratud asendajad, kellel on IT-süsteemide halduse jaoks sobiv kvalifikatsioon ja kes tunnevad konkreetseid süsteeme või on läbinud asjakohase koolituse.

b. Asendajate nimed ja kontaktandmed on dokumenteeritud.

c. On kehtestatud protseduur asendajale pääsuõiguste andmiseks.

d. Juurdepääs IT-süsteemide halduskontodele eriolukorras võimaldatakse ainult volitatud isikutele. Selleks vajalikke pääsuandmeid hoitakse volitatud isikutele kättesaadavas ja turvalises asukohas.

OPS.1.1.2.M4 IT-haldurina töötamise lõpetamine [personaliosakond]

a. IT-halduri vabastamisel tööülesannete täitmisest blokeeritakse kohe kõik temaga seotud personaliseeritud halduskontod ja eemaldatakse pääsuõigused (sh juurdepääsud välistele teenustele).

b. Lahkunud IT-haldurile teadaolevad paroolid, pääsukoodid ja salajased krüptovõtmed vahetatakse.

c. Kui töölt lahkunud IT-haldur oli määratud kolmandate poolte kontaktisikuks (nt lepinguga või halduskontaktina), siis teavitatakse asjaomaseid pooli tema lahkumisest ja määratakse uus kontaktisik.

d. Meetmeid rakendatakse ka juhul, kui IT-halduri ülesanded olid määratud ettevõttevälisele isikule.

OPS.1.1.2.M5 IT-süsteemide halduse toimingute tõendamine

a. Igal IT-halduril ja IT-halduri asendajal on personaalne eeliskonto (ingl *privileged account*), mida ta kasutab üksnes haldustoiminguteks.

b. Haldustoiminguid tehakse üksnes personaalselt määratud halduskontoga.

c. Kõik haldustoimingud (sh mida tehti, millal ja kelle poolt) on tagantjärele tuvastatavad.

OPS.1.1.2.M6 Halduskontode turve

a. Halduskontosid kaitstakse sobivate autentimismehhanismidega. Kui selleks kasutatakse paroole, siis samu paroole ei kasutata muudes haldustsoonides. Suurema kaitsetarbe korral on rakendatud mitmikautentimine (ingl *multifactor authetication*).

b. Igapäevaste töökohustuste täitmiseks on IT-halduril tavaõigustega kasutajakonto, eeliskontot igapäevaste töökohustuste täitmiseks ei kasutata.

c. Juurdepääs IT-süsteemi haldusliidesele ja haldusfunktsioonidele on ainult IT-halduritel.

d. Kui IT-süsteemi halduseks ei kasutata lokaalset konsooli, on halduskontode kasutamine kaitstud turvaliste võrguprotokollide (nt SSH, TLS) ja piisava tugevusega krüpteerimisega.

OPS.1.1.2.M21 IT-süsteemide halduse rollide määramine

a. On määratud IT-süsteemide halduse rollid. Rollide määramisel on arvestatud IT-süsteemist tulenevaid vajadusi ja kasutajaõiguste minimaalsuse põhimõtet.

b. Rollide määramisel on arvestatud IT-süsteemi kaitsetarvet, nt tuleks kaaluda operatsioonisüsteemi ja rakenduste halduse rollide eraldamist.

OPS.1.1.2.M22 IT-süsteemide halduse eraldamine tavatöödest

a. IT-halduse tööriistad on selgelt eristatavad tavatööks kasutatavatest tööriistadest.

b. IT-halduse rakendusi ei kasutada peale IT haldustoimingute teiste tööülesannete täitmiseks.

c. IT-halduseks kasutatavad kasutajakontod ning sisselogimiseks vajalikud paroolid on erinevad muudest kontodest ja paroolidest.

3.3 Standardmeetmed

OPS.1.1.2.M7 IT-halduri kohustuste määramine

a. Tööülesannete jaotamisel mitme IT-halduri vahel on kõik tööülesanded kaetud ja vastusalad selgelt eristatud.

b. Igale IT-süsteemile ja rakendusele on määratud vastutav haldur.

c. IT-halduri kohustuste määramisel on arvestatud rollide lahususe nõuet. Halduri rolli ei saa teatud rollidega (nt IT-audiitor) ühildada.

d. IT-halduri õigusi ja kohustusi ajakohastatakse regulaarselt IT-halduri ametijuhendis.

OPS.1.1.2.M8 Rakenduste haldus

a. Rakenduse- ja süsteemihaldurite vaheline ülesannete jaotus on määratletud ja dokumenteeritud.

b. Võimalikud kokkupuutekohad rakenduste ja IT süsteemide halduse eest vastutavate isikute tööjaotuses on omavahel kooskõlastatud (nt töötajate asendamise korral).

c. Kui IT-halduril on vajalik sekkuda rakenduse käitamisse (nt versioonivahetusel), kooskõlastatakse see eelnevalt rakenduse kasutajatega, arvestades kasutajate vajadusi.

OPS.1.1.2.M11 Haldustegevuste dokumenteerimine

a. Kõik halduse käigus tehtud IT-süsteemi muudatused dokumenteeritakse. Dokumentatsioonist on arusaadav, milliseid muudatusi ja millal on tehtud, kes muudatused tegi ning mis on muudatuse põhjus.

b. Teave muudatuste kohta peab IT-halduri eemaloleku korral olema kättesaadav ka asendajatele.

OPS.1.1.2.M16 Halduspääsu tehniline eraldamine

a. Haldusliidestele juurdepääs on eraldatud tehniliste meetmetega (nt lubatud ühest konkreetsest võrgusegmendist).

b. Haldusrühma mittekuuluvatel isikutel haldusliidestele juurdepääs puudub.

c. Halduspääs teises turvatsoonis asuvale IT-süsteemile on loodud vastava turvatsooni hüppeserveri kaudu. Muud juurdepääsuvõimalused teistest süsteemidest või võrgusegmentidest on tõkestatud.

d. Haldusliidesed ei tohi olla juurdepääsetavad otse välisest võrgust.

OPS.1.1.2.M23 IT-süsteemide halduse rollide ja kasutajaõiguste määramise põhimõtted

a. Organisatsioon on kehtestanud IT-süsteemide halduse rollide ja kasutajaõiguste määramise põhimõtted.

b. IT-süsteemide halduse rollide ja kasutajaõiguste määramise põhimõtted sätestavad, kuidas toimub rolli:

- taotlemine;
- loomine;
- kaasnevate õiguste määramine;
- sidumine konkreetse isikuga.

OPS.1.1.2.M24 IT-süsteemide halduse toimingute kontrollimine

a. Enne IT-süsteemi haldustoimingutega alustamist veendutakse, et kavandatu vastavad püstitatud lähteülesandele.

b. Enne IT-süsteemi haldustoimingutega alustamist kontrollitakse, kas kavandatud toimingud ei mõjuta negatiivselt IT-halduse tööriistade kasutamist.

c. Pärast IT-süsteemi haldustoimingute lõpetamist veendutakse, kas hallatava IT-komponendi konfiguratsioon vastab soovitud sihtseisundile.

d. Kõrgendatud turbevajadusega IT-süsteemi haldustegevusi kontrollib tegevuste läbiviijast erinev isik.

OPS.1.1.2.M25 IT-halduse toimingute läbiviimise ajastamine

a. IT- halduse toimingud viiakse läbi sellest eelnevalt IT-süsteemi kasutajaid ette teavitades ja/või kavandatud hooldusaknas määratud ajaperioodi jooksul.

OPS.1.1.2.M26 IT-komponentide konfiguratsiooni varundamine

a. Enne IT-komponendi haldustoimingute alustamist veendutakse, et IT-komponendi kehtivast konfiguratsioonist on olemas varukoopia.

b. Enne võimalike negatiivsete tagajärgedega haldustoimingut varundatakse IT-komponendi konfiguratsioon täiendavalt vahetult enne toiminguga alustamist.

OPS.1.1.2.M27 Alternatiivlahendus kesksele IT-halduse tööriistale

a. Keskset IT-halduse tööriista on vajadusel võimalik asendada asjakohastele haldusvõrkudele juurdepääsu tagamisega läbi turvalise hüppeserveri (ingl *jump server*).

b. Kui hüppeserverit ei kasutata, tagatakse haldustoimingute läbiviimiseks IT-komponendile otsene füüsiline juurdepääs.

OPS.1.1.2.M28 IT-süsteemide haldustoimingute logimine

a. Kõik halduskontoga tehtud tegevused ja pääsukatsed logitakse. Logitud andmete terviklust kaitstakse.

b. IT-süsteemide haldustoimingute logisid säilitatakse piisavalt pika ajavahemiku jooksul.

3.4 Kõrgmeetmed

OPS.1.1.2.M17 IT-haldurite nelja silma põhimõte (C-I)

a. Juurdepääs turvakriitilistele süsteemidele on reguleeritud nii, et selleks on alati vaja kahte töötajat (nt halduskonto parooli jaotamisega kaheks osaks, millest kumbki pool on teada ainult ühele IT-halduritest).

b. Haldusprotseduuride läbiviimisel täidab üks IT-haldur ettenähtud haldusülesandeid ja teine kontrollib tema tegevust.

OPS.1.1.2.M18 Haldustoimingute täielik logimine (C-I)

a. Turvakriitilistes süsteemides logitakse lisaks IT-halduri tegevustele ka kõik IT-süsteemiülema rakendatud käsud ja käivitatud funktsioonid.

b. IT-süsteemiülematel ei ole salvestatud logifailide muutmise ega kustutamise õigusi.

c. Logifaile säilitatakse terviklikult ning kaitsetarbele vastava ajavahemiku jooksul.

OPS.1.1.2.M19 Kõrgkäideldavuse tagamine (A)

a. On tagatud IT-süsteemide haldustööriistade liiasus.

b. IT-süsteemi haldustööriista võimaliku rikke korral on IT-süsteemide haldustoiminguid võimalik läbi viia ilma oluliste piiranguteta.

OPS.1.1.2.M29 IT-süsteemide halduse tööriistade toimimise seire (A)

a. IT-süsteemide halduse tööriistadele on kehtestatud käideldavuse nõuded.

b. IT-halduse tööriistade käideldavusparameetreid seiratakse regulaarselt, hälvete ilmnemisel teavitatakse vastutavat IT-haldurit.

OPS.1.1.2.M30 IT-süsteemide halduse integreerimine turvateabe halduse süsteemiga (C-I-A)

a. IT-süsteemide haldustoimingute logimine on liidestatud turvateabe ja -sündmuste halduse (ingl *security information and event management*, SIEM) süsteemiga.

OPS.1.1.3 Paiga- ja muudatusehaldus

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed organisatsiooni paiga- ja muudatusehalduse protseduuride kohaldamiseks, juhtimiseks ja optimeerimiseks.

1.2 Vastutus

Paiga- ja muudatusehalduse meetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Vastutav spetsialist.

1.3 Piirangud

Moodul käsitleb tarkvarauuendite paigaldamist ning muudatuste halduse infoturbega seotud aspekte. Konkreetsete IT-süsteemide uuendamist käsitletakse mooduligruppides SYS ja APP. Paikade ja muudatuste testimist ja käidukeskkonda paigaldamist käsitletakse moodulis OPS.1.1.6 *Tarkvara testimine ja kasutuselevõtt.* Tarkvaraarenduse käigus tehtavaid muudatusi kirjeldatakse moodulis CON.8 *Tarkvaraarendus*.

2 Ohud

2.1 Puudulikult kehtestatud kohustused

Ebaselged, määramata või kattuvad töökohustused paiga- ja muudatusehalduses põhjustavad protsessi aeglustumist ja eksimusi. Paikade ja muudatuste ennatlik kinnitamine ilma neid testimata ja kõiki aspekte arvestamata võib IT-süsteemide turvalisust märkimisväärselt mõjutada. Kui turvapaiku ei paigaldata või seda tehakse liiga hilja, võib see mõjutada IT-süsteemide konfidentsiaalsust ja terviklust.

2.2 Puudulik teabevahetus muudatuste haldamisel

Kui paiga- ja muudatusehaldus ei ole organisatsioonis reguleeritud ja asjaomased isikud piisaval määral ei suhtle, võib see põhjustada valesid otsuseid või muudatuste paigaldamisega hilinemist. Puuduliku teabevahetuse korral muutub IT-haldus ebatõhusaks ja tekivad turvanõrkused. Eelnevalt teadvustamata muudatus võib tekitada tööseisaku, kuna kasutaja ei oska muutunud olukorras tegutseda.

2.3 Äriprotsessidega mittearvestamine

Kontrollimatud muudatused võivad ohustada äriprotsesside toimimist ja põhjustada mõjutatud IT-süsteemides ulatuslikke tõrkeid. Kui muudatust pole kavandatud ja testitud koos asjaomaste põhiüksustega, võidakse hinnata muudatuste mõju, prioriteetsust ja oodatavat turvataset valesti. Tulem ei pruugi vastata tegelikele ärivajadustele.

2.4 Piiratud ressursid paiga- ja muudatusehalduses

Kui paiga- ja muudatusehalduseks puuduvad sobivad töötajad, võib IT-üksuse ja äriüksuste vaheline koostöö kahjustuda. Ressursside puudumisel ei ole võimalik luua nõuetekohast test- ja käidukeskkonna taristut. Töötajate nappus muutub eriti oluliseks juhtudel, kui tegutseda tuleb viivitamata, näiteks avariipaikade paigaldamisel.

2.5 Probleemid paikade ja muudatuste automaatse paigaldamisega

Paigahaldustarkvara tsentraalsel kasutamisel võidakse väljastada kogu IT-süsteemi ulatuses vigaseid uuendeid, põhjustades ulatuslikke turvaprobleeme.

Kui IT-seadmed ei ole kohtvõrgus püsivalt kättesaadavad, võib kindlal ajavahemikul turvapaiku paigaldav süsteem jätta osad seadmed ajakohastamata.

2.6 Puudulikud taastevõimalused paiga- ja muudatusehalduses

Kui paikasid või muudatusi paigaldatakse ilma taastevõimalust ette nägemata, ei ole võimalik vea ilmnedes IT-süsteemi kiiresti parandada. Sama oht on ka siis, kui tarkvara taasteprotseduurid ei ole tõhusad või need kõigil juhtudel ei toimi.

2.7 Paikade ja muudatuste prioriteetsuse väär hindamine

Muudatuste prioriteetsuse määramisega eksimisel võidakse olulised paigad installida alles viimases järjekorras, mistõttu seonduv turvarisk püsib kauem. Paiga- ja muudatusehalduse tööriistas võib esineda vigu, mis põhjustavad paiga või muudatuse kohta puuduliku või vale teabe esitamist.

2.8 Andmete ja tööriistade manipuleerimine muudatuste haldamisel

Kui ründaja suudab tsentraalsed paiga- ja muudatusehalduse tööriistad üle võtta, saab ta levitada manipuleeritud tarkvara ühekorraga paljudesse IT-süsteemidesse. Kui neid tööriistu haldab väline partner, siis saab rünnet algatada ka partneri võrgust.

3 Meetmed

3.1 Elutsükkel

Kavandamine

OPS.1.1.3.M1 Paiga- ja muudatusehalduse kord

OPS.1.1.3.M2 Vastutuse määramine

OPS.1.1.3.M5 Muutmistaotluste käsitlus

OPS.1.1.3.M8 Paiga- ja muudatusehalduse tööriistade turvaline rakendamine

Evitus

OPS.1.1.3.M9 Uue riistvara testimise ja kasutuselevõtu protseduurid

OPS.1.1.3.M11 Infotöötluse pidev dokumenteerimine

Käitus

OPS.1.1.3.M3 Automaatuuenduste turvaline seadistus

OPS.1.1.3.M6 Muudatuste kooskõlastamine

OPS.1.1.3.M7 Muudatusehalduse sobitamine äriprotsessidega

OPS.1.1.3.M10 Tarkvarapakettide tervikluse ja autentsuse tagamine

OPS.1.1.3.M15 IT-süsteemide regulaarne uuendamine

Lisanduvad kõrgmeetmed

OPS.1.1.3.M12 Muudatusehalduse tööriistade kasutamine

OPS.1.1.3.M13 Muudatuste tulemuslikkuse hindamine

3.2 Põhimeetmed

OPS.1.1.3.M1 Paiga- ja muudatusehalduse kord [vastutav spetsialist]

a. IT-komponentide, tarkvara ja konfiguratsiooniandmete muudatuste läbiviimiseks on kehtestatud paiga- ja muudatusehalduse kord.

b. Paiga- ja muudatusehalduse kord reguleerib, kuidas tarkvara paikade (ingl *patch*) ja uuendite (ingl *update*) paigaldamist plaanitakse, kooskõlastatakse ja dokumenteeritakse.

c. Paikasid ja uuendeid testitakse enne nende rakendamist (vt OPS.1.1.6 *Tarkvara testimine ja kasutuselevõtt*).

d. Paikade ja uuendite paigaldamise ebaõnnestumise puhuks on koostatud muudatuste tagasivõtmise protseduur.

e. Suuremate muudatuste korral kaasatakse muudatuse kavandamisse infoturbejuht. Taotletava turvataseme säilimine tagatakse nii muudatuse tegemise ajal kui ka pärast muudatuse elluviimist.

OPS.1.1.3.M2 Vastutuse määramine

a. Kõigis äriprotsessides on määratud paiga- ja muudatusehalduse eest vastutajad.

b. Paiga- ja muudatusehalduse eest vastutaja klassifitseerib ja aktsepteerib muutmistaotlused (ingl *change request*) ja koordineerib muudatuste läbiviimist.

c. Keeruka IT-taristuga organisatsioonis toetab vastutajat kindla aja tagant kogunev muutenõukogu (ingl *change advisory board*), kuhu peale muudatuste tehnilise rakendamisega seotud isikute kuuluvad ka organisatsiooni põhiüksuste esindajad.

OPS.1.1.3.M3 Automaatuuenduste turvaline seadistus

a. Uute toodete kasutuselevõtul kontrollitakse, millised uuendusmehhanismid neis on ja kuidas neid konfigureeritakse. Automaatuuendused seadistatakse vastavalt organisatsiooni paigahalduse nõuetele.

b. Vajadusel tõkestatakse uuendite päringud avalikust uuendusserverist ja blokeeritakse uuendite installimise automaatne käivitus.

c. Võimalusel võetakse kasutusele organisatsioonisisene uuendusserver (nt Windows Server Update Services, WSUS). Uuendusserver suhtleb sel juhul otse tootja serveritega ja laadib soovitud uuendid paigaldamiseks sobival hetkel.

d. Mobiilsetele seadmetele, mis võivad tihti asuda väljaspool ettevõtte võrku, laetakse turvapaigad otse tootja uuendusserverist ning võimalikult kiiresti pärast uuendi ilmutamist.

OPS.1.1.3.M15 IT-süsteemide regulaarne uuendamine

a. Põhivara (ingl *firmware*), operatsioonisüsteeme ja rakendusi uuendatakse regulaarselt. Uuendamine viiakse läbi võimalikult kiiresti pärast turvauuendi ilmutamist ja testimist.

b. Paikasid ja muudatusi paigaldatakse vastavalt prioriteetsusele ja rakendamise kiireloomulisusele.

c. Uuendite paigaldamise järgselt kontrollitakse, kas kõik vajalikud seadmed ja rakendused on uuendused saanud.

d. Kui turvauuend otsustatakse mitte paigaldada, siis vastav otsus ja mittepaigaldamise põhjendus dokumenteeritakse.

e. Tootja tarkvaratoe lõppemisel analüüsitakse, kuidas edasiste turvapaikade puudumine mõjutab seadmete või rakenduste turvalist kasutamist. Ebaturvalised seadmed või rakendused kõrvaldatakse kasutusest.

3.3 Standardmeetmed

OPS.1.1.3.M5 Muutmistaotluste käsitlus [vastutav spetsialist]

a. Muutmistaotlusi (ingl *Request for Changes, RfC*) esitatakse, registreeritakse ja dokumenteeritakse vastavalt paiga- ja muudatusehalduse korrale.

b. Muudatuste kavandamisel hinnatakse, kuidas võib muudatus mõjutada organisatsiooni toimimist, määratakse tehnilised ja inimressursid ning teostamise tähtajad.

c. Muudatuse läbiviimise eest vastutaja kontrollib, kas muutmistaotluse juures on piisavalt arvestatud infoturbe aspekte.

OPS.1.1.3.M6 Muudatuste kooskõlastamine

a. Muudatuste kooskõlastusprotsessi on kaasatud kõik asjassepuutuvad sihtrühmad, sh infoturve.

b. Muudatusega hõlmatud sihtrühmadel on võimalik muudatuste kohta oma arvamust avaldada, et vältida sihtrühma seisukohalt soovimatuid muudatusi.

c. Aegkriitilisi muudatusi on võimalik kinnitada lihtsustatud korras.

OPS.1.1.3.M7 Muudatusehalduse sobitamine äriprotsessidega

a. Muudatuse kavandamisel arvestatakse eelkõige organisatsiooni põhitegevuslikke vajadusi ja mõju äriprotsessidele, sh infoturbe seisukohast.

b. Kõiki muudatusest mõjutatavaid üksusi teavitatakse aegsasti eelseisvatest muudatustest.

c. Muudatuse tegemiseks valitakse aeg nii, et äriprotsesse võimalikult vähe häiritaks. Kui äriprotsessi katkestamine on vältimatu, arvestatakse otsustamisel katkestuse võimalike mõjudega.

d. Organisatsiooni juhtkonnal on õigus vajadusel riist- ja tarkvara muudatuste prioriteete ja planeeritud täitmistähtaegu muuta.

OPS.1.1.3.M8 Paiga- ja muudatusehalduse tööriistade turvaline rakendamine

a. Paiga- ja muudatusehalduse tööriistade valimisel võetakse arvesse erinevate tarkvaraplatvormide toetust, uuendite väljastamise sagedust ja nende verifitseerimist, konfiguratsiooni paindlikkust ja muudatuste tagasipööramise võimekust.

b. On kehtestatud paiga- ja muudatusehalduse tööriistade turvanõuded, mis käsitlevad tööriistade turvalist haldust ja logimise, andmevarunduse ning avariivalmenduse nõudeid.

OPS.1.1.3.M9 Uue riistvara testimise ja kasutuselevõtu protseduurid

a. Uut riistvara testitakse enne kasutuselevõttu spetsiaalselt selleks otstarbeks loodud, käidukeskkonnast eraldatud testkeskkonnas.

b. Testimise käigus kontrollitakse toote funktsionaalsust, ühilduvust ja soovimatute kõrvaltoimete puudumist. Testimiseesmärgid valitakse sõltuvalt riistvara iseloomust.

c. Riistvara testimistulemused ja kasutuselevõtuks kinnitamise tulemused dokumenteeritakse.

d. Kui testimise ja kinnitusprotseduuri läbimisest hoolimata avastatakse kasutamisel riistvara vigu, algatatakse veaparandusprotsess.

OPS.1.1.3.M10 Tarkvaratoodete tervikluse ja autentsuse tagamine

a. Tarkvara ja selle uuendeid hangitakse ainult teadaolevalt usaldusväärsetest allikatest.

b. Enne paketi installimist kontrollitakse selle autentsust näiteks kontrollkoodi (ingl *checksum*) või signatuuri põhjal.

c. Organisatsioonis on olemas tervikluse ja autentsuse kontrolliks vajalikud kontrollivahendid.

OPS.1.1.3.M11 Infotöötluse pidev dokumenteerimine

a. Organisatsioonis on kehtestatud kord IT-süsteemides tehtud muudatuste dokumenteerimiseks.

b. Olemas on ajakohane dokumentatsioon IT-rakenduste ja IT-komponentide konfiguratsiooni, lisatud komponentide, kasutajate, andmevarunduse, avastatud ja kõrvaldatud rikete ja vigade ning teostatud hooldetoimingute kohta.

3.4 Kõrgmeetmed

OPS.1.1.3.M12 Muudatusehalduse tööriistade kasutamine (A)

a. Muudatusehalduse tööriista valimisel on arvestatud muudatuste paigaldamise jõudlusega ja võimekusega vea ilmnemisel taastada muudatuseelne olukord paralleelselt paljudes tööjaamades või serverites.

b. Paiga- või muudatusehalduse tööriist võimaldab paigaldamise vajadusel teadlikult katkestada. Uuendite paigaldamise katkestamist on eelnevalt testitud.

OPS.1.1.3.M13 Muudatuste tulemuslikkuse hindamine [vastutav spetsialist] (I-A)

a. Muudatuse tulemuslikkuse hindamiseks viiakse läbi muudatusejärgset olukorda muudatusele eelneva olukorraga võrdlev järeltestimine.

b. Järeltestimist teevad kasutajad, kes tunnevad organisatsiooni äriprotsesse, kehtivaid kvaliteedi- ja turvanõudeid ja oskavad tuvastada ning hinnata võimalikke vigu.

c. Järeltestimise tulemused dokumenteeritakse.

OPS.1.1.3.M14 Muudatuste sünkroniseerimine (C-I-A)

a. Paigad ja muudatused paigaldatakse kõigisse IT-süsteemidesse võimalikult kiiresti ja korraga.

b. On olemas protseduur ja vahendid, mis võimaldavad kontrollida muudatuste jõudmist kõigisse sihtkohtadesse.

c. Vältimatult hilinevad muudatused (nt mobiilsetes IT-süsteemides) tehakse esimesel võimalusel.

OPS.1.1.4 Kaitse kahjurprogrammide eest

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed kahjurprogrammide vastase kaitse korraldamiseks.

1.2 Vastutus

„Kaitse kahjurprogrammide eest“ meetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Kasutaja.

1.3 Piirangud

Spetsiifilised nõuded organisatsiooni konkreetsete IT-süsteemide kaitsmiseks kahjurprogrammide eest on esitatud asjakohastes SYS moodulites (nt SYS.2.2.3 *Windows 10 klient).*

Tuvastatud kahjurprogramme eemaldamist ja IT-süsteemide taastamist käsitletakse moodulites DER.2.1 *Turvaintsidentide käsitlus* ja DER.2.3 *Ulatuslike turvaintsidentide lahendamine*.

Kasutajate koolitust käsitletakse moodulis ORP.3 *Infoturbe teadlikkuse tõstmine ja koolitus*.

2 Ohud

2.1 Tarkvara nõrkused ja kahjurkoodi allalaadimine

Kui IT-süsteemid ei ole kahjurprogrammide vastu vajalikul määral kaitstud (nt paikade õigeaegse paigaldamise ja rakenduste turvalise konfigureerimisega), võib ründaja kasutada tarkvara nõrkusi kahjurkoodi paigaldamiseks. Ainuüksi kahjurveebisaidi külastamisest piisab brauseri või mõne installitud pistikprogrammi (nt *Java* või *Adobe Flash*) nõrkuse ärakasutamiseks ja IT-süsteemi nakatamiseks. Eriti ohustatud on IT-süsteemid, mida regulaarselt ei uuendata (nt paljud nutitelefonid).

2.2 Väljapressimine lunavaraga

Levinud kahjurvara (ingl *malware*) tüüp on lunavara (ingl *ransomware*), mis krüpteerib nakatatud IT-süsteemis asuvad andmed. Selleks kasutavad ründajad krüpteerimismeetodeid, kus dekrüpteerimine on võimalik ainult ründajale teadaoleva võtme abil. Võti avaldatakse alles pärast suure rahasumma ründajatele ülekandmist. Kui kahjurvara eest puudub tõhus kaitse ja kasutusele ei ole võetud täiendavaid meetmeid (nt andmevarundus), võib lunavararünne põhjustada suurt finants- ja mainekahju.

2.3 Siht- ja suhtlusründed

Sageli kasutatakse organisatsioonide ründamiseks kohandatud kahjurprogramme, mida viirusetõrjeprogrammid ei suuda veel tuvastada. Ründe käigus meelitatakse näiteks juhtivtöötajaid suhtlusründe (ingl *social engineering*) abil avama kahjulikke e-kirja manuseid. Kui ründajal on õnnestunud sellisel viisil üks arvuti nakatada, saab ta selle kaudu organisatsioonis oma tegevust laiendada.

2.4 Bottnetid

Kahjurprogrammide kaudu võivad organisatsiooni IT-süsteemides levida ka robotvõrgud ehk bottnetid (ingl *botnet*). Ründaja, kes kontrollib robotvõrgus tuhandeid arvuteid, võib robotvõrku kasutada erinevate eesmärkide täitmiseks, näiteks spämmi saatmiseks või teenusetõkestusründe käivitamiseks. Isegi, kui otsene negatiivne mõju organisatsiooni teenuste ja IT-süsteemide käideldavusele ja terviklusele puudub, on tegemist seaduserikkumisega, millega kaasneb mainekahju.

2.5 Tootmissüsteemide ja esemevõrgu seadmete nakatamine

Peale tavapäraste IT-süsteemide rünnatakse kahjurprogrammidega üha enam ka seadmeid, mis esmapilgul ei tundu tavapärase sihtmärgina. Näiteks võib ründaja spioneerimiseks nakatada Interneti kaudu juurdepääsetava valvekaamera või bottneti osana kasutada võrguga ühendatud nutivalgusteid, kui need ei ole kahjurvara eest piisavalt kaitstud. Tööstuslikke juhtimissüsteeme kahjurprogrammiga manipuleerides võib ründaja rikkuda vara või tekitada pikaajalisi töökatkestusi.

3 Meetmed

3.1 Elutsükkel

Kavandamine

OPS.1.1.4.M1 Kahjurprogrammide tõrje kontseptsioon

OPS.1.1.4.M7 Kasutajate teadlikkuse suurendamine

Soetamine

OPS.1.1.4.M3 Kahjurvaratõrje tarkvara valimine lõppseadmetele

Evitus

OPS.1.1.4.M2 Süsteemikohaste turvamehhanismide kasutamine

OPS.1.1.4.M5 Kahjurvaratõrje tarkvara rakendamine

Käitus

OPS.1.1.4.M6 Viirusetõrjeprogrammide ja viiruse käekirja andmestike ajakohastamine

OPS.1.1.4.M9 Kahjurprogrammiga nakatumisest teatamine

Lisanduvad kõrgmeetmed

OPS.1.1.4.M10 Spetsiaalse analüüsikeskkonna kasutamine

OPS.1.1.4.M11 Mitme skaneerimismootori rakendamine

OPS.1.1.4.M12 Andmekandjalüüside rakendamine

OPS.1.1.4.M13 Ebausaldusväärsete failide käitlus

OPS.1.1.4.M14 Infoturbe toodete valimine ja kasutuselevõtt sihtrünnete tõrjeks

3.2 Põhimeetmed

OPS.1.1.4.M1 Kahjurprogrammide tõrje kontseptsioon

a. On koostatud kontseptsioon, mis määrab, milliseid IT-süsteeme kahjurprogrammide eest kaitstakse ja kuidas.

b. IT-süsteemide kasutamist välditakse seni, kuni neid on võimalik kahjurvara eest usaldatavalt kaitsta.

c. Kahjurprogrammide tõrje kontseptsiooni vaadatakse üle regulaarselt, vajadusel kontseptsioon uuendatakse.

OPS.1.1.4.M2 Süsteemikohaste turvamehhanismide kasutamine

a. On teada, millised turvamehhanismid on kasutatavatesse IT-süsteemidesse lisatud.

b. Kõik IT-süsteemi turvamehhanismid on kasutusele võetud, välja arvatud juhul, kui on olemas vähemalt samaväärne asendusmehhanism või kui turvamehhanismi mitterakendamiseks on mõjuvad põhjused.

c. Turvamehhanismide teadliku mitterakendamise juhud dokumenteeritakse koos asjakohase põhjendusega.

OPS.1.1.4.M3 Kahjurvaratõrje tarkvara valimine lõppseadmetele

a. Kahjurvaratõrje tarkvara valimisel on lähtutud kasutatavatest platvormidest, muudest olemasolevatest turvamehhanismidest, kahjurvaratõrje tarkvara eeldatavast jõudlusest ja avastusvõimest.

b. Lõppseadmetes kasutatakse ärikasutuseks kohandatud, kehtiva hooldus- ja tugiteenusega tooteid.

c. Kahjurvaratõrje tarkvara valimisel arvestatakse andmekaitse- ja konfidentsiaalsusnõudeid.

OPS.1.1.4.M5 Kahjurvaratõrje tarkvara rakendamine

a. Kahjurvaratõrje tarkvara on enne kasutuselevõtuks kinnitamist testitud.

b. Kahjurvaratõrje tarkvara on konfigureeritud vastavalt kasutuskeskkonnale.

c. Kui mõni toote turvafunktsioon on välja lülitatud, peab olema selleks dokumenteeritud põhjendus.

d. Kasutaja õigused teha kahjurvaratõrje tarkvara turvaseadetes muudatusi on piiratud.

OPS.1.1.4.M6 Viirusetõrjeprogrammide ja viiruse käekirja andmestike ajakohastamine

a. Viirusetõrjeprogrammi ja viiruse käekirja (ingl *virus signature*) andmestikke uuendatakse regulaarselt, vastavalt tarkvara valmistaja soovitustele.

b. Viirusetõrjeprogrammi uuenduste korral tutvutakse muudatuste dokumentatsiooniga ning vajadusel muudetakse tarkvara konfiguratsiooni.

OPS.1.1.4.M7 Kasutajate teadlikkuse suurendamine [kasutaja]

a. Kasutajatele selgitatakse regulaarselt kahjurvaraga seotud võimalikke ohte.

b. Kasutajatele on edastatud juhised kahjurvaraga seotud ohtude vältimiseks.

c. Kasutajad teavad, et ebausaldusväärsetest allikatest pärinevaid faile ei tohi avada.

d. Kasutajad on kohustatud kahjurprogrammiga nakatumisest või nakatumiskahtlusest teavitama organisatsiooni määratud kontaktisikut.

3.3 Standardmeetmed

OPS.1.1.4.M9 Kahjurprogrammiga nakatumisest teatamine

a. Kahjurprogrammi avastamisel edastab kahjurvaratõrje rakendus sündmusest teate kesksesse käsitluskohta ja blokeerib nakatatud programmi.

b. Vastutav töötaja otsustab, kas kahjurprogrammi teade võib tähendada turvaintsidenti ja millised on edasised tegevused.

c. On loodud protseduur kahjurvaratõrje rakenduse sündmuseteadete ja hoiatuste käsitluseks.

d. On dokumenteeritud ja testitud tegevuskava kahjurprogrammide eemaldamiseks ja nakatuseelse olukorra taastamiseks.

3.4 Kõrgmeetmed

OPS.1.1.4.M10 Spetsiaalse analüüsikeskkonna kasutamine (C-I-A)

a. Nakatuskahtlusega failide automatiseeritud analüüsiks kasutatakse tunnustatud veebipõhiseid viiruskontrolli tööriistu.

b. Eesti riigiasutuste andmesidevõrgu kasutajad ja erasektori koostööpartnerid kasutavad e-kirjaga saabunud kahtlaste manuste ja teiste ebakindla päritoluga failide kontrollimiseks veebipõhist tööriista aadressil *irma.cert.ee*.

OPS.1.1.4.M11 Mitme skaneerimismootori rakendamine (C-I-A)

a. Suurema kaitsetarbega süsteemides on avastusvõime tõstmiseks rakendatud erinevaid skaneerimismootoreid kasutavad kahjurvaratõrje vahendid.

OPS.1.1.4.M12 Andmekandjalüüside rakendamine (C-I-A)

a. Enne väliselt osapoolelt saadud andmekandja ühendamist organisatsiooni IT-süsteemiga kontrollitakse andmekandjat selleks otstarbeks konfigureeritud arvutil.

OPS.1.1.4.M13 Ebausaldusväärsete failide käitlus (C-I-A)

a. Ebausaldusväärseid faile avatakse ainult selleks otstarbeks konfigureeritud, teistest IT-süsteemidest isoleeritud arvutis.

b. Kahtlaste failide sisu viiakse edasiseks töötluseks turvalisse vormingusse või prinditakse välja.

OPS.1.1.4.M14 Infoturbe toodete valimine ja kasutuselevõtt sihtrünnete tõrjeks (C-I-A)

a. Suurema kaitsetarbe korral valitakse kasutamiseks tavapärastest toodetest turvalisemad, täiendava kaitsefunktsionaalsusega tooted.

b. Enne kasutamiseks kinnitamist testitakse valitud toote turvatoimet ja ühilduvust ettevalmistatud testkeskkonnas.

OPS.1.1.5 Logimine

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed logiandmete turvaliseks kogumiseks, talletamiseks, analüüsimiseks ja nõuetekohaseks kõrvaldamiseks.

1.2 Vastutus

Logimise meetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Vastutav spetsialist.

1.3 Piirangud

Spetsiifiliste IT-süsteemide ja rakenduste logimist ja nende kaitset käsitletakse täiendavalt teemakohastes moodulites (nt operatsioonisüsteemi sündmuste logimist käsitletakse moodulites SYS.1.1 *Server üldiselt* ja SYS.2.1 *Klientarvuti üldiselt*). Logiandmete arhiveerimist käsitletakse moodulis OPS.1.2.2 *Arhiveerimine*. Isikuandmete käitlemise meetmed on esitatud moodulis CON.2 *Isikuandmete kaitse*. IT-süsteemide logide kasutamist turvaintsidentide avastamiseks ja käsitlemiseks kirjeldatakse moodulites DER.1 *Turvaintsidentide avastamine* ja DER.2 *Turvaintsidentide haldus*.

2 Ohud

2.1 Puuduv või piisamatu logimine

Kui IT-süsteemide konfigureerimisel on logimine jäetud aktiveerimata või logimine pole võimalik, jäävad turvasündmused registreerimata ja ründed tuvastamata. Rünnet ei tuvastata ka juhul, kui logimist rakendatakse, kuid logiandmeid ei analüüsita. Samuti jääb rünne tuvastamata, kui logiandmed ei sisalda vajalikku ja asjakohast teavet.

2.2 Asjassepuutuvate logiandmete puudulik valimine

Suure hulga logiteadete reaalajas analüüsimine nõuab palju arvuti- ja inimressursse. Kui kogutud andmetest ainult väike osa informatiivne, muutub logiandmete analüüsimine info ülekülluse tõttu ajamahukaks. Kui IT-süsteemi või logitaristu töömälu või kõvaketta maht on ebapiisav, võib juhtuda, et olulist teavet sisaldavad logiandmed kirjutatakse üle või kustutatakse enneaegselt.

2.3 Sünkroniseerimata aeg logimisel

Kui organisatsiooni kõikide IT-süsteemide kellaaegasid ei sünkroniseerita, siis erinevate IT-süsteemide logiandmed omavahel ei korreleeru ning võivad põhjustada ekslikke sündmusteateid. Selliselt kogutud logiandmeid on keeruline analüüsida ning neid logisid ei pruugi olla võimalik kasutada IT-kriminalistikas asitõenditena.

2.4 Logimise halb plaanimine

Kui logimist ei ole üksikasjalikult plaanitud, võivad IT-süsteemid jääda järelevalveta ning nende IT-süsteemidega seotud turvasündmused jäävad tuvastamata. Kui isikuandmete kasutamist ei logita, võivad andmekaitserikkumised jääda avastamata.

2.5 Logiandmete konfidentsiaalsuse ja tervikluse kadu

Teatud IT-süsteemid tekitavad füüsiliste isikutega seostatavaid logiandmeid. Kui logiandmeid, mis sisaldavad kasutajanimesid, IP-aadresse, e-posti aadresse ja arvutinimesid, ei edastata krüpteeritult ega talletata turvaliselt, saab neid andmeid kopeerida ja pealt kuulata. Ründaja saab juurdepääsu konfidentsiaalsele teabele või kasutada kogutud isikuandmeid organisatsiooni struktuuri tundmaõppimiseks ja rünnete sihipärasemaks suunamiseks.

2.6 Valesti konfigureeritud logimine

Kui IT-süsteemi logimisreeglid on valesti konfigureeritud, võib oluline teave jääda logimata. Kui logitakse liigseid andmeid (nt isikuandmeid juhul, kui selleks vajadus puudub), võib organisatsioon rikkuda õigusaktide nõudeid. Kui logiandmeid ei saa teiste andmetega seostada, on logide analüüs raskendatud ning turvaintsidendid võivad jääda avastamata.

2.7 Andmeallikate tõrge

Kui IT-süsteemid vajalikke logiandmeid ei edasta, pole võimalik logiandmete põhjal turvaintsidente avastada. Andmeallikate tõrgete põhjuseks võivad olla riist- ja tarkvara vead, aga ka puudulikult hallatud IT-süsteemid. Kui andmeallikate tõrked jäävad märkamata, jääb organisatsiooni turvalisusest petlik mulje. Infiltreerunud ründaja võib jääda pikaks ajaks märkamatuks.

2.8 Liiga väike logitaristu

Komplekssete infosüsteemide puhul suurenevad vastavalt ka logimisele esitatavad nõuded. Kui logitaristu ei võimalda talletada ja analüüsida tuleb väga palju logiandmeid. Kui logitaristu seda ei võimalda, ei saa turvasündmusi analüüsida või tehakse seda ebapiisavalt.

3 Meetmed

3.1 Elutsükkel

Kavandamine

OPS.1.1.5.M1 Logimise eeskiri

OPS.1.1.5.M3 Sündmuste logimise konfigureerimine

OPS.1.1.5.M6 Keskse logitaristu rajamine

Käitus

OPS.1.1.5.M4 Aja sünkroniseerimine

OPS.1.1.5.M5 Õiguslike raamtingimuste täitmine

OPS.1.1.5.M8 Logiandmete arhiveerimine

OPS.1.1.5.M9 Logiandmete valmendus analüüsimiseks

OPS.1.1.5.M10 Logiandmete kaitse lubamatu juurdepääsu eest

Lisanduvad kõrgmeetmed

OPS.1.1.5.M11 Logimisjõudluse suurendamine

OPS.1.1.5.M12 Logiandmete krüpteerimine

OPS.1.1.5.M13 Kõrgkäideldav logimissüsteem

OPS.1.1.5.ME1 Logide räsiaheldamine

3.2 Põhimeetmed

OPS.1.1.5.M1 Logimise eeskiri [vastutav spetsialist]

a. Organisatsioonis on kehtestatud infoturvapoliitikaga vastavuses olev logimise eeskiri, mis sätestab, kuidas logimist turvaliselt plaanida, korraldada ja rakendada.

b. Logimise eeskiri määrab kaitsetarbest lähtuvalt, millises ulatuses ja milliseid IT-süsteeme ja rakendusi logitakse.

c. Kõrvalekalded logimise eeskirjast kooskõlastatakse infoturbejuhiga ja dokumenteeritakse.

d. Eeskirja täitmist kontrollitakse regulaarselt, tulemused dokumenteeritakse.

OPS.1.1.5.M3 Sündmuste logimise konfigureerimine

a. Kõik IT-süsteemide ja rakenduste turvasündmused logitakse.

b. Logimise eeskirjaga hõlmatud IT-süsteemide ja rakenduste sisemised logimisfunktsioonid on kasutusele võetud.

c. Logimise toimimist ja korrektsust kontrollitakse regulaarselt, logimise eeskirjas määratud sagedusega.

d. Kui turvasündmusi ei saa IT-süsteemi või rakenduse siseselt logida, on kasutusele võetud kompenseerivad meetmed (nt võrgutaseme sündmuste logimine) vastavalt IT-süsteemi või rakenduse valmistaja soovitustele.

OPS.1.1.5.M4 Aja sünkroniseerimine

a. Logitavate IT-süsteemide ja rakenduste süsteemiajad on alati sünkroniseeritud.

b. Logides on kasutusel ühtne ajavorming, vt NET.1.2 *Võrguhaldus*.

OPS.1.1.5.M5 Õiguslike raamtingimuste täitmine [infoturbejuht]

a. Logimisel järgitakse andmekaitse ja muude asjakohaste õigusaktide nõudeid (vt CON.2 *Andmekaitse*).

b. Logiandmeid kustutatakse ettenähtud protseduuri kohaselt.

c. Logiandmete lubamatu kustutamine või muutmine on tõkestatud tehniliste meetmetega.

3.3 Standardmeetmed

OPS.1.1.5.M6 Keskse logitaristu rajamine

a. Kõik ärikriitiliste IT-süsteemide turbe jaoks olulised logiandmed talletatakse keskses logiserveris või logiserverite taristus.

b. Logide salvestamiseks antakse juurdepääs logiserverite võrgusegmendile ainult määratud logiserveri klientidele (vt NET.1.1 *Võrgu arhitektuur ja lahendus*).

c. Lisaks turvasündmustele (vt OPS.1.1.5.M3 *Logimise konfigureerimine*) logitakse keskses logitaristus ka võimalikele vigadele viitavaid sündmusi (nt süsteemi liigne koormamine või tavapäratute operatsioonide käitamine).

d. Logimise laiendamise puhul on logitaristusse võimalik lisada täiendavaid ressursse.

e. Logitaristu rajamisel organisatsioonist väljapoole kasutatakse usaldusväärse ja spetsialiseerunud teenuseandja teenuseid.

OPS.1.1.5.M8 Logiandmete arhiveerimine

a. Logiandmed arhiveeritakse kooskõlas logimise eeskirjaga (vt OPS.1.1.5.M1 *Logimise eeskiri*). Arhiveerimisel arvestatakse asjakohaste õigusaktide nõuetega (vt OPS.1.2.2 *Arhiveerimine*).

OPS.1.1.5.M9 Logiandmete valmendus analüüsimiseks

a. Kasutatav logimisrakendus võimaldab töödeldud logiandmeid analüüsida.
b. Logiandmete töötlus ja analüüsimine toimub kooskõlas logimise eeskirjaga (vt OPS.1.1.5.M1 Logimise eeskiri).
c. Logiandmete analüüsil arvestatakse organisatsiooni infoturvapoliitikat ja andmetöötluse õiguslikke aluseid.
d. Logiandmed säilitatakse algsel kujul.

OPS.1.1.5.M10 Logiandmete kaitse lubamatu juurdepääsu eest

a. Kõik logiandmed talletatakse ja neid kaitstakse volitamata juurdepääsu eest, pääsuõigused logiandmetele dokumenteeritakse.
b. IT-süsteemide ja rakenduste haldurid ei saa logiandmeid muuta ega kustutada.

3.4 Kõrgmeetmed

OPS.1.1.5.M11 Logimisjõudluse suurendamine (C-I-A)

a. Logimisjõudlus on piisav tsentraalsesse asukohta kogutud logiandmestiku võimalikult reaalajas toimuva analüüsi läbiviimiseks. Selleks salvestatakse logiandmeid võimalikult lühikeste ajavahemike tagant.
b. Suure kaitsetarbe puhul laiendatakse logitavate sündmuste tüüpe ja hulka.
c. Suure kaitsetarbe puhul ei kasutata IT-süsteeme ja rakendusi, mida ei saa logida tsentraalsesse asukohta.

OPS.1.1.5.M12 Logiandmete krüpteerimine (C-I)

a. Logiandmed edastatakse ainult krüpteeritult.
b. Salvestatavad logiandmed signeeritakse digitaalselt.
c. Arhiveeritud ja väljaspool logitaristut hoitavad logiandmed on alati krüpteeritud (vt CON.1 *Krüptokontseptsioon).*

OPS.1.1.5.M13 Kõrgkäideldav logimissüsteem [infoturbejuht] (A)

a. Logitaristu rajamisel on arvestatud kõrgkäideldavuse nõuetega.

OPS.1.1.5.ME1 Logide räsiaheldamine (I)

a. Logide tervikluse tagamiseks kasutatakse plokiahela tehnoloogiat (ingl *blockchain technology*), mille puhul logikirjete lokaalsed ajatemplid seotakse kronoloogilises järjekorras krüptograafiliselt kaitstud räsiahelasse (ingl *hash chain*).
b. Logide räsiahel on usaldatavalt seotud ning välistab logiandmete volitamata muutmise.
c. Logide räsiahela terviklust kontrollib volitatud töötaja regulaarselt.

4 Lisateave

Lühend	Publikatsioon
[NIST]	NIST, Special Publication 800-92 „Guide to Computer Security Log Management“

OPS.1.1.6 Tarkvara testimine ja kasutuselevõtt

1 Kirjeldus

1.1 Eesmärk

Esitada tarkvara testimise ja kasutuselevõtu soovituslikud protseduurid ning meetmed kasutusele võetava tarkvara tehnilistele ja korralduslikele turvanõuetele vastavuse tagamiseks.

1.2 Vastutus

Tarkvara testimise ja kasutuselevõtu meetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Personaliosakond, andmekaitsespetsialist, vastutav spetsialist, testija.

1.3 Piirangud

Mooduli meetmeid rakendatakse koos meetmetega moodulitest CON.8 *Tarkvaraarendus* ja APP.6 *Tarkvara üldiselt*. Tarkvara testimist pärast muudatuste elluviimist käsitleb moodul OPS.1.1.3 *Paiga- ja muudatusehaldus*.

2 Ohud

2.1 Tarkvara testimine tööandmetega

Kuigi tarkvara testimine tööandmetega on mugav, võivad tarkvara testimisse kaasatud isikud seejuures näha konfidentsiaalseid töö- või isikuandmeid. Kui testimiseks kasutatakse käidukeskkonna (ingl *operational environment*) andmeid, mitte andmete koopiaid, võidakse neid andmeid tahtmatult muuta või kustutada. Kui tööandmeid kasutatakse IT-süsteemide integratsiooni testimisel, võib testandmete töötlus mõjutada tahtmatult toiminguid tegelike andmetega teistes süsteemides.

2.2 Puuduv või piisamatu testimisprotseduur

Kui uut tarkvara ei testita või kui seda tehakse piisamatult, võivad tarkvara- või installimisvead jääda märkamata. Kui muudatusi või uuendeid piisavalt ei testita, võivad tekkida tõsised käideldavus- ja terviklusprobleemid. Näiteks eelnevalt testimata andmebaasisüsteemi uuendi laadimine võib põhjustada andmekao.

2.3 Puuduv või piisamatu kinnitusprotseduur

Puuduva või piisamatu kinnitusprotseduuri tulemusena võidakse kasutusele võtta tehniliselt puudulik tarkvara. Tarkvarast võivad puududa vajalikud funktsioonid või on jäänud lähtekoodi sisse mittevajalikke komponente. Samuti ei pruugi kinnitamata tarkvara ühilduda muude kasutusel olevate rakendustega.

2.4 Testide ja testimistulemuste puudulik dokumenteerimine

Kui tarkvara testimise dokumentatsioon on puudulik, ei ole hiljem võimalik tuvastada, millist funktsionaalsust testiti ja milliseid tegevusi testimisel tehti. Kui tuvastatud tarkvaravigu või puuduvaid funktsioone dokumenteeriti puudulikult, kanduvad vead üle käidukeskkonna IT-süsteemidesse.

2.5 Kinnituskriteeriumide puudulik dokumenteerimine

Kui kinnituskriteeriumid ei ole üheselt kokku lepitud ja dokumenteeritud, võidakse paigaldamiseks kinnitada vigu sisaldav tarkvaraversioon. Vead võivad ilmneda alles käidukeskkonnas ning põhjustada tarkvaraprojekti valmimisega hilinemise ja rahalise kahju.

3 Meetmed

3.1 Elutsükkel

Kavandamine

OPS.1.1.6.M1 Tarkvara testimise kavandamine

OPS.1.1.6.M7 Personali valimine tarkvara testijaks

OPS.1.1.6.M10 Testimise vastuvõtu kord

Evitus

OPS.1.1.6.M6 Tarkvara testija juhendamine

OPS.1.1.6.M13 Testkeskkonna lahutamine käidukeskkonnast

Käitus

OPS.1.1.6.M2 Tarkvara funktsionaaltestimine

OPS.1.1.6.M3 Testimistulemuste analüüsimine

OPS.1.1.6.M4 Tarkvara kinnitamine

OPS.1.1.6.M5 Mittefunktsionaalsete testide tegemine

OPS.1.1.6.M11 Testandmete anonüümimine või pseudonüümimine

OPS.1.1.6.M12 Regressioontestimine

OPS.1.1.6.M15 Paigaldamise ja seadistamise juhendi järgimine

Lisanduvad kõrgmeetmed

OPS.1.1.6.M14 Läbistustestide sooritamine

OPS.1.1.6.M16 Testija taustakontroll

3.2 Põhimeetmed

OPS.1.1.6.M1 Tarkvara testimise kavandamine

a. Kaitsetarbest, tehnilistest võimalustest ja testimiskeskkonnast lähtudes määratakse enne tarkvara testimist testimise raamtingimused.

b. Testimisel tuginetakse testimise raamtingimustele ja tarkvara spetsifikatsioonile.

c. Testilood katavad tarkvara kogu funktsionaalsust.

d. Testkeskkond on käidukeskkonnaga võimalikult sarnane.
e. Testimise käigus kontrollitakse tarkvara funktsioneerimist kõigis kavandatud kasutuskeskkondades (nt eri tüüpi seadmetes) ja toetatavates operatsioonisüsteemides.

OPS.1.1.6.M2 Tarkvara funktsionaaltestimine [testija]

a. Kõiki tarkvara funktsioone kontrollitakse tarkvara funktsionaaltestimisega (ingl *functional testing*). Funktsionaaltestimise käigus veendutakse tarkvara nõuetekohases toimimises.
b. Funktsioonide testimine ei avalda mõju tarkvara edasisele toimimisele.

OPS.1.1.6.M3 Testimistulemuste analüüsimine [testija]

a. Testimistulemuste analüüsi käigus võrreldakse testimisel saadud tegelikke väärtusi oodatavate tulemustega.
b. Testimistulemuste analüüsi tulemused dokumenteeritakse.

OPS.1.1.6.M4 Tarkvara kinnitamine [vastutav spetsialist]

a. Kinnitav struktuuriüksus kontrollib, kas tarkvara testiti nõuetekohaselt ja kas testimise tulemused vastavad eelnevalt kindlaks määratud tingimustele.
b. Pärast edukat tarkvara testimist kinnitatakse tarkvara kasutuselevõtt dokumenteeritud otsusega.

OPS.1.1.6.M5 Mittefunktsionaalsete testide tegemine [testija]

a. Mittefunktsionaalsete testidega (ingl *non-functional testing*) testitakse tarkvara jõudlust, kvaliteedinäitajaid ja turvalisust.
b. Turvakriitiliste funktsioonide olemasolul on turvatestide läbiviimine kohustuslik.
c. Valitud testilood ja testimise tulemused dokumenteeritakse.

OPS.1.1.6.M11 Testandmete anonüümimine või pseudonüümimine [andmekaitsespetsialist, testija]

a. Tundlike andmete põhjal koostatud tarkvara testandmed on testkeskkonnas andmete avalikustamise eest piisavalt kaitstud.
b. Kõik füüsiliste isikutega seotud testandmed on vähemalt pseudonüümitud. Kui testandmetest on võimalik tuletada seost isikuga, otsustatakse nende andmete kasutamine koos andmekaitsespetsialistiga.
c. Võimaluse korral kõik füüsiliste isikutega seotud testandmed anonüümitakse.

3.3 Standardmeetmed

OPS.1.1.6.M6 Tarkvara testija juhendamine [vastutav spetsialist]

a. IT-talitus annab tarkvara testijale piisava ajavaruga teada eelseisva testimise tüübi ja testimisobjekte puudutava teabe.
b. Testijat teavitatakse tarkvara kasutusviisidest ja võimalikest täiendavatest nõuetest.

OPS.1.1.6.M7 Personali valimine tarkvara testijaks [vastutav spetsialist, personaliosakond]

a. Tarkvara testija valimisel arvestatakse vajalikku erialast kvalifikatsiooni ning teadmisi kasutatavatest programmeerimiskeeltest, arenduskeskkondadest ja testimismeetoditest.

b. Lähtekoodi ülevaatust teevad testijad, kes ei osalenud sama tarkvaramooduli programmeerimisel.

OPS.1.1.6.M10 Testimise vastuvõtu kord

a. On kehtestatud testimise vastuvõtu kord, mis määrab:
   - kohustuslikud testid;
   - oodatavad tulemused;
   - testimise vastuvõtu kriteeriumid.

b. On kehtestatud protseduur testimise vastuvõtust keeldumise korral tegutsemiseks.

OPS.1.1.6.M12 Regressioontestimine [testija]

a. Pärast tarkvara muutmist viiakse tarkvara ühilduvuse kontrollimiseks ja võimalike uute vigade avastamiseks läbi täiemahuline regressioontestimine (ingl *regression test*).

b. Valitud testimisjuhtumid ja testimistulemused dokumenteeritakse. Testimisjuhtumite väljajätmist põhjendatakse kirjalikult.

OPS.1.1.6.M13 Testkeskkonna lahutamine käidukeskkonnast

a. Tarkvara testitakse ainult selleks ettenähtud test- ja käidueelses (ingl *prelive*) keskkonnas.

b. Test- ja käidueelne keskkond on käidukeskkonnast (ingl *operational environment*) lahutatud ja käidukeskkonnast selgelt eristatavad.

c. Testkeskkonna arhitektuur ja tehnilised parameetrid on dokumenteeritud.

OPS.1.1.6.M15 Paigaldamise ja seadistamise juhendi järgimine [testija]

a. Testkeskkonna ettevalmistamisel on järgitud tarkvara paigaldamise ja seadistamise juhendit (vt APP.6 *Tarkvara üldiselt*).

3.4 Kõrgmeetmed

OPS.1.1.6.M14 Läbistustestide sooritamine [testija] (C-I-A)

a. On koostatud läbistustestimise (ingl *penetration testing*) juhend, mis määrab testimismeetodid ja tulemuskriteeriumid.

b. Läbiviidud läbistustestimised vastavad läbistustestimise juhendile.

c. Läbistustestimise käigus tuvastatud nõrkused liigitatakse vastavalt riskiastmele ja dokumenteeritakse.

d. Tuvastatud olulised nõrkused kõrvaldatakse enne tarkvara kasutuselevõttu.

OPS.1.1.6.M16 Testija taustakontroll [personaliosakond] (C)

a. Suure kaitsetarbega valdkondades viiakse läbi enne testimislepingu sõlmimist testimisettevõtte ja testimises osalevate testijate täiendav taustakontroll.

b. Salastatud teavet sisaldava IT-süsteemi või tarkvara testijad omavad kehtiva seadusandluse kohast riigisaladusele juurdepääsu luba.

OPS.1.1.7 Süsteemihaldus

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed süsteemihalduse lahenduse, selle komponentide ja hallatavate IT-süsteemide turvaliseks konfigureerimiseks, seireks ja andmevahetuseks. Süsteemihaldust kasutatakse integreeritud ja hallatavate süsteemide keskseks haldamiseks. Süsteemihalduse lahenduse moodustab keskhalduslahenduse, hallatavate IT-süsteemide ja andmesideliideste ühtne tervik.

1.2 Vastutus

Süsteemihalduse meetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Lisavastutajad puuduvad.

1.3 Piirangud

IT-süsteemide halduse üldised meetmed on kirjeldatud moodulis OPS.1.1.2 *IT-süsteemide haldus*.

Võrguhalduse meetmeid käsitletakse moodulis NET.1.2 *Võrguhaldus*. IT-süsteemide turvalist liidestamist süsteemihaldusega käsitletakse mooduligrupi SYS süsteemikohastes moodulites. Meetmed süsteemihalduse lahenduse logimiseks ja varundamiseks on esitatud moodulites OPS.1.1.5 *Logimine* ja OPS.1.2.2 *Arhiveerimine*.

Süsteemihalduse lahenduse muudatuste haldust käsitletakse moodulis OPS.1.1.3 *Paiga- ja muudatusehaldus*. Meetmed IT-süsteemide kaughalduseks on esitatud moodulis OPS.1.2.5 *Kaughooldus.*

2 Ohud

2.1 Volitamata juurdepääs süsteemihalduse lahendusele

Süsteemihalduse lahendus on ründajate jaoks prioriteetne sihtmärk, sest tänu süsteemihalduse lahenduse laialdastele juurdepääsuõigustele saab ründaja kontrollida ja manipuleerida kõiki hallatud IT-süsteeme. Ründajal on võimalik saada juurdepääs tundlikule teabele või häirida äriprotsesse, mida hallatud süsteemid toetavad.

Kui ründaja muudab keskses konfiguratsioonihaldusserveris olevaid konfiguratsioonifaile, rakendatakse vastavad muudatused kõikides hallatud IT-süsteemides. Näiteks saab nii klientarvutitesse installida lunavara, mis krüpteerib kõikide hallatavate tööjaamade sisu.

2.2 Vead süsteemihalduse automatiseerimisel

Süsteemihalduse protsesside automatiseerimisel tehtud vead (nt skriptides) võivad muuta hallatavad süsteemid töövõimetuks või oluliselt kahjustada IT-süsteemide turvalisust. Tänu automatiseerimisele võib tehtud viga mõjutada väga lühikese aja jooksul suurt hulka IT-süsteeme, sh kriitilisi IT-süsteeme, mille kõrge käideldavus on äriliselt väga oluline.

2.3 Süsteemihalduse komponentide andmeside häirimine

Suunatud rünne või juhuslik häiring süsteemihalduse komponentide vahelises andmesides võib rikkuda hallatavate IT-süsteemide terviklust ja piirata IT-teenuste kättesaadavust.

Süsteemihalduse side pealtkuulamisel ja manipuleerimisel saab ründaja mõjutada hallatavate IT-süsteemide toimimist ja vaadata IT-süsteemide vahel edastatavaid andmeid.

2.4 Puudulik kellade sünkroniseerimine

Kui süsteemihalduse komponentide süsteemiajad ei ole sünkroniseeritud, on turvaintsidentide haldus raskendatud. Kasutatavad logiandmed ei pruugi olla omavahel korrelatsioonis, mistõttu jääb potentsiaalne turvaintsident avastamata.

Kui andmevahetusprotokoll kasutab side kehtivuse hindamiseks ajatempleid, võib kehtivuskinnituse andmine olla osapoolte erinevate süsteemiaegade tõttu häiritud.

2.5 Süsteemihalduse lahendusega mitteühilduvad IT-süsteemid

Süsteemihalduse lahendusega mitteühilduvaid süsteeme ei saa kavandatud ulatuses keskselt hallata. Võib tekkida olukord, mil IT-süsteemid pole kättesaadavad või neis esinevaid tõrkeid ei raporteerita kesksesse haldussüsteemi. IT-süsteemid võivad jääda ilma keskselt rakendatavatest süsteemiuuenditest või haldusliideste konfiguratsioonimuudatustest.

2.6 Juurdepääsu puudumine süsteemihalduse lahendusele

Kui volitatud kasutajal (halduril) pole võimalik vajalikul hetkel süsteemihalduse lahendusele juurde pääseda, võib see kaasa tuua hallatavate IT-süsteemide mittetoimimise.

Toimunud IT- intsident võib eskaleeruda ja selle mõju suureneda, kui intsidenti ei saa süsteemihalduse vahenditega ohjata. Haldur ei saa juurdepääsu katkemisel teha IT-süsteemide tõrkeotsingut ja läbi viia kavandatud haldustoiminguid, nt paigaldada süsteemidele turvauuendeid.

2.7 Ühenduse katkemine süsteemihalduse lahenduse ja hallatavate süsteemide vahel

Ühenduse katkemine hallatavate süsteemidega võib kahjustada IT-teenuste kättesaadavust ja/või IT-süsteemide terviklust. Kahju suurus sõltub sidekatkestuse ulatusest ja katkestuse ajalisest kestvusest. Ühenduse puudumisest tingitud tõrkeid on keeruline analüüsida ja ilmnevaid vigu on raske parandada.

2.8 Süsteemihalduse ja võrguhalduse ebapiisav koordineerimine

Kui võrguhalduses kavandatavaid muudatusi süsteemihalduse eest vastutajatega eelnevalt ei kooskõlastata, võib võrgus tehtud muudatus tulla ootamatuna ning süsteemihaldust negatiivselt mõjutada. Vastuolud võrgu ja IT-süsteemide konfiguratsioonis võivad muuta hallatavad IT-süsteemid süsteemihalduse lahendusele kättesaamatuks, kaasnevad tõrked võivad tekitada hulga veateateid ja prognoosimatute tagajärgedega sündmusi.

3 Meetmed

3.1 Elutsükkel

Kavandamine

OPS.1.1.7.M1 Süsteemihalduse nõuete määratlemine

OPS.1.1.7.M2 Süsteemihalduse lahenduse kavandamine

OPS.1.1.7.M7 Süsteemihalduse turvaeeskiri

OPS.1.1.7.M8 Süsteemihalduse kontseptsioon

Evitus

OPS.1.1.7.M9 Süsteemihalduse rakendusplaan

OPS.1.1.7.M10 Süsteemihalduse turvalise käituse juhised

OPS.1.1.7.M13 Lubatud haldusliideste määramine

Käitus

OPS.1.1.7.M3 Kellade sünkroniseerimine

OPS.1.1.7.M4 Süsteemihalduse andmeside kaitse

OPS.1.1.7.M5 Süsteemihalduse lahenduse ja hallatavate IT-süsteemide vastastikune autentimine

OPS.1.1.7.M6 Süsteemihalduse lahenduse juurdepääsu turve

OPS.1.1.7.M11 Süsteemihalduse regulaarne lahknevusanalüüs

OPS.1.1.7.M12 Keskne süsteemihalduse toimingute käivitamine

OPS.1.1.7.M14 Keskne hallatavate IT-süsteemide konfiguratsioonihaldus

OPS.1.1.7.M15 Süsteemihalduse lahenduse seire, logimine ja teavitused

OPS.1.1.7.M17 Süsteemihalduse andmevahetuse piiramine

OPS.1.1.7.M18 Süsteemihalduse lahenduse seisundi kontroll

OPS.1.1.7.M19 Süsteemihalduse lahenduse andmeside turve

Avariivalmendus

OPS.1.1.7.M16 Süsteemihalduse integreerimine avariivalmendusega

Lisanduvad kõrgmeetmed

OPS.1.1.7.M20 Kõrgkäideldav süsteemihalduse lahendus

OPS.1.1.7.M21 Süsteemihalduse võrgu füüsiline eraldamine

OPS.1.1.7.M22 Süsteemihalduse integreerimine turvateabe halduse süsteemiga

OPS.1.1.7.M23 Kellade sünkroniseerimine erinevate asukohtade vahel

OPS.1.1.7.M24 Hallatavate süsteemide turvakonfiguratsiooni kontrollimine

OPS.1.1.7.M25 Süsteemihalduse lahenduse kasutajasessioonide logimine

OPS.1.1.7.M26 Süsteemihalduse lahendusele juurdepääsu piiramine

3.2 Põhimeetmed

OPS.1.1.7.M1 Süsteemihalduse nõuete määratlemine

a. Organisatsioon on määratlenud süsteemihalduse (ingl *systems management*) nõuded, sh turvanõuded, arvestades kõiki süsteemihalduse protsesse.

b. On kehtestatud süsteemihalduse taristu tehnilised nõuded.

c. On määratletud hallatavad IT-süsteemid ja dokumenteeritud hallatavate IT-süsteemide liidestused süsteemihalduse keskse komponendiga.

OPS.1.1.7.M2 Süsteemihalduse lahenduse kavandamine

a. Süsteemihalduse lahenduse kavandamise tulemina on dokumenteeritud:

- süsteemihalduse nõuete detailanalüüs;
- süsteemihalduse lahenduse üldkontseptsioon;
- terviklik projektiplaan süsteemihalduse lahenduse juurutamiseks;
- projekti etappide lõpetamise eeldused ja läbiviidavad kvaliteedikontrollid.

b. Süsteemihalduse lahenduse turbe kavandamisel on arvestatud vähemalt järgmisi aspekte:
   - süsteemihalduse lahendusega kaetud võrgusegmendid;
   - süsteemihalduse lahenduse turvaline juurdepääs;
   - autentimine ja volitamine hallatavates IT-süsteemides;
   - võrguühendused ja võrguprotokollid süsteemihalduse lahenduse komponentide vaheliseks andmesideks;
   - süsteemihalduse sündmuste logimine ja logide integreerimine keskse logihalduslahendusega;
   - süsteemihalduse lahenduse tootja või arendaja tugiteenuste olemasolu kavandatud kasutusaja vältel;
   - süsteemihalduse lahenduse uuendite paigaldamine, sh hallatavatesse IT-süsteemidesse;
   - süsteemihalduse lahenduse aruandlus ja liidestamine teiste IT-süsteemidega;
   - hallatavatele IT-süsteemidele esitatavad turvanõuded.

OPS.1.1.7.M3 Kellade sünkroniseerimine

a. Süsteemihalduse lahenduse kesksete komponentide ning hallatavate IT-süsteemide kellaaeg on sünkroniseeritud.

b. Kellade sünkroniseerimiseks kasutatakse sobivat võrguaja protokolli.

OPS.1.1.7.M4 Süsteemihalduse andmeside kaitse

a. Süsteemihalduse lahenduse ja hallatavate süsteemide vahelise andmeside loomisel kasutatakse turvalisi võrguprotokolle (nt SSH, TLS).

b. Kui turvalisi võrguprotokolle ei saa kasutada, toimub süsteemihalduse lahenduse andmeside tavavõrgust eraldatud spetsiaalses haldusvõrgus (vt NET.1.1 *Võrgu arhitektuur ja lahendus*). Haldusvõrgu puudumisel rakendatakse virtuaalset privaatvõrku (ingl *virtual private network*, VPN) või sellega võrreldava turvatasemega andmesidelahendust.

OPS.1.1.7.M5 Süsteemihalduse lahenduse ja hallatavate IT-süsteemide vastastikune autentimine

a. Süsteemihalduse lahenduse ja hallatavate IT-süsteemide vaheline autentimine on vastastikune (toimub mõlemas suunas).

b. Süsteemihalduse lahenduse komponentide autentimismehhanismid on kooskõlas organisatsiooni üldise autentimispõhimõtetega.

c. Autentimisel kasutatakse turvalisi protokolle.

OPS.1.1.7.M6 Süsteemihalduse lahenduse juurdepääsu turve

a. Kasutajate juurdepääs süsteemihalduse lahendusele on turvatud asjakohaste kasutaja autentimis- ja volitusmehhanismidega.

b. Kasutaja autentimisel krüpteeritakse edastatavad andmed.
c. Kasutajate autentimise autentimismehhanismi valikuprotsess on dokumenteeritud.
d. Kasutusele võetud krüptomehhanismide ja krüptovõtmete tugevust kontrollitakse regulaarselt.
e. Süsteemihalduse lahenduse volitusmehhanism võimaldab kasutajatel teha ainult toiminguid, milleks kasutajad on volitatud.

3.3 Standardmeetmed

OPS.1.1.7.M7 Süsteemihalduse turvaeeskiri

a. Süsteemihalduse turvalisuse tagamiseks on koostatud süsteemihalduse turvaeeskiri.
b. Süsteemihalduse turvaeeskiri sisaldab vähemalt järgmist:
   - valdkonnad ja IT-süsteemid, millele keskne süsteemihalduse lahendus rakendub;
   - süsteemihalduse automatiseeritud protsessid ja tegevused;
   - süsteemihalduse lahenduses sisalduva konfiguratsioonihalduse kirjeldus (nt versioonihaldus);
   - pääsu reguleerimise spetsifikatsioonid;
   - logimise nõuded;
   - nõuded automatiseeritud tegevuste (nt skriptide kasutamise) kvaliteedi kontrollimiseks;
   - nõuded andmeside turvalisuse tagamiseks;
   - võrgu segmenteerimise reeglid (juhul kui segmenteerimist kasutatakse);
   - süsteemihalduse lahenduse võrguspetsifikatsioon (IP-aadressid, DNS jne).
c. Süsteemihalduse turvaeeskiri on volitatud töötajatele kättesaadav. Süsteemihaldusega tegelevad töötajad järgivad süsteemihalduse turvaeeskirja.
d. Süsteemihalduse turvaeeskirja täitmist kontrollitakse regulaarselt. Kontrolli tulemused dokumenteeritakse.

OPS.1.1.7.M8 Süsteemihalduse kontseptsioon

a. Organisatsioon on koostanud süsteemihalduse turvanõudeid (vt. OPS.1.1.7.M1 *Süsteemihalduse nõuete määratlemine* ja OPS.1.1.7.M7 *Süsteemihalduse turvaeeskiri*) arvestava süsteemihalduse kontseptsiooni.
b. Süsteemihalduse kontseptsioon sisaldab vähemalt järgmist:
   - süsteemihalduse meetodid, tehnikad ja tööriistad;
   - süsteemihalduse lahenduse juurdepääsu reguleerimine
   - andmeside turbe meetmed;
   - süsteemihalduse lahenduse komponentide paigutus võrgusegmentides;
   - süsteemihalduse lahenduse komponentide seire ja automaatsed teavitused;
   - süsteemihalduse lahenduse logimine;
   - automatiseeritud tegevuste (nt konfiguratsioonihaldus) spetsifikatsioonid;
   - automatiseeritud tegevuste väljatöötamine ja testimine;

- tegevused ja teavituskanalid tõrgete ja turvaintsidentide puhul tegutsemiseks;
- süsteemihalduse andmete integreerimine organisatsiooni muude protsessidega;
- süsteemihalduse integreerimine organisatsiooniülese avariivalmenduse kontseptsiooniga;
- süsteemihalduse lahenduse rakendamiseks ja käitamiseks vajalikud ressursid, sh vajalik inimressurss ja nõuded võrgu jõudlusele.

OPS.1.1.7.M9 Süsteemihalduse rakendusplaan

a. Süsteemihalduse lahenduse evitamiseks on koostatud detailne rakendusplaan, mis arvestab kõiki süsteemihalduse turvaeeskirjas ja kontseptsioonis sisalduvaid nõudeid.

OPS.1.1.7.M10 Süsteemihalduse turvalise käituse juhised

a. On koostatud juhised süsteemihalduse lahenduse turvaliseks käituseks.

b. Süsteemihalduse turvalisuse käituse juhised arvestavad kõiki süsteemihalduse lahendusele ja baastaristule kehtestatud turvanõudeid.

OPS.1.1.7.M11 Süsteemihalduse regulaarne lahknevusanalüüs

a. Süsteemihalduse lahenduse ja hallatavate IT-süsteemide andmete terviklust kontrollitakse regulaarselt.

b. Süsteemihalduse lahendusega hallatavate IT-süsteemide konfiguratsioonid vastavad keskselt kavandatud konfiguratsioonidele.

c. Süsteemihalduse lahenduse skriptide ja muude automaatsed tegevuste tulemite õigsust kontrollitakse regulaarselt.

OPS.1.1.7.M12 Keskne süsteemihalduse toimingute käivitamine

a. Hallatavates IT-süsteemides saab süsteemihalduse toiminguid käivitada ainult süsteemihalduse lahendus.

b. Süsteemihalduse lahendusega hallatud IT- süsteemides on aktiveeritud ainult vajalikud haldusfunktsioonid.

OPS.1.1.7.M13 Lubatud haldusliideste määramine

a. Haldusjuurdepääs hallatavatele süsteemidele on lubatud ainult määratud süsteemihalduse lahenduse liideste kaudu.

b. Erandjuhtudel (nt avariiolukorras, mil süsteemihalduse lahendus ei toimi) on võimalik hallatavaid IT-süsteeme konfigureerida ka otsejuurdepääsu kaudu.

c. Otsejuurdepääsu kasutamise juhud ning süsteemihalduse lahenduse väliselt tehtud konfiguratsioonimuudatused dokumenteeritakse. Tehtud muudatused kajastatakse hiljem süsteemihalduse lahenduses.

OPS.1.1.7.M14 Keskne hallatavate IT-süsteemide konfiguratsioonihaldus

a. Hallatavate IT-süsteemide konfiguratsioone hallatakse süsteemihalduse lahenduse osana käsitletavas konfiguratsioonihalduse süsteemis.

b. Keskse konfiguratsioonihalduse süsteemi andmed on alati täielikud ja ajakohased. Andmete muudatused versioonitakse, tehtud muudatusi on võimalik jälitada. Konfiguratsioonihalduse andmed on lisatud regulaarselt tehtavasse varukoopiasse.

c. Juurdepääs konfiguratsioonihalduse andmetele on lubatud ainult volitatud tarbijatele.

d. Keskse konfiguratsioonihalduse toimimist ja süsteemis sisalduvate andmete õigsust kontrollitakse regulaarselt.

e. Kõik liidesed süsteemihalduse lahenduse ning hallatavate IT-süsteemide vahel on dokumenteeritud keskses konfiguratsioonihalduse süsteemis. Seotud osapooled kooskõlastavad liideste funktsionaalsed muudatused enne muudatuste rakendamist.

f. Hallatavate süsteemide konfiguratsiooniandmeid on võimalik üle võrgu jagada ning aktiveerida automaatselt, ilma viivituseta ja IT-teenuseid katkestamata.

OPS.1.1.7.M15 Süsteemihalduse lahenduse seire, logimine ja teavitused

a. Süsteemihalduse lahenduse ja hallatavate süsteemide jõudluse ja käideldavuse näite seiratakse, arvestades eelnevalt määratud läviväärtusi. Läviväärtuse ületamisest teavitatakse vastutavaid töötajaid automaatselt.

b. Süsteemihalduse veaanalüüsi läbiviimisel arvestatakse lisaks teiste süsteemide seiretulemusi ja häireteateid (nt. süsteemihalduse tõrge võib olla põhjustatud toimunud võrguhäiringust).

c. Olulised sündmused hallatavates süsteemides ja süsteemihalduse lahenduses edastatakse automaatselt kesksesse logihaldussüsteemi (vt OPS.1.1.5 *Logimine*).

d. Olulise sündmuse määratlemisel on kaalutletud järgmisi aspekte:
   - hallatavate IT-süsteemide tõrge (nt käideldavuse kadu);
   - süsteemihalduse lahenduse tõrge;
   - riistvara või IT-taristu komponendi talitlushäire;
   - ebaõnnestunud sisselogimise katse süsteemihalduse lahendusse;
   - ebaõnnestunud sisselogimise katse hallatavasse IT-süsteemi;
   - hallatavate süsteemi kriitiline seisund (nt ülekoormus);
   - süsteemihalduse lahenduse kriitiline seisund.

e. Süsteemihalduse lahenduse automaatsed häireteated edastatakse ilma viivituseta.

OPS.1.1.7.M16 Süsteemihalduse integreerimine avariivalmendusega

a. Süsteemihalduse lahendus on integreeritud organisatsiooni avariivalmenduse kontseptsiooniga.

b. Süsteemihalduse lahenduse ja kõikide hallatavate süsteemide konfiguratsiooniandmed on varundatud, andmete taaste on lisatud taasteplaanidesse.

OPS.1.1.7.M17 Süsteemihalduse andmevahetuse piiramine

a. Andmevahetus süsteemihalduse kasutajate, süsteemihalduse lahenduse komponentide ja hallatavate IT-süsteemide vahel on piiratud minimaalselt vajaliku määrani.

b. Andmeside piiramiseks kasutatakse sobivaid andmefiltreerimist võimaldavaid tööriistu.

OPS.1.1.7.M18 Süsteemihalduse lahenduse seisundi kontroll

a. Süsteemihalduse lahenduse seisundi vastavust määratud normaalolukorrale kontrollitakse regulaarselt.

b. Lahknevuse tuvastamisel taastatakse süsteemihalduse lahenduse normaalolukord esimesel võimalusel.

OPS.1.1.7.M19 Süsteemihalduse lahenduse andmeside turve

a. Süsteemihalduse lahenduse ja hallatavate süsteemide vaheline andmeside on krüpteeritud.

b. Kasutusele võetud krüptomehhanismide ja krüptovõtmete tugevust kontrollitakse regulaarselt.

3.4 Kõrgmeetmed

OPS.1.1.7.M20 Kõrgkäideldav süsteemihalduse lahendus (A)

d. Süsteemihalduse lahenduse käideldavuse tõstmiseks kasutatakse dubleeritud süsteemikomponente ja liiasusega (ingl *redundancy*) kavandatud arvutivõrku.

OPS.1.1.7.M21 Süsteemihalduse võrgu füüsiline eraldamine (C-I)

a. Süsteemihalduse võrk on muudeks tööülesanneteks kasutatavast võrgust füüsiliselt eraldatud.

OPS.1.1.7.M22 Süsteemihalduse integreerimine turvateabe halduse süsteemiga (C-I-A)

a. Süsteemihalduse lahenduse turvasündmuste logimine on liidestatud turvateabe ja -sündmuste halduse (ingl *security information and event management*, SIEM) süsteemiga.

b. Süsteemihalduse lahenduse valikul arvestatakse SIEM süsteemiga liidestamise võimalusi ning toetatud andmeliideseid ja -formaate.

c. Süsteemihalduse lahendus on võimalike turvanõrkuste tuvastamiseks kaetud automaatse seirega.

OPS.1.1.7.M23 Kellade sünkroniseerimine erinevate asukohtade vahel (C-I-A)

a. Süsteemihalduse lahenduse komponentide ja hallatavate IT-süsteemide kellad on kõigis organisatsiooni asukohtades sünkroniseeritud kokkulepitud etalonaja allikaga.

OPS.1.1.7.M24 Hallatavate süsteemide turvakonfiguratsiooni kontrollimine (C-I-A)

a. Süsteemihalduse lahenduse ja hallatavate süsteemide turvakonfiguratsioone kontrollitakse regulaarselt.

b. Määratud normaalolekust kõrvalekallete ja võimalike turvanõrkuste avastamiseks kasutatakse sobivaid tuvastamissüsteeme.

OPS.1.1.7.M25 Süsteemihalduse lahenduse kasutajasessioonide logimine (C-I)

a. Kogu süsteemihalduse lahenduse andmevahetus (sh kõik süsteemikäsud) logitakse.

b. Kõiki süsteemihalduse lahenduse süsteemikäsud läbivad automaatse kontrolli, anomaaliate ja tavapärasest erinevast käitumismustrite tuvastamisel saadetakse automaatteavitus.

OPS.1.1.7.M26 Süsteemihalduse lahendusele juurdepääsu piiramine (C-I)

a. Süsteemihalduse lahenduse haldusjuurdepääs on võimalik ainult selleks otstarbeks loodud hüppeserveri (ingl *jump server*) kaudu.

OPS 1.2: Abitegevused

OPS.1.2.2 Arhiveerimine

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed dokumentide muutmatul kujul pikaajaliseks, turvaliseks ja ennistatavaks säilitamiseks. Moodul sisaldab meetmeid arhiivisüsteemi turvaliseks kavandamiseks, rajamiseks ja käigus hoidmiseks.

1.2 Vastutus

Arhiveerimise meetmete täitmise eest vastutab vastutav spetsialist.

Lisavastutajad

Kasutaja, IT-talitus.

1.3 Piirangud

Operatiivse andmevarundusega seotud meetmed on esitatud moodulis CON.3 *Andmevarunduse kontseptsioon*. Andmevarunduslahenduste turvalist kasutamist käsitlevad meetmed on esitatud moodulites APP.4.3 *Relatsioonbaasisüsteemid*, SYS.1.1 *Server üldiselt* ja SYS.1.8 *Salvestilahendused.*

2 Ohud

2.1 Andmekandjate sobimatus pikaajaliseks säilitamiseks

Aja möödudes võivad andmekandjad füüsiliselt ja tehnoloogiliselt vananeda ning seetõttu kasutuskõlbmatuteks muutuda. Kui andmete migreerimine pole asjakohaselt korraldatud, võivad tekkida aja jooksul probleemid kasutatavate andmevormingute ühilduvusega.

2.2 Arhiivisüsteemi puudulikud liigituskriteeriumid

Ebasobivate liigituskriteeriumide või piisamatu indekseerimise korral võib arhiveeritud dokumentide otsing või tunnuse järgi koondamine osutuda väga keeruliseks. Dokumentide otstarve ei ole aja möödudes enam selgelt määratav. Samuti on oht, et dokumentide liigituskriteeriumid ei ole vastavuses andmete säilitamise eesmärkidega.

2.3 Arhiivipääsude puudulik dokumenteerimine

Piisava logimise puudumisel võivad lubamatud juurdepääsukatsed arhiivile jääda avastamata. Ründaja võib märkamatult saada juurdepääsu arhiivis talletatavale teabele, andmeid kopeerida või muuta.

2.4 Paberandmete puudulik ülekandmine elektroonilisse arhiivi

Dokumentide skannimisel võidakse talletatavate andmete välisilmet ja sisu moonutada. Samuti võivad dokumendid kaotsi minna. Kui dokumentide olulised osad jäävad skannimata, siis võidakse neid ekslikult tõlgendada.

2.5 Krüpteerimisprotseduuride puudulik uuendamine arhiveerimisel

Kui arhiivi krüpteerimisprotseduure tõendusväärtuse säilimiseks regulaarselt ei kohandata, kaob krüpteerimiskaitse usaldatavus. Vananenud ning ebaturvalise signatuuri puhul saab kahelda dokumendi tervikluses, krüpteeritud andmeid ei saa enam kohtus asitõendina kasutada. Kui krüptoalgoritm ei vasta tänapäeva nõuetele, võib kannatada ka krüpteeritud dokumendi konfidentsiaalsus. Sertifikaatide muutmisel (nt Eesti ID-kaardi sertifikaadi muudatuse tõttu) võib andmete hilisem dekrüpteerimine osutuda võimatuks.

2.6 Puudulik järelevalve arhiveerimise üle

Kui arhiveerimisprotsessi toimimist ei kontrollita või seda tehakse liiga üldiselt, ei pruugi protsess vastata kehtestatud turvanõuetele. Dokumentide tervikluse või konfidentsiaalsuse rikkumine võib organisatsioonile kaasa tuua õiguslikke ja majanduslikke tagajärgi.

2.7 Õiguslike raamtingimuste rikkumine arhiveerimisel

Elektrooniliste dokumentide arhiveerimisel õiguslike raamtingimuste arvestamata jätmine võib kaasa tuua tsiviil- või karistusõiguslikke sanktsioone (nt maksu-, eelarve- või muudel õiguslikel põhjustel kehtestatud säilitustähtaegade eiramise korral).

3 Meetmed

3.1 Elutsükkel

Kavandamine

OPS.1.2.2.M1 Elektroonilise arhiveerimise mõjurite väljaselgitamine

OPS.1.2.2.M2 Arhiveerimise kontseptsiooni väljatöötamine

Evitus

OPS.1.2.2.M3 Arhiivisüsteemi ja arhiivimeediumite hoiu sobiv korraldus

OPS.1.2.2.M11 Arhiivisüsteemi haldajate koolitus

OPS.1.2.2.M17 Sobiva arhiivisüsteemi valimine

OPS.1.2.2.M18 Sobivad arhiivimeediumid

Käitus

OPS.1.2.2.M4 Andmete ühtne indekseerimine arhiveerimisel

OPS.1.2.2.M5 Arhiveeritavate andmestike asjakohane valmendus

OPS.1.2.2.M6 Arhiivisüsteemi indeksiandmebaasi tervikluse kaitse

OPS.1.2.2.M8 Arhiivipöörduste logimine

OPS.1.2.2.M10 Arhiivisüsteemi kasutamise eeskirja väljatöötamine

OPS.1.2.2.M12 Arhiivimeediumi salvestusressursside seire

OPS.1.2.2.M13 Arhiveerimisprotsesside regulaarne läbivaatus

OPS.1.2.2.M19 Arhiveerimise ja taaste regulaarne kontroll

Migreerimine

OPS.1.2.2.M9 Arhiveerimiseks sobiva andmevormingu valimine

OPS.1.2.2.M14 Arhiivisüsteemide turu regulaarne jälgimine

OPS.1.2.2.M15 Krüptomehhanismide ajakohastus arhiveerimisel

OPS.1.2.2.M16 Arhiivisüsteemi tehniliste komponentide uuendamine

Avariivalmendus

OPS.1.2.2.M7 Süsteemi- ja arhiiviandmete regulaarne varundamine

Lisanduvad kõrgmeetmed

OPS.1.2.2.M20 Krüptoprotseduuride dubleerimine

OPS.1.2.2.M21 Dokumentide turvaline üleviimine elektroonilisse arhiivi

3.2 Põhimeetmed

OPS.1.2.2.M1 Elektroonilise arhiveerimise mõjurite väljaselgitamine

a. Enne arhiveerimiskontseptsiooni koostamist on välja selgitatud võimalikud tehnilised mõjurid, sealhulgas:
   - IT-keskkond;
   - turvamehhanismid;
   - oodatavad andmemahud ja reaktsiooniajad;
   - failivormingud;
   - muudatuste mahud ja põlvkondade arv;
   - ressursitarve.

b. On välja selgitatud elektroonilise arhiveerimise õiguslikud ja korralduslikud mõjurid, sealhulgas:
   - arhiveerimise õiguslikud alused;
   - minimaalsed ja maksimaalsed säilitusajad;
   - pääsuõigused;
   - pöörduste sagedus;
   - liidestused;
   - ergonoomika.

c. On koostatud ja kinnitatud elektroonilise arhiveerimise konfidentsiaalsus-, terviklus-, käideldavus- ja autentsusnõuded.

OPS.1.2.2.M2 Arhiveerimiskontseptsiooni väljatöötamine

a. On välja töötatud arhiveerimiskontseptsioon, mis kirjeldab, milliseid eeskirju on vaja järgida, kes on vastutajad, milliseid andmeid ja millisel kujul tuleb arhiveerida ning millised on vajalikud turvameetmed.

b. Arhiveerimiskontseptsiooni dokumenteerimisel on arvestatud moodulis *OPS.1.2.2.M1 Elektroonilise arhiveerimise mõjurite väljaselgitamine* kirjeldatud mõjureid.

c. Arhiveerimiskontseptsioon on kinnitatud organisatsiooni juhtkonnas.

d. Arhiveerimiskontseptsioon vaadatakse regulaarselt üle. Vajadusel kohandatakse arhiveerimiskontseptsioon muutunud olukorraga.

OPS.1.2.2.M3 Arhiivisüsteemi ja arhiivimeediumite hoiu sobiv korraldus [IT-talitus]

a. Arhiivisüsteemid ja nendega seotud IT-komponendid on paigutatud turvatud ruumidesse. Olenevalt salvestus- või arhiivisüsteemi tüübist ja suurusest on rakendatud meetmed moodulitest INF.1 *Hoone üldiselt*, INF.2 *Serveriruum ja andmekeskus* ja INF.6 *Andmekandjate arhiiv*.

b. Arhiivisüsteemidele ligipääs, sh ruumidesse sisenemisõigus on ainult volitatud isikutel.

c. Arhiivimeediumite pikaajaliseks säilitamiseks tagatakse arhiivisüsteemi füüsiline turvalisus ja sobivad keskkonnatingimused.

OPS.1.2.2.M4 Andmete ühtne indekseerimine arhiveerimisel [IT-talitus, kasutaja]

a. Kõik arhiivis säilitatavad andmed, dokumendid ja andmekirjed indekseeritakse, et need oleksid hilisemates otsingupäringutes kiiresti leitavad.

b. Kontseptsiooni väljatöötamise käigus määratakse ühtne arhiivi indeksiteabe struktuur.

c. Indeksisüsteemi toimimist kontrollitakse pisteliste otsingutega.

OPS.1.2.2.M5 Arhiveeritavate andmestike asjakohane valmendus [IT-talitus]

a. Kogu arhiveerimisperioodi jooksul on tagatud kasutatud andmevormingute ja salvestuskandjate failisüsteemide tugi ja kasutatavus.

b. Arhiveeritud andmed on tehniliste raskusteta loetavad, reprodutseeritavad ja tõendusjõulised.

c. Krüpteerimiseks ja tõendusväärtuse säilitamiseks kasutatavad krüptomehhanismid vastavad hetkel nõutavale tasemele.

d. Salvestatud andmed on vajadusel võimalik teisendada kehtivasse andmevormingusse või migreerida uutele salvestuskandjatele, IT-riistvarasse või IT-tarkvarasse.

OPS.1.2.2.M6 Arhiivisüsteemi indeksiandmebaasi tervikluse kaitse [IT-talitus]

a. Indeksiandmebaasi terviklust kontrollitakse regulaarselt. Tervikluse kahjustumine kõrvaldatakse viivitamata, sellekohased andmed dokumenteeritakse.

b. Indeksiandmebaasi varundatakse regulaarselt, varunduse taastatavust kontrollitakse pärast igat varundust.

c. Suurte arhiivibaaside puhul indeksiandmebaasid dubleeritakse.

OPS.1.2.2.M7 Süsteemi- ja arhiiviandmete regulaarne varundamine [IT-talitus]

a. Kõiki arhiiviandmeid, indeksiandmebaase ja asjakohaseid süsteemiandmeid varundatakse varunduskontseptsioonis määratud perioodilisusega (vt CON.3 *Andmevarunduse kontseptsioon*).

OPS.1.2.2.M8 Arhiivipöörduste logimine [IT-talitus]

a. Kõikide arhiivipöörduste puhul logitakse pöördumise kuupäev, kellaaeg, kasutaja, arhiivipöörduse põhjus, klientsüsteem, tehtud toimingud ning vigade esinemisel ka veateated.

b. Arhiivipöördumiste logiandmeid analüüsitakse võimalike kõrvalekallete tuvastamiseks regulaarselt. Kõrvalekalde tuvastamisel algatatakse intsidendikäsitluse protsess.

c. Kriitilisi sündmusi, nagu andmete kustutamine või andmekandja arhiivisüsteemist eemaldamine, kontrollitakse kohe pärast vastava logikirje tekkimist.

d. Arhiivipöördumiste logiandmeid säilitatakse arhiveerimiskontseptsioonis määratud säilitustähtaja jooksul.

OPS.1.2.2.M9 Arhiveerimiseks sobiva andmevormingu valimine [IT-talitus]

a. Logiandmete arhiveerimisel kasutatakse standardseid, elektrooniliselt töödeldavaid andmevorminguid, mille süntaks ja semantika on laiemalt avaldatud.

b. Valitud lahendus tagab andmete võimalikult pikaajalise säilitamise.

c. Valitud andmevormingud võimaldavad reprodutseerida arhiveeritud materjali tõetruul algkujul.

d. Dokumentide tõendusväärtuse säilitamise ja muutmiskindla arhiveerimise tagamiseks sobilik vorming on PDF (ver A-2a või /A-2u), mis võimaldab dokumendi ühesuguse esituse erineva riist- ja tarkvaralise konfiguratsiooniga arvutites.

e. Pildimaterjalide tõendusväärtuse säilitamise ja muutmiskindla arhiveerimise tagamiseks kasutatakse kadudeta reprodutseerimist võimaldavaid vorminguid ja pilditihendusprotseduure, selleks sobilikud vormingud on TIFF (ver 6) või PNG (ver 1.2).

f. Audio- ja videofailide arhiivivorminguteks on sobilikud WAV, FLAC (ver 1.21), AVI (pakkimata), MOV (pakkimata) ja MPEG-4 (koodek H.264) vormingud.

g. Digiallkirjastatud dokumendi konteinerite arhiveerimiseks kasutatakse andmevormingut ASICE.

3.3 Standardmeetmed

OPS.1.2.2.M10 Arhiivisüsteemi kasutamise eeskiri [IT-talitus]

a. Organisatsioonis on kehtestatud arhiivisüsteemi kasutamise eeskiri, mis hõlmab järgnevat:
   - käituse ja halduse rollide lahusus ja vastutused;
   - kokkulepitud teenusetase;
   - pääsuõiguste haldus;
   - andmete ja andmekandjate käitluse protseduurid;
   - arhiivisüsteemi ja keskkonna järelevalve;
   - andmete varundamise protseduurid;
   - arhiivitoimingute logimine;
   - arhiivisüsteemi muudatuste haldus.

b. Arhiivisüsteemi haldajad järgivad arhiivisüsteemi kasutamise eeskirja.

OPS.1.2.2.M11 Arhiivisüsteemi haldajate koolitus [IT-talitus]

a. Arhiivisüsteemi haldajaid koolitatakse vähemalt järgmistel teemadel:
   - kasutuselevõetud arhiivisüsteemi ja selle operatsioonisüsteemi arhitektuur ja turvamehhanismid;
   - arhiivisüsteemi installimine ja hooldus;
   - andmete ja andmekandjate käitlemise kord;
   - haldustoimingute dokumenteerimine;
   - konfigureerimis-, uuendus-, ja kõrvaldusprotseduurid;
   - eeskirjast lahknevuste käsitlemine.

b. Koolitus ja sellest osavõtt dokumenteeritakse.

c. Arhiivisüsteemi muudatuste korral korraldatakse haldajatele täiendkoolitusi.

OPS.1.2.2.M12 Arhiivimeediumi salvestusressursside seire [IT-talitus]

a. Arhiivimeediumi vaba salvestusmahtu kontrollitakse vahetult enne salvestust.

b. Kui vaba salvestusmaht väheneb alla määratud piirmäära, teavitatakse sellest süsteemi haldajat.

c. Salvestusmahu suurendamiseks on olemas varuressurss ja koostatud protseduur selle kasutusele võtmiseks.

OPS.1.2.2.M13 Arhiveerimisprotsessi regulaarne läbivaatus

a. Arhiveerimisprotsessi õigsust ja nõuetekohasust kontrollitakse regulaarselt.

b. Läbivaatuse läbiviimiseks koostatakse küsimuste kontroll-loetelu, lähtudes arhiveerimiskontseptsioonist (vt OPS.1.2.2.M2 *Arhiveerimiskontseptsiooni väljatöötamine*) ja arhiivisüsteemi kasutamise eeskirjast (vt OPS.1.2.2.M10 *Arhiivisüsteemi kasutamise eeskiri*).

c. Läbivaatuse käigus tuvastatud kõrvalekallete ja nõrkustega tegeletakse esimesel võimalusel.

OPS.1.2.2.M14 Arhiivisüsteemide turu regulaarne jälgimine [IT-talitus]

a. Arhiivisüsteemide turu ja arengute jälgimisel pööratakse tähelepanu järgmistele aspektidele:
   - standardite muutumine või lisandumine;
   - muudatused kasutusel oleva süsteemi valmistaja toodangus;
   - teated avastatud nõrkustest, näiteks krüptoalgoritmides;
   - teated krüptoalgoritmide kaitsevõime vähenemise ohust;
   - seniste andmevormingute muutumine ja uute ilmumine.

b. On määratud vähemalt üks töötaja, kes jälgib regulaarselt ülalnimetatud teavet, hindab selle olulisust ja vajadusel soovitab parendustegevusi.

OPS.1.2.2.M15 Krüptomehhanismide ajakohastus arhiveerimisel [IT-talitus]

a. Regulaarselt kontrollitakse algoritmide, võtmete, krüptotoodete ja protseduuride ajakohasust ja vastavust kehtivatele standarditele (vt CON.1.M1 *Krüptovahendi valimise kord*).

b. On kehtestatud turvaprotseduur krüptomehhanismi nõrgenemise puhuks (nt krüpteeritakse nõrgenenud krüptomehhanismiga arhiiviandmed uuesti, kasutades turvalisemat krüptoalgoritmi).

OPS.1.2.2.M16 Arhiivisüsteemi tehniliste komponentide uuendamine [IT-talitus]

a. Arhiivisüsteemi tehnilist ajakohasust kontrollitakse (vt OPS.1.2.2.M14 *Arhiivisüsteemide turu regulaarne jälgimine*) regulaarselt.

b. Uute komponentide sobivust testitakse enne nende kasutuselevõttu.

c. On kehtestatud migratsiooniprotseduur üleminekuks uutele vormingutele või vahenditele.

d. Kõik arhiivisüsteemi komponentide muudatused, konverteerimised, testimised ja asenduskavad dokumenteeritakse.

OPS.1.2.2.M17 Sobiva arhiivisüsteemi valimine [IT-talitus]

a. Arhiivisüsteemi valimisel lähtutakse koostatud arhiveerimiskontseptsioonist (vt OPS.1.2.2.M2 *Arhiveerimiskontseptsiooni väljatöötamine*).

b. Arhiveerimisüsteemi valimisel arvestatakse järgmist:
   - dokumentide ja andmete versioonihalduse tugi;
   - funktsioonide ja protsesside vastavus standardile ISO 14721;
   - pääsu reguleerimise mehhanism mitmeastmelise õiguste süsteemiga;
   - logimine, vt OPS.1.2.2.M8 *Arhiivipöörduste logimine*;
   - järelevalvele pääsu korraldus;
   - süsteemi laiendatavus;
   - pöördusaeg;
   - piisav salvestusmaht;
   - käsitsi tehtavate operatsioonide võimalikkus;
   - vaba salvestusmahu automaatkontroll ja mahupiiri alarm;
   - ühilduvus muude komponentide ja süsteemidega;
   - krüptomehhanismid või nende tugi.

OPS.1.2.2.M18 Sobivad arhiivimeediumid [IT-talitus]

a. Arhiivimeediumite valimisel arvestatakse arhiivimeediumi vastavust nõutavale andmemahule, maksimaalsele lubatud pöördusajale ja samaaegsete pöördumiste arvule.

b. Arhiivimeediumi eeldatav tööiga võimaldab arhiveerimist nõutud säilitusaja jooksul.

OPS.1.2.2.M19 Arhiveerimise ja taaste regulaarne kontroll [IT-talitus]

a. Arhiveerimisprotsessi toimimist kontrollitakse logiandmete või arhiivimeediumite regulaarsete ülevaatustega.

b. Arhiivimeediumi loetavust ja terviklust testitakse vähemalt kord aastas.

c. Arhiivisüsteemi riistvarakomponentide (eriti arhiivi mehaaniliste osade) töövõimet kontrollitakse regulaarselt.

d. Vigade ja eelmääratud sündmuste (nt andmete kopeerimine) ilmnemisel teavitatakse määratud töötajaid toimunud sündmusest automaatselt.

e. Avastatud vigade ja ilmnenud tõrgete käsitluseks on kehtestatud protseduur.

3.4 Kõrgmeetmed

OPS.1.2.2.M20 Krüptoprotseduuride dubleerimine [IT-talitus] (C-I)

a. Arhiiviandmete pikaajaliseks säilitamiseks kasutatakse üksnes kehtivate standardite ja normide kohaseid krüptoprotseduure.

b. Arhiveeritavaid andmeid töödeldakse paralleelselt vähemalt kahe erineva krüptoprotseduuriga.

OPS.1.2.2.M21 Dokumentide turvaline üleviimine elektroonilisse arhiivi (C-I)

a. Paberdokumentide skaneerimiseks on määratud rollid ja kohustused.

b. Skaneerimise väljasttellimisel on teenuselepingus määratud kohustuslikud turvanõuded.
c. On koostatud protseduur dokumentide skaneerimiseks ettevalmistamiseks.
d. Paberdokumentide elektrooniline kuju vastab sisult ja esitusvormilt originaalile.

4 Lisateave

Lühend	Publikatsioon
[RT]	Vabariigi Valitsuse määrus „Arhiivieeskiri“ , vastu võetud 22.11.2011, https://www.riigiteataja.ee/akt/129122011229?leiaKehtiv

OPS.1.2.4 Kaugtöö

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed kaugtöö raames talletatava, töödeldava ja edastatava teabe kaitseks.

1.2 Vastutus

Kaugtöö meetmete täitmise eest vastutab infoturbejuht.

Lisavastutajad

IT-talitus, töötaja, personaliosakond, ülemus.

1.3 Piirangud

Kaugtöökoha taristu turbe meetmed esitatakse moodulis INF.8 *Kodutöökoht.* Täiendavad meetmed esitatakse moodulis INF.9 *Mobiiltöökoht.*

2 Ohud

2.1 Kaugtöökoha eeskirja puudumine või puudulikkus

Kaugtöökoha eeskirja puudumisel ei pruugi töötaja oma kohustusi täpselt teada. Kui töötaja ei oska kaugtöökohal infoturbe intsidenti ära tunda või ei tea, keda sellest teavitada, võib konfidentsiaalne teave sattuda võõrastesse kätesse.

2.2 Teenistusliku kaugtööarvuti lubamatu privaatkasutus

Tööandja otsese kontrolli alt väljas olevasse arvutisse võidakse paigaldada tundmatu päritoluga tarkvara. Kasutaja hoolimatuse tõttu võib arvutisse sattuda kahjurvara. Arvutile võivad ligi pääseda lisaks kaugtöötajale ka tema pereliikmed ja külalised.

2.3 Viivitused kaugtöötaja kättesaamatuse tõttu

Kui kaugtöötajaga pole kokku lepitud kindlaid aegu, millal töötaja peab olema kättesaadav, võib ta osutuda vajalikul hetkel kättesaamatuks. See võib tuua kaasa viivitusi tööprotsessis. Sõltuvalt organisatsioonist võib see oluliselt mõjutada tervet äriprotsessi.

2.4 Teabe mittejõudmine töötajani

Kaugtöötajal on vähem võimalusi osaleda tööalases teabevahetuses. Seetõttu kahaneb seotus organisatsiooni äriprotsessidega ja väheneb kaugtöötaja jõudlus. Kui ei ole tagatud teabe liikumine, ei jõua kaugtöötajale kohale ka olulised infoturbe teated.

2.7 Turvameetmete eiramine

Kaugtöökoha järelevalvevõimaluse piiratuse tõttu võib juhtuda, et töötaja ei rakenda soovitatud või kohustuslikke turvameetmeid või ei tee seda täies mahus. Turvameetmete mitterakendamisest kaugtöökohas võib tekkida kahju, mida tavaolukorras oleks võimalik vältida. Konfidentsiaalne teave võib sattuda volitamata isikute kätte.

3 Meetmed

3.1 Elutsükkel

Kavandamine

OPS.1.2.4.M1 Kaugtöö eeskiri

OPS.1.2.4.M6 Kaugtöö turbekontseptsioon

OPS.1.2.4.M7 Sidevahendite kasutamise kord

OPS.1.2.4.M9 Kaugtöökoha kasutajatugi ja hooldus

OPS.1.2.4.M10 Kaugtöökoha nõuete analüüs

Evitus

OPS.1.2.4.M2 Kaugtööarvuti turve

Käitus

OPS.1.2.4.M5 Kaugtöötajate teadlikkuse tõstmine ja koolitus

OPS.1.2.3.M8 Regulaarne teabevahetus organisatsiooniga

3.2 Põhimeetmed

OPS.1.2.4.M1 Kaugtöö eeskiri [ülemus, personaliosakond]

e. Töötajatele järgimiseks on koostatud ja tehtud töötajatele kättesaadavaks kaugtöö korraldust reguleeriv eeskiri.

f. Kaugtöö eeskirjas on arvestatud järgmisi turvaaspekte:
    c. konfidentsiaalse teabe käitlus;
    d. andmekaitsenõuded;
    e. andmevarundus ja andmete sünkroniseerimine;
    f. andmeside kasutamine;
    g. kaugpääsuõigused;
    h. dokumentide ja andmekandjate transport ja säilitamine;
    i. turvasündmustest teatamise kord.

g. On koostatud töökaitse õiguslikke aspekte arvestavad, tööandja ja töötaja vahelised kaugtöö kokkulepped, milles on määratletud vähemalt järgmine:

d. kaugtöö vabatahtlikkus;
e. töövahendid;
f. tööaeg ja kättesaadavus;
g. reageerimisajad, näiteks e-kirjade lugemise sagedus;
h. ületunnitöö, lisatasud ja täiendavate kulude tasumine;
i. materiaalne vastutus;
j. kaugtöö lõpetamine.

h. Kaugtöö eeskirja vaadatakse üle ja seda ajakohastatakse regulaarselt.

OPS.1.2.4.M2 Kaugtööarvuti turve

a. Kaugtööarvutit kasutatakse ainult määratud otstarbeks (nt ei tohi kasutaja installida kaugtööarvutisse heakskiitmata tarkvara).
b. Kaugtööarvutit kasutab ainult selleks volitatud isik. Volitatud isikuteks on kaugtöötaja ja kaugtööarvutite haldur.
c. Kaugtööarvuti turvameetmed sõltuvad töödeldavate andmete kaitsetarbest. Rakendatud on vähemalt järgmised meetmed:
    - turvalised identifitseerimis- ja autentimismehhanismid, mis reageerivad vigasele sisestusele juurdepääsu ajutise sulgemisega;
    - automaatne ekraanilukk, mida saab avada alles pärast uut identifitseerimist ja autentimist;
    - turvakriitiliste parameetrite miinimumnõuded (nt paroolinõuded) tagavad piisava turvalisuse;
    - arvutis tehakse regulaarset andmevarundust;
    - logimise sisu ja maht on rikete ja turvasündmuste avastamiseks piisav;
    - arvuti kõvaketas on krüpteeritud;
    - arvutis on vahendid failide krüpteerimiseks;
    - arvuti süsteemikonfiguratsioon on seatud maksimaalselt turvaliseks.

OPS.1.2.4.M5 Kaugtöötajate teadlikkuse tõstmine ja koolitus

- Kaugtöötajad on läbinud kaugtöö turvameetmete alase koolituse.
- Kaugtöötaja koolitusel on käsitletud järgmisi aspekte:
    a. kaugtöö ohud;
    b. tööalaste dokumentide turvaline hoidmine;
    c. kaugtöökoha füüsiline turve;
    d. võrguturve;
    e. andmekandjate turvaline kasutamine;
    f. lihtsamad hooldetööd ja probleemilahendused.
- Kaugtöötajate koolitamisel järgitakse meetmeid moodulist ORP.3 *Infoturbe teadlikkuse tõstmine ja koolitus*.
- Kaugtöötaja koolitust korratakse regulaarselt.

3.3 Standardmeetmed

OPS.1.2.4.M6 Kaugtöö turbekontseptsioon

a. On koostatud kaugtöö turbekontseptsioon, mis esitab kaugtöökoha kaitsetarbe, turvaeesmärgid ja turvanõuded.
b. Kaugtöö turbekontseptsioonis dokumenteeritakse vähemalt järgmine:
    - andmete, dokumentide ja andmekandjate käitluse kord;
    - organisatsiooni ja kaugtöökoha vahelise side korraldamine;
    - autentimismehhanismid;
    - võrguühenduste kasutamise kord;
    - andmevahetuse kord;
    - andmevarunduse kord.
c. Kaugtöö turbekontseptsioon on kooskõlas organisatsiooni üldise turbekontseptsiooniga.
d. Kontseptsiooni ajakohastatakse regulaarselt.

OPS.1.2.4.M7 Sidevahendite kasutamise kord [IT-talitus, töötaja]

a. Sidevahendite kasutamise raamtingimused on määratud kaugtöö turbekontseptsioonis.
b. Sidevahendite kasutamise korras on määratud vähemalt:
    c. teabevahetuseks kasutatavad sidevõimalused (sh sõnumiside, telefon, e-post);
    d. andmete edastamiseks kasutatavad teenused;
    e. videokonverentsiteenuste kasutamine;
    f. teabevahetuse turvameetmed;
    g. digiallkirjastamise kasutamine;
    h. juhised avalike Interneti-teenuste kasutamisel tööks ja isiklikuks tarbeks.

OPS.1.2.4.M8 Regulaarne teabevahetus organisatsiooniga [ülemus, töötaja]

a. On korraldatud kaugtöötaja regulaarne teabevahetus organisatsiooni ja kaastöötajatega.
b. Tööalased teadaanded ja teave infoturbe muudatuste kohta jõuab kaugtöötajani operatiivselt ja viivitusteta.
c. Kõik kaastöötajad teavad, kuidas kaugtöötajaga ühendust võtta.

OPS.1.2.4.M9 Kaugtöökoha kasutajatugi ja hooldus [IT-talitus, töötaja]

a. Kaugtöökoha arvuti tark- ja riistvara probleemide lahendamiseks on loodud kasutajatoe funktsioon ja määratud kontaktisikud.
b. Kasutajatoel on teada kaugtöökoha arvuti riist-ja tarkvara konfiguratsioon.
c. Kaughooldust tehakse eelnevalt kokkulepitud ajal. Kaugligipääs arvutile võimaldatakse ainult kaughoolduse ajaks ning selleks volitatud töötajale.
d. Kokku on lepitud, kuidas toimub IT-vahendite transport hooldusesse.

OPS.1.2.4.M10 Kaugtöökoha nõuete analüüs [IT-talitus]

- Enne kaugtöökohtade loomist on läbi viidud nõuete analüüs, mis sisaldab vähemalt järgmist:
    - konfidentsiaalsusnõuded kaugtöökohas käideldavale teabele;

- organisatsioonile juurdepääsu saamise eesmärgid;
- andmeliikluse maht kaugtöökoha ja organisatsiooni vahel;
- sisevõrguteenuste kasutamise vajadused;
- Interneti kasutamise vajadused;

a. nõuded dokumentide ja andmekandjate transportimisele:
b. kaugtöökoha riist- ja tarkvarakomponentide vajadus ja valik (kooskõlastatakse IT-haldusega).

- Konkreetse kaugtöökoha nõuded dokumenteeritakse ja kooskõlastatakse IT-juhiga.

3.4 Kõrgmeetmed

Antud moodulis kõrgmeetmed puuduvad.

OPS.1.2.5 Kaughooldus

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed aktiivse ja passiivse kaughoolduse käigus salvestatava, töödeldava ja edastatava teabe ning hooldusliideste kaitseks.

1.2 Vastutus

Kaughoolduse meetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Kasutaja.

1.3 Piirangud

Moodulis ei käsitleta kõiki kaughoolduse tegevusi, seega tuleb lisaks arvestada meetmeid moodulitest OPS.1.1.3 *Paiga- ja muudatusehaldus*, ORP.3 *Infoturbe teadlikkuse tõstmine ja koolitus*, CON.1 *Krüptokontseptsioon* ja CON.3 *Andmevarunduse kontseptsioon*.

Samuti tuleb rakendada meetmeid moodulitest OPS.2 *Käidutööd teenusena* ja OPS.3 *Teenuseandja käidutööd*. Pilvteenuste puhul tuleb lisaks arvestada moodulit OPS.2.2 *Pilvteenuste kasutamine.*

IT-süsteemide keskhaldust käsitletakse moodulites OPS.1.1.2 *IT-süsteemide haldus* ja OPS.1.1.7 *Süsteemihaldus*.

Käidutehnoloogia süsteemide kaughooldust käsitletakse moodulis IND.3.2 *Käidutehnoloogia komponentide kaughooldus*.

2 Ohud

2.1 Kaughoolduse eeskirjade puudulik järgimine

Kui asjaosalised ei tunne või ei järgi kaughoolduse eeskirju, võidakse hooldustööde käigus teha vigu. Kuna kaughooldust tegevatel töötajatel on ka tavapärasest suuremad õigused, võib tähelepanematusest või mugavusest tingitud eksimus kaasa tuua olulise kahju.

Turvameetmete eiramine kaughoolduse käigus on raskesti tuvastatav ning sellest tingitud turvanõrkuste ärakasutamisel tehtud ründeid on raske avastada ja tõrjuda.

2.2 Kaughoolduse kavandamise ja reguleerimise puudumine või puudulikkus

Kui kaughoolduse kavandamisel tehakse vigu ega arvestata võimalike turvanõrkustega, võidakse mõjutada mitte ainult ühe IT-süsteemi, vaid organisatsiooni kõikide IT-süsteemide turvalisust. Kaughooldusega seotud turvanõrkused võivad esineda nõrkades sideprotokollides, paigahalduse protsessides, krüpto- ja autentimismehhanismides.

2.3 Väär autentimine kaughoolduses

Ebaturvaliste autentimismehhanismide kasutamise tagajärjel võib kaughooldusarvuti või -tööriistade haldusõiguse saada volitamata isik. See võib kaasa tuua IT-süsteemide ja rakenduste lubamatuid konfiguratsioonimuutusi, andmete kustutamise või konfidentsiaalse teabe lekke. Risk on veelgi suurem, kui kaughooldust teostab väline partner.

2.4 Tegemata või väär kaughooldus

Kui pidevat hooldust vajavatele IT-süsteemidele jäetakse kaughooldus tegemata, võib see halvimal juhul muuta IT-süsteemi kasutuskõlbmatuks.

Kaughoolduse käigus tehtud vead võivad IT-süsteemide käitamisel põhjustada tõrkeid. Kui hooldus hilineb või seda tehakse vääralt, võivad teadaolevad turvanõrkused jääda parandamata.

2.5 Ebaturvaliste protokollide kasutamine kaughoolduses

Kui kaughoolduse andmeside on krüpteerimata või kui kahe lõpp-punkti või võrgu vahel tunneli loomiseks kasutatakse ebaturvalisi protokolle, näiteks IPSec, SSH või SSL/TLS aegunud versioone, ei ole andmeside turvalisus piisavalt tagatud.

2.6 Kaughooldusfunktsioonide kontrollimatu kasutamine

Kui kaughooldustöid tegevate isikute tööülesanded pole lepinguga reguleeritud või dokumenteeritud, võivad kaughoolduse tegijad oma volitusi ületada ja IT-süsteemile kahju tekitada.

2.7 Võrgustatud kaughooldusteenuse lubamatu kasutamine

Kui IT-süsteemide kaughoolduseks on võimaldatud juurdepääs veebibrauserist läbi kolmanda osapoole veebiserveris asuva, võrgustatud teenuse (ingl *online service*), siis puudub süsteemiülematel kontroll selle üle, kes, millal ja mis otstarbel seda ühendust kasutab. IT-süsteemi ja serveri vaheline andmesidekanal on pidevalt avatud. Krüpteerimata andmeside puhul on võimalik saadetavaid andmeid manipuleerida.

2.8 Integreeritud kaughoolduskomponentide lubamatu kasutamine

Kui IT-süsteemide käitamisel ei arvestata IT-süsteemi integreeritud kaughoolduse funktsionaalsust ega piirata selle kasutamist, võib süsteemidele ja andmetele tekkida volitamata juurdepääs. IT-süsteemidesse integreeritud kaughoolduskomponentide funktsionaalsus pole tihti piisavalt dokumenteeritud, need võivad sisaldada turvanõrkusi ja võimaldada möödapääsu võrgu ja operatsioonisüsteemi tasandil rakendatud turbemehhanismidest.

3 Meetmed

3.1 Elutsükkel

Kavandamine

OPS.1.2.5.M1 Kaughoolduse rakendamise kava

OPS.1.2.5.M6 Kaughoolduse eeskiri

OPS.1.2.5.M7 Kaughoolduse dokumentatsioon

ORP.4 Identiteedi ja õiguste haldus

Soetamine

OPS.1.2.5.M9 Sobivate kaughooldustööriistade valimine

Evitus

OPS.1.2.5.M3 Sideühenduste turve kaughooldusel

OPS.1.2.5.M5 Võrgustatud hooldusteenuste turvaline rakendamine

OPS.1.2.5.M8 Turvalised kaughoolduse protokollid

OPS.1.2.5.M10 Kaughooldustööriistade turvaline kasutamine

OPS.1.2.5.M17 Autentimismehhanismid kaughooldusel

OPS.1.2.5.M19 Kaughooldus kolmandate kaudu

Käitus

OPS.1.2.5.M2 Turvaline ühenduse loomine kaughooldusel

OPS.1.2.5.M20 Kaughoolduse turvaline läbiviimine

OPS.1.2.5.M24 Integreeritud kaughooldusfunktsioonide turve

OPS.1.2.5.M25 Väljaspoolt haldusvõrku tehtava kaughoolduse piiramine

Avariivalmendus

OPS.1.2.5.M21 Avariiplaan kaughoolduse tõrke puhuks

Lisanduvad kõrgmeetmed

OPS.1.2.5.M14 Kaughooldusklientide turvaline seadistus

OPS.1.2.5.M22 Mobiilsidevõrkude liiasus

3.2 Põhimeetmed

OPS.1.2.5.M1 Kaughoolduse rakendamise kava

a. Kaughoolduse kavandamisel on arvestatud organisatsiooni vajadusi ja kaughoolduse tehnilisi ning korralduslikke aspekte.

b. Kaughoolduse rakendamise kavas on määratud:

- kaitsetarve ja turvaeesmärgid;
- vastutused kaughoolduse teostamisel;
- õiguslikud ja korralduslikud kitsendused;

- kaughoolduse kanalid;
- teenuseandja kasutamine;
- võrgueraldusnõuded.

c. Suurema kaitsetarbe korral on kaughooldus võimaldatud ainult läbi spetsiaalse haldusvõrgu.

OPS.1.2.5.M2 Turvaline ühenduse loomine kaughooldusel [kasutaja]

a. Kaughoolduse ühenduse saab algatada ainult IT-süsteemi kasutaja ehk hooldatav pool.

b. Kaughoolduse alustamisel autenditakse väline hooldaja turvaliselt. Kui ühendus kaughoolduskohaga mingil põhjusel katkeb, on uus juurdepääs võimalik ainult ennast uuesti autentides.

OPS.1.2.5.M3 Sideühenduste turve kaughooldusel

a. Pääsuõigused ja sideühenduste loomise võimalused on piiratud minimaalsuse põhimõtte alusel.

b. Andmevahetus kaughooldusserveri ja -kliendi vahel krüpteeritakse.

c. Pärast kaugpääsu kasutamise lõpetamist suletakse (desaktiveeritakse) kõik kasutatud sideühendused.

d. Kaughooldustööriistad paigaldatakse ainult tööjaamadesse, mida kasutatakse kaughoolduseks.

e. Andmeedastuse jälitatavuse tagamiseks andmevahetus logitakse.

3.3 Standardmeetmed

OPS.1.2.5.M5 Võrgustatud hooldusteenuste turvaline rakendamine [kasutaja]

a. Kaughooldus võrgustatud teenuse (ingl *online service*) kaudu on üldjuhul keelatud ja blokeeritud.

b. Võrgustatud hooldusteenuseid rakendatakse ainult põhjendatud erandina, võimalikud kasutusjuhud on reguleeritud, kasutamine registreeritakse ning kinnitatakse.

c. Klientarvutite automaatne ühendumine võrgustatud teenustega on keelatud, ühenduse takistamiseks rakendatakse tehnilisi meetmeid.

OPS.1.2.5.M6 Kaughoolduse eeskiri

a. Kaughoolduse nõuded on dokumenteeritud infoturvapoliitikas. Eraldi kaughoolduse eeskirja olemasolul on sellele infoturvapoliitikas viidatud.

b. Kaughoolduse eeskirjaga on tutvunud kõik osapooled, kes osalevad kaughoolduse kava väljatöötamisel, elluviimisel, kasutamisel ja kasutamise lõpetamisel.

c. Kaughoolduse eeskirja järgimist kontrollitakse regulaarselt.

OPS.1.2.5.M7 Kaughoolduse dokumentatsioon

a. Kaughoolduse dokumentatsioon on piisav ja ajakohane.

b. Kaughoolduse dokumentatsioon sisaldab vähemalt järgmist:
   - hooldatavate IT-süsteemide konfiguratsioonid;
   - süsteemide kasutajad ja nende õigusteprofiilid;
   - lisandunud riist-ja tarkvarakomponendid;

- andmevarunduse ja andmekandjate käituse protseduurid;
- avastatud ja kõrvaldatud rikete kirjeldused.

c. Dokumentatsiooni hoitakse turvaliselt. Volitatud isikutel on vajadusel võimalik dokumentatsioonile kiiresti juurde pääseda.

OPS.1.2.5.M8 Turvalised kaughoolduse protokollid

a. Kaughoolduseks kasutatakse ajakohaseid ja turvaliseks loetud sideprotokolle.

b. Andmevahetus on krüpteeritud. Tunneldamiseks kasutatakse kaitsetarbele vastavaid krüpteerimisprotseduure (vähemalt SSH v2, TLS 1.2, SNMP v3, IPSec IKEv2-ga).

c. Kaughoolduseks kasutatakse sideprotokolle, mis võimaldavad tuvastada edastatavates andmetes juhuslikke häireid ning neid automaatselt kõrvaldada. Saaja kinnitab andmete vastuvõttu.

d. Kasutatavate protokollide ajakohasuse tagamiseks jälgitakse regulaarselt teavet avastatud nõrkuste kohta.

OPS.1.2.5.M9 Sobivate kaughooldustööriistade valimine

a. Kaughooldustööriistade valimisel arvestatakse meedet OPS.2.4.M1 *Kaughoolduse rakendamise kava*.

b. Kaughooldustööriistad valitakse organisatsiooni käitus-, turva- ja andmekaitsenõuetel põhineva analüüsi ja kaasneva riskihinnangu alusel.

c. Kõik kaughooldustööriistade hankimise otsused kooskõlastatakse hankimise, süsteemide ja rakenduste eest vastutajate ning turbehaldusega.

OPS.1.2.5.M10 Kaughooldustööriistade turvaline kasutamine [kasutaja]

a. Kaughooldustööriistade kasutamiseks on koostatud kasutusjuhendid koos näidisprotseduuride kirjeldustega.

b. Kasutajad on läbinud kaughooldustööriistade kasutamise koolituse.

c. Kaughooldustööriistadega seotud tehniliste küsimuste lahendamiseks on määratud kontaktisik.

OPS.1.2.5.M17 Kaughoolduse autentimismehhanismid

a. Kaughooldussessiooni alustamiseks kasutatakse mitmikautentimist (ingl *multifactor authentication*).

b. Autentimismeetodi valik ja selle valimise põhjused on dokumenteeritud.

OPS.1.2.5.M19 Kaughooldus välisteenusena

a. Kõik välise teenuseandja poolt kaughooldusena tehtud muudatused (nt konfigureerimisseadetes, lähtekoodis) dokumenteeritakse. Muudatuste dokumentatsioon antakse üle kaughooldatavale organisatsioonile.

b. Välise teenuseandja töötajad kohustuvad täitma lepingus kokku lepitud nõudeid, sealhulgas konfidentsiaalsusleppeid.

c. Välise teenuseandja töötajate tehtavaid hooldustoiminguid jälgitakse ja võimalusel need salvestatakse. Organisatsioonis on määratud kaughoolduse seire eest vastutaja.

d. Kaughooldus algatatakse ainult sisevõrgust ja ainult kindlaks perioodiks.

e. Kaughoolduspääs välisele teenuseandjale antakse minimaalsuse põhimõtte alusel.

f. Välise teenuseandja töötajad autendivad ennast alati isikustatud kasutajana.

g. Kaughooldust saab mistahes ajal sisevõrgust katkestada.

h. Kaughoolduse tegemisel kolmandate kaudu rakendatakse lisaks mooduli OPS.2.3 *Väljasttellimine* meetmeid.

OPS.1.2.5.M20 Kaughoolduse turvaline läbiviimine

a. Kaughooldust teostatakse eelneva teavituse ja kinnituse alusel.

b. Kaughoolduspääs antakse ainult alles pärast tulemuslikku autentimist.

c. Kaughoolduseks ei anta täielikke haldusõigusi. Kaughooldajal puudub ligipääs IT-süsteemidele, mida hoolduseks vaja ei ole.

d. Andmevahetust kaughooldusserveri ja -kliendi vahel kontrollitakse tulemüüri abil. Kasutusel on ummistusrünnete avastamise ja tõrje meetmed.

e. Kõik kaughooldustoimingud, kaughoolduse algus, lõpp ja asjaosalised registreeritakse ja logitakse.

OPS.1.2.5.M21 Avariiplaan kaughoolduse tõrke puhuks

a. On välja töötatud avariiplaan tõrgetest tuleneva kahju minimeerimiseks, hooldustoimingute tagasivõtmiseks ning tavapärase töö kiireks taasteks.

b. Avariiplaani koostamisel ja testimisel rakendatakse meetmeid moodulist DER.4 *Avariihaldus*.

OPS.1.2.5.M24 Integreeritud kaughooldusfunktsioonide turve

a. IT-süsteemide hankimisel hinnatakse integreeritud kaughooldusfunktsioonide võimalusi ja turvalisust.

b. Juhul kui IT-süsteemidesse integreeritud kaughooldusfunktsioone ei kasutata või kui need võivad sisaldada turvanõrkusi, on integreeritud kaughooldusfunktsioonid desaktiveeritud.

c. IT-süsteemi komponentidele, mille kaughooldus on realiseeritud püsivara tasemel, on juurdepääs ainult eraldiseisvast haldusvõrgust.

OPS.1.2.5.M25 Väljaspoolt haldusvõrku tehtava kaughoolduse piiramine

a. Võimalusel välditakse kaughooldust väljastpoolt haldusvõrku asuvast seadmest.

b. Kaughoolduse teostamine väljaspool haldusvõrku asuvast klientseadmest on lubatud ainult läbi haldusvõrgus asuva hüppeserveri (ingl *jump server*).

c. Hüppeserveri juurdepääs on lubatud ainult usaldusväärsetele ja vastavava vajadusega klientseadmetele.

3.4 Kõrgmeetmed

OPS.1.2.5.M14 Kaughoolduskliendi turvaline seadistus (C)

a. Kaughoolduseks kasutatakse ainult kaughoolduse teostamiseks ettevalmistatud klientseadmeid.

b. Kaughoolduse klientseadmesse paigaldatud kaughooldustööriistade kõik funktsioonid ja komponendid, mis ei ole hooldustööde läbiviimiseks vajalikud, on desaktiveeritud.

c. Kaughooldustööriistad ja tööjaamad, milles neid kasutatakse, on turvaliselt konfigureeritud ja seadistatud.

d. Kaughoolduse klientseadme andmesideühendus on piiratud. Lubatud on ainult hooldustööde läbiviimiseks vajalikud andmesideühendused.

e. Kaughoolduseks kasutatakse spetsiaalselt selleks otstarbeks loodud kasutajakontot.

OPS.1.2.5.M22 Kaughoolduse sidevõrkude liiasus (A)

a. Kaughoolduse tegemiseks avariiolukorras on võimalik IT-süsteemile juurdepääsuks kasutada varusideühendust (nt. 4G mobiilsidevõrku).

OPS.1.2.6 Kellade sünkroniseerimine NTP-serveriga

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed NTP-serveri (NTP- Network Time Protocol) ja NTP-klientseadmete kellade turvaliseks sünkroniseerimiseks ning usaldusväärse ja täpse kellaaja tagamiseks kõigis seotud IT-süsteemides.

1.2 Vastutus

Kellade sünkroniseerimise meetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Lisavastutajad puuduvad.

1.3 Piirangud

Moodulis esitatud meetmed rakenduvad kõigile NTP-d kasutavatele IT-süsteemidele.

Serveritele kehtestatud üldisi turvameetmeid käsitletakse moodulis SYS.1.1 *Server üldiselt*, klientarvutitele kohalduvad meetmed on esitatud moodulis SYS.2.1 *Klientarvuti üldiselt*.

2 Ohud

2.1 Viga NTP-serveri rakendamisel

Võib juhtuda, et kõik IT-süsteemid ei ole täpse ajateabe saamiseks NTP-serveriga ühendatud. Näiteks võib NTP-serveri ja klientide ühenduse katkestada võrgu kavandamisel või segmenteerimisel tehtud viga. Sageli ei tuvastata kellade erinevust enne kui see on põhjustanud IT-intsidendi, nt kui automatiseeritud toimingud käivituvad valel ajal.

2.2 Väär kellaaeg või kellaaja puudumine

NTP-server võib olla ajutiselt kättesaamatu või edastada valet ajateavet.

Kui IT-süsteem ei saa NTP-serveritega pikema aja vältel ühendust, siis võivad NTP-klientseadmete süsteemiajad muutuda ebatäpseks. Kui NTP-server annab NTP-klientidele vale ajateabe, kasutatakse tegelikkusest erinevat kellaaega ka kõigis klientarvuti rakendustes. Kui logiandmetes kasutatavad kellaajad on IT-süsteemides erinevad, ei anna IT-süsteemide logide korreleerimine soovitud tulemust.

Vale ajateave võib põhjustada häireid IT-teenustes, nt sertifikaadipõhiste või ühekordseid paroole kasutavate teenuste toimimises. Seetõttu ei saa kasutajad enam IT-süsteemidesse ega võrguteenustesse sisse logida.

2.3 Vastuoluline ajateave

Erinevatest allikatest pärinev ajateave võib olla vastuolus. Kui IT-süsteem kasutab kella sünkroniseerimiseks mitmeid NTP-servereid, võib NTP-serverite kellaaegades olla erinevus. Kellaaegade märgataval erinemisel ei suuda IT-süsteem kindlaks teha, milline esitatud ajateave on õige. Kellaaegade erinevus võib põhjustada tõrkeid IT-süsteemis, andmete valesti tõlgendamist ja häireid andmevahetuses teiste IT-süsteemidega.

2.4 NTP andmeside manipuleerimine

Võrguründe puhul on ründajal võimalik NTP andmesidet manipuleerida, nt muuta võrgupakettide ajateavet andmete edastamise ajal või suunata NTP päringud ümber enda määratud serverisse. Sel viisil saab ründaja NTP-klientide süsteemiaega muuta ning seda kasutada ajaliselt piiratud või antud hetkeks aegunud pääsuõiguste kuritarvitamiseks.

3 Meetmed

3.1 Elutsükkel

Kavandamine

OPS.1.2.6.M1 NTP kasutuselevõtu kavandamine

OPS.1.2.6.M2 Väliste NTP-serverite turvaline kasutamine

Evitus

OPS.1.2.6.M3 NTP-serveri turvaline konfigureerimine

OPS.1.2.6.M4 Soovimatute ajateabe allikate keelamine

OPS.1.2.6.M7 NTP-klientide turvaline konfigureerimine

Käitus

OPS.1.2.6.M5 NTP käitamine klient-server režiimis

OPS.1.2.6.M6 Võrgusiseste NTP-serverite seire

OPS.1.2.6.M8 Turvalise protokolli kasutamine kellade sünkroniseerimisel

Lisanduvad kõrgmeetmed

OPS.1.2.6.M9 Erinevate täpse ajateabe allikate kasutamine

OPS.1.2.6.M10 Ainult võrgusiseste NTP-serverite kasutamine

OPS.1.2.6.M11 NTP-serverite liiasuse tagamine

OPS.1.2.6.M12 NTP-serverite autentsuse tagamine

3.2 Põhimeetmed

OPS.1.2.6.M1 NTP kasutuselevõtu kavandamine

a. Organisatsioon on kaardistanud täpset ajateavet vajavad IT-süsteemid ja dokumenteerinud IT-süsteemide nõuded ajateabe täpsuse ja kättesaadavuse osas.

b. NTP (Network Time Protocol) kasutuselevõtul on dokumenteeritud, milliseid NTP-servereid ja milliste NTP-klientide poolt kasutatakse.

c. On määratud, kas NTP-serverid töötavad klient-server või leviedastusrežiimis (ingl Broadcast Mode).

OPS.1.2.6.M2 Väliste NTP-serverite turvaline kasutamine

a. Enne väljastpoolt kohtvõrku asuva NTP-serveri kasutuselevõttu analüüsitakse teenuseandja usaldusväärsust ja NTP-serveri töökindlust.

b. IT-süsteemide kellade sünkroniseerimisel väljastpoolt kohtvõrku on lubatud kasutada ainult usaldusväärseid NTP-servereid.

c. Välise NTP-serveri kasutamisel järgitakse NTP-serveri operaatori kehtestatud kasutustingimusi.

OPS.1.2.6.M3 NTP-serveri turvaline konfigureerimine

a. NTP-serveri konfiguratsiooniteavet saavad küsida ainult volitatud NTP-kliendid.

b. NTP-serveri konfiguratsiooni muutmine on lubatud ainult volitatud kasutajatel ning selgesõnaliselt määratletud juhtudel.

c. Organisatsioonisisese täpse kellaja allika puudumisel on võrgusisene NTP-server konfigureeritud saama regulaarset ja täpset ajateavet väliselt NTP-serverilt.

OPS.1.2.6.M4 Soovimatute ajateabe allikate keelamine

a. NTP-klientide seadistustes on IT süsteemide kellade sünkroniseerimine võimaldatud vaid lubatud ajateabe allikatega, muud ajateabe allikad on seadistustes blokeeritud.

3.3 Standardmeetmed

OPS.1.2.6.M5 NTP käitamine klient-server režiimis

a. NTP-serverid on konfigureeritud suhtluseks klient-server režiimis. NTP-server edastab ajateavet ainult vastustena aktiivsete NTP-klientide päringutele.

OPS.1.2.6.M6 Võrgusiseste NTP-serverite seire

a. Organisatsiooni arvutivõrgus asuvate NTP-serverite käideldavust, ressursikasutust ja kellaaja korrektsust seiratakse regulaarselt.

b. NTP-serverina toimiva IT-seadme puhul logitakse vähemalt järgmist:

- ootamatud taaskäivitused;
- NTP-teenuse ootamatud taaskäivitused;
- NTP-teenuse tõrked;
- anomaalsed ajateabe näidud.

c. NTP-serveri töötamisel leviedastusrežiimis (ingl Broadcast Mode) seiratakse ajateabe hälvete avastamiseks täiendavalt NTP-klientide kellaaja õigsust.

OPS.1.2.6.M7 NTP-klientide turvaline konfigureerimine

a. On üheselt määratud ja konfigureeritud, millisest allikast võtab IT-süsteem ajateavet IT-süsteemi käivitusel ja taaskäivitusel ning pärast NTP-teenuse taaskäivitust.

b. On määratud, kuidas NTP-kliendid reageerivad oodatust oluliselt erinevale ajateabele, väärat vastuvõetud ajateavet ignoreeritakse.

c. NTP-klientidele on tagatud piisav ajateave ka juhul, kui NTP-server piirab ajapäringutele vastamist või keelab päringute saatmise.

OPS.1.2.6.M8 Turvalise protokolli kasutamine kellade sünkroniseerimisel

a. IT-süsteemide kellade sünkroniseerimisel kasutatakse turvalisi andmevahetusprotokolle.

3.4 Kõrgmeetmed

OPS.1.2.6.M9 Erinevate täpse ajateabe allikate kasutamine (A)

a. Kõrget ajalist täpsust nõudva põhiprotsessiga organisatsioon kasutab oma arvutivõrgus rohkem kui ühte Stratum 1 NTP-serverit.

b. Iga Stratum 1 NTP-server on primaarse ja täpse kellaaja saamiseks ilma arvutivõrgu vahenduseta otse ühendatud sõltumatu riistvaralise (Stratum 0) ajateabe allikaga, nt GPS- või raadiokellaga.

OPS.1.2.6.M10 Ainult võrgusiseste NTP-serverite kasutamine (I)

a. Sisevõrku ühendatud IT-süsteemid (NTP-kliendid) kasutavad oma kellade sünkroniseerimiseks eranditult võrgusiseseid NTP-servereid.

OPS.1.2.6.M11 NTP-serverite liiasuse tagamine (A)

a. Kõrget ajalist täpsust nõudvate protsessidega organisatsiooni IT-süsteemid hangivad ajateavet vähemalt neljalt sõltumatult NTP-serverilt.

OPS.1.2.6.M12 NTP-serverite autentsuse tagamine (I)

a. NTP-klient veendub enne andmevahetust NTP-serveri autentsuses. NTP-klient aktsepteerib ainult autenditud NTP-serverilt saadud ajateavet.

b. Autentimise nõue kehtib ka NTP-serveritele, mis jagavad ajateavet alama taseme NTP-serveritele.

OPS.2: Käidutööd teenusena

OPS.2.2 Pilvteenuste kasutamine

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed pilvteenuste turvaliseks kasutuselevõtuks ja kasutamiseks.

1.2 Vastutus

Pilvteenuste kasutamise meetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Andmekaitsespetsialist, vastutav spetsialist, organisatsiooni juhtkond, personaliosakond.

1.3 Piirangud

Mooduli meetmed täiendavad väljasttellimist (vt OPS.2.3 *Väljasttellimine*) pilvteenustele omaste erisustega (sama infrastruktuuri kasutatakse paljude klientide teenindamiseks). Teenuseandjapoolsed meetmed on kirjeldatud moodulis OPS.3.2 *Teenuseandja infoturve*. Pilvteenuste kasutamise moodulis ei käsitleta ka pilvteenuste vastavate rakendusliideste (ingl

Application Programming Interface, API) spetsiifilisi turvameetmeid. Meetmed sõltuvad tarbitavast pilvteenusest, seega võib meetmete valik teenuseti erineda.

2 Ohud

2.1 Pilvteenuste strateegia puudumine või puudulikkus

Puuduva või piisamatu pilvteenuste strateegia korral võib juhtuda, et organisatsioon teeb otsuse sobimatu pilvteenuse või teenuseandja kasuks. Valitud pilvteenus ei pruugi organisatsiooni infotehnoloogia ja äriprotsessidega ühilduda ega vastata nõutud kaitsetarbe tasemele.

2.2 Sõltuvus pilvteenuseandjast (kontrolli kaotamine)

Välise pilvteenuse kasutamisel sõltub organisatsioon pilvteenuseandjast ega oma täit kontrolli äriprotsesside ja nende turvalisusega seotud teabe üle. Organisatsioon ei tea, kas pilvteenuseandja rakendab turvameetmeid nõuetekohaselt. Väliste pilvteenuste kasutamine toob tihti kaasa organisatsiooni infoturbe ja IT alase oskusteabe vähenemise.

2.3 Puudulik nõuete haldus pilvteenuste kasutamisel

Kui organisatsioon otsustab hakata kasutama pilvteenust, kaasnevad sellega kasutajate suured ootused paremale jõudlusele või funktsionaalsusele. Samas on organisatsiooni juhtkonna eesmärk sageli seotud kulude vähendamisega. Kui pilvteenuse nõuete määratlemisel ei arvestata kõikide osapoolte arvamust, võib juhtuda, et pilvteenusele üleminek ei pruugi tuua soovitud lisandväärtust.

2.4 Õigusaktide nõuete rikkumine

Rahvusvahelised pilvteenuse pakkujad lähtuvad sageli kolmandate riikide õigusaktidest. Pilvteenuse kliendid ei pruugi õiguslikele raamtingimustele piisavat tähelepanu pöörata. Seetõttu võidakse teadmatusest rikkuda kohalike õigusaktide nõudeid ja ohustada välisteenuse teabe turvalisust.

2.5 Simultaanteeninduse võime puudumine pilvteenuse andjal

Pilvtöötlusel kasutavad erinevad kliendid enamasti ühist taristut (nt IT-süsteemid, võrgud ja rakendused). Kui eri klientide ressursid ei ole üksteisest piisavalt turvaliselt lahutatud, võib klient saada lubamatu juurdepääsu teise kliendi andmetele.

2.6 Pilvteenuse andjaga sõlmitud lepingu puudulikkus

Kui pilvteenuse andja lepingus on vastutusalasid, ülesandeid, tulemusnäitajaid või kulusid ebapiisavalt või ebaselgelt kirjeldatud, võib juhtuda, et pilvteenuse andja kas tahtmatult või puuduvate ressursside tõttu kõiki vajalikke turvameetmeid ei rakenda. Pilvteenuse klienti võivad negatiivselt mõjutada lepingus määratlemata asjaolud. Näiteks kui ei ole teada teenuseandja sõltuvus kolmandast poolest, võib see negatiivselt mõjutada organisatsiooni infoturvet ning teenuse kvaliteeti.

2.7 Pilvteenustele migreerimise puudulik kavandamine

Ebapiisav pilvteenusele ülemineku plaan seab ohtu andmete turvalisuse. Kui organisatsioon loobub migratsiooni testandmetega testimisest ja väiksemahulisest pilootprojektist, on oht, et pärast täismahulist migratsiooni teenused nõutaval viisil ei tööta.

2.8 Pilvteenuste puudulik integreerimine omaenda IT-süsteemidega

Kui pilvteenuseid ei integreerita organisatsiooni IT-taristusse sobival viisil või tehakse seda puudulikult, ei saa kasutajad pilvteenust täies mahus kasutada. Kokkulepitud funktsionaalsus ja jõudlus võivad jääda saavutamata, tekivad häired äriprotsessi töös. Puudulik integratsioon organisatsiooni infotehnoloogiaga võib põhjustada märkimisväärseid turvanõrkusi.

2.9 Pilvteenuse kasutamise lõpetamise puudulik reguleerimine

Kui lepingu lõpetamine on puudulikult kokku lepitud, võib see organisatsioonile kaasa tuua märkimisväärse kahju. Piisava sisemise valmisolekuta on organisatsioonil keeruline pilvteenust kiiresti teisele teenuseandjale üle anda või oma organisatsiooni IT-süsteemidega lõimida. Kui teenuse üleandmine ajaliselt venib ja kõiki andmeid ei suudeta üle viia, võivad tekkida tööseisakud ja andmekadu.

2.10 Pilvteenuste halduse raamistiku puudulikkus

Pilvteenuse kasutuselevõtt muudab sageli teenusega seotud rollide jaotust (nt võivad süsteemiülematest saada teenusehaldurid). Muutused pilvteenuse halduses võivad ajutiselt mõjutada teenuse kvaliteeti. Kui töötajaile uusi ülesandeid tutvustavat koolitust ei tehta või seda tehakse piisamatult, võivad tekkida teenusehäired ja probleemid teenuse haldamisega.

2.11 Avariivalmenduse kontseptsiooni puudulikkus

Pilvteenuse osalise või täieliku katkestuse korral võivad ootamatud olukorrad ja puudused avariivalmenduse kontseptsioonis põhjustada seisakuaja pikenemist. Kui teenuse ostja ja teenuseandja pole kokku leppinud, kuidas avariistsenaariumi korral tegutsetakse (nt kui riiklikul tasemel otsustatakse välisühendused sulgeda), pikeneb taasteaeg veelgi.

2.12 Pilvteenuse andja süsteemi tõrge

Kui pilvteenuse andja juures toimub IT-süsteemide tõrge, mõjutab see ka pilvteenuse klienti, halvemal juhul katkeb teenus täielikult. Samasuguse tulemuseni viivad tõrked liidestuses pilvteenuse andja ja kliendi vahel või juhul, kui pilvtöötluse platvormi vastu sooritatakse tulemuslik rünne.

3 Meetmed

3.1 Elutsükkel

Kavandamine

OPS.2.2.M1 Pilvteenuste strateegia

OPS.2.2.M2 Pilvteenuste turvapoliitika

OPS.2.2.M3 Pilvteenuste loendi koostamine

OPS.2.2.M4 Vastutusalade ja liidestuste määramine

OPS.2.2.M5 Pilvteenusele migreerimise kava

OPS.2.2.M6 Pilvteenusega liitumise tegevusplaan

OPS.2.2.M7 Pilvteenuste turbe programm

Soetamine

OPS.2.2.M8 Pilvteenuse andja hoolikas valimine

Evitus

OPS.2.2.M9 Kliendi vajadustele vastav pilvteenuse leping

OPS.2.2.M10 Turvaline migratsioon pilvteenusele

Käitus

OPS.2.2.M12 Infoturve pilvteenuste kasutamisel

OPS.2.2.M13 Pilvteenuste turbe piisavuse tõendamine

Kõrvaldamine

OPS.2.2.M14 Pilvteenuselepingu korrakohane lõpetamine

Avariivalmendus

OPS.2.2.M11 Pilvteenuse avariivalmenduse programm

Lisanduvad kõrgmeetmed

OPS.2.2.M15 Pilvteenuse ülekantavuse tagamine

OPS.2.2.M16 Andmete täiendav varundamine

OPS.2.2.M17 Krüpteerimine pilvteenuse kasutamisel

OPS.2.2.M18 Liidendusteenuste korrakohane kasutamine

OPS.2.2.M19 Töötajate taustakontroll

3.2 Põhimeetmed

OPS.2.2.M1 Pilvteenuste strateegia [vastutav spetsialist, organisatsiooni juhtkond, andmekaitse spetsialist]

a. On kehtestatud pilvteenuste strateegia, mis on kooskõlas organisatsiooni eesmärkidega ja kus on dokumenteeritud:
   - pilvteenuste eesmärgid, eelised ja riskid;
   - pilvteenuste kasutamisega seotud õiguslikud, korralduslikud, majanduslikud ja tehnilised raamtingimused;
   - eeldatavad pilvteenused ja nende kasutusviisid;
   - pilvteenuste lõpetamise tingimused.
b. Iga kavandatava pilvteenuse kohta viiakse läbi teostatavuse, tasuvuse ja turvalisuse analüüs.
c. Pilvteenuste kasutuselevõtuks koostatakse etapiviisiline teenuse kasutuselevõtu plaan.

OPS.2.2.M2 Pilvteenuste turvapoliitika [vastutav spetsialist]

a. Pilvteenuste strateegiast (vt OPS.2.2.M1 *Pilvteenuste strateegia*) lähtuvalt on koostatud pilvteenuste turvapoliitika.
b. Turvanõuete määramisel on lähtutud teenuse kaitsetarbest ja korralduslikest, tehnilistest ning õiguslikest raamtingimustest.
c. Rahvusvaheliselt tegutsevate teenuseandjate puhul on arvestatud riigipõhist spetsiifikat ja regulatsioonidest tulenevaid nõudeid.

OPS.2.2.M3 Pilvteenuste loendi koostamine [vastutav spetsialist]

a. Kõik kavandatavad ja kasutatavad pilvteenused dokumenteeritakse ühtsetel alustel.

b. Iga pilvteenuse kohta on esitatud vähemalt järgmised andmed:
   - teenuse nimetus ja tähis;
   - teenuse eesmärk;
   - teenuse parameetrid ja/või lepinguline teenusetase;
   - teenuse ajaraamid;
   - arveldusandmed;
   - pääsuõigused ja autentimismeetod;
   - kontaktisikud.

OPS.2.2.M4 Vastutusalade ja liidestuste määramine [vastutav spetsialist]

a. Määratletakse ja dokumenteeritakse pilvteenuse kasutamisega seotud vastutusalad ja teenusepoolte tegevused.

b. Valitakse ja dokumenteeritakse pilvteenuse rakenduseks vajalikud IT-komponendid (nt. andmete varundussüsteem) ning riist- ja tarkvaraline liidestus.

3.3 Standardmeetmed

OPS.2.2.M5 Pilvteenusele migreerimise kava [vastutav spetsialist]

a. Pilvteenusele siirdumiseks koostatakse pilvteenusele migreerimise kava, mis määrab:
   - rollid ja kohustused;
   - IT-keskkonna ja käiduprotseduuride ettevalmistuse;
   - testimis- ja üleviimisprotseduurid;
   - teenusetaseme ja turvataseme vastavuskontrolli;
   - pilvteenusest loobumise protseduurid.

b. Pilvteenusele üleminekul hinnatakse pilvteenuse mõju olemasolevale IT-keskkonnale ja organisatsiooni tööprotsessidele, kavandatakse liidestused olemasolevate IT-süsteemidega ja plaanitakse täiendavad koolitused.

OPS.2.2.M6 Pilvteenusega liitumise tegevusplaan

a. Pilvteenuse kasutuselevõtuks koostatakse teenusega liitumise tegevusplaan, mis sisaldab vähemalt järgmisi tegevusi:
   - liidestuste ettevalmistus ja käivitamine;
   - võrguühenduste sobivus ja kontroll;
   - teenuse halduse korraldus;
   - andmete haldus.

b. Pilvteenusega liitumise tegevusplaan on dokumenteeritud, tegevusplaani uuendatakse regulaarselt.

OPS.2.2.M7 Pilvteenuste turbe programm

a. Pilvteenuste turvapoliitika (vt OPS.2.2.M2 *Pilvteenuste turvapoliitika*) põhjal on koostatud pilvteenuste turbe programm, mis käsitleb pilvespetsiifilisi riske (nt sõltuvus

pilvteenuse andjast, simultaanteenindus, fikseeritud andmevormingud, andmetele juurdepääs).

b. Pilvteenuste turbe programm on kooskõlas pilvteenuse andja ja võrgutarnijaga sõlmitud lepingutega ning teenuse kasutustingimustega.

OPS.2.2.M8 Pilvteenuse andja valimise kriteeriumid [organisatsiooni juhtkond]

a. Pilvteenuse andja valimiseks koostatakse pilvteenuste loendi (vt OPS.2.2.M3 *Pilvteenuste loendi koostamine*) andmeid sisaldav ja neid täiendav nõuete spetsifikatsioon.

b. Pilvteenuse andja valimisel arvestatakse järgmisi aspekte:
   - teenuseandja maine;
   - teenuseandja tegevusvaldkond ja spetsialiseerumine pilvteenustele;
   - avalikud turuanalüüsid ja soovitused;
   - teenuseandja asukoht ja jurisdiktsioon;
   - teenuse jõudlus ja käideldavus;
   - kliendisõbralikkus;
   - alltöövõtjate kasutamine;
   - lepingutingimuste sobivus;
   - teenuse lõpetamine;
   - tasuvus.

c. Pilvteenuse andjalt saadud teenusekirjelduste õigsust ja sertifikaatide kehtivust kontrollitakse, küsides teenuseandjalt täiendavat teavet.

OPS.2.2.M9 Kliendi vajadustele vastav pilvteenuse leping [organisatsiooni juhtkond]

a. Organisatsiooni ja pilvteenuse andja vahelises lepingus on määratud alljärgnev:
   - õiguslikud raamtingimused;
   - pilvteenusega seotud teabe liik ja maht;
   - teenuse jõudlus ja kvaliteet;
   - turvanõuded;
   - teenuse saamise koht;
   - allhankijad või muud kolmandad pooled;
   - nõuded pilvteenuse andja personalile;
   - suhtlusteed ja kontaktisikud;
   - töökorraldus, vastutused ja pääsuõigused;
   - muudatuste kord;
   - teenuse testimine ja seire;
   - tõrke- ja intsidendikäsitlus;
   - lepingu lõpetamine, järeltoimingud, andmete kustutus.

OPS.2.2.M10 Turvaline migratsioon pilvteenusele [vastutav spetsialist]

a. Migratsioonil pilvteenusele arvestatakse eelnevalt väljatöötatud kava (vt OPS.2.2.M5 *Pilvteenusele migreerimise kava*) ja turbe programmi (vt OPS.2.2.M7 *Pilvteenuste turbe programm*).

b. Enne tegelikku kasutuselevõttu testitakse migratsiooni toimimist testkeskkonnas.

c. Pärast IT-süsteemide migreerimist käidukeskkonda (ingl *operational environment*) kontrollitakse teenuse vastavust lepingu tingimustele.

OPS.2.2.M11 Pilvteenuse avariivalmenduse programm

a. Kasutuselevõetud pilvteenuste jaoks on välja töötatud avariivalmenduse programm, mis sätestab:

- kontaktisikud;
- avariikäsitluse korra, vastutused, toimingud ja dokumenteerimise;
- andmete, liideste, vahendite ja taristu varunduse;
- vajalikud tehnilised vahendid;
- avariikäsitluse õppuste korraldamise.

OPS.2.2.M12 Infoturve pilvteenuste kasutamisel

a. Pilvteenuste dokumentatsiooni ja kasutusjuhiseid ajakohastatakse regulaarselt.

b. Pilvteenuse vastavust teenuselepingus kokku lepitud tingimustele ja turvanõuetele kontrollitakse regulaarselt.

c. Pilvteenuste turbe programmi (vt OPS.2.2.M7 *Pilvteenuste turbe programm*) järgimist ja selle ajakohasust kontrollitakse regulaarselt.

d. Pilvteenuste haldurid järgivad moodulites ORP.3 *Infoturbe teadlikkuse suurendamine ja koolitus* ja OPS.1.1.2 *IT-süsteemide haldus* toodud meetmeid.

e. Andmevarunduse toimimist kontrollitakse regulaarselt.

f. Avariikäsitlust harjutatakse koostöös teenuseandjaga regulaarselt.

OPS.2.2.M13 Pilvteenuste turbe piisavuse tõendamine

a. Pilvteenuse andja tõendab infoturbe vastavust regulatsioonidest tulenevatele nõuetele ja/või rahvusvaheliselt tunnustatud kriteeriumidele, esitades vastavad sertifikaadid, akrediteeringud või auditite tulemused.

b. Tõendusmaterjali hindamisel kontrollitakse, kas sertifikaatide kehtivusala hõlmab kasutatavat pilvteenust.

c. Pilvteenuse puhul allhankijate kasutamisel nõutakse samade kriteeriumide täitmise tõendamist ka nendelt.

OPS.2.2.M14 Pilvteenuselepingu korrakohane lõpetamine [vastutav spetsialist, organisatsiooni juhtkond]

a. Pilvteenuselepingu lõppemise puhuks on kehtestatud protseduurid üleminekuks sisemisele teenusele või teisele pilvteenuseandjale, täites kõiki seniseid teenusenõudeid.

b. Pilvteenusepingu lõppemisel tagatakse, et see ei mõjuta negatiivselt organisatsiooni äriprotsesside jätkuvust.

c. Pilvteenuselepingus on lepingu lõppemise puhuks määratletud:

- lepingupoolte omandiõigused teenusevahenditele;
- teenuse dokumentatsiooni ja vajalike andmete üleandmine kliendile;
- kliendi andmete turvaline kõrvaldamine teenuseandja käsutusest.

3.4 Kõrgmeetmed

OPS.2.2.M15 Pilvteenuse ülekantavuse tagamine [vastutav spetsialist] (A)

a. Pilvteenuse andja vahetamiseks või siseteenusele üleminekuks on kehtestatud kriteeriumid, mis sisaldavad porditavusnõudeid ja teenuse ülekantavuse testimise kohustuse.

b. Vajalik porditavus on pilvteenuse lepingu kohaselt võimalik (vt OPS.2.2.M9 *Kliendi vajadustele vastav pilvteenuse leping*).

OPS.2.2.M16 Andmete täiendav varundamine [vastutav spetsialist] (I-A)

a. Pilvteenuselepingus on esitatud teenuseandjale andmevarunduse detailsed nõuded.

b. Pilvteenuselepinguga on määratletud kliendi õigus täiendava andmevarunduse tegemiseks.

c. On otsustatud, kas pilvteenuse andja andmevarundusele lisaks tehakse ka omapoolset andmete varundamist.

OPS.2.2.M17 Krüpteerimine pilvteenuse kasutamisel (I-A)

a. Kõiki käideldavaid andmeid vahetatakse pilvteenuse andja ja organisatsiooni vahel krüpteeritult.

b. Andmete krüpteerimiseks nende salvestus- või töötluskohas on kokku lepitud, kas andmed krüpteerib pilvteenust kasutav organisatsioon (enne nende edastamist pilvteenuse andjale) või krüpteeritakse edastatavad andmed pilvteenuse andja IT-süsteemides.

c. Kui andmed krüpteerib pilvteenuse andja, määratakse lubatud krüpteerimismehhanismid, võtme pikkused ja turvalise võtmehalduse nõuded pilvteenuselepingus.

d. Kui andmeid krüpteerib organisatsioon, kooskõlastatakse see eelnevalt teenuseandjaga. Meetme rakendamisel järgitakse ka moodulit CON.1 *Krüptokontseptsioon*.

OPS.2.2.M18 Liidendusteenuste korrakohane kasutamine [vastutav spetsialist] (C-I-A)

a. Kui pilvteenuste jaoks kasutatakse liidendusteenuseid (ingl *Federation Service*), edastatakse kesksest kataloogiteenusest saadud identsustõendiga (nt SAML-pilet (SAML-Security Assertion Markup Language)) pilvteenuse andjale üksnes vajalikku teavet.

b. Kasutajate õigusi kontrollitakse regulaarselt ja identsustõendi saavad ainult volitatud kasutajad.

OPS.2.2.M19 Pilvteenuse andja töötajate taustakontroll [personaliosakond] (C-I-A)

a. Pilvteenuse andjaga on lepitud kokku personali kvalifikatsiooni ja usaldusväärsuse kontrollimise nõuetes ja kriteeriumides.

b. Pilvteenuse andja tõendab kliendile oma töötajate usaldatavust ja vastavust kliendi kriteeriumidele.

4 Lisateave

Lühend	Publikatsioon
[CSA]	Cloud Security Alliance, „Security Guidance for Critical Areas of Focus in Cloud Computing“
[NIST]	NIST Special Publication 800-144 „Guidelines on Security and Privacy in Public Cloud Computing“

OPS.2.3 Väljasttellimine

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed väljasttellimise (ingl *outsourcing*) turvaeesmärkide saavutamiseks ja infoturbe parendamiseks kogu allhanke elutsükli kestel.

1.2 Vastutus

Väljasttellimise meetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Hankeosakond, vastutav spetsialist, organisatsiooni juhtkond, avariiülem, personaliosakond, haldusosakond.

1.3 Piirangud

Moodulis käsitletakse väljasttellimise turvariske allhanke tellija seisukohast. Teenuseandja vaade on esitatud moodulis OPS.3.2 *Teenuseandja infoturve*.

Väljasttellimisena käsitletakse antud moodulis IT allhankeid. Hanked, mis käsitlevad infotehnoloogiat ainult osaliselt, vajavad täiendavat turvaanalüüsi.

Moodul ei käsitle teenuseandjaga suhtlemise andmevahetuskanalite turvet. Pilvteenuseid käsitletakse moodulis OPS.2.2 *Pilvteenuste kasutamine*. Nõudeid teenuseandja töötajatele ning füüsilisele turbele käsitletakse mooduligruppides ORP. *Organisatsioon ja personal* ja INF.*Taristu*.

2 Ohud

2.1 Väljasttellimise strateegia puudumine

Kui väljasttellimise kavandamisel ei esitata teenuseandjale infoturbe nõudeid ega kirjeldata hanke objektiga seotud turbevajadusi kogu objekti elutsükli jooksul, võib infoturbe tegelik olukord teenuseandja juures osutuda tellija äriprotsesside jaoks ebapiisavaks. Eksisteerib oht, et tellija äriprotsessid võivad saada kahjustada ning tundlik teave võib lekkida.

2.2 Ärikriitiliste protsesside kontrolli puudulikkus

Kui osa vajalikest teadmistest ja oskustest läheb üle teenuseandjale, kaotab organisatsioon täieliku kontrolli oma võtmetähtsusega äriprotsesside üle. Protsesse pole võimalik piisavalt

kiiresti ja adekvaatselt juhtida. Äriprotsessi katkemisel võivad tekkida probleemid äriprotsessi õigeaegse ja nõutaval kujul taastamisega.

2.3 Sõltuvus teenuseandjast

Otsus kasutada väljasttellimist võib viia organisatsiooni teenuseandjast täielikku sõltuvusse, põhjustades oskusteabe kaotust ja äriprotsessi üle kontrolli kadumist. Rakendatavad turvameetmed ei pruugi olla vastavuses tegeliku kaitsetarbega. Klient ei pruugi puudujääke teenuseandja infoturbes ise märgata. Teenuseandja võib tekkinud olukorda oma huvides ära kasutada (nt tõsta märkimisväärselt teenuse hinda).

2.4 Teenuseandja ebapiisav infoturbe tase

Kui väljasttellimisel ei esitata teenuseandjale infoturbe nõudeid, võib teenuseandja IT-süsteemid või teenus ise sisaldada turvanõrkusi, mida ründajal on võimalik organisatsiooni IT-süsteemide ründamiseks ära kasutada. Teenuseandja süül tekkinud intsidendil võivad olla organisatsiooni jaoks otsesed rahalised tagajärjed, samuti tekib mainekahju.

2.5 Ebapiisav kontroll hangitava teenuse üle

Kui sisseostetavaid teenuseid või protsesse juhitakse ebapiisavalt, väheneb protsesside läbipaistvus ja hallatavus. Teenuse tellijal puudub kontroll teenuseandja protsesside ja tegevuste üle. Organisatsioon ei saa tagada, et allhanke protsessis teenuseandja rakendab vajalikku hoolsust, et tagada teenuse kvaliteet ja nõutav turvatase.

2.6 Teenust reguleerivate lepete puudulikkus

Teenuseandjaga sõlmitud lepped ei pruugi sisaldada kõiki teenuseandja kohustusi ja kõiki rakendamisele kuuluvaid turvameetmeid. Turvanõuete dokumenteerimata jätmine võib takistada hilisemaid nõudeid teenuseandjale. Näiteks, kui leping seda ei reguleeri, ei pruugi teenuseandja kinni pidada kliendi teavitamiskohustusest. Rakendamata turvameetmed võivad kaasa tuua ka õigusaktide nõuete eiramise. Puudulikud turvameetmed teenuseandjaga sõlmitud lepingus on risk äriprotsessi käideldavusele ja andmete konfidentsiaalsusele.

2.7 Pääsuõiguste halduse puudulikkus

Sõltuvalt hanke objektist võivad teenuseandja töötajad vajada pääsuõigusi organisatsiooni IT-süsteemidele, andmetele või ruumidele. Kui pääsuõiguste andmine, haldamine ja kontrollimine on teenuseandja poolelt halvasti korraldatud, võivad ohtu sattuda klientide andmed. Teenuseandja töötajatele kontrollimatult pääsuõiguste andmine soodustab antud õiguste ärakasutamist teabe kopeerimise või manipuleerimise eesmärgil.

2.8 Teenuseandja allhangete kontrollimatus

Teenuseandja võib omakorda teenuse pakkumiseks vajalikke ressursse hankida oma allhankijatelt. Kogu protsess muutub täiendavate osapoolte lisandumise tõttu seeläbi keerumaks ja vähem läbipaistvamaks. Kontroll teenuseandja üle väheneb. Täiendavalt lisandunud partnerettevõtete töötajad ei pruugi teada ega järgida algselt kokkulepitud turvanõudeid.

2.9 Sooritusindikaatorite (KPI) puudumine

Organisatsioon peab saama kontrollida, kas väljasttellitav teenus on teenuseandja poolt nõuetekohaselt ellu viidud ja hallatud. Kui teenustaseme mõõtmiseks puuduvad kvalitatiivsed või kvantitatiivsed sooritusindikaatorid (ingl *key performance indicator*, KPI) või ei ole teenustaset võimalik adekvaatselt mõõta, võib teenuse kvaliteet aja jooksul langeda. Samuti ei ole võimalik kontrollida ja aru saada, kas teenuseandja täidab kokkulepitud turvanõudeid.

2.10 Puudulikud sätted väljasttellimise lõpetamiseks

Kui teenuslepped ei sätestata täpseid teenuse lõpetamise tingimusi, võib juhtuda, et teenuse klient ei saa lepingut ilma märkimisväärsete kuludeta lõpetada. Teenuseandja poolt soovitud liiga lühike lepingu ülesütlemise tähtaeg võib sundida klienti kiiresti otsustama uue ning sobimatu teenuseandja kasuks. Samuti võivad teenuse lõpetamisega kaasneda erinevad turvaprobleemid. Puudulik andmete (sh varundatud andmete) kustutamise kord võib põhjustada konfidentsiaalsete andmete lekke.

2.11 Väljastellitavate teenuste puudulik avariihaldus

Avariiolukorra tekkides või kriisi puhkedes võivad väljasttellitud teenused katkeda. Tavaolukorras hästi toimivate protsesside taastamine ei pruugi avariiolukorras õnnestuda. Häiringuid ja avariiolukorrad on tavaliselt ootamatud ja neid pole võimalik lõpuni kontrollida. Kaasnev teenusekatkestus toob kaasa vahetuid negatiivseid ärilisi tagajärgi. Kannatajateks osutuvad kõik seotud ettevõtted, nii need, kellelt teenust ostetakse ja kellele ise teenuseid pakutakse. Selline kaskaadina kasvav efekt omab allhangete kontekstis märkimisväärset mõju.

3 Meetmed

3.1 Elutsükkel

Kavandamine

OPS.2.3.M1 Turvanõuded väljasttellitavale teenusele

OPS.2.3.M2 Riskipõhine lähenemine hangete korraldamisel

OPS.2.3.M8 Väljasttellimise strateegia koostamine

OPS.2.3.M9 Hankepoliitika kehtestamine

Evitus

OPS.2.3.M3 Teenuseandja valimise kriteeriumid

OPS.2.3.M4 Teenuselepingu vastavus kliendi nõuetele

OPS.2.3.M5 Teenuseandja simultaanteeninduse võimekuse hindamine

OPS.2.3.M6 Väljasttellitava teenuse turbe põhimõtted

OPS.2.3.M10 Vastutavate kontaktisikute määramine

OPS.2.3.M13 Huvide konflikti vältimine teenuselepingu sõlmimisel

OPS.2.3.M14 Laiendatud nõuded teenuselepingule

Käitus

OPS.2.3.M7 Välisteenuselepingu korrakohane lõpetamine

OPS.2.3.M11 Väljasttellitud teenuste register

OPS.2.3.M12 Väljasttellitud teenuste aruandlus

OPS.2.3.M15 Teenuseandja ja kliendi turvaline võrguühendus

OPS.2.3.M16 Teenuseandja infoturbe läbivaatus

OPS.2.3.M17 Teenuseandja personali kasutamise kord

OPS.2.3.M18 Teenuseandjaga sõlmitud lepete läbivaatus

OPS.2.3.M19 Alternatiivsete teenuseandjate kaardistamine

Avariivalmendus

OPS.2.3.M20 Avariivalmendus väljasttellimisel

Lisanduvad kõrgmeetmed

OPS.2.3.M21 Tarkvara lähtekoodi hoiustuslepingute sõlmimine

OPS.2.3.M22 Ühiste avariiõppuste läbiviimine

OPS.2.3.M23 Tundlike andmete krüpteerimine

OPS.2.3.M24 Teenuseandja töötajate taustakontroll

OPS.2.3.M25 Teenuseandja andmete aedikkäitus

3.2 Põhimeetmed

OPS.2.3.M1 Turvanõuded väljasttellitavale teenusele [vastutav spetsialist]

a. Kõikidele väljasttellitavatele teenustele on kehtestatud kaitsetarbe määramisele ja/või ärimõjude hindamisele (ingl *business impact assessment*, BIA) põhinevad turvanõuded.
b. Teenuse turvanõuete määramisel on arvestatud, mis andmeid töödeldakse ning milline peab olema andmevahetusprotseduuride ja -liideste turve.
c. Väljasttellitava teenuse turvanõuete määramisel on arvestatud äriprotsesside vahelist sõltuvust ning protsesside sisendeid ja väljundeid.

OPS.2.3.M2 Riskipõhine lähenemine hangete korraldamisel

a. Teenuse väljasttellimise võimalikkus otsustatakse riskipõhiselt, eelnevalt määratud kaitsetarbe ja riskiprofiili alusel.
b. Väljasttellitava teenuse jätkuvat vastavust lubatud riskiprofiilile kontrollitakse regulaarselt.

OPS.2.3.M3 Teenuseandja valimise kriteeriumid [vastutav spetsialist, hankeosakond]

a. Teenuseandja valimiseks on koostatud turvanõudeid sisaldav nõuete profiil.
b. On kehtestatud järgmised teenuseandja valimise ja hindamise kriteeriumid:
    - teenuse sobivus ja läbipaistvus;
    - teenuse vastavus kliendi turvanõuetele;
    - teenuseandja maine ja soovitused;
    - teenuseandja ärikultuur (välismaise teenuseandja korral);
    - teenuseandja personali kvalifikatsioon.
c. Teenuseandja valimisel hinnatakse võimalike huvide konfliktide olemasolu.
d. Teenuseandja jätkuvat vastavust teenuseandja valimise kriteeriumitele kontrollitakse regulaarselt.

OPS.2.3.M4 Teenuselepingu vastavus kliendi nõuetele

a. Kõik väljasttellitava teenuse aspektid lepitakse teenuseandjaga kirjalikult kokku teenuselepingus. Teenuselepingute tarbeks on loodud ühtne lepinguvorm.

b. Teenuselepingus määratletud lepingupartnerite infoturbealased õigused ja kohustused lähtuvad eelnevalt kaardistatud riskidest (vt OPS.2.3.M1 *Turvanõuded väljasttellitavale teenusele*).

c. Teenuseleping sätestab väljasttellitava teenuse haldusega seotud üksikasjad, näiteks taristu kasutustingimused, alltöövõtu lubamine või mittelubamine, töötajatele püstitatud nõuded, isikuandmete kaitse, huvide konflikti vältimine ning tõrgete ja intsidentide käsitlus.

d. Teenuseandja tagab nõuete täitmise kontrollimiseks vajalikud teabe saamise ja juurdepääsu õigused ning vajadusel ka auditeerimisvõimalused.

e. Vajadusel sõlmitakse tundlike andmete kaitseks teenuseandjaga konfidentsiaalsuslepe (ingl *non-disclosure agreement*, NDA).

OPS.2.3.M5 Teenuseandja simultaanteeninduse võimekuse hindamine

a. Teenuseandja tagab erinevatele klientidele sarnaste teenuste pakkumisel kliendi andmete turvalise eraldatuse ning esitab sellekohase kinnituse.

b. Kliendi nõudel esitab teenuseandja tehnilise kirjelduse, kuidas kliendi andmeid kaitstakse ning kuidas need on eraldatud avalikest ja teiste klientide andmetest.

OPS.2.3.M6 Väljasttellitava teenuse turbe põhimõtted

a. Teenuseandja on rakendanud infoturbe halduse süsteemi (ingl *information security management system*, ISMS) vähemalt väljasttellitava teenuse ulatuses.

b. Organisatsioon on määratlenud ja teenuseandjaga kokku leppinud E-ITS moodulid ja infoturbe meetmed, mida teenuseandja on kohustatud rakendama.

c. Teenuseandja on teenuse käsitlusala ulatuses tõendatavalt rakendanud E-ITS infoturbe meetmed kõigist asjakohastest E-ITS moodulitest. Valitud turbeviis vastab tellija poolt esitatud kaitsetarbe määrangutele. Alternatiivlahendusena võib teenuseandja rakendada infoturbestandardit ISO 27001.

d. Infoturbe meetmete rakendatust tõendab teenuseandja välise audiitori poolt väljastatud E-ITS auditi järeldusotsusega või ISO27001 sertifikaadiga. Auditi järeldusotsuses või sertifikaadil esitatud auditi käsitlusala hõlmab kõiki väljasttellitava teenusega seotud äriprotsesse ja tugiteenuseid.

e. E-ITS auditi järeldusotsuse või ISO27001 sertifikaadi puudumisel veendub organisatsioon (kui teenuse tarbija) selles, et tema poolt esitatud ning rakendamisele kuuluvad infoturbe meetmed on teenuseandja poolt rakendatud.

f. Organisatsioonil on lepingujärgne õigus teenuseandja juures läbi viia infoturbe läbivaatusi ja auditeid või tellida nende läbiviimine sõltumatult kolmandalt poolelt.

OPS.2.3.M7 Välisteenuselepingu korrakohane lõpetamine [vastutav spetsialist, hankeosakond]

a. Teenuselepingus lepitakse kokku lepingu korralise lõpetamise tingimused (nt etteteatamise tähtaeg). Tingimustekohane teenuse lõpetamine ei mõjuta kliendi tööprotsesside jätkuvust.

b. Teenuselepingus lepitakse kokku lepingu erakorralise lõpetamise tingimused.

c. Teenuseleping määrab poolte õigused ja kohustused lepingu lõppemisel, sealhulgas teenuseandja kohustuse tema valduses olevad kliendi andmed turvaliselt üle anda või kustutada.

d. On kokku lepitud, kuidas toimub andmete, tarkvara ja riistvara tagastamine. Tagastamisel järgitakse seadusandlusest tulenevaid nõudeid.

e. On kokku lepitud, kuidas toimub teenuseandjaga lepingulise suhte lõppemisel kasutajakontode sulgemine ja pääsuõiguste eemaldamine.

3.3 Standardmeetmed

OPS.2.3.M8 Väljasttellimise strateegia koostamine [organisatsiooni juhtkond]

a. Organisatsioonis on kehtestatud majanduslikke, tehnilisi, korralduslikke ja õiguslikke raamtingimusi ning infoturbe aspekte käsitlev väljasttellimise strateegia.

b. Väljasttellimise strateegias on kirjeldatud väljasttellimise eesmärgid, võimalused ja riskid.

c. Väljasttellitava teenuse kliendil on vajalikud võimed, pädevus ja ressursid teenuse infoturbenõuete määramiseks ja kontrollimiseks.

OPS.2.3.M9 Hankepoliitika kehtestamine [organisatsiooni juhtkond]

a. Väljasttellimise strateegiast (vt OPS.2.3.M8 *Väljasttellimise strateegia*) lähtudes on koostatud ja kinnitatud organisatsiooni hankepoliitika.

b. Hankepoliitika arvestab organisatsiooni infoturbe vajadusi ja sisaldab tüüpseid nõudeid teenuseandjaga sõlmitavatele lepingutele (vt OPS.2.3.M4. *Teenuselepingu vastavus kliendi nõuetele*).

c. Hankepoliitika sätestab, kuidas toimub väljasttellitava teenuse testimine ja kasutusevõtuks kinnitamine.

d. Hankepoliitikas on määratud, kas või mis tingimustel on teenusandjal lubatud kasutada oma teenuse tarnimisel alltöövõtjaid.

OPS.2.3.M10 Vastutavate kontaktisikute määramine [personaliosakond]

a. Iga väljastellitava teenuse jaoks on määratud organisatsioonisisesed ja -välised suhtluspartnerid, nende õigused ja edastatava teabe sisu.

b. Mõlemad pooled kontrollivad suhtluspartneri volituste olemasolu ja kehtivust. Suhtluspartnerite andmed on ajakohased ja dokumenteeritud.

OPS.2.3.M11 Väljasttellitud teenuste register

a. Väljasttellimise eest vastutaja koondab allhankeid käsitleva dokumentatsiooni väljasttellitud teenuste registrisse.

b. Väljasttellitud teenuste register sisaldab teavet teenuseandjate, peamiste sooritusindikaatorite (ingl key process indicator, KPI), protsesside ärikriitilisuse, sõlmitud lepete ning teenusemuudatuste kohta.

OPS.2.3.M12 Väljasttellitud teenuste aruandlus

a. Väljasttellimise eest vastutaja koostab juhtkonnale perioodiliselt aruandeid teenuse hetkeseisust ja võimalikest kitsaskohtadest.

b. Teenuste aruandlus sisaldab teavet toimunud infoturbe sündmuste ja intsidentide kohta.

OPS.2.3.M13 Huvide konflikti vältimine teenuselepingu sõlmimisel [organisatsiooni juhtkond]

a. Teenuselepingu tingimuste läbirääkimisel osalevad organisatsiooni erinevate valdkondade esindajad.

b. Teenuselepingu koostamisel on välditud võimalikku äripoole ja infoturbe huvide konflikti.

OPS.2.3.M14 Laiendatud nõuded teenuselepingule

a. Teenuselepingus on määratud, millistele objektidele ja võrguteenustele tohib teenuseandja kliendi võrgus juurde pääseda.

b. Teenuse peamised sooritusindikaatorid (KPI) on dokumenteeritud teenuselepingu osana. Kui teenus ei vasta kokkulepitud sooritusindikaatoritele, on võimalik teenuseandjale kehtestada sanktsioone (nt leppetrahv).

c. Teenuseleping sisaldab erinevaid võimalusi väljastellitava teenuse lõpetamiseks ning seonduvaid protseduure kliendi andmete ja varade tagastamiseks.

d. Teenuseleping sisaldab osapoolte kohustusi ja käitumisjuhiseid avariiolukorras tegutsemiseks.

OPS.2.3.M15 Teenuseandja ja kliendi turvaline võrguühendus

a. Enne teenuseandja kliendi võrku lubamist on kokku lepitud ja dokumenteeritud:
   - ühenduse kasutamise korralduslikud ja tehnilised tingimused;
   - ühenduse kaitsetarve ja turvameetmed;
   - poolte konfidentsiaalsuskohustused;
   - eritingimused välismaise teenuseandja puhul.

b. Teenuseandja ja klient on määranud võrguühendusega seotud organisatoorsete ja tehniliste küsimuste lahendamiseks kontaktisikud.

c. Teenuseandja ja klient on leppinud kokku võrguühenduse intsidentidest teavitusteed ning intsidentide käsitlemise korra.

OPS.2.3.M16 Teenuseandja infoturbe läbivaatus

a. Teenuselepingus määratletud turvanõuete rakendamist teenuseandja juures kontrollitakse regulaarselt.

b. Teenuseandja infoturbe läbivaatuste tulemused dokumenteeritakse.

OPS.2.3.M17 Teenuseandja personali kasutamise kord

a. Enne teenusega alustamist selgitatakse teenuseandja töötajatele kliendi juures kehtivaid nõudeid. Teenuseandja töötajad kinnitavad allkirjaga oma kohustust kliendi juures kehtivaid nõudeid järgida.

b. Teenuseandja ja kliendi vahel on kokku lepitud teenuseandja töötajate asendamise ja nendega töösuhte lõpetamise protseduurid.

c. Kliendi territooriumil lühiajaliselt või ühekordselt viibivat välispersonali käsitletakse sarnaselt külastajaga.

OPS.2.3.M18 Teenuseandjaga sõlmitud lepete läbivaatus

a. Teenuseandjaga sõlmitud lepetes sisalduvate turvameetmete asja- ja -ajakohasust hinnatakse regulaarselt. Ebapiisavate turvameetmete ilmnedes täiendatakse teenuseandjaga sõlmitud leppeid.

b. Teenuseandjaga sõlmitud lepped vaadatakse üle ja vajadusel täiendatakse pärast infoturbe intsidenti, riskimaastiku olulise muutumise ja seadusandluses tehtavate muudatuste puhul.

OPS.2.3.M19 Alternatiivsete teenuseandjate kaardistamine

a. Väljastellitava teenuse korralise või erakorralise lõpetamise puhuks on koostatud tegevuskavad teenuse migreerimiseks alternatiivsele teenuseandjale.

b. On kaardistatud potentsiaalsed teenuseandjad, kellel on teenuse üleandmiseks sobiv ettevõtte profiil ja piisav infoturbe tase.

OPS.2.3.M20 Avariivalmendus väljasttellimisel [avariiülem]

a. Väljasttellitava teenuse jaoks töötatakse välja avariivalmenduse plaan, mis hõlmab teenusepoolte IT-komponentide, liidestuste ja sidekanalite taastet.

b. Väljasttellitava teenuse avariivalmenduse plaanis dokumenteeritakse teenusepoolte vastutus, kontaktisikud ja protseduurid.

c. Organisatsioon kontrollib teenuseandja avariimeetmete rakendamist, selleks korraldavad teenusepooled ühiseid intsidendikäsitluse õppuseid.

3.4 Kõrgmeetmed

OPS.2.3.M21 Tarkvara lähtekoodi hoiustuslepingute sõlmimine (I-A)

a. Teenuseandjalt tarkvara tellimisel on kaalutud tarkvara lähtekoodi (ingl *source code*) jm olulise materjali usaldatavale hoiule andmise (ingl *escrow*) vajadust.

b. Hoiustusleping reguleerib vähemalt järgnevat:

- tarkvara kasutus- ja muutmisõigused;
- lähtekoodi avaldamise juhud;
- lähtekoodi asjakohane säilitus ja turve;
- lähtekoodi deponeerimise kord ja sagedus.

OPS.2.3.M22 Ühiste avariiõppuste läbiviimine [avariiülem] (A)

a. Organisatsioon viib koos teenuseandjatega läbi ühiseid avariiõppuseid.

b. Avariihalduse õppuse tulemite analüüsi kasutatakse avariihalduse kontseptsiooni ja pooltevahelise koostöö parendamiseks.

c. Teenuseandjatega ühiselt läbiviidavaid avariiõppuseid korraldatakse regulaarselt.

OPS.2.3.M23 Tundlike andmete krüpteerimine (C)

a. Teenuseandja ja kliendi vahelises andmevahetuses edastatakse tundlikud andmed krüpteeritult.

b. Andmekandjale salvestatud andmeid kaitstakse volitamata juurdepääsu eest andmete või andmekandja krüpteerimisega.

c. Võimalusel kasutatakse riiklikult heaks kiidetud ning sertifitseeritud krüpteerimistarkvara.

OPS.2.3.M24 Teenuseandja töötajate taustakontroll [personaliosakond] (C-I-A)

a. Teenuselepingus kehtestavad teenusepooled teenuseandja töötajate turvakontrolli läbiviimise kriteeriumid.

b. Teenusepooled lepivad kokku, milliseid turvakontrolle tehakse ja kumb pool taustakontrolli läbi viib.

OPS.2.3.M25 Teenuseandja andmete aedikkäitus (C-I-A)

a. Teenuseandjalt sissetulevatele andmetele rakendatakse aedikkäitust (ingl *sandboxing*).

b. Saabuvate e-kirjade manused avatakse kõigepealt aedikus (ingl *sandbox*).

c. Tarkvara väljatöötava teenuseandja rakendusi ja uuendeid (ingl *update*) testitakse esmalt aedikus.

OPS.3: Teenuseandja käidutööd

OPS.3.2 Teenuseandja infoturve

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed teenuseandja infoturbe kavandamiseks, rakendamiseks, juhtimiseks ja kontrollimiseks ning nõutava turbetaseme hoidmiseks teenuseandja vaatest. Teenuse pakkumisega seotud riskid ei tohi ohustada teenuse kasutajaid. Üldine vastutus teenuse turbe eest jääb teenuse kasutajale.

1.2 Vastutus

Teenuseandja infoturbe meetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Avariiülem, personaliosakond.

1.3 Piirangud

Teenustena käsitletakse antud moodulis IT-teenuseid.

Moodul sisaldab teenuseandjale kohalduvaid turvameetmeid. Teenusesaaja vaadet käsitletakse moodulis OPS.2.3 *Väljasttellimine*. Seda tuleb silmas pidada ka juhul, kui teenuseandja ise kasutab väljasttellimist.

Moodulis ei käsitleta teenuseandja ja väljasttellitava teenuse kliendi vaheliste sidekanalite turvet.

2 Ohud

2.1 Teenuseandja puudulik infoturbe haldus

Puudulikult kehtestatud või nõuetele mittevastav teenuseandja infoturbe haldus väljendub infoturbe valdkonna eest vastutuse puudumises, puudulikus juhtkonnapoolses toetuses ja turbeprotsessi läbipaistmatuses. Puuduliku infoturbe halduse korral ei suuda teenuseandja teenust kasutava organisatsiooni infoturbe nõudeid täita. Teenuseandja infoturbealane suutmatus kujutab ohtu kõigile teenust kasutavatele organisatsioonidele.

2.2 Teenuseandja puudulik avariihaldus

Teenuseandja IT-süsteemides toimuvad häired ja katkestused võivad mõjutada teenuse kasutajate protsesside tavapärast toimimist. Kui teenuseandja pole avariiolukordadeks piisavalt valmistunud, võib teenuste taastamine võtta kauem aega ja klientide äriprotsessid olla häiritud suuremal määral, kui teenuselepingutes kokku lepitud.

2.3 Puudulikud teenuselepingud teenuse saajatega

Kui kaitsetarve ja sellel põhinevad andmete ja süsteemide turvanõuded ei ole kliendi ja teenuseandja vahel kokku lepitud, võivad kliendi andmed jääda vajaliku kaitseta. Kui turvanõuded pole teenuselepetes määratletud, puudub osapooltel alus turvarikete puhul teisele poolele rahaliste nõuete esitamiseks.

2.4 Teenuseandja IT-süsteemidega liidestuse nõrkused

Kui väljasttellitava teenuse kliendi ja teenuseandja vaheline IT-liidestus ei ole piisavalt kaitstud, võivad tekkida teenusekatkestused ja esineda andmekadu. Ründaja võib kaitseta või halvasti kaitstud andmeliideseid kasutada ründe algatamiseks. Samuti pole välistatud kõrvaliste isikute volitamata juurdepääs andmetele. Kui osapooled ei ole kokku leppinud avariiprotseduurides, võib see mõjutada avariiolukordade lahendamise tõhusust.

2.5 Teenuse saaja sõltuvus teenuseandjast

Väljasttellimine võib teenuse saaja viia teenuseandjast täielikku sõltuvusse, põhjustades oskusteabe kaotust ja äriprotsessi üle kontrolli kadumist. Teenuseandja saab tekkinud olukorda oma huvides ära kasutada. Teenuse kvaliteet võib langeda, teenuseandja rakendatavad turvameetmed ei pruugi olla enam vastavuses teenuselepingus kokku lepitud turvnõuete ja teenuse saaja tegeliku kaitsetarbega. See mõjutab pooltevahelisi suhteid ja kaasa tuua mainekahju ning lepingu rikkumisest tulenevaid rahalisi tagajärgi.

2.6 Pääsuõiguste puudulik haldamine

Kui pääsuõiguste andmine, haldamine ja kontrollimine on teenuseandja juures halvasti korraldatud, võib kliendi töötajatele õiguste andmine ajaliselt venida või tehakse õiguste andmisel vigu.

Kui teenuseandja IT-talitus annab klientidele liigseid õiguseid, võidakse seetõttu saada juurdepääs ka teiste klientide andmetele. Andmete konfidentsiaalsuse ja tervikluse rikkumine võib teenuseandjale tähendada nõudeid lepingu rikkumisega kaasnevate kahjude korvamiseks.

2.7 Simultaanteeninduse võime puudumine teenuseandjal

Kui erinevate klientide IT-süsteemid ja andmed ei ole üksteisest piisavalt turvaliselt lahutatud, kaasneb oht, et üks klient pääseb juurde teise kliendi andmetele. Samuti peab teenuseandja otsustama, millise kliendi huvisid ta eelisjärjekorras kaitseb. Kui

asjassepuutuvad kliendid on omavahel konkurendid, võib see tuua kaasa teenuseandja jaoks väga ebamugavaid olukordi.

2.8 Teenuseandja sõltuvus allhankijatest

Kui teenuseandja kasutab väljasttellimist, võib teenuseandjal tekkida sõltuvus oma partnerite poolt pakutavate teenuste toimimisest. Teenuseandja ei oma äriprotsesside üle täielikku kontrolli, häired allhangete toimimises mõjutavad negatiivselt ka väljapoole pakutavate teenuste kvaliteeti. Teenuseandjal võib tekkida lepingu mittetäitmisest tulenev finants- ja mainekahju.

2.9 Teenuselepingu lõpetamise puudulik kord

Kui teenuselepingu lõpetamise kord on puudulik, võivad tekkida probleemid andmete kliendile üleandmisega. Näiteks erakorralisel lepingu lõpetamisel võivad andmed jääda kliendile terviklikult ja nõuetekohaselt üleandmata. Kui andmed jäävad teenusandja juures kustutamata, pole tagatud andmete turvaline säilitamine ning andmed võivad sattuda volitamata isikute kätte. Andmete pikaajalisel hoidmisel tekib oht rikkuda seadusest tulenevaid andmete säilitustähtaegu.

3 Meetmed

3.1 Elutsükkel

Kavandamine

OPS.3.2.M1 Teenuste turbe kavandamine

OPS.3.2.M2 Teenuselepingu tüüptingimused

OPS.3.2.M3 Turvanõuded allhankijate kasutamisel

OPS.3.2.M8 Teenuse osutamise põhimõtted

Evitus

OPS.3.2.M5 Teenuste turvakontseptsioon

OPS.3.2.M7 Allhankijate asendamise kord

OPS.3.2.M10 Turvaliste suhtluskanalite loomine ja kontaktisikute määramine

OPS.3.2.M13 Turvalised andmesidekanalid

OPS.3.2.M18 Allhankija töötajate teadlikkuse tõstmine

Käitus

OPS.3.2.M4 Klientide andmete eraldamise põhimõtted

OPS.3.2.M6 Teenuselepingu korralise ning erakorralise lõpetamise kord

OPS.3.2.M9 Teenuselepingute perioodiline läbivaatus

OPS.3.2.M12 Teenuseandja protsesside ja IT-süsteemide riskianalüüs

OPS.3.2.M14 Teenuseandja protsesside ja IT-süsteemide seire

OPS.3.2.M15 Klientidele esitatavad aruanded

OPS.3.2.M16 Teenuse tarneahela läbipaistvuse tagamine

OPS.3.2.M17 Pääsu reguleerimine

Avariivalmendus

OPS.3.2.M11 Teenuste avariivalmenduse plaan

Lisanduvad kõrgmeetmed

OPS.3.2.M19 Teenuseandja töötajate taustakontroll

OPS.3.2.M20 Andmesidekanalite ja salvestatud andmete krüpteerimine

OPS.3.2.M21 Ühised avarii- ja kriisiõppused

3.2 Põhimeetmed

OPS.3.2.M1 Teenuste turbe kavandamine

a. Teenuseandja on teenuste kavandamisel arvestanud teenuse saajate infoturbe vajadusi.
b. Teenuseandja on võimeline klientidele tagama nende poolt soovitud minimaalselt lubatava infoturbe taseme.
c. Teenus on vastavuse seadusandlusest tulenevate (sh andmekaitse) nõuetega.

OPS.3.2.M2 Teenuselepingu tüüptingimused

a. Teenuseandja on välja töötanud teenuselepingu tüüptingimused.
b. Teenuselepingu tüüptingimused sisaldavad vähemalt järgmist:
    - teenuse kasutamise üldised turvanõuded;
    - tundlike andmete kaitse põhimõtted ja vajadusel vastava lepingu (ingl *non-disclosure agreement*, NDA) sõlmimine;
    - teenuseandja õigused ja piirangud alltöövõtu (nt kolmandate poolte pilvteenused) kasutamiseks;
    - kliendi õigus läbi viia teenuseandja infoturbe nõuete täitmise kontrollimiseks infoturbe ülevaatusi või auditeid;
    - teabevahetuse kord;
    - teenusetasemete kirjeldused.
c. Teenuseandja on välja töötanud tüüptingimusi sisaldavad teenuselepingu vormid.
d. Teenuselepingu tüüptingimusi rakendatakse kõigis klientidega sõlmitud teenuselepingutes.

OPS.3.2.M3 Turvanõuded allhankijate kasutamisel

a. Väljasttellimise kasutamisel teenuseandja poolt on tagatud kliendiga sõlmitud teenuselepingus sätestatud tingimuste täitmine ja nõutava turvataseme säilitamine.
b. Kliendile osutatava teenuse toimimiseks vajalike tööde üleandmisel allhankijale sõlmitakse teenuseandja ja allhankija vahel leping, milles kirjeldatakse üleantavad tööülesanded ja seonduvad turvanõuded.
c. Kliendil on õigus tutvuda teenuseandja ja tema allhankijate vaheliste lepetega kliendile osutatava teenuse osas.

OPS.3.2.M4 Klientide andmete eraldamise põhimõtted

a. Teenuseandja on välja töötanud ja dokumenteerinud vahendid ja protseduurid, millega teenuseandja IT-süsteemides on erinevate klientide andmed ja käitluskeskkonnad üksteisest piisavalt turvaliselt eraldatud.

b. Teenuseandja on rakendanud kaitsetarbele vastavad meetmed klientide andmete eraldamiseks IT-süsteemides.

c. Kliendil on soovi korral võimalik tutvuda, milliste vahendite ja protseduuridega tagatakse andmete eraldatus teiste klientide andmetest.

OPS.3.2.M5 Teenuste turvakontseptsioon

a. Teenuseandja on koostanud kõiki klientidele pakutavaid teenuseid hõlmava turvakontseptsiooni.

b. Turvakontseptsioon sisaldab kõiki üldiseid turvameetmeid ja üksikutele teenustele kohaldatavaid täiendavaid turvameetmeid.

c. Enne teenuselepingu sõlmimist kooskõlastatakse teenuse turvakontseptsioon kliendiga. Klient võib vajadusel teha temale osutatava teenuse osas muudatusettepanekuid.

d. Kliendiga kooskõlastatud teenuse turvakontseptsioon ja teabe klassifitseerimise reeglid on osa kliendiga sõlmitavast teenuselepingust.

e. Teenuseandja kontrollib teenuste turvakontseptsiooni elluviimist ja meetmete rakendamist regulaarselt.

OPS.3.2.M6 Teenuselepingu korralise ning erakorralise lõpetamise kord

a. Teenuselepingus on kokku lepitud lepingu korralise lõpetamise tingimused.

b. Teenuselepingus on kokku lepitud lepingu erakorralise lõpetamise tingimused eesmärgil, et lepingu lõpetamine ei mõjutaks negatiivselt kliendi ega teenuseandja äriprotsesse.

c. Teenuselepingus on sätestatud teenuse andmisel kasutatud riist-ja tarkvara omandiõigus ja nende kasutamise jätkumise tingimused pärast lepingu lõpetamist.

d. Teenuselepingus on dokumenteeritud lepingu lõpetamisel üleantava teabe, andmete ja riistvara tagastamise protseduurid.

e. Kui ei ole teisiti kokku lepitud, kustutatakse teenuseandja juures edasi hoiustatavad kliendi andmed turvaliselt pärast seadusest tuleneva säilitustähtaja täitumist. Andmete kustutamise fakt dokumenteeritakse.

f. Lepingu lõppemisel vaadatakse üle teenuseandja ja kliendi töötajate pääsuõigused, mittevajalikud pääsuõigused eemaldatakse.

3.3 Standardmeetmed

OPS.3.2.M7 Allhankijate asendamise kord

a. Allhankijate teenuseid kasutav teenuseandja on koostanud alternatiivsete allhankijate loendi.

b. Allhankijaga sõlmitud lepingu korralisel või erakorralisel lõpetamisel on teenuseandjal võimalik ilma negatiivsete mõjutusteta ja olulise viivituseta tegevused üle anda teisele allhankijale või loobuda allhankija kasutamisest.

OPS.3.2.M8 Teenuse osutamise põhimõtted

a. Teenuseandja on dokumenteerinud põhimõtted teenuste loomiseks, testimiseks ja kasutusele võtuks.

b. Teenuseandja on määranud, kas teenuse osutamisel on lubatud kaasata väliseid partnereid (teenuseandja allhankijaid).

c. Teenuseandja on loonud protsessi teenusega seonduvate riskide (sh allhanke riskide) hindamiseks.

OPS.3.2.M9 Teenuselepingute perioodiline läbivaatus

a. Teenuselepingutes sätestatud turvameetmete täitmist ja turvameetmete jätkuvat asjakohasust kontrollitakse perioodiliselt ja/või sündmusepõhiselt. Ebapiisavate turvameetmetega kliendilepingud ajakohastatakse.

b. Teenuselepingutes sisalduvad turvanõuded vaadatakse täiendavalt üle teenusega seotud riskihinnangute ja seadusandlike aktide muutmisel. Vajadusel täiendatakse turvanõudeid.

OPS.3.2.M10 Turvaliste suhtluskanalite loomine ja kontaktisikute määramine

a. Teenuseandja loob andmevahetuseks klientidega turvalised suhtluskanalid.

b. Teenuseandja ja klient on kokku leppinud ja dokumenteerinud, millist teavet suhtluspartnerite vahel edastatakse ning kes on poolte kontaktisikud.

c. Määratud kontaktisikute volituste kehtivust kontrollitakse regulaarselt.

d. Teenuseandja ja klient on leppinud kokku andmekaitse intsidentide teavitusteedes, kontaktisikutes ning intsidentide lahendamise korras.

OPS.3.2.M11 Teenuste avariivalmenduse plaan [avariiülem]

a. On koostatud teenuste avariivalmenduse plaan, mis hõlmab mõlema teenusepoole asjakohaseid protsesse, komponente ja teenuseliideseid.

b. Avariivalmenduse plaan on kooskõlastatud teenuse kliendiga.

OPS.3.2.M12 Teenuseandja protsesside ja IT-süsteemide riskianalüüs

a. Enne uute rakenduste, IT-süsteemide või protsesside klientidele kättesaadavaks tegemist on teenuseandja läbi viinud riskianalüüsi ja määranud sobivad riskikäsitlusmeetmed.

b. Riskianalüüsi tulemid dokumenteeritakse ja neid kasutatakse infoturbe edasiseks täiustamiseks.

OPS.3.2.M13 Turvalised andmesidekanalid

a. Enne andmevahetuse alustamist lepitakse kokku ja dokumenteeritakse:
   - kasutatavad rakendused;
   - kasutatavad andmevormingud;
   - andmete käideldavuskriteeriumid (siinhulgas päringutele reageerimise aeg);
   - teabevahetuse turbe meetmed (vt CON.9 *Teabevahetus*);
   - turvamehhanismid (viirusetõrje, krüpteerimine, signeerimine, võtmehaldus jms).

b. Enne andmevahetuse käivitamist kontrollitakse andmesidekanaleid võimalike turvanõrkuste avastamiseks ning veendutakse nõutava turvataseme saavutamises.

c. Andmevahetuse toimimist testitakse enne teenuse kasutamist testandmetega.

d. Teenuseandja ja klient on leppinud kokku turvaintsidentide teavitusteedes, kontaktisikutes ning intsidentide lahendamise korras.

OPS.3.2.M14 Teenuseandja protsesside ja IT-süsteemide seire

a. Klientidele osutavate teenustega seotud protsesside ja IT-süsteemide toimimist seiratakse pidevalt.

OPS.3.2.M15 Klientidele esitatavad aruanded

a. Kliendiga on kokku lepitud tüüparuande formaat ja kasutatavad suhtluskanalid.

b. Teenuseandja esitab kliendile kindlaksmääratud ajavahemike järel aruande teenuse toimimisest.

c. Eelseisvatest muudatustest teenusega seotud protsessides teavitatakse kliente võimalikult varajases etapis.

OPS.3.2.M16 Teenuse tarneahela läbipaistvuse tagamine

a. Teenuseandja on dokumenteerinud allhankijate osalusega protsessid, peamised tulemusnäitajad, teenuse osutamisega seotud allhankijad ja nendega sõlmitud lepingud.

b. Teenuseandja kontrollib regulaarselt allhankijatega seotud dokumentatsiooni aja- ja asjakohasust. Allhankijatega sõlmitud lepingute muudatused dokumenteeritakse.

OPS.3.2.M17 Pääsu reguleerimine

a. Teenuseandja ja kliendi töötajate sissepääsu ruumidesse, süsteemidesse ja võrkudesse ning juurdepääsu andmetele ja tarkvarale reguleeritakse sobivate korralduslike ja tehniliste vahenditega.

b. Pääsuõigused on jagatud minimaalsuse põhimõttel vastavalt tööalastele vajadustele.

c. Audiitoritele tagatakse nende tööks vajalikud pääsuõigused.

OPS.3.2.M18 Allhankija töötajate teadlikkuse tõstmine

a. Allhankija töötajaid on juhendatud nende tööülesannete täitmise osas ning teavitatud kehtivatest infoturbe nõuetest ja infoturvet reguleerivatest dokumentidest.

b. Allhankija töötajad on kinnitanud, et kohustuvad järgima neile eelnevalt tutvumiseks esitatud eeskirju, protseduurireegleid, infoturbe nõudeid ja konfidentsiaalsuslepinguid.

c. Kõrgendatud turvanõuete puhul kontrollitakse allhankijate töötajate tausta ja vastavust teenuseandja või kliendi kehtestatud kvalifikatsiooninõuetele.

3.4 Kõrgmeetmed

OPS.3.2.M19 Teenuseandja töötajate taustakontroll [personaliosakond] (C-I-A)

a. Teenuseandja kontrollib enne töölepingu sõlmimist uute töötajate ja allhankija personali usaldusväärsust.

b. Teenusepooled lepivad kokku teenuseandja töötajate taustakontrolli läbiviimise kriteeriumid.

OPS.3.2.M20 Andmesidekanalite ja salvestatud andmete krüpteerimine (C)

a. Andmete turvaliseks edastamiseks ning nende hoidmiseks teenuseandja juures on kokku lepitud andmete kaitsetarbel põhinevad turvalised krüpteerimismehhanismid.

b. Krüpteerimismehhanismi toimimist kontrollitakse regulaarselt.

OPS.3.2.M21 Ühised avarii- ja kriisiõppused (A)

a. Teenuseandja viib teenuse klientidega koostöös regulaarselt läbi ühiseid avarii- ja kriisiõppuseid.

b. Ühisõppuste tulemusi kasutatakse teenuste avariivalmendusplaani (vt OPS.3.2.M11 *Teenuste avariivalmenduse plaan*) ja ühiste avariiprotseduuride täiustamiseks.

DER: Avastamine ja reageerimine

DER.1 Turvaintsidentide avastamine

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed turvasündmusega seonduvate andmete kogumiseks, seostamiseks ja hindamiseks, et tagada turvaintsidentide terviklik ja õigeaegne avastamine.

1.2 Vastutus

Turvaintsidentide avastamise meetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Kasutaja, vastutav spetsialist, töötaja, ülemus.

1.3 Piirangud

Moodul ei käsitle kõiki turvaintsidentide avastamisega seotud aspekte. Kohustuste lahusust käsitletakse moodulis ORP.1 *Infoturbe korraldus*. Sündmuste logimise meetmed on esitatud moodulis OPS.1.1.5 *Logimine*. Turvaintsidentide andmekaitse aspekte käsitletakse moodulis CON.2 *Isikuandmete kaitse*. Sissetungitõrje süsteeme käsitletakse moodulites OPS.1.1.4 *Kaitse kahjurvara eest* ja NET.3.2 *Tulemüür*.

2 Ohud

2.1 Õigusaktide sätete eiramine

Turvaintsidentide avastamiseks ja logiandmete analüüsiks kasutatavad tehnilised lahendused võivad koguda konfidentsiaalset teavet ja tundlikke isikuandmeid (nt töötajate tegevuste jälgimisel saadud teave). Selline isikuandmete töötlemine võib olla vastuolus isikuandmete kaitse üldmääruse ja isikuandmete kaitse seaduse sätetega.

2.2 Vastutajate puudulik kvalifikatsioon

Kui vastutajad ei suuda puuduliku koolituse tõttu eristada turvasündmusi organisatsiooni igapäevases IT-töös sageli esinevatest tõrgetest ja vigadest, võivad turvaintsidendid jääda märkamata.

2.3 Sissetungituvastuse süsteemide puudulik seadistus

Kui sissetungituvastuse süsteemid on valesti seadistatud, võib see tekitada rohkelt ebaolulisi hoiatusteateid. Turvaintsidendile viitavat teavitust ei suudeta neist eristada ja võimalik rünne võib jääda tuvastamata.

2.4 Teabe puudumine kaitstava IT-süsteemi kohta

Kui kasutatava IT-süsteemi kohta pole piisavalt teavet, on tõenäoline, et IT-süsteemi olulisi komponente ei suudeta piisavalt kaitsta ning need jäävad avastussüsteemide poolt katmata. Arvutivõrku tunginud ründaja tegevus võib jääda pikaks ajaks märkamatuks.

2.5 Avastussüsteemide vähene kasutamine

Kui avastussüsteeme ei kasutata ning IT-süsteemide ja rakenduste turvasündmuste avastusfunktsioone ei aktiveerita, on ründajal oluliselt lihtsam võrku sisse tungida. Oht on veelgi suurem, kui võrk on segmentimata ja võrkudevahelist liiklust ei monitoorita. Ründaja tegevus võrgus jääb märkamatuks.

2.6 Ebapiisav inimressurss

Kui logiandmete ja ründevektorite analüüsimiseks ei jätku inimressurssi või kui töötajad ei jälgi väliseid teabeallikaid turvanõrkuste kohta, võivad turvasündmused jääda tuvastamata või avastatakse intsident alles pärast olulise kahju tekkimist. Kui turvanõrkused organisatsiooni IT-süsteemides jäävad õigeaegselt parandamata, on ründajal võimalik kasutada turvanõrkust organisatsioonivastase ründe sooritamiseks.

3 Meetmed

3.1 Elutsükkel

Kavandamine

DER.1.M1 Turvaintsidentide avastamise eeskiri

DER.1.M2 Logiandmete analüüsi õiguspärasus

DER.1.M3 Turvasündmustest teavitamise kord

DER.1.M4 Töötajate teadlikkuse tõstmine

DER.1.M7 Vastutajate koolitus

Käitus

DER.1.M5 IT-süsteemi avastusfunktsioonide rakendamine

DER.1.M6 Logiandmete pidev seire ja analüüs

DER.1.M9 Täiendavad avastussüsteemid

DER.1.M11 Keskne logimistaristu turvasündmuste analüüsiks

Parendamine

DER.1.M12 Välisallikate teabe analüüs

DER.1.M13 Regulaarne avastussüsteemide läbivaatus

Lisanduvad kõrgmeetmed

DER.1.M10 TLS- ja SSH-proksid

DER.1.M14 Logiandmete analüüsile spetsialiseerunud töötajad

DER.1.M15 Reaalajas toimuv sündmuseteadete keskhaldus

DER.1.M16 Avastussüsteemide rakendamine kaitsetarbe alusel

DER.1.M17 Automaatne reageerimine turvasündmustele

DER.1.M18 Regulaarne tervikluse kontroll

3.2 Põhimeetmed

DER.1.M1 Turvaintsidentide avastamise eeskiri

a. Organisatsiooni üldisest turvapoliitikast lähtudes on koostatud eeskiri, milles on kirjeldatud turvaintsidentide õigeaegseks avastamiseks vajalikud plaanimis- ja operatiivtegevused.

b. Turvaintsidentide avastamise eest vastutajad on eeskirjast teadlikud ja võtavad selle oma tegevuse aluseks. Eeskirja muudatused ja eeskirjast lahknevused kooskõlastatakse infoturbejuhiga ja dokumenteeritakse.

c. Turvaintsidentide avastamise eeskirja järgimist kontrollitakse regulaarselt, kontrolli tulemused dokumenteeritakse.

DER.1.M2 Logiandmete analüüsi õiguspärasus

a. Logiandmete analüüsiks on koostatud juhend, milles on esitatud kohaldatavad õigusaktide nõuded. Juhendit ajakohastatakse õiguslike raamtingimuste muutumisel.

b. Logiandmete analüüsimisel ja avastussüsteemide kasutamisel järgitakse andmekaitsealaste ja muude kohalduvate õigusaktide (nt töösuhete korraldamist reguleerivate seaduste) nõudeid.

DER.1.M3 Turvasündmustest teavitamise kord

a. Organisatsioonis on kehtestatud turvasündmustest teavitamise kord, kus dokumenteeritakse teavitusteed ja adressaadid eri liiki intsidentide puhuks, teavitatavad isikud, isikute kättesaadavus ja intsidendi kiireloomulisusest sõltuv sidekanali valik.

b. Töötajad on teadlikud oma ülesannetest ja kohustustest. Turvasündmuse kahtluse korral teavitatakse sellest koheselt turvasündmustest teavitamise korras määratud isikuid, kasutades korras esitatud teavitusteid ja sidekanaleid.

c. Kasutusele võetud teavitusteede toimimist testitakse regulaarselt, vajadusel turvasündmustest teavitamise kord ajakohastatakse.

DER.1.M4 Töötajate teadlikkuse tõstmine [ülemus, kasutaja, töötaja]

a. Töötajad on võimelised turvaintsidenti ära tundma ja on motiveeritud sellest teatama.

b. Töötajatele on selgitatud, et klientide või IT-süsteemide saadetud sündmuseteateid ei tohi jätta tähelepanuta ega teateid ignoreerida.

c. Töötajad teavad, kellele tuleb turvasündmuse info edastada ja milliseid teavitusteid seejuures kasutada (vt DER.2.1 *Turvaintsidentide käsitlus*).

DER.1.M5 IT-süsteemi avastusfunktsioonide rakendamine [vastutav spetsialist]

a. Kui kasutataval IT-süsteemil on funktsioonid, mida saab turvaintsidentide avastamiseks rakendada, on need aktiveeritud.

b. Turvasündmuse korral analüüsitakse mõjutatud IT-süsteemi sündmuseteateid, võimalusel hinnatakse ka muudes IT-süsteemidest samal ajal logitud sündmusi.

c. Sündmuseteadete kogumist IT-süsteemides kontrollitakse regulaarselt.

d. Võimaluse korral sündmuseteadete edastus automatiseeritakse. Kahjurkoodi avastamise skanner edastab vastutavatele isikutele turvasündmuse teate edasiseks analüüsiks automaatselt.

3.3 Standardmeetmed

DER.1.M6 Logiandmete pidev jälgimine ja analüüs

a. Organisatsioonis on määratud logiandmete pideva jälgimise ja analüüsi eest vastutavad töötajad.

b. Turvaintsidentide avastamiseks on koostatud IT-süsteemide põhised logiandmete analüüsi juhised.

c. On olemas piisav inimressurss logiandmete pideva jälgimise ja analüüsi teostamiseks.

DER.1.M7 Vastutajate koolitus [ülemus]

a. Sündmuseteadete analüüsi eest vastutajail on vajalik kvalifikatsioon ja läbitud vastav koolitus.

b. IT-süsteemide või rakenduste hankimisel arvestatakse eelarves turvasündmustega tegelevate töötajate koolitusvajadusega.

DER.1.M9 Täiendavad avastussüsteemid [vastutav spetsialist]

a. Võrguskeemi (vt NET.1.1 *Võrgu arhitektuur ja lahendus*) alusel on määratud, milliseid võrgusegmente kaitstakse täiendavate avastussüsteemide abil.

b. Turvaintsidentide avastamise tõhustamiseks rakendatakse täiendavaid avastussüsteeme ja andureid.

c. Sissetungituvastuse süsteeme (ingl *intrusion detection system*, IDS) hallatakse tsentraalselt.

d. Välisvõrgu ja sisevõrgu segmentide vahelise liikluse kaitseks kasutatakse võrkutungi tuvastuse süsteemi (ingl *network intrusion detection system*, NIDS).

DER.1.M11 Keskne logimistaristu turvasündmuste analüüsiks [vastutav spetsialist]

a. IT-süsteemidest kogutud sündmuseteated hoiustatakse keskses logimistaristus (vt OPS.1.1.5 *Logimine*).

b. Logimistaristu võimaldab mitmetest allikatest edastatud sündmuseteateid sünkroniseerida, korreleerida, analüüsida ja talletada.

c. Kogutud sündmuseteateid analüüsitakse kõrvalekallete avastamiseks regulaarselt.

d. Logimistaristus talletatud turvasündmusi on võimalik analüüsida ka tagantjärele.

DER.1.M12 Välisallikate teabe analüüs [vastutav spetsialist]

a. IT-süsteemidega seotud turvanõrkuste kohta hangitakse teavet kvalifitseeritud välisallikatest, asjakohane teave jõuab õigete töötajateni.

b. Kvalifitseeritud allikatest pärinevat teabe asjakohasust hinnatakse, vajadusel muudetakse turvaintsidentide avastamise ja käsitluse protsessi (vt ka DER.2.1. Turvaintsidentide käsitlus).

DER.1.M13 Regulaarne avastussüsteemide läbivaatus

a. Avastussüsteemide ja nendes rakendatavate meetmete ajakohasust ning toimivust kontrollitakse regulaarselt.

b. Läbivaatuse tulemused dokumenteeritakse ja neid võrreldakse eelmiste läbivaatuste tulemustega. Kõrvalekaldeid kontrollitakse.

3.4 Kõrgmeetmed

DER.1.M10 TLS- ja SSH-proksid [vastutav spetsialist] (C)

a. Välisvõrku üleminekul kasutatakse TLS- ja SSH-proksit, mis katkestavad krüpteeritud ühenduse ja võimaldavad edastatavaid andmeid kahjurvara suhtes kontrollida.

b. TLS- ja SSH-proksides kasutakse turvasündmuste automaatset avastamist ja teavitamist.

DER.1.M14 Logiandmete analüüsile spetsialiseerunud töötajad (C-l)

a. Logiandmete analüüsile spetsialiseerunud töötajad on vajaliku kvalifikatsiooniga ja saanud erialast täiendkoolitust.

b. Spetsiifilisi teadmisi nõudva logianalüütikaga (nt kriminalistika valdkonnas) tegelevad selleks spetsialiseerunud töötajad.

DER.1.M15 Reaalajas toimuv sündmuseteadete keskhaldus (C-I-A)

a. Turvasündmuste tuvastamiseks, seoste loomiseks ja turbega seotud asjaolude nähtavaks muutmiseks kasutakse tsentraalsel tarkvaralahendusel põhinevat automaatanalüüsi.

b. Kogutavad logiandmed on terviklikud ja neid saab automaatselt analüüsida.

c. Logianalüüsi tehakse pidevalt ja reaalajas, analüüsiparameetrite etteantud läviväärtuste ületamisel alarmeeritakse määratud töötajat sündmusest automaatselt.

d. Analüüsiparameetreid ja otsustuskriteeriume korrigeeritakse regulaarselt, uute parameetrite rakendamisel analüüsitakse ka eelnevalt kontrollitud andmeid.

DER.1.M16 Avastussüsteemide rakendamine kaitsetarbe alusel (C-I-A)

a. Suurema kaitsetarbega IT-süsteeme kaitstakse avastussüsteemidega, millel on tehniline võimekus ja suutlikkus suurema kaitsetarbe tingimustes opereerimiseks.

DER.1.M17 Automaatne reageerimine turvasündmustele (C-I)

a. Kasutusele on võetud automaatne sissetungitõrje süsteem (ingl *intrusion prevention system*, IPS), mis on võimeline:

b. tuvastama ründeid, väärkasutusi ja rikkumisi;

c. teatama turvasündmustest automaatselt;

d. reageerima turvasündmusele automaatse kaitsetoiminguga.

DER.1.M18 Regulaarne tervikluse kontroll (C-I)

a. Regulaarselt kontrollitakse kõigi avastussüsteemide korrasolekut ja kasutajate õigusi süsteemis.

b. Automaatselt kontrollitakse failide terviklust ja alarmeeritakse tervikluse kao korral.

DER.2: Turvaintsidentide haldus

DER.2.1 Turvaintsidentide käsitlus

1 Kirjeldus

1.1 Eesmärk

Esitada juhised turvaintsidentide süstemaatiliseks käsitlemiseks.

1.2 Vastutus

Turvaintsidentide käsitluse meetmete täitmise eest vastutab infoturbejuht.

Lisavastutajad

Andmekaitsespetsialist, vastutav spetsialist, IT-talitus, organisatsiooni juhtkond, avariiülem.

1.3 Piirangud

Moodul ei käsitle kõiki turvaintsidentidega seotud toiminguid. Intsidentide avastamise meetmed esitatakse moodulis DER.1 *Turvaintsidentide avastamine*. Esmast kriminalistikauuringut käsitletakse moodulis DER.2.2 *IT-kriminalistika võimaldamine* ja kinnisründe intsidendile järgnevat tegevust moodulis DER.2.3 *Ulatuslike turvaintsidentide lahendamine*. Intsidendi tulemusena tekkinud avariiolukorras tegutsemist käsitletakse moodulis DER.4 *Avariihaldus*.

2 Ohud

2.1 Turvaintsidentide puudulik käsitlus

Kui turvaintsidentidele reageeritakse ebasobival viisil või meetmeid kiiresti ei rakendata, võib ründaja turvanõrkust ära kasutada pikema perioodi jooksul. Väärad otsused turvaintsidentide käsitluses võivad tekitada väga suurt kahju, sealhulgas ka asjatuid kahjusid kolmandatele osapooltele. Näited juhtumitest, mis viitavad turvaintsidentide puudulikule käsitlemisele:

- tulemüüri logifailid sisaldavad kahtlasi kirjeid;
- intsidendist teavitamisega venitatakse;
- kontoris toimunud varguse käsitlemisel ei arvestata, et varastatud sülearvutis võis olla konfidentsiaalseid andmeid.

2.2 Tõendusjälgede hävitamine turvaintsidendi käsitlusel

Turvaintsidentide hoolimatu käsitluse korral võivad olulised tõendusjäljed enne asjaolude väljaselgitamist või hilisemat kohtumenetlust hävida või puudub andmetel piisav tõendusväärtus. Näited tõendusjälgede hävimisest:

- Kasutaja sulges aktiveerunud kahjurkoodiga arvuti, mistõttu ei saa koguda täiendavat infot aktiivsete protsesside ja põhimällu laetud komponentide kohta;
- Serveri haldur kustutas serveri koormust tõstva protsessi tulemusena tekkinud ajutised failid ilma nende sisu analüüsimata;

- Serveri haldur otsustas kohe pärast intsidendi avastamist installida serverisse puuduvad turvapaigad ja uuendid.

3 Meetmed

3.1 Elutsükkel

Kavandamine

DER.2.1.M1 Turvaintsidendi määratlemine
DER.2.1.M2 Turvaintsidentide käsitluse juhend
DER.2.1.M3 Vastutuste ja kontaktisikute määramine
DER.2.1.M7 Turvaintsidentide käsitluse metoodika
DER.2.1.M8 Turvaintsidentide käsitluse töörühm
DER.2.1.M9 Turvaintsidentidest teavitamise juhend
DER.2.1.M11 Turvaintsidentide hindamine
DER.2.1.M14 Turvaintsidentide eskalatsiooniplaan

Käitus

DER.2.1.M4 Turvaintsidendist teavitamise kord
DER.2.1.M5 Turvaintsidendi lahendamise kord
DER.2.1.M10 Turvaintsidentide toime piiramine
DER.2.1.M12 Turvaintsidentide ning IT-intsidentide käsitluse ühendamine
DER.2.1.M13 Turbe- ja avariihalduse integreerimine
DER.2.1.M15 IT-talituse töötajate valmidus turvaintsidentide käsitluseks
DER.2.1.M16 Turvaintsidentide käsitluse dokumenteerimine

Avariivalmendus

DER.2.1.M6 Töökeskkonna taastamine pärast turvaintsidenti

Täiustamine

DER.2.1.M17 Turvaintsidentide järeltoimingud
DER.2.1.M18 Protsessi täiustamine kogemuste ja välisarengute põhjal

Lisanduvad kõrgmeetmed

DER.2.1.M19 Turvaintsidentide käsitlusprioriteedid
DER.2.1.M20 Organisatsiooni turvaintsidentide teatamiskeskus
DER.2.1.M21 Ekspertrühm turvaintsidentide käsitluseks
DER.2.1.M22 Turvaintsidentide käsitluse korralduse läbivaatus

3.2 Põhimeetmed

DER.2.1.M1 Turvaintsidendi määratlemine

a. Organisatsioon on määratud, millised intsidendid on turvaintsidendid. Turvaintsident on IT-tõrgetest selgesti eristatav.

b. Turvaintsidentide käsitlusse kaasatud töötajad teavad turvaintsidendi määratlust.

c. Turvaintsidendi määratluse ja käsitluse aluseks võetakse konkreetsete äriprotsesside, IT-süsteemide ja rakenduste kaitsetarve.

DER.2.1.M2 Turvaintsidentide käsitluse juhend

a. Turvaintsidentide käsitluseks on koostatud protseduurijuhend. Juhendis on määratud käsitlusala, millele juhend laieneb.

b. Juhend sisaldab praktilisi ja sihtrühmakohaseid tegevusjuhiseid käitumiseks turvaintsidendi toimumise puhul.

c. Juhend tehakse teatavaks kõigile töötajatele.

d. Turvaintsidentide käsitlemise juhendit vaadatakse üle ja ajakohastatakse regulaarselt.

DER.2.1.M3 Vastutuste ja kontaktisikute määramine

a. Turvaintsidentide käsitlusega seotud vastutus ja kohustused rakenduvad kõikidele töötajatele.

b. Turvaintsidentidega tegelevad töötajad on läbinud vastava koolituse.

c. Organisatsioonis on määratud, kes ja mis alustel saab otsustada kriminalistikauuringu algatamise.

d. Töötajad teavad eri tüüpi turvaintsidentide kontaktisikuid, vastav teave on ajakohane ja töötajatele kättesaadav.

DER.2.1.M4 Turvaintsidendist teavitamise kord [organisatsiooni juhtkond, IT-talitus, andmekaitsespetsialist, avariiülem]

a. Turvaintsidendi ilmnemisel teavitatakse sellest organisatsioonisiseseid ja -väliseid asjaosalisi viivitamata ning turvaintsidentide käsitluse juhendi kohaselt.

b. Igakordselt otsustatakse, kas intsidendi lahendamisse kaasatakse lisaks ka andmekaitsespetsialist, jurist või organisatsiooni juhtkond.

c. Kui turvaintsidentidest tuleb teavitada väliseid ametiasutusi (CERT-EE, politsei, Andmekaitse Inspektsioon), tehakse seda teavitamiskohustustes määratud perioodi jooksul, teavitamiseks kasutatakse turvalisi suhtlusteid.

DER.2.1.M5 Turvaintsidendi lahendamise kord [IT-talitus]

a. Turvaintsidendi lahendamiseks isoleeritakse mõjutatud komponendid, intsident dokumenteeritakse ja selgitatakse välja selle põhjus.

b. Vajadusel kaasatakse turvaintsidendi eri teemavaldkondadega seotud küsimuste lahendamiseks organisatsioonisiseseid või -väliseid spetsialiste. Selleks on loodud turvalised suhtlusteed.

c. Intsidendi lahendamise käigus taastatakse võimalikult kiiresti intsidendile eelnenud normaalolukord (vt DER.2.1.M6 *Töökeskkonna taastamine pärast turvaintsidenti*).

DER.2.1.M6 Töökeskkonna taastamine pärast turvaintsidenti [IT-talitus]

a. Turvaintsidendi analüüsimiseks eraldatakse intsidendist mõjutatud seadmed võrgust.

b. Intsidendi käsitlemiseks vajalikud andmed varundatakse andmete hilisemaks analüüsiks.

c. Võimalike mõjude ja muutuste avastamiseks kontrollitakse mõjutatud seadme operatsioonisüsteemi ja kõiki rakendusi, paigaldatakse puuduvad turvapaigad ja uuendid.

d. Intsidendijärgsel andmete ennistamisel kontrollitakse andmete õigsust ja terviklust. Varundatud andmete taastamisel veendutakse, et need ei ole turvaintsidendist mõjutatud.

e. Enne mõjutatud seadmete taaskasutuselevõttu muudetakse kõik seadmes kasutatud paroolid, viiakse läbi turvatestimine ja kontrollitakse koos kasutajaga komponendi funktsioneerimist.

f. Uute või korduvate anomaaliate avastamiseks seiratakse pärast töökeskkonna taastamist mõjutatud ja ennistatud seadmete võrguliiklust

3.3 Standardmeetmed

DER.2.1.M7 Turvaintsidentide käsitluse metoodika [organisatsiooni juhtkond]

a. Turvaintsidentide käsitlemise juhendis (vt DER.2.1.M2 *Turvaintsidentide käsitluse juhend*) on dokumenteeritud metoodika ja protseduurid eri liiki turvaintsidentide käsitlemiseks.

b. Organisatsiooni juhtkond on turvaintsidentide käsitluse metoodika kinnitanud ja kasutajatele teatavaks teinud.

c. Turvaintsidentide käsitluse metoodikat kontrollitakse ja ajakohastatakse regulaarselt.

DER.2.1.M8 Turvaintsidentide käsitluse töörühm

a. Turvaintsidentide käsitluseks moodustatakse töörühm, töörühma koosseisu võidakse olenevalt intsidendi liigist muuta.

b. Töörühma liikmetele on eelnevalt määratud konkreetne roll ja ülesanded, mida nad on valmis vajadusel täitma.

c. Turvaintsidentide käsitluse töörühma koosseisu muudetakse vastavalt vajadusele.

DER.2.1.M9 Turvaintsidentidest teavitamise juhend

a. Intsidentidest teavitamiseks koostatakse juhend, mis sätestab vähemalt järgmist:

- lubatavad ja sobivad teavitusteed eri liiki intsidentide puhuks;
- isikute nimekiri, keda informeeritakse kindlasti ja keda vajadusel;
- kelle kaudu, millises järjekorras ja millise täpsusega teave liigub;
- kes edastab turvaintsidentidega seotud teavet kolmandatele pooltele.

DER.2.1.M10 Turvaintsidentide toime piiramine [avariiülem, IT-talitus]

a. Turvaintsidendi põhjuste analüüsiga paralleelselt kogutakse intsidendi mõju hindamiseks vajalikku teavet.

b. Kõige tõenäolisemate intsidendistsenaariumide jaoks on koostatud intsidendi käsitlemise tegevuskava.

DER.2.1.M11 Turvaintsidentide hindamine [IT-talitus]

a. Turbehalduse ja intsidendihalduse funktsioonidele on kehtestatud turvaintsidentide ja muude häiringute (nt IT-rikete) hindamiseks ja liigitamiseks ühtne protseduur.

DER.2.1.M12 Turvaintsidentide ja IT-intsidentide käsitluse ühendamine [avariiülem]

a. Organisatsioon on analüüsinud turvaintsidentide ja IT-intsidentide kokkupuutekohti ning määratlenud ressursid, mida kasutatakse mõlemat tüüpi intsidentide puhul.

b. IT-intsidentide lahendajatele on selgitatud turvaintsidentide käsitluse erisusi.

c. Turbehalduse töötajatel on IT-intsidentide haldusvahendile lugemisõigusega ligipääs.

DER.2.1.M13 Turbe- ja avariihalduse integreerimine [avariiülem]

a. Kui turvaintsidendi tulemusel on käivitatud avariihalduse protsess, koordineerib intsidendi lahendamist avariiülem.

b. Vajadusel kaasatakse intsidendi lahendamisse täiendavaid, spetsiifiliste oskustega spetsialiste.

DER.2.1.M14 Turvaintsidentidest teavitamise eskalatsiooniplaan [IT-talitus]

a. Lisaks kommunikatsiooniplaanile (vt DER.2.1.M9 *Turvaintsidentidest teavitamise juhend*) luuakse turvaintsidentidest teavitamise eskalatsiooniplaan, mis kooskõlastatakse infoturbejuhiga.

b. Turvaintsidentidest teavitamise eskalatsiooniplaan sisaldab tegevusjuhiseid, keda ja mis juhtudel intsidendi lahendamiseks täiendavalt kaasata.

c. Eskalatsiooniplaani rakendamiseks valitakse vahendid ja teavitusteed, mis on kättesaadavad ka eriolukorras ning sobivad konfidentsiaalse teabe jagamiseks.

d. Turvaintsidentidest teavitamise eskalatsiooniplaani testitakse regulaarselt. Vajadusel eskalatsiooniplaan ajakohastatakse.

DER.2.1.M15 IT-talituse töötajate valmidus turvaintsidentide käsitluseks [IT-talitus]

a. IT-talituse töötajad teavad oma hallatavate süsteemide kaitsetarvet.

b. IT-talituse töötajatel on turvaintsidentide tuvastamiseks vajalikud vahendid ja kontroll-küsimustikud.

c. IT-talituse töötajad on tutvunud turvaintsidentide käsitluse juhendiga ning läbinud vajalike vahendite kasutamise koolituse.

DER.2.1.M16 Turvaintsidentide käsitluse dokumenteerimine

a. Turvaintsidendid dokumenteeritakse ühtse tüüpprotseduuri kohaselt.

b. Turvaintsidendi dokumenteerimisel fikseeritakse kõik käsitluse käigus tehtud tegevused koos läbiviimise ajaga ning talletatakse mõjutatud komponentide logiandmed.

c. Turvaintsidendi käsitluse raport arhiveeritakse viisil, mis tagab selle tervikluse ja konfidentsiaalsuse.

DER.2.1.M17 Turvaintsidentide järeltoimingud

a. Turvaintsidendi käsitluse järgselt hinnatakse:

- kui kiiresti turvaintsident tuvastati ja lahendati;
- kas teavitusteed toimisid;

- kas oli piisavalt andmeid mõjuhinnangu läbiviimiseks;
- kas avastamismeetmed ja käsitlusmeetmed olid tõhusad.

b. Varasemate turvaintsidentide kogemusi kasutatakse sarnaste turvaintsidentide käsitlemise tegevuskava koostamiseks. Tegevuskava muudatused tehakse sihtrühmadele teatavaks.

c. Juhtkonda teavitatakse toimunud turvaintsidendist ja selle käsitluse tulemustest.

DER.2.1.M18 Protsessi täiustamine kogemuste ja välisarengute põhjal [vastutav spetsialist]

a. Turvaintsidentide käsitluse täiustamiseks küsitakse turvaintsidentide lahendamisel kaasatud olnud isikute arvamusi ja vastutajate tagasisidet.

b. Pärast IT-süsteemides ja intsidendihalduses toimunud muudatusi ajakohastatakse intsidentide avastamis- ja haldusvahendeid ning juhendeid.

3.4 Kõrgmeetmed

DER.2.1.M19 Turvaintsidentide käsitluse prioriteedid [organisatsiooni juhtkond] (C-I-A)

a. Äriprotsesside erinevast kaalukusest tulenevalt määratakse intsidentide käsitluse prioriteedid.

b. Turvaintsidentide käsitluse prioriteedid kinnitab organisatsiooni juhtkond. Sarnastel alustel prioriteete kasutatakse ka IT- intsidendihalduses.

c. Turvaintsidentide käsitlusega seotud otsustajad tunnevad ja kasutavad prioriteete, arvestades ka turvaintsidendile antud esmast hinnangut (vt DER.2.1.M11 *Turvaintsidentide hindamine*).

DER.2.1.M20 Organisatsiooni turvaintsidentidest teatamise keskus (C-I-A)

a. Organisatsioon on loonud turvaintsidentidest teatamise keskuse.

b. Turvaintsidentidest teatamise keskus reageerib intsidenditeadetele tavapärasel tööajal ilma viivituseta.

c. Turvaintsidentidest teatamise keskuse töötajad on saanud piisava infoturbe koolituse.

d. Kogu turvaintsidentidega seotud teavet käsitletakse turvaintsidentidest teatamise keskuses konfidentsiaalsena.

DER.2.1.M21 Ekspertrühm turvaintsidentide käsitluseks (C-I-A)

a. Turvaintsidentide käsitlemiseks on moodustatud kogenud ja usaldusväärsetest töötajatest koosnev ekspertrühm. Ekspertrühm on varustatud piisavate tehniliste ja rahaliste ressurssidega.

b. Ekspertrühma liikmetel on organisatsiooni süsteemide analüüsimiseks hea ettevalmistus. Rühma liikmed tegelevad pideva teadmiste täiendamisega nii kasutusele võetud süsteemide kui ka turvaintsidentide avastamise ja nendele reageerimise valdkonnas.

c. Ekspertrühma liikmete usaldusväärsust kontrollitakse ning rühma koosseisu uuendatakse vastavalt vajadusele.

d. Ekspertrühma liikmed on kaasatud intsidentide eskalatsiooni- ja teavituskanalitesse.

e. Ekspertrühm on lõimitud intsidentide halduse korraldusse (vt DER.2.1.M8 *Turvaintsidentide käsitluse töörühm*), ekspertrühma vastutus on määratud ja kooskõlastatud (vt DER.2.1.M3 *Vastutuste ja kontaktisikute määramine*).

DER.2.1.M22 Turvaintsidentide käsitluse korralduse läbivaatus (C-I-A)

a. Turvaintsidentide käsitluse korraldust ning sellega seotud mõõdetavaid näitajaid (nt turvaintsidentide avastamisel, intsidentidest teavitamisel ja intsidentide eskaleerimisel) hinnatakse regulaarselt.
b. Turvaintsidentide käsitluse toimivust kontrollitakse nii plaanitud läbivaatuste kui etteteatamiseta läbivaatuste teel. Kontrollimine on eelnevalt juhtkonnaga kooskõlastatud.
c. Praktilise kogemuse saamiseks harjutatakse intsidendikäsitlust simuleeritud turvaintsidentidega.

DER.2.2 IT-kriminalistika võimaldamine

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed infoturvaintsidendi kriminalistikauuringu meetmete rakendamiseks. Moodulis käsitletakse IT-kriminalistika (ingl *computer forensics*) strateegilise ettevalmistuse, algatamise, asitõendite turbe, analüüsi ning tulemuste esituse etappe.

1.2 Vastutus

„IT-kriminalistika võimaldamine“ meetmete täitmise eest vastutab infoturbejuht.

Lisavastutajad

Andmekaitsespetsialist, vastutav spetsialist, organisatsiooni juhtkond.

1.3 Piirangud

Moodul ei sisalda ründetuvastuse meetmeid (vt DER.1 *Turvaintsidentide avastamine*). Samuti ei selgitata kriteeriume ja protsesse otsustamaks kriminalistikauuringu vajalikkust, see tehakse turvaintsidendi käsitluse ajal (vt DER.2.1 *Turvaintsidentide käsitlus*).

Samuti ei hõlma moodul õigusrikkumistega seotud õiguskaitseorganite poolt läbiviidavaid turvakriminalistika ekspertiise.

2 Ohud

2.1 Õiguslike raamtingimuste rikkumine

Kriminalistikauuringu käigus kopeeritakse ja analüüsitakse klientide, töötajate või partnerite isikuandmeid. Kui isikuandmeid kasutatakse põhjendamatult, rikub organisatsioon õigusaktide nõudeid.

2.2 Asitõendite kaotus puuduliku turbe tõttu

Kui asitõendite turvalisusele, eriti asitõendite autentsuse tagamisele ei pöörata tähelepanu, võivad olulised asitõendid kaotsi minna või kaotada tõendusväärtuse. Intsidendi käigus tekkinud ajutised failid võivad sisaldada uuringu seisukohast olulist teavet. Kui neid õigeaegselt teise asukohta ei salvestada, ei saa neid andmeid kriminalistikauuringus kasutada.

Kui IT-kriminalistika töövahendeid kasutatakse oskamatult, ei täida nende tööriistade kasutamine oma eesmärki.

3 Meetmed

3.1 Elutsükkel

Kavandamine

DER.2.2.M2 Esmameetmete juhend infoturvaintsidendi puhuks

DER.2.2.M3 Kriminalistikateenuse tarnijate kaardistamine

DER.2.2.M4 Kriminalistikauuringu seotus kriisi- ja intsidendihaldusega

DER.2.2.M5 Infoturvaintsidendi asitõendite turbe juhend

Evitus

DER.2.2.M6 Personali koolitus IT-kriminalistika alal

DER.2.2.M7 IT-kriminalistika töövahendite õige valimine

Käitus

DER.2.2.M1 Andmekäitluse õiguslike raamtingimuste kontroll

DER.2.2.M8 Asitõendite õige valimine ja järjestamine

DER.2.2.M9 Analüüsitavate andmete õige valimine

DER.2.2.M10 Asitõendite IT-kriminalistika turve

DER.2.2.M11 Asitõendite turbe dokumenteerimine

DER.2.2.M12 Originaal-andmekandjate ja asitõendite turvaline säilitus

Lisanduvad kõrgmeetmed

DER.2.2.M13 Raamlepingud kriminalistikateenuse tarnijatega

DER.2.2.M14 Tüüpprotseduurid asitõendite turbeks

DER.2.2.M15 Asitõendite turbe õppused

3.2 Põhimeetmed

DER.2.2.M1 Andmekäitluse õiguslike raamtingimuste järgimine [andmekaitsespetsialist, organisatsiooni juhtkond]

a. Kriminalistikauuringu tarbeks andmete kogumine ja analüüs viiakse läbi õigusaktidega lubatud piires (vt ORP.5 *Vastavushaldus (nõuetehaldus)*).

b. Andmete töötlemine kooskõlastatakse andmekaitsespetsialistiga. Andmete töötlemisel ei rikuta organisatsiooni sise-eeskirju ega personalikokkuleppeid.

c. Organisatsiooni ja töötajate huvide konflikti ilmnemisel kaalutakse töötaja eemaldamist protsessist.

DER.2.2.M2 Esmameetmete juhend infoturvaintsidendi puhuks

a. Infoturvaintsidendile järgnevad tegevused viiakse läbi intsidendist mõjutatud IT-süsteemides intsidendi jälgi rikkumata.

b. Esmameetmete juhendis on kirjeldatud, kuidas vältida kasutatavates IT-süsteemides asitõendite hävimist.

3.3 Standardmeetmed

DER.2.2.M3 Kriminalistikateenuse tarnijate kaardistamine

a. Organisatsioonisisese IT-kriminalistika võimekuse puudumisel on kaardistatud sobivad kriminalistikateenuse tarnijad.

b. Kriminalistikateenuse tarnijate kontaktandmed on esitatud esmameetmete juhendis.

DER.2.2.M4 Kriminalistikauuringu seotus kriisi- ja intsidendihaldusega

a. Infoturvaintsidentide kriminalistikauuringu liidestus kriisi- ja intsidendihaldusega on dokumenteeritud infoturbe kontseptsioonis.

b. On määratud valdkonnaülesed teavitusteed ja vastutajad, kontaktisikud on vajadusel kättesaadavad.

DER.2.2.M5 Infoturvaintsidendi asitõendite turbe juhend

a. On koostatud asitõendite turbe juhend, mis sisaldab meetodeid, tehnilisi vahendeid, õiguslikke raamtingimusi ja dokumenteerimisnõuded asitõendite tõendusväärtuse tagamiseks.

DER.2.2.M6 Personali koolitus IT-kriminalistika alal

a. Vastutajatele korraldatakse koolitusi IT-kriminalistika töövahendite kasutamiseks ja kogutud asitõendite turvalisuse tagamiseks.

DER.2.2.M7 IT-kriminalistika töövahendite õige valimine

a. Asitõendite ja jälgede analüüsiks on olemas sobivad töövahendid.

b. Enne IT-kriminalistika töövahendi kasutamist veendutakse, et see on töökorras ning töövahendit pole manipuleeritud. Kontrolli tulemused dokumenteeritakse.

DER.2.2.M8 Asitõendite õige valimine ja järjestamine [vastutav spetsialist]

a. Kriminalistikauuringule seatakse võimalikult täpne eesmärk. Andmeallikad valitakse eesmärgist lähtudes.

b. Asitõendite kogumiseks ja turbeks koostatakse tegevuskava. Tegevuste järjestamisel lähtutakse asitõendite volatiilsusest.

DER.2.2.M9 Analüüsitavate andmete õige valimine [vastutav spetsialist]

a. Õiguslike raamtingimuste alusel määratakse, millised sekundaarandmed (nt logiandmed või võrguliiklus) saavad olla asitõendid, mis viisil võib neid töödelda ja kui kaua säilitada.

DER.2.2.M10 Asitõendite IT-kriminalistikaturve [vastutav spetsialist]

a. Asitõendeid sisaldavad andmekandjad kloonitakse võimaluse korral tervikuna. Kui ekspertiistõmmist (ingl *forensic image*) teha ei saa, valitakse meetod, mille korral andmed muutuvad võimalikult vähe.

b. Andmete tervikluse tõendamiseks hoitakse originaal-andmekandjaid pitseerituna.

c. Krüptograafiliste kontrollkoodide kasutamisel originaalandmete või uurimiskoopiate tervikluse tagasiulatuvaks tõendamiseks tehakse kontrollkoodidest mitu koopiat. Koopiaid säilitatakse andmekandjast eraldi, dokumenteeritult ja turvaliselt.

d. Andmete kohtukõlblikkuse tagamiseks kinnitavad andmekandjatega tehtud toiminguid ja kontrollkoodide õigsust sõltumatud tunnistajad.

e. Asitõendite tagamiseks kriminalistikauuringu jaoks tohib kasutada üksnes sobiva väljaõppega personali (vt DER.2.2.M6 Personali koolitus *IT-kriminalistika alal*) või kriminalistikateenuse tarnijat (vt ka DER.2.2.M3 *Kriminalistikateenuse tarnija valimine).*

DER.2.2.M11 Asitõendite turbe dokumenteerimine [vastutav spetsialist]

a. Kriminalistikauuringu käigus dokumenteeritakse kõik läbiviidud sammud, kasutatud meetodid, kasutamise põhjused ja läbiviimise eest vastutajad.

b. Dokumentatsiooni abil on võimalik tagantjärele terviklikult tõendada, kuidas originaalasitõendeid hoiti ja kasutati.

DER.2.2.M12 Originaal-andmekandjate ja asitõendite turvaline säilitus [vastutav spetsialist]

a. Originaal-andmekandjaid hoiustatakse nii, et juurdepääs andmekandjatele on üksnes uurimisega tegelevail ja nimeliselt teadaolevail isikutel.

b. Originaal-andmekandjate ja asitõendite säilitamisele on määratud tähtaeg.

c. Tähtaja möödumisel hinnatakse andmekandjate ja asitõendite edasise säilitamise vajadust. Edasise säilitamise vajaduse puudumisel asitõendid hävitatakse või kustutatakse turvaliselt, originaal-andmekandjad tagastatakse omanikule.

3.4 Kõrgmeetmed

DER.2.2.M13 Raamlepingud kriminalistikateenuse tarnijatega (C-I-A)

a. Infoturvaintsidentide kriminalistikauuringu kiiremaks käivitamiseks on organisatsioon sõlminud kriminalistikateenuse tarnijatega kaasamislepped või raamlepingud.

DER.2.2.M14 Tüüpprotseduurid asitõendite turbeks (C-I-A)

a. Suure kaitsetarbega rakenduste, IT-süsteemide ja enamlevinud süsteemikonfiguratsioonide terviklikuks salvestamiseks on koostatud kriminalistikanõuetele vastavad tüüpprotseduurid. Ptotseduurid arvestavad nii volatiilseid kui vähemuutuvaid andmeid.

b. Väljatöötatud tüüpprotseduuride rakendamine on automatiseeritud ja eelnevalt testitud. Protseduure toetavad kontroll-loetelud ja tehnilised abivahendid.

DER.2.2.M15 Asitõendite turbe õppused (C-I-A)

- Kriminalistikauuringu ja analüüsiga seotud töötajad harjutavad regulaarselt infoturvaintsidendi asitõendite turbe rakendamist.

DER.2.3 Ulatuslike turvaintsidentide lahendamine

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed ulatuslike turvaintsidentide lahendamiseks.

Käesolevas moodulis käsitletakse ulatusliku turvaintsidendi näitena kinnisrünnet. Moodul kirjeldab, kuidas taastada kinnisründe ohu (ingl *Advanced Persistent Threat, APT*) realiseerumisel organisatsioonis IT-süsteemide tavaline ja turvaline tööseisund.

1.2 Vastutus

„Ulatuslike turvaintsidentide lahendamine“ meetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Infoturbejuht.

1.3 Piirangud

Moodul keskendub küberintsidentidele, moodulis ei käsitleta tegutsemist ulatuslike füüsiliste rünnete ega korruptsioonijuhtumite korral. Moodulis vaadeldakse kinnisründe intsidentide käsitlemist, üldine turvaintsidentide haldus on esitatud moodulites DER.1 *Turvaintsidentide avastamine* ja DER.2.1 *Turvaintsidentide käsitlus*.

Moodul ei hõlma kinnisründe sissetungijälgede avastamist turvarikkemärkide (ingl *indicator of compromise)* abil ega tagauste (ingl *backdoor)* tuvastamist.

2 Ohud

2.1 Lahendamise puudulikkus

Ründaja kasutab kinnisründe käigus kõiki vahendeid, et muuta juurdepääs IT-süsteemi püsivaks. Ründaja manipuleeritud riistvarakomponente ja püsivara on väga keeruline tuvastada. On oht, et intsidendi lahendamise käigus ei suudeta kõiki sisendpunkte (ingl *entry-point*) tuvastada ja kahjurvara täielikult IT-süsteemidest eemaldada. Selle tulemusel võib ründaja hiljem uuesti IT-süsteemidele ligi pääseda.

2.2 Jälgede hävitamine

Pärast kinnisründe intsidenti installitakse IT-süsteemid sageli uuesti või kõrvaldatakse kasutuselt. Kui eelnevalt ei tehta operatsioonisüsteemist või põhivarast ekspertiisikõlblikku koopiat, võivad hävida intsidendi edasise väljaselgitamise või kohtumenetluse tarbeks vajalikud asitõendid.

2.3 Ründaja enneaegne alarmeerimine

Enne kinnisründe intsidendi lahendamise aktiivseid tegevusi enamasti analüüsitakse rünnet, et tuvastada kasutatud pöördusteed, sisendpunktid ja kasutatud vahendid. Kui ründaja märkab selles järgus, et ta on avastatud, võib ta oma jäljed kõrvaldada või üritada kiiresti rünnata teisi IT-süsteeme. Samuti võib ründaja oma tegevuse ajutiselt peatada ja luua ründe tulevikus jätkamiseks tagauksi.

2.4 Andmete kaotus ja IT-süsteemi tõrge

Kinnisründe intsidendi lahendamisel üldjuhul installitakse IT-süsteemid uuesti ja isoleeritakse hetkel kasutatavad võrgusegmendid. IT-süsteemide seiskamine mõjutab teenuste käideldavust. Kui intsidendi lahendamine kestab kaua, võib see põhjustada märkimisväärseid kahjusid.

2.5 Võrguteabe muutmata jätmine pärast kinnisrünnet

Kinnisründe käigus omandab ründaja üksikasjalikud teadmised sihtmärgi keskkonna ülesehituse ja konfiguratsioonide kohta. Näiteks võib ta omada teadmisi olemasolevate võrgusegmentide, IT-süsteemide nimeskeemide, kasutaja- ja teenusekontode, kasutusele võetud tarkvara ja teenuste kohta. Nende teadmistega saab sama ründaja pärast intsidendi lahendamist sobiva võimaluse korral uuesti luua juurdepääsu sihtmärgi keskkonnale ja selle uuesti nakatada.

3 Meetmed

3.1 Elutsükkel

Kavandamine ja algatamine

DER.2.3.M1 Juhtrühma moodustamine

DER.2.3.M2 Lahendusstrateegia valimine

Soetus

DER.2.3.M8 Ründekäsitluse sidekanalite turve

Käitus

DER.2.3.M3 Mõjutatud võrguosade isoleerimine

DER.2.3.M5 Algse sissetungitee sulgemine

DER.2.3.M4 Pääsuandmete ja krüptovõtmete blokeerimine ja muutmine

DER.2.3.M6 Tööseisundi taastamine

DER.2.3.M9 Mõjutatud IT-süsteemide asendamine

Täiustamine

DER.2.3.M7 IT-süsteemi sihipärane tugevdamine

Lisanduvad kõrgmeetmed

DER.2.3.M10 Ümberkujundused sama ründaja uue ründe takistamiseks

3.2 Põhimeetmed

DER.2.3.M1 Juhtrühma moodustamine

a. Kinnisründe (ingl *Advanced Persistent Threat, APT*) intsidendi lahendamiseks on moodustatud juhtrühm, mis kavandab, koordineerib ja jälgib vajalikke tegevusi. Juhtrühmal on oma ülesannete täitmiseks volitused ja otsustusõigus.

b. Kui kinnisründe intsidendi analüüsimisel kasutatakse spetsialiseerunud kriminalistikateenuse tarnijat, kaasatakse selle eksperdid ka intsidendi lahendamisse.

c. Kui IT-süsteemid on olulisel määral rikutud või kui lahendusmeetmed on väga ulatuslikud, luuakse juhtrühma kõrvale ärijätkuvuse tagamise ja kommunikatsiooniga tegelev kriisistaap. Pärast kriisistaabi loomist on juhtrühma ülesandeks lahendamismeetmete rakendamine ja nende tulemuste teatamine kriisistaabile.

DER.2.3.M2 Lahendusstrateegia valimine

a. Kinnisründe intsidendi lahendamiseks koostab juhtrühm lahendusstrateegia, otsustades, kas:
   - kahjurvara saab turvarikkega IT-süsteemidest eemaldada;
   - mõjutatud IT-süsteemid installitakse uuesti;
   - mõjutatud IT-süsteemid tuleb asendada.

b. Vaatlusjärgus kogutakse ja uuritakse turvarikke märke ründajale märkamatult.

c. Lokaliseerimisjärgus lahutatakse kahjustatud süsteem või võrguosa muudest (vt DER.2.3.M3 *Mõjutatud võrguosade isoleerimine*) ja tehakse kriminalistikauuring otsustusteabe saamiseks.

d. Analüüsi tulemuste põhjal otsustatakse iga kahjustatud süsteemi taaste viis ja ajakava.

e. IT-süsteemide uuesti installimisel kontrollitakse, et värskelt tehtud varukoopiatelt ei taastata juba rikutud andmeid ega tarkvarakomponente.

f. Kui organisatsioon otsustab IT-süsteemid jätta uuesti installimata, käivitub spetsiaalne kinnisründe lahendamise protseduur.

g. Pärast kinnisründe intsidendi lahendamist seiratakse mõjutatud IT-süsteemide andmevahetust, et tuvastada ründajaga ühenduse võtmise katsed.

DER.2.3.M3 Mõjutatud võrguosade isoleerimine

a. Kriminalistikauuringu tulemustele toetudes määratakse intsidendist mõjutatud võrguosad.

b. Kinnisründe intsidendist mõjutatud võrguosad isoleeritakse. Kui mõjutatud võrguosi ei õnnestu täpselt kindlaks määrata, isoleeritakse ka kahtlased ja tõenäoliselt nakatunud võrguosad.

c. Ründaja takistamiseks isoleeritakse mõjutatud võrguosad üheaegselt.

d. Võrguosade isoleerimisel katkestatakse internetiühendused alamvõrkudest.

DER.2.3.M4 Pääsuandmete ja krüptovõtmete blokeerimine ja muutmine

a. Pärast kahjustatud süsteemi ja/või võrguosa eraldamist vahetatakse kõik pääsuandmed, sealhulgas hoolduskontode andmed ja keskselt (näiteks Active Directory või LDAP abil) hallatavad pääsuandmed.

b. Kui ründest on mõjutatud ja keskne autentimisserver (domeenikontroller või LDAP server), blokeeritakse sellest tehtavad pöördumised ja kõik paroolid muudetakse. Seda teevad kogenud süsteemiadministraatorid, vajadusel kriminalistikaspetsialistide kaasabil.

c. Kui kinnisrünne on rikkunud TLS-võtmeid või sisemist sertifitseerimiskeskust, blokeeritakse usaldatavalt vastavad võtmed ning luuakse võtmed ja nende taristu uuesti.

DER.2.3.M5 Algse sissetungitee sulgemine

a. Kui kriminalistikauuringu käigus tuvastati, et ründaja pääses organisatsiooni võrku tänu tehnilisele nõrkusele, kõrvaldatakse nõrkus pärast võrguosa eraldamist. Viirusetõrjet, autentimist, tulemüürireegleid, meili filtreerimist jms täiustatakse.

b. Tarkvaranõrkuse kõrvaldamiseks kasutatakse paikamist ja versiooniuuendusi. Nullpäevaeksploidi (ingl *zero-day exploit*) korral võetakse ühendust tarkvara valmistajaga ja lahenduse saamiseni rakendatakse nõrkuse korvamiseks ajutisi meetmeid.

c. Kui ründajal õnnestus IT-süsteeme rikkuda inimlikku eksimust ära kasutades, rakendatakse selliste intsidentide kordumise vältimiseks korralduslikke, tehnilisi ja personalimeetmeid. Ebaturvaline konfiguratsioon või parool asendatakse.

DER.2.3.M6 Tööseisundi taastamine

a. Pärast võrgu tulemuslikku puhastamist taastatakse IT-süsteemide korrakohane tööseisund. Välditakse andmevahetust juba taastatud ja taastamata süsteemide vahel. Taastatud süsteeme seiratakse võimaliku ründe tuvastamiseks.

b. Pärast jälgimisperioodi lõppu lõpetatakse ajutiste seire- ja analüüsivahendite kasutamine või võetakse need korralisse kasutusse.

c. Asitõendid ja kõrvaldatud IT-komponendid kas hävitatakse, kustutatakse turvaliselt või arhiveeritakse sobival viisil.

3.3 Standardmeetmed

DER.2.3.M7 IT-süsteemi sihipärane tugevdamine

a. Pärast kinnisrünnet tugevdatakse intsidendist mõjutatud IT-süsteeme, tuginedes kriminalistikauuringu tulemustele (vt DER.2.2. *IT-kriminalistika võimaldamine*). Peale seda kontrollitakse IT-süsteemide turvalisust uuesti.

b. IT-süsteemi tugevdamist alustatakse võimalikult ruttu, juba IT-süsteemi korrastamisel. Aeganõudvate meetmete rakendamine plaanitakse hilisema rakendamistähtajaga.

c. Tugevdamise plaani koostamise ja meetmete rakendamise eest vastutab infoturbejuht.

DER.2.3.M8 Ründekäsitluse sidekanalite turve

a. Juhtrühm ja lahendamisse kaasatud isikud kasutavad suhtlemiseks turvalisi sidekanaleid (nt mobiiltelefon, suhtlusäpp, isiklikud kohtumised), mille liiklust ei saa ründaja jälgida.

DER.2.3.M9 Mõjutatud IT-süsteemide asendamine

- Suure kaitsetarbega IT-süsteemide korral vahetatakse riistvara pärast kinnisründe intsidenti täielikult välja.
- Kui pärast kinnisründe intsidendi lahendamist tuvastatakse üksikutes IT-süsteemides endiselt kahtlast käitumist (nt põhjendamatut võrguliiklust), asendatakse mõjutatud IT-süsteem.

3.4 Kõrgmeetmed

DER.2.3.M10 Ümberkujundused sama ründaja uue ründe takistamiseks (C-I)

a. Sama ründaja tehtava kinnisründe takistamiseks kujundatakse ümber võrgukeskkonna sisemine ülesehitus, muutes ära:
   - võrgusegmentide IP-aadressivahemikud ja IT-süsteemide IP-aadressid;
   - IT-süsteemide nimed;
   - kasutaja- ja hoolduskontode nimeskeemid;
   - veebirakenduste ja veebiteenuste URL-teed.

b. Pärast võrgu ümberkujundust ajakohastatakse dokumentatsioon ja informeeritakse kasutajaid.

c. Luuakse mehhanismid kordusründe avastamiseks ning jälgitakse, kas endiste võrguandmete põhjal tehakse uusi pöördumisi. Sõltuvalt ründe üksikasjadest täiendatakse seiremehhanismi.

4 Lisateave

Lisa 1. Näiteid üksikkeskkondade tugevdusmeetmetest.

- **Võrgu segmentimine.** Kui ründaja sai paljudele IT-süsteemidele juurdepääsu tänu lihtsale võrguarhitektuurile, tuleks võrk täpselt määratud ja jälgitavate üleminekute abil jaotada väiksemateks segmentideks. See võimaldab ühe segmendi kaudu juurdepääsetavate (ja seega rünnatavate) IT-süsteemide arvu vähendada. Samuti võimaldavad väiksemate ja täpselt määratud segmentide vahelised üleminekud paremat jälgimist.
- **Haldussüsteemide eraldamine.** Eespool nimetatud segmentimise erimeetod on IT-haldussüsteemide eraldamine. Suurte privileegide ja ulatusliku juurdepääsu tõttu võrgukeskkonnale tuleks süsteemiadministraatorite kasutatavad haldussüsteemid tavavõrgust eraldada ja haldustegevusi ebanormaalsete tegevusmustrite suhtes kontrollida (nt sobiva jälgimiseabil). IT-süsteemidesse halduspääse (nt RDP või SSH kaudu) saab teha ainult tugevdatud ja seiratud hüppe- või terminaliserveri kaudu.
- **Teenusekontode piirang.** Teenusekontode tugevdamiseks kasutatakse minimaalselt vajalike privileegidega teenusekontosid, mida on üksnes vaja konkreetseks kasutusotstarbeks. Lisaks saab kasutada priviligeeritud kontode haldusvahendeid.
- **Väliste juurdepääsude täiendav turve.** Kui ründaja kasutas lubatud väliseid juurdepääse (nt töötajate VPN-pääsud), tuleb neid juurdepääse tugevdada. Sellised meetmed võivad olla multiautentimise kasutuselevõtt, suuremate andmemahtude edastuse seire või pöördusaegade piirang.

DER.3: Infoturbe hindamine

DER.3.1 Auditid ja läbivaatused

1 Kirjeldus

1.1 Eesmärk

Esitada üldised juhised infoturbe auditite ja läbivaatuste läbiviimiseks, eesmärgiga täiustada organisatsiooni infoturvet, vältida soovimatuid suundumusi valdkonnas ja optimeerida turvameetmeid ja -protsesse. Läbivaatuste puhul, erinevalt auditist, pole läbivaataja sõltumatus audititeemast nõutav, läbivaataja võib tegeleda ka tähelepanekute põhjal tehtud soovituste elluviimisega.

1.2 Vastutus

„Auditid ja läbivaatused“ meetmete täitmise eest vastutab infoturbejuht.

Lisavastutajad

Organisatsiooni juhtkond, auditirühm, infoturbe läbivaatuse rühm.

1.3 Piirangud

Moodulis toodud meetmed rakendatakse üldmeetmetena nii siseauditite kui väljasttellitud auditite puhul. Moodulis ei käsitleta, kuidas auditeid ja läbivaatusi lõimida organisatsiooni sisekontrollisüsteemi.

Moodulit ei rakendata sertifitseerimisauditite läbiviimisel. Nende ja seadusandlusest tulenevate kohustuslike auditite läbiviimist käsitletakse moodulis DER.3.2: *Infoturbe vastavusauditid*.

2 Ohud

2.1 Turvameetmete puudulik või plaanimata rakendamine

Organisatsiooni võimekus tegeleda infoturbe ohtudega langeb, kui turvameetmeid ei rakendata süsteemselt ja terviklikult. Samuti võib juhtuda, et pärast turvameetmete ajutist piiramist (nt arendusprojekti teatud järgus) unustatakse turvaline olukord taastada.

2.2 Turvameetmete toimetu või ebamajanduslik rakendamine

Turvameetmete osalisel rakendamisel või juhul, kui ei arvestata parimaid praktikaid, võivad kasutusele võetud meetmed osutuda mittetoimivaks (nt peaukse turvamine, kui sama ei tehta külguksega). Samuti võib kasutusel olla üksikuid meetmeid, mis on võimalikku riski kaaludes majanduslikult ebaotstarbekad.

2.3 Infoturbe halduse süsteemi puudulik rakendamine

Sageli unustatakse infoturbe halduse süsteemi toimimise hindamisse kaasata sõltumatu kolmas pool. Kui infoturbejuht ise vaatab turvameetmete rakendamist üle, ei pruugi tulemus olla objektiivne. Seetõttu ei pruugi infoturbe halduse süsteem tegelikkuses tulemuslikult toimida.

2.4 Kontrollija puudulik kvalifikatsioon

Kui kontrollijal puudub piisav kvalifikatsioon või kui ta on ebapiisavalt valmistunud, võib ta organisatsiooni infoturbe küpsustaset valesti hinnata. Seetõttu võivad aruandesse jõuda mittevajalikud või sobimatud parendusettepanekud. Tagajärjeks on ebamajanduslikud kulutused infoturbele või kaitsetarbe alahindamine, mistõttu olulised riskid jäävad vähendamata.

2.5 Keskpika perioodi plaanimise puudumine

Kui auditeid ei kavandata keskselt ja etteulatuvalt, võib juhtuda, et mõnda valdkonda kontrollitakse väga sageli, mõnda aga üldse mitte. Seetõttu on infoturbe tegelikku olukorda väga keeruline hinnata.

2.6 Puudulik auditi plaanimine ja kooskõlastamine

Kui auditiplaan ei ole organisatsiooni kõigi asjassepuutuvate töötajatega kooskõlastatud, võivad võtmeisikud auditiprotseduuride läbiviimise ajal puududa.

Kui audiitor on konkreetsete valdkondade kontrollimiseks määranud liiga tiheda ajakava, võivad kontrollid jääda liiga pealiskaudseks.

2.7 Isikuandmete kasutamise kooskõlastamatus

Auditi käigus võivad auditi läbiviijad saada juurdepääsu isikuandmetele või teha järeldusi üksikute töötajate töötulemuste kohta. Kui selleks ei ole andmekaitsespetsialisti ja/või personaliesindaja kooskõlastust, võib isikuandmete töötlemine kaasa tuua töötaja õiguste rikkumise.

2.8 Sihilik turvaprobleemide varjamine

Töötajad võivad turvaprobleeme varjata, sest kardavad, et auditi käigus avastatakse neid negatiivses valguses näitavaid vigu või tegematajätmisi. Seetõttu võib infoturbe hetkeseisust jääda ebatäpne ülevaade.

3 Meetmed

3.1 Elutsükkel

Kavandamine ja algatamine

DER.3.1.M1 Vastutaja määramine

DER.3.1.M6 Kontrollimisaluse ja ühtse hindamissüsteemi kehtestamine

DER.3.1.M7 Auditikava

DER.3.1.M8 Läbivaatuste objektide loend

DER.3.1.M5 Lõimimine infoturbeprotsessi

DER.3.1.M11 Teabevahetuse ja kontrollide läbiviimise kord

Käitus

DER.3.1.M2 Auditi ettevalmistamine

DER.3.1.M3 Auditi läbiviimine

DER.3.1.M4 Infoturbe läbivaatuse sooritamine

DER.3.1.M9 Sobiv auditi- või läbivaatuse meeskond

DER.3.1.M10 Auditiplaani või läbivaatuse plaani koostamine

DER.3.1.M12 Auditi avakoosolek

DER.3.1.M13 Dokumentide ülevaatus ja kontroll

DER.3.1.M14 Pistelised kontrollid

DER.3.1.M15 Sobivad kontrollimeetodid

DER.3.1.M16 Kohapealse kontrolli tegevuskava

DER.3.1.M17 Kohapealse kontrolli kord

DER.3.1.M18 Intervjuude läbiviimine

DER.3.1.M19 Riskikäsitlusplaani läbivaatus

DER.3.1.M20 Lõpukoosolek

DER.3.1.M21 Tulemuste hindamine

DER.3.1.M22 Auditi aruanne

DER.3.1.M23 Läbivaatuse tulemuste dokumenteerimine

DER.3.1.M24 Auditi või läbivaatuse lõpetamine

DER.3.1.M25 Järeltoimingud ja järelkontroll

DER.3.1.M26 Auditiplaani jälgimine ja kohandamine

DER.3.1.M27 Auditite ja läbivaatuste dokumentide säilitamine ja arhiveerimine

Lisanduvad kõrgmeetmed

DER.3.1.M28 Audiitorite taustakontroll

3.2 Põhimeetmed

DER.3.1.M1 Vastutaja määramine [organisatsiooni juhtkond]

a. Organisatsiooni juhtkond on määranud auditite plaanimise ja algatamise eest vastutaja. Seejuures jälgitakse, et ei tekiks huvide vastuolu (nt enda osakonna kontrollimine).

b. Vastutaja kontrollib, et auditi tulemusi käsitletakse vastavalt organisatsioonis kehtestatud kordadele.

DER.3.1.M2 Auditi ettevalmistamine

a. Auditi kavandamisel lepitakse kokku ja dokumenteeritakse auditi käsitlusala ja eesmärgid.

b. Enne auditi alustamist teavitatakse asjaomaseid töötajaid. Personali puudutavast auditist teavitatakse lisaks personaliesindajat.

DER.3.1.M3 Auditi läbiviimine [auditirühm]

a. Auditi käigus kontrollitakse auditi eesmärkidega seotud turvameetmete täitmist. Seonduvad nõuded on kontrollitavale organisatsioonile ja auditeeritavatele teada.

b. Audit sisaldab dokumentide ülevaatust, testimisi ja kohapealseid kontrolle.

c. Kohapealsete kontrollide käigus ei tohi audiitorid sekkuda iseseisvalt IT-süsteemide töösse ega anda otseseid tegevusjuhiseid kontrolliobjekti muutmiseks.

d. Auditi tulemused dokumenteeritakse ja vormistatakse kirjaliku auditiaruandena.

e. Auditiaruanne esitatakse määratud kontaktisikule kokkulepitud tähtajal.

DER.3.1.M4 Infoturbe läbivaatuse sooritamine [infoturbe läbivaatuse rühm]

a. Läbivaatuse käigus kontrollitakse, kas vaatlusalused meetmed on rakendatud terviklikult, sobivalt ja ajakohaselt.

b. Tuvastatud lahknevused kõrvaldatakse võimalusel viivitamatult.

c. Läbivaatuse tulemused dokumenteeritakse. Tulemuste muutmine on tuvastatav ja isikustatav.

3.3 Standardmeetmed

DER.3.1.M5 Lõimimine infoturbeprotsessi

a. Regulaarseid auditeid käsitletakse osana organisatsiooni infoturbe halduse süsteemist ja turbeprotsessist. Auditid algatatakse sellest lähtudes.

b. Auditite tulemusi kasutatakse infoturbe halduse süsteemi täiustamiseks.

c. Auditite tulemused ja puuduste kõrvaldamise ning kvaliteedi parandamisega seotud tegevused esitatakse infoturbejuhi regulaarses aruandes organisatsiooni juhtkonnale.

DER.3.1.M6 Kontrollimisaluse ja ühtse hindamissüsteemi kehtestamine

a. Auditite ja läbivaatuste läbiviimiseks on kehtestatud ühtsetel alustel põhinev kontrolliraamistik.

b. Meetmete rakendamise hindamiseks on kehtestatud ja dokumenteeritud ühtne hindamissüsteem.

DER.3.1.M7 Auditikava

a. Organisatsioon koostab mitmeaastast perioodi hõlmava auditite ja läbivaatuste kava.

b. Auditikavas sõnastatakse organisatsiooni ja infoturbe eesmärkidest tulenevad kontrollieesmärgid.

c. Ettenägematute sündmuste tarbeks jäetakse iga-aastases ressursside plaanimises reserv, et oleks vajadusel võimalik auditikava muuta.

d. Auditikava korrigeeritakse vastavalt muutuvatele riskihinnangutele.

DER.3.1.M8 Läbivaatuste objektide loend

a. Läbivaatuste kavandamiseks on koostatud loendid, milles dokumenteeritakse kontrolliobjektide hetkeseis ja plaanitud läbivaatused.

DER.3.1.M9 Sobiv auditi- või läbivaatusrühm [auditirühm, infoturbe läbivaatuse rühm]

a. Iga auditi või läbivaatuse jaoks luuakse sobivatest liikmetest koosnev rühm, mida juhib auditijuht või läbivaatuse juht, kes vastutab auditi või läbivaatuse läbiviimise eest.

b. Auditi- või läbivaatusrühm komplekteeritakse lähtudes kontrollivaldkonnast, arvestades kontrollivaldkonnas kehtestatud pädevusnõudeid, auditi või läbivaatuse mahtu ja kontrolliobjektide asukohti.

c. Auditi- või läbivaatusrühma liikmed on sobiva kvalifikatsiooniga ja auditeeritava suhtes neutraalsed ning sõltumatud.

d. Kui audiitori või läbivaatajana kasutatakse välist teenuseandjat, kontrollitakse eelnevalt tema sõltumatust ja rakendatakse konfidentsiaalsuskohustust.

e. Auditi- või läbivaatuse rühma jaoks tagatakse piisavad ressursid.

DER.3.1.M10 Auditiplaani või läbivaatuse plaani koostamine [auditirühm, infoturbe läbivaatuse rühm]

a. Enne auditi algust koostab auditijuht auditiplaani, mis võetakse auditi läbiviimise aluseks.

b. Enne läbivaatuse algust koostab juhtläbivaataja läbivaatuse plaani, mis võetakse läbivaatuse aluseks.

c. Auditiplaani või läbivaatuse plaani kohandatakse vastavalt vajadusele. Auditi korral on auditiplaan osa auditi lõpparuandest.

d. Väiksemaid läbivaatuseid kavandatakse läbivaatuste objektide loendi alusel.

DER.3.1.M11 Teabevahetuse ja kontrollide läbiviimise kord [auditirühm, infoturbe läbivaatuse rühm]

a. Auditirühma ning organisatsiooni või osakonna töötajate vaheliseks teabevahetuseks on kehtestatud kindel kord.

b. Auditi käigus edastatud teabe konfidentsiaalsuse ja tervikluse kaitseks rakendatakse sobivaid meetmeid.

c. Auditisse kaasatud isikud ei tohi auditiprotseduure mõjutada.

d. Auditisse kaasatud isikutele rakendub konfidentsiaalsuskohustus.

DER.3.1.M12 Auditi avakoosolek [auditirühm]

a. Auditirühma ja asjaomaste isikute osavõtul viiakse läbi avakoosolek, mille käigus selgitatakse auditi või läbivaatuse protseduure.

b. Avakoosoleku käigus kooskõlastatakse kohapealse kontrolli läbiviimise tingimused ja saadakse vastutajailt kinnitus auditiplaanile.

DER.3.1.M13 Dokumentide ülevaatus ja kontroll [auditirühm, infoturbe läbivaatuse rühm]

a. Dokumente vaadatakse üle vastavalt kontrolliraamistikus ettenähtud korrale.

b. Dokumentide ülevaatuse käigus kontrollitakse, kas dokumendid on ajakohased, terviklikud ja arusaadavad.

c. Dokumentide ülevaatuse tulemused dokumenteeritakse. Tulemusi arvestatakse kohapealsete kontrollide läbiviimisel.

DER.3.1.M14 Pistelised kontrollid [auditirühm, infoturbe läbivaatuse rühm]

a. Kohapealse kontrolli osana tehtavad pistelised kontrollid valitakse riskipõhiselt, valikud dokumenteeritakse ja põhjendatakse.

b. Kui pistelist kontrolli tehakse standardi sihtobjektide ja moodulipõhiste meetmete alusel, valitakse kontrollitavad sihtobjektid ja meetmed eelnevalt määratud protseduuri kohaselt.

c. Pisteliste kontrollide valimisel arvestatakse varasemate auditite ja läbivaatuste tulemusi.

DER.3.1.M15 Sobivad kontrollimeetodid [auditirühm, infoturbe läbivaatuse rühm]

a. Auditirühm või infoturbe läbivaatuse rühm kasutab auditi või läbivaatuse eesmärkidele vastavaid kontrollimeetodeid, näiteks intervjueerimist (vt DER.3.1.M18 *Intervjuude läbiviimine*) või dokumentide ülevaatust (vt DER.3.1.M13 *Dokumentide ülevaatus ja kontroll*).

b. Läbiviidavad kontrolliprotseduurid on tõhusad ja eesmärgipärased.

DER.3.1.M16 Kohapealse kontrolli tegevuskava [auditirühm]

a. Auditirühm koos auditeeritava kontaktisikutega töötab välja kohapealse kontrolli tegevuskava.

b. Kohapealse kontrolli tegevuskava dokumenteeritakse auditiplaanis.

DER.3.1.M17 Kohapealse kontrolli kord [auditirühm, infoturbe läbivaatuse rühm]

a. Kohapealset kontrolli alustades korraldatakse koos organisatsiooni vastutavate isikutega avakoosolek.

b. Auditiplaanis ettenähtud nõudeid kontrollitakse kehtestatud kontrollimeetodite kohaselt.

c. Kui valitud pistelise kontrolli objekt erineb selle dokumenteeritud seisust, laiendatakse kontrollimist, kuni erinevuse asjaolud on välja selgitatud.

d. Pärast auditiprotseduuride läbiviimist korraldab auditirühm lõpukoosoleku, mille käigus esitletakse lühidalt ja koondhinnangut andmata tulemusi ja edasisi tegevusi. Kohapealse kontrolli lõpukoosolek protokollitakse.

DER.3.1.M18 Intervjuude läbiviimine [auditirühm]

a. Läbiviidavad intervjuud on sobivalt struktureeritud. Esitatavad küsimused on lühidalt, täpselt ja arusaadavalt sõnastatud.

b. Intervjuu läbiviimisel rakendatakse kontrolli eesmärkidele vastavat ja sihtrühmale sobivat küsitlusmetoodikat.

DER.3.1.M19 Riskikäsitlusplaani läbivaatus [auditirühm]

a. Auditirühm hindab, kas jääkriskid on adekvaatsed ja juhtkonna poolt aktsepteeritud. Infoturbe tagamiseks oluliste põhimeetmete mitterakendamist ei aktsepteerita.

b. Audiitor kontrollib pisteliselt, kas ja millises ulatuses on riskikäsitlusplaanis ettenähtud meetmed rakendatud.

DER.3.1.M20 Lõpukoosolek [auditirühm]

a. Auditi lõpetamisel korraldab auditirühm koos auditeeritava organisatsiooni asjaomaste vastutajatega lõpukoosoleku.

b. Lõpukoosolekul esitletakse esialgseid auditितulemusi ja tutvustatakse edasisi tegevusi.

DER.3.1.M21 Tulemuste hindamine [auditirühm]

a. Pärast auditiprotseduuride läbiviimist koondab ja analüüsib auditirühm kogutud andmeid.

b. Vajadusel küsitakse auditeeritavalt täiendavat tõendusmaterjali. Tõendusmaterjali kogumiseks antakse auditeeritavale piisavalt aega. Dokumendid, mida ei ole kokkulepitud tähtajaks esitatud, loetakse puuduvateks.

c. Auditirühm annab auditeeritud meetmete rakendamisele lõplik hinnangu pärast täiendava tõendusmaterjali analüüsi.

DER.3.1.M22 Auditi aruanne [auditirühm]

a. Auditirühm dokumenteerib auditi tulemused arusaadavalt ja põhjalikult ning esitab need auditi aruandena. Auditirühm on valmis vajadusel auditितulemusi selgitama.

b. Auditeeritav organisatsioon tagab, et asjassepuutuvad isikud saaksid neile olulised auditi aruande väljavõtted kätte mõistliku aja jooksul.

DER.3.1.M23 Läbivaatuse tulemuste dokumenteerimine [infoturbe läbivaatuse rühm]

a. Läbivaatuse tulemused dokumenteeritakse ühtsel, eelnevalt kokkulepitud kujul.

DER.3.1.M24 Auditi või läbivaatuse lõpetamine [auditirühm, infoturbe läbivaatuse rühm]

a. Pärast auditit või läbivaatust tagastatakse või hävitatakse auditeeritud organisatsiooniga kooskõlastatult audiitorile antud asjassepuutuvad dokumendid, andmekandjad või muu materjal, mille kohta ei kehti kohaldatavad õigusaktide või muudest siduvate dokumentide säilitusnõuded.

b. Infoturbejuht korraldab kõigi auditi- või läbivaatusrühma liikmetele ajutiselt loodud pääsuõiguste desaktiveerimise või tühistamise.

c. Audiitorite ja tulemuste läbivaatajatega lepitakse kokku tulemuste avaldamise õigused ja piirangud, kaasaarvatud selle, et auditितulemusi ei edastataks ilma kontrollitud organisatsiooni nõusolekuta muudele organisatsioonidele.

DER.3.1.M25 Järeltoimingud ja järelkontroll

a. Auditi aruandes esitatud või läbivaatuse käigus tuvastatud puudused kõrvaldatakse mõistliku aja jooksul.

b. Parandusmeetmete plaanitavad rakendamisajad ja vastutajad dokumenteeritakse.

c. Rakendatud parandusmeetmed dokumenteeritakse vastavalt infoturbe halduse süsteemiga kehtestatud korrale.

d. Märkimisväärsete puuduste esinedes teeb auditi- või läbivaatusrühm parandusmeetmete rakendamise järelauditi või järelkontrolli.

DER.3.1.M26 Auditikava jälgimine ja kohandamine

a. Auditi tähtaegade, eesmärkide, sisu ja kvaliteedi tagamise eesmärgil on võimalik auditikava jooksvalt kohandada.

b. Auditikava muutmisel arvestatakse läbiviidud auditite käsitlusala ja tulemusi.

DER.3.1.M27 Auditite ja läbivaatuste dokumentide säilitamine ja arhiveerimine

a. Auditikava, auditiplaane ning auditite ja läbivaatuste dokumente säilitatakse vastavalt õigusaktide või sise-eeskirjade nõuetele.

b. Dokumente säilitatakse turvaliselt. Dokumendid peavad olema säilitusaja jooksul kaitstud muudatuste ja lubamatu juurdepääsu eest.

c. Tagatakse, et auditite aruannetele omavad juurdepääsu üksnes pääsuõigusega isikud.

d. Pärast arhiveerimistähtaja möödumist hävitatakse asjakohased dokumendid turvaliselt.

3.4 Kõrgmeetmed

DER.3.1.M28 Audiitorite taustakontroll (C-I)

a. Kui auditi käigus võivad audiitorid saada ligipääsu väga tundlikule teabele, hangitakse eelnevalt tõendid audiitorite aususe ja maine kohta.

b. Kui on vajalik audiitorite juurdepääs riigisaladuseks liigitatud teabele, saavad nad selleks õiguse riigisaladust käsitlevate õigusaktidega määratud korras.

4 Lisateave

Lühend	Publikatsioon
[ISO 19011]	EVS-EN ISO 19011:2018, “Juhtimissüsteemi auditeerimise juhised“
[ISO 27007]	ISO ISO/IEC 27007:2020, “Guidelines for information security management systems auditing“
[ISACA]	ISACA, ITAF: A Professional Practices Framework for IS Audit/Assurance, 3rd Edition, 2014

DER.3.2 Infoturbe vastavusauditid

1 Kirjeldus

1.1 Eesmärk

Esitada juhised auditeeritavale organisatsioonile infoturbe vastavusauditite korraldamiseks. Infoturbe vastavusauditi eesmärk on tagada vastavus õigusaktidega ja organisatsioonisisese infoturvapoliitikaga, täiustada organisatsiooni infoturvet ja optimeerida turvameetmeid ning turbeprotsesse.

1.2 Vastutus

„Infoturbe vastavusauditid“ meetmete järgimise eest vastutab infoturbejuht.

Lisavastutajad

Organisatsiooni juhtkond, auditirühm.

1.3 Piirangud

Moodulis on arvestatud Eesti infoturbestandardil (E-ITS) põhineva vastavusauditi läbiviimise nõudeid, mistõttu ei pruugi kõik alammeetmed olla relevantsed muude vastavusauditite puhul.

Moodul ei ole piisav sõltumatute sertifitseerimisauditite (nt ISO27001 sertifitseerimisauditi) läbiviimiseks.

2 Ohud

2.1 Väliste turbesuuniste rikkumine

Infoturbe halduse süsteemi vastavusnõuded võivad lisaks infoturbe standardile tulla ka valdkondlikust regulatsioonist. Infoturbe regulaarset kontrollimist infoturbe vastavusauditiga võivad nõuda järelevalveasutused ja organisatsiooni partnerid. Auditi tegemata jätmine võib organisatsioonile kaasa tuua mainekao, lepingute katkestamise või rahalisi sanktsioone.

2.2 Turvameetmete puudulik või plaanimata rakendamine

Organisatsiooni võimekus tegeleda infoturbe ohtudega langeb, kui turvameetmeid ei rakendata süsteemselt ja terviklikult. Samuti võib juhtuda, et pärast turvameetmete ajutist piiramist (nt arendusprojekti teatud järgus) unustatakse turvaline olukord taastada.

2.3 Turvameetmete toimetu või ebamajanduslik rakendamine

Turvameetmete osalisel rakendamisel või juhul, kui ei arvestata parimaid praktikaid, võivad rakendatud meetmed osutuda mittetoimivaks (nt peaukse turvamine, kui sama ei tehta külguksega). Samuti võib kasutusel olla üksikuid meetmeid, mis on võimalikku riski kaaludes majanduslikult ebaotstarbekad.

2.4 Infoturbe halduse süsteemi puudulik rakendamine

Sageli unustatakse infoturbe halduse süsteemi toimimise hindamisse kaasata sõltumatu kolmas pool. Kui infoturbejuht ise vaatab turvameetmete rakendamist üle, ei pruugi tulemus olla objektiivne. Seetõttu ei pruugi infoturbe halduse süsteem tegelikkuses tulemuslikult toimida.

2.5 Audiitori puudulik kvalifikatsioon

Kui audiitoril puudub piisav kvalifikatsioon või kui ta on ebapiisavalt valmistunud, võib ta organisatsiooni infoturbe küpsustaset valesti hinnata. Seetõttu võivad aruandesse jõuda mittevajalikud või sobimatud parendusettepanekud. Tagajärjeks on ebamajanduslikud kulutused infoturbele või kaitsetarbe alahindamine, mistõttu olulised riskid jäävad vähendamata.

2.6 Huvide konflikt organisatsioonisiseses auditirühmas

Kui organisatsioon on moodustanud auditirühma oma töötajatest, ei pruugi audiitorid olla täielikult sõltumatud. Kui auditirühma liikmed puutuvad auditeeritavate protsessidega sageli kokku oma igapäevatöös, ei ole auditi tulemus erapooletu.

2.7 Keskpika perioodi plaanimise puudumine

Kui auditeid ei kavandata keskselt ja etteulatuvalt, võib juhtuda, et mõnda valdkonda kontrollitakse väga sageli, mõnda aga üldse mitte. Seetõttu on infoturbe tegelikku olukorda väga keeruline hinnata.

2.8 Puudulik auditi plaanimine ja kooskõlastamine

Kui auditiplaan ei ole organisatsiooni kõigi asjassepuutuvate töötajatega kooskõlastatud, võivad võtmeisikud auditiprotseduuride läbiviimise ajal puududa.

Kui audiitor on konkreetsete valdkondade kontrollimiseks määranud liiga tiheda ajakava, võivad kontrollid jääda liiga pealiskaudseks.

2.9 Personaliesindusega kooskõlastamatus

Auditi käigus võivad auditi läbiviijad saada juurdepääsu isikuandmetele või teha järeldusi üksikute töötajate töötulemuste kohta. Kui selleks ei ole personaliesindaja kooskõlastust, võib see kaasa tuua töötaja õiguste rikkumise.

2.10 Sihilik lahknevuste ja probleemide varjamine

Töötajad võivad turvaprobleeme varjata, sest kardavad, et auditi käigus avastatakse neid negatiivses valguses näitavaid vigu või tegematajätmisi. Seetõttu võib infoturbe hetkeseisust jääda ebatäpne ülevaade.

2.11 Kaitset vajava teabe leke

Infoturbe auditi käigus saavad audiitorid ligipääsu konfidentsiaalsele teabele, samuti teabele nõrkuste ja ründevõimaluste kohta. Kui need asjaolud saavad volitamata isikutele teatavaks, võidakse teavet kasutada organisatsiooni ründamiseks või laimamiseks.

3 Meetmed

3.1 Elutsükkel

Kavandamine

DER.3.2.M1 Infoturbe auditite vastutaja määramine

DER.3.2.M2 Auditite läbiviimise juhend

DER.3.2.M3 Kontrollimisaluse määramine

DER.3.2.M4 Infoturbe vastavusauditite kavandamine

DER.3.2.M9 Lõimimine infoturbeprotsessi

DER.3.2.M10 Teabevahetus

Käitus

DER.3.2.M6 Infoturbe auditi ettevalmistamine

DER.3.2.M8 Infoturbe auditite aruannete säilitamine

DER.3.2.M22 Infoturbe auditi järeltegevused

3.2 Põhimeetmed

DER.3.2.M1 Infoturbe auditite vastutaja määramine [organisatsiooni juhtkond]

a. Organisatsioon on määranud infoturbe auditite eest vastutaja, kes auditeid kavandab, algatab ning nende tulemusi käsitleb.

DER.3.2.M2 Auditite läbiviimise juhend

a. Organisatsioonis on koostatud ja juhtkonnas kinnitatud auditite läbiviimise juhend, milles esitatakse auditi eesmärgid, vastavusnõuded ning teave auditi tellimise, korralduse ja ressursside kohta.

b. Auditite läbiviimise juhendis on esitatud auditi dokumentatsiooni ja auditi tulemuste esitamise ja säilitamise nõuded.

DER.3.2.M3 Kontrollimisaluse määramine

a. Kui seadusandlusest ei tulene teisiti, võetakse infoturbe vastavusauditi kontrollimisaluseks kehtiv infoturbe standard ja selle osaks olev infoturbe meetmete kataloog.

b. Kontrollimisalusena kasutatakse meetmete kataloogi põhi-ja standardmeetmeid. Kui organisatsioon rakendab kaitsetarbest tulenevalt kõrgmeetmeid, auditeeritakse ka kõrgmeetmete rakendamist.

c. Kõiki asjaosalisi on eelnevalt kontrollimise alusest teavitatud.

DER.3.2.M4 Infoturbe vastavusauditite kavandamine

a. Kogu käsitlusala ja kõiki rakendamisele kuuluvaid meetmeid hõlmav audit viiakse läbi perioodiliselt.

b. Pärast oluliste muudatuste toimumist infoturbe kaitsealas või IT-süsteemides viiakse muudatustest mõjutatud osas läbi täiendav vaheaudit.

c. Auditirühma juht koostab kogu audititsüklit hõlmava auditikava, mille põhjal täpsustatakse ja kinnitatakse igal aastal infoturbe auditite aastaplaan.

DER.3.2.M6 Infoturbe auditi ettevalmistamine [auditirühm]

a. Infoturbe auditi algatab organisatsiooni juhtkond.

b. Organisatsioon edastab auditirühmale infoturbe kontseptsiooni, infoturvapoliitika, auditi objektiga seonduvad poliitikad ning muud auditirühma nõutud dokumendid.

DER.3.2.M8 Auditiaruannete säilitamine

a. Kui säilitustähtaja pikkus ei tulene muudest õigusaktidest või eeskirjadest, säilitatakse infoturbe auditi aruannet ja alusdokumente turvaliselt vähemalt üheksa aastat.

b. Infoturbe auditi aruanded ja seonduvad alusdokumendid on kaitstud muudatuste eest. Juurdepääs neile on lubatud üksnes vastava pääsuõigusega isikutel.

3.3 Standardmeetmed

DER.3.2.M9 Infoturbe vastavusauditite lõimimine infoturbeprotsessi

a. Perioodilised infoturbe vastavusauditid on osa organisatsiooni infoturbe kontseptsioonist.

b. Infoturbe vastavusauditite tulemusi kasutatakse infoturbe halduse süsteemi täiustamiseks.

c. Auditite tulemused ja puuduste kõrvaldamise ning kvaliteedi parandamisega seotud tegevused esitatakse infoturbejuhi regulaarses aruandes organisatsiooni juhtkonnale.

DER.3.2.M10 Teabevahetus

a. Auditirühma ja organisatsiooni vahelise teabevahetuse lubatavad viisid määratakse auditite läbiviimise juhendis (vt DER.3.2.M2 *Auditite läbiviimise juhend*).

b. Osapooled tagavad auditi teabevahetuse konfidentsiaalsuse ja tervikluse.

DER.3.2.M22 Infoturbe auditi järeltegevused

a. Infoturbe auditi aruandes esitatud lahknevused kõrvaldatakse mõistliku ajaga.

b. Parandusmeetmete kasutuselevõtu vastutajad, tähtajad rakendamise hetkeseis dokumenteeritakse.

c. Parandusmeetmete rakendamist jälgitakse pidevalt, vajadusel uuendatakse rakendamise seisu.

d. Parandusmeetmete rakendamise põhjal otsustatakse täiendava infoturbe järelauditi vajadus, sellisel juhul kohandatakse auditikava.

3.4 Kõrgmeetmed

Antud moodulis kõrgmeetmed puuduvad.

4 Lisateave

Lühend	Publikatsioon
[EISAÜ]	Eesti Infosüsteemide Audiitorite Ühing, Infosüsteemide audiitorkontrolli eeskirjad, 1997, https://eisay.ee/infosusteemide-audiitorkontrolli-eeskirjad
[EISAÜ]	ISACA kutse-eetika koodeks, https://eisay.ee/kutse-eetikakoodeks
[ISACA]	ISACA, ITAF: A Professional Practices Framework for IS Audit/Assurance, 3rd Edition, 2014

DER.4 Avariihaldus

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed infoturbe ja jätkuvuse halduse tagamiseks avariiolukordades.

1.2 Vastutus

Avariihalduse meetmete täitmise eest vastutab avariiülem.

Lisavastutajad

Infoturbejuht, organisatsiooni juhtkond, personaliosakond, ülemus.

1.3 Piirangud

Selles moodulis ei esitata avariihalduse käivitamise kriteeriume, asjakohane otsus tehakse turvaintsidendi käsitluse ajal (vt DER.2.1 *Turvaintsidentide käsitlus).*

Kriise käsitletakse eraldi kriisihalduse raames, millel on antud mooduliga üksnes kokkupuutekohad (nt avariiolukordade edasise laiendamise raames).

2 Ohud

2.1 Personali väljalangemine

Personali väljalangemine laiemalt (nt epideemia või streigi tõttu) või oluliste võtmeisikute lahkumine võib organisatsioone äriprotsesse tugevalt häirida. Äriprotsesside käitamiseks või IT-süsteemide taastamiseks vajalik teave ei pruugi olla kättesaadav.

2.2 IT-süsteemi tõrge

IT-süsteemi osise (nt riistvarakomponendi) tõrkest põhjustatud IT-süsteemi katkestus mõjutab negatiivselt IT-süsteemist sõltuvate äriprotsesside toimimist.

2.3 Laivõrgu (WAN) tõrge

Laivõrgu (ingl *Wide Area Network*, WAN) tõrked mõjutavad äriprotsesse, mille jaoks on vaja pidevat internetiühendust. Pikemaajalised laivõrgu katkestused võivad kaasa tuua suuri side- ja kättesaadavusprobleeme terves piirkonnas.

2.4 Hoone avarii

Erakordsete ning ettenägematute asjaolude (nt tulekahju, torm, üleujutus, plahvatus) tagajärjel võivad hooned osaliselt või täielikult hävida. Hoonega seotud avarii korral ei saa hoonesse enam siseneda, mistõttu on äriprotsessi toimimine häiritud.

2.5 Tarnija või teenuseandja teenuse katkemine

Äriprotsessi sõltumisel ühest või mitmest teenuseandjast võib osaline või täielik tarnija või teenuseandja teenuse peatamine avaldada organisatsiooni jätkusuutlikkusele märkimisväärset mõju.

3 Meetmed

3.1 Elutsükkel

Kavandamine ja algatamine

DER.4.M1 Avariiteatmik

DER.4.M2 Avariihalduse lõimimine üleorganisatsioonilistesse protsessidesse

Lisanduvad kõrgmeetmed

DER.4.M3 Avariihalduse käsitlusala ja strateegia

DER.4.M4 Avariihalduse poliitika ja juhtkonna vastutus

DER.4.M5 Avariihalduse korraldus

DER.4.M6 Vajalike ressursside olemasolu

DER.4.M7 Avariikontseptsioon

DER.4.M8 Töötajate kaasamine avariihalduse protsessi

DER.4.M9 Avariihalduse lõimimine üleorganisatsioonilistesse protsessidesse

DER.4.M10 Testid ja avariiõppused

DER.4.M12 Avariihalduse protsessi dokumenteerimine

DER.4.M13 Avariihalduse süsteemi läbivaatus ja juhtimine

DER.4.M14 Avariimeetmete regulaarne läbivaatus ja täiustamine

DER.4.M15 Avariihalduse süsteemi toimivuse hindamine

DER.4.M16 Väljasttellitavate komponentide avariivalmendus

3.1 Põhimeetmed

Selles moodulis põhimeetmed puuduvad.

3.2 Standardmeetmed

DER.4.M1 Avariiteatmik

a. Organisatsioon on koostanud avarii korral tegutsemise juhiseid sisaldava avariiteatmiku, milles on esitatud vähemalt:
   - kaasatud rollid, töötajate õigused ja kohustused;
   - kiirjuhised töötajatele;
   - alarmeerimine ja käsitluse laiendamine;
   - teabevahetuse, jätkusuutlikkuse tagamise ja taaskäivituse korrad;
   - IT-süsteemide taasteplaanid.

b. Avariiolukorras tagatakse asjakohase väljaõppega personali kättesaadavus. Vastutused kirjeldatakse ja neid rakendatakse avariiteatmiku alusel.

c. Regulaarselt läbiviidavate testimiste ja õppuste käigus kontrollitakse, kas avariiteatmikus esitatud meetmed toimivad ettenähtud viisil.

d. Avariiteatmikku ajakohastatakse regulaarselt ja vajaduse korral täiendatakse tüüpavariide (nt tulekahju) tegutsemisjuhistega, muudatused avariiteatmikus tehakse avariihaldusesse kaasatud töötajaile teatavaks.

e. Avariiteatmik on avariihaldusesse kaasatud töötajatele avariiolukorras kättesaadav.

DER.4.M2 Avariihalduse lõimimine üleorganisatsioonilistesse protsessidesse [infoturbejuht]

a. Avariihaldus on kooskõlas turbehalduse (vt ISMS.1 *Turbehaldus*) ja intsidendihalduse (vt DER.2.1 *Turvaintsidentide käsitlus*) protsessidega.

3.3 Kõrgmeetmed

DER.4.M3 Avariihalduse käsitlusala ja strateegia [organisatsiooni juhtkond] (C-I-A)

a. Avariihalduse käsitlusala ja strateegia kehtestatakse organisatsiooni juhtkonnas vastavalt organisatsiooni eesmärkidele ja jääkriskide tasemele.

DER.4.M4 Avariihalduse poliitika ja juhtkonna vastutus [organisatsiooni juhtkond] (C-I-A)

a. Organisatsiooni juhtkond on kinnitanud avariihalduse poliitika.

b. Avariihalduse poliitikat kontrollitakse regulaarselt, vajadusel uuendatakse poliitikat.

c. Avariihalduse poliitika on kõigile töötajatele teatavaks tehtud.

DER.4.M5 Avariihalduse korraldus [organisatsiooni juhtkond] (C-I-A)

a. Avariihalduseks on määratud organisatsiooni tingimustele sobivad rollid.

b. Rollide ülesanded, õigused ja kohustused dokumenteeritakse avariiteatmikus (vt DER.4.M1 *Avariiteatmik*).

c. Rolle täitma on määratud piisava kvalifikatsiooniga töötajad.

d. Avariihalduse korralduse praktilisust, toimivust ja tõhusust kontrollitakse regulaarselt.

DER.4.M6 Vajalike ressursside olemasolu [organisatsiooni juhtkond] (C-I-A)

a. Avariihalduse eesmärkide saavutamiseks on eraldatud piisavad rahalised, tehnilised ja inimressursid.

b. Avariihalduril ja avariihalduse rühmal on piisavalt aega avariihaldusega seotud ülesannete täitmiseks.

DER.4.M7 Avariikontseptsioon [organisatsiooni juhtkond] (C-I-A)

a. On määratud kriitilised äriprotsessid ja nendega seotud varad (nt äritoime analüüsi abil).

b. On tuvastatud kriitiliste äriprotsesside ja varadega seotud olulised riskid.

c. Iga riski korral otsustatakse, millist strateegiat riskikäsitluses rakendatakse.

d. Avariikontseptsiooni osana on valitud meetmed ja koostatud tegevuskavad kriitiliste äriprotsesside taaskäivituseks ja taasteks. Taastamine peab olema võimalik kokkulepitud aja piires.

e. Avariikontseptsioonis on esitatud avariiolukorras tegutsemisel kasutatavad turvameetmed.

DER.4.M8 Töötajate kaasamine avariihalduse protsessi [ülemus, personaliosakond] (C-I-A)

a. Töötajate regulaarseks teavitamiseks on koostatud rollipõhine avariihalduse teadvustus- ja koolituskava.

b. Avariihalduse rühma kuuluvaid töötajaid koolitatakse regulaarselt.

DER.4.M9 Avariihalduse lõimimine üleorganisatsioonilistesse protsessidesse [organisatsiooni juhtkond] (C-I-A)

a. Avariihalduse aspekti arvestatakse organisatsiooni kõigis äriprotsessides.

b. Avariihalduse protsessid, nõuded ja vastutusalad on kooskõlastatud riski- ja kriisihaldusega.

DER.4.M10 Testid ja avariiõppused [organisatsiooni juhtkond] (C-I-A)

a. On koostatud õppuste plaan, mille kohaselt regulaarselt ja juhtumipõhiselt testitakse ja harjutatakse olulisemaid avariihalduse tegevuskavasid ja meetmeid.

b. Testide ja õppuste väljatöötamiseks, plaanimiseks ja läbiviimiseks eraldatakse piisavalt ressursse.

DER.4.M12 Avariihalduse protsessi dokumenteerimine (C-I-A)

a. Avariihalduse toimingud, vahetulemused ja olulised otsused dokumenteeritakse.

b. On kehtestatud avariihalduse dokumentide regulaarse ajakohastamise protseduur.

c. Juurdepääs dokumentatsioonile võimaldatakse ainult volitatud isikutele.

DER.4.M13 Avariihalduse süsteemi läbivaatus ja juhtimine [organisatsiooni juhtkond] (C-I-A)

a. Avariihalduse aruanded esitatakse regulaarselt juhtkonnale.

b. Juhtkond kontrollib, hindab ja korrigeerib avariihalduse toimimist.

DER.4.M14 Avariimeetmete regulaarne läbivaatus ja täiustamine [organisatsiooni juhtkond] (C-I-A)

a. Juhtkond koordineerib IT, infoturbe ja avariihalduse läbivaatusi ning määrab avariimeetmete kontrollijad ja kontrollimise ajad.

b. Avariimeetmeid vaadatakse läbi regulaarselt või suuremate muudatuste korral. Kontrollitakse, kas meetmed on endiselt sobivad määratud eesmärkide saavutamiseks.

c. Kontrollitakse tehniliste meetmete rakendamise ja IT-süsteemide konfiguratsiooni õigsust ning korralduslike meetmete toimivust ja tõhusust.

d. Läbivaatuse käigus tuvastatud probleemide põhjused selgitatakse välja ning kavandatakse sobivad parandusmeetmed.

e. Parandusmeetmete rakendamise tulemusaruande kinnitab juhtkond. Viivitustest meetmete rakendamisel teatatakse juhtkonnale aegsasti.

DER.4.M15 Avariihalduse süsteemi toimivuse hindamine [organisatsiooni juhtkond] (C-I-A)

a. Avariihalduse süsteemi toimivust ja tõhusust hinnatakse regulaarselt vastavalt määratud mõõtmis- ja hindamiskriteeriumitele, tulemust võrreldakse eelmiste hindamiste tulemustega.

b. Hindamistulemustest teavitatakse juhtkonda, kes otsustab avariihalduse täiustamise. Juhtkonna otsused dokumenteeritakse.

DER.4.M16 Väljasttellitavate komponentide avariivalmendus [organisatsiooni juhtkond] (C-I-A)

b. Avariitestid ja -õppused kooskõlastatakse tarnija või teenuseandjaga, vajaduse korral korraldatakse ühisõppusi.
c. Teavet testitulemuste, kontrollide ja täiustusmeetmete kohta vahetatakse tarnija või teenuseandjaga regulaarselt.

APP: Rakendused

APP.1: Klientrakendused

APP.1.1 Kontoritarkvara

1 Kirjeldus

1.1 Eesmärk

Esitada kontoritarkvaras töödeldavate andmete kaitse ja kontoritarkvara turvalise halduse meetmed. Kontoritarkvara hulka kuuluvad dokumentide koostamise, töötlemise ja andmeanalüüsi jaoks ettenähtud rakendused.

1.2 Vastutus

Kontoritarkvara turvameetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Kasutaja.

1.3 Piirangud

Kontoritarkvara valimise ja kasutuselevõtu juures järgitakse täiendavalt APP.6 *Tarkvara üldiselt* meetmeid.

E-posti rakenduse meetmed on esitatud moodulis APP.5.3 E-posti server ja klient üldiselt.

Pilvepõhise kontoritarkvara puhul järgitakse moodulis OPS.2.2 *Pilvteenuste kasutamine* esitatud meetmeid.

Kontoritarkvarasse integreeritud andmebaasisüsteemide (nt *LibreOffice Base* ja *Microsoft Access*) kasutamisel rakendatakse lisaks meetmeid moodulist APP.4.3 A*ndmebaasisüsteemid.*

2 Ohud

2.1 Organisatsiooni vajadustega mittearvestamine

Kontoritarkvara hankimisel või kohandamisel ärinõuetega mittearvestamine võib kaasa tuua sooritusvõime kaotuse, tõrked ja vead äriprotsessides. Põhjusteks võivad olla olemasolevate dokumendimallide ja dokumentidega mitteühildumine, uue kontoritarkvara puudulik funktsionaalsus või koostalitlusvõime puudumine äripartnerite rakendustega.

2.2 Dokumendi manipuleerimine

Dokumentide automatiseerimise aktiivsisu (nt makrod või *ActiveX* komponendid) võib sisaldada kahjurkoodi, mis dokumendi avamise korral aktiveeritakse. Kahjurkood võib peale konkreetse dokumendi manipuleerimise levida ka teistesse dokumentidesse ning häirida seeläbi organisatsiooni äriprotsesse. Manipuleerimise tuvastamata jätmine on oluline turvanõrkus.

2.3 Dokumendi tervikluse kadu

Kontoritarkvara andmetes tehtud muudatusi üldjuhul ei logita. Kasutaja eksimuse või toote nõrkuse ärakasutamise tõttu on võimalik dokumendi sisu tahtlikult või tahtmatult muuta. Kui muudetud dokumente ei tuvastata ja nendega töötatakse edasi, on oht teha vääraid äriotsuseid või tekitada organisatsioonile mainekahju.

2.4 Dokumendi puudulik tõendatavus

Kui dokumendi koostaja, läbivaataja või kinnitaja isikut ei ole võimalik usaldusväärselt tõendada või kui vastavat kontoritarkvara funktsiooni on võimalik manipuleerida, on võimalik dokumendi autentsust rikkuda. See võib kaasa tuua näiteks lepingu kehtetuks tunnistamise.

3 Meetmed

3.1 Elutsükkel

Kavandamine

APP.1.1.M2 Aktiivsisu piiramine

APP.1.1.M10 Kontoritarkvara kasutajapoolsete lisaarenduste reguleerimine

APP.1.1.M11 Kontoritarkvara lisandprogrammide nõuetekohane kasutuselevõtt

Evitus

APP.1.1.M6 Kontoritarkvara uute versioonide testimine

Käitus

APP.1.1.M3 Välisallikatest pärit dokumentide turvaline avamine

APP.1.1.M12 Pilvtalletusest loobumine

APP.1.1.M13 Vaatefunktsioonide kasutamine

APP.1.1.M14 Andmete kaitsmine tagantjärele muutmise eest

APP.1.1.M17 Kontoritarkvara turvafunktsioonide rakendamise koolitus

Lisanduvad kõrgmeetmed

APP.1.1.M15 Krüpteerimine, digisignatuur ja digiallkirjastamine

APP.1.1.M16 Dokumentide tervikluse kontroll

3.2 Põhimeetmed

APP.1.1.M2 Aktiivsisu piiramine

a. Kontoritarkvaras on aktiivsisu automaatkäivitus seadetes välja lülitatud.

b. Kui aktiivsisu on tööks vajalik, installitakse see lubatud allikast.

APP.1.1.M3 Välisallikatest pärit dokumentide turvaline avamine [kasutaja]

a. Igat välisallikast pärit dokumenti kontrollitakse kahjurvara suhtes enne dokumendi avamist (vt OPS.1.1.4 *Kaitse kahjurvara eest*).

b. Organisatsioonis problemaatiliseks liigitatud ja ebavajalikud failivormingud on keelatud.

APP.1.1.M17 Kontoritarkvara turvafunktsioonide rakendamise koolitus

a. Kasutajad on teadlikud aktiivsisuga seotud ohtudest ja aktiivsisu piiramise võimalustest.

b. Kasutajad on teadlikud välistest allikatest pärinevate dokumentide kasutamise ohtudest.

c. Kasutajad on läbinud kontoritarkvara turvalise kasutamise ja turvafunktsioonide (sh krüpteerimisfunktsioonide) rakendamise koolituse.

d. Kasutajad on teadlikud, milliseid failivorminguid dokumentide salvestamisel kasutada et kaitsta neid hilisemate muudatuste ja võimaliku manipuleerimise eest.

3.3 Standardmeetmed

APP.1.1.M6 Kontoritarkvara uute versioonide testimine

a. Enne kontoritarkvara kasutamiseks kinnitamist testitakse eelnevalt koostatud testikava kohaselt tarkvara ühilduvust organisatsiooni infotehnoloogilise keskkonnaga (nt dokumendimallid, vormid, kasutatavad dokumendimakrod).

b. Kontoritarkvara võetakse esmalt pilootkasutusse, et veenduda toote toimimises käidukeskkonnas ning tegelike andmetega. Pilootkasutuse tulemused dokumenteeritakse.

c. Kontoritarkvara uute versioonide mitteühildumisel vanemate dokumentidega koostatakse tegevuskava sobiva lahenduse leidmiseks (nt dokumentide konverteerimiseks).

APP.1.1.M10 Kontoritarkvara kasutajapoolsete lisaarenduste reguleerimine

a. Eksisteerib kirjalik otsus, kas kasutajate tehtud kontoritarkvara lisaarendused (nt makrode ja lingitud arvutustabelite abil) on organisatsioonis lubatud.

b. Kui kontoritarkvaral põhinevad lisaarendused on organisatsioonis lubatud, rakendatakse neile sobivaid turvameetmeid (vt APP.1.1.M2 *Aktiivsisu piiramine)*.

c. Organisatsioonis on kehtestatud kontoritarkvara lisaarenduste tegemise kord, mis määratleb dokumenteerimise ja testimise nõuded, vastutavate töötajate kompetentsid ja tulemi kasutuselevõtu protseduurid.

d. Kasutaja loodud lisaarendused dokumenteeritakse ja dokumentatsioon tehakse töötajaile kättesaadavaks.

APP.1.1.M11 Kontoritarkvara lisandprogrammide nõuetekohane kasutuselevõtt

a. Kontoritarkvara lisandprogramme (ingl *add-on, plugin*) testitakse ja nende kasutuselevõtt kinnitatakse sarnaselt uute versioonide testimisele (vt APP.1.1.M6 *Kontoritarkvara uute versioonide testimine*). Lisandprogrammide testimine annab kindlust negatiivse kõrvalmõju puudumisest kontoritarkvarale ja kasutavatele IT-süsteemidele.

b. Kontoritarkvara lisandprogramme testitakse muudest IT-süsteemidest isoleeritud testimissüsteemis.

APP.1.1.M12 Pilvtalletusest loobumine [kasutaja]

a. Kontoritarkvara pilvtalletuse funktsionaalsus ja pilves pakutav salvestusruum on blokeeritud.

b. Dokumente hoitakse ühtses, tsentraalselt hallatavas keskkonnas.

c. Organisatsioonivälistele isikutele dokumentide jagamiseks kasutatakse sobivate turva- ja õiguste halduse funktsioonidega (nt krüpteeritud andmetalletus ja -edastus) erirakendusi või andmevahetusruume.

APP.1.1.M13 Vaatefunktsioonide kasutamine [kasutaja]

a. Potentsiaalselt ebaturvalistest allikatest (nt Internetist või e-kirja manusest) pärit dokumendid avatakse automaatselt piiratud režiimis, milles andmeid ei saa vahetult töödelda.

b. Kui dokumentidele on antud ainult lugemisõigus, kasutatakse dokumentide avamiseks arvutisse paigaldatud spetsiaalset dokumendivaatluse rakendust.

APP.1.1.M14 Andmete kaitsmine tagantjärele muutmise eest [kasutaja]

a. Olenevalt dokumendi plaanitud kasutusotstarbest kasutatakse loodud faili edasise töötlemise piiramiseks kontoritarkvaras olevaid turvamehhanisme.

b. Organisatsioonist välja saadetavaid dokumente kaitstakse digiallkirjaga. Kõik Euroopa Liidu ametiasutused peavad aktsepteerima eIDAS kvalifitseeritud digiallkirja, mille saab Eestis anda ID-kaardi, m-ID või Smart-ID sertifikaadiga.

3.4 Kõrgmeetmed

APP.1.1.M15 Krüpteerimine ja digisignatuurid (C-I)

a. Suurema kaitsetarbega andmed krüpteeritakse enne andmete edastamist või talletamist.

b. Enne kontoritarkvarasse integreeritud krüptomehhanismide kasutuselevõttu on kontrollitud, kas krüptomehhanism tagab piisava kaitse (eelkõige vanemate tooteversioonide korral) ja vastab organisatsiooni nõuetele (vt CON.1 *Krüptokontseptsioon*).

c. Saatja ja vastuvõtja IT-süsteemides on juurdepääs krüpomehhanismile piiratud.

d. Dokumendid ja dokumendi makrod signeeritakse digitaalselt autentsuse ja tervikluse tagamiseks.

APP.1.1.M16 Dokumentide tervikluse kontroll (I)

a. Terviklusnõuetega dokumendi edastamisel kaitstakse seda kontrollkoodi (nt CRC või SHA räsi) või digisignatuuriga (vt APP.1.1.M15 *Krüpteerimine ja digisignatuurid*).

b. Tahtmatute muudatuste korrigeerimiseks kasutatakse kontoritarkvarasse integreeritud automaatseid taastefunktsioone.

APP.1.2 Veebibrauser

1 Kirjeldus

1.1 Eesmärk

Esitada turvameetmed klientseadmete (sh laua- ja sülearvutite, tahvelarvutite ja nutitelefonide) veebibrauserite kaitseks. Seejuures käsitletakse nii tsentraalselt hallatavaid kui ka iseseisvaid töökeskkondi.

1.2 Vastutus

Veebibrauseri meetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Kasutaja.

1.3 Piirangud

Selles moodulis ei käsitleta brausereid, kui need on kasutusel üksnes juurdepääsuks kohalikele andmesidevõrkudele ilma Internetti pääsuta.

Kuna veebibrauser on tihedalt seotud klientseadme operatsioonisüsteemiga ja kasutab selle liideseid ning funktsioone, rakendatakse täiendavalt meetmeid moodulitest SYS.2 Lauaarvutid ja SYS.3.2.1 Nutitelefon ja tahvelarvuti üldiselt.

Brauseriga seotud veebirakendusi ja servereid käsitletakse moodulites APP.3.1 Veebirakendused ja APP.3.2 Veebiserver. Tarkvarale kehtivaid üldisi turvanõudeid käsitletakse moodulis APP.6. Tarkvara üldiselt.

2 Ohud

2.1 Veebibrauseri kaudu leviv kahjurkood

Veebibrauseriga ebausaldusväärsest allikast kahjursisu (ingl malicious content) allalaadimisel on oht kasutaja seade märkamatult nakatada. Aktiveerunud kahjurkood (ingl malicious code) võib alla laadida täiendavat kahjurvara. Koodi võib aktiveerida brauser ise (nt JavaScript) või brauseriga seotud plugin (nt Adobe Flash, Java või PDF-dokumentide komponendid). Lisaks võib veebibrauser paigaldada koodi klientarvutisse ja mis käivitatakse väljaspool brauseriprotsessi.

2.2 Eksploidipakid

Kahjurprogrammide levitamise muudavad oluliselt lihtsamaks nõrkuste loendid ja nn eksploidipakid (ingl *exploit kit*). Ründaja võib veebibrauseri või selle laienduste nõrkusi ära kasutada ründe läbiviimiseks ilma eriteadmisi omamata.

2.3 Andmevahetuse pealtkuulamine

Autentimine ja krüpteerimine andmete edastusel on tihti puudulikult teostatud. Kui veebiteenustes jätkuvalt kasutatakse aegunud krüpteerimismeetodeid, saab ründaja võrguliiklust pealt kuulata või muuta.

2.4 Tervikluskadu veebibrauseris

Brauserile lisatud kahjurprogramm, kahjulik plugin või võltsitud brauserikomponent võib veebisaidil kasutajale kuvatavaid andmeid muuta või andmeid ründajale edastada. Rikutud veebisaidi kaudu on võimalik läbi viia õngitsusründeid (ingl *phishing attack*).

2.5 Privaatsusrike

Brauseri turvalise seadistuseta võivad tundlikud andmed olla kättesaadavad kõrvalistele isikutele. Brauseri kaudu on võimalik tahtmatult edasi anda kasutaja paroole. Ründaja valdusesse võivad sattuda tundlikud andmed salvestatud brauseriküpsistest (ingl *browser cookie, cookie*), ajaloost, sisestusandmetest või otsingupäringutest.

3 Meetmed

3.1 Elutsükkel

Evitus

APP.1.2.M1 Veebibrauseri turvamehhanismide kasutamine

APP.1.2.M2 Side krüpteerimine

Käitus

APP.1.2.M3 Turvalised sertifikaadid

APP.1.2.M6 Paroolihalduri kasutamine veebibrauseris

APP.1.2.M7 Andmete kaitse veebibrauseris

APP.1.2.M13 DNS-over-HTTPS protokolli kasutamine

Lisanduvad kõrgmeetmed

APP.1.2.M9 Isoleeritud brauserikeskkond

APP.1.2.M10 Brauseri privaatrežiim

APP.1.2.M11 Kahjursisu olemasolu kontroll

APP.1.2.M12 Kahe brauseri strateegia

3.2 Põhimeetmed

APP.1.2.M1 Veebibrauseri turvamehhanismide kasutamine

a. Veebibrauseris on rakendatud aedikkäitus (ingl *sandboxing*). Igal brauseri instantsil ja töötlusprotsessil on juurdepääs üksnes oma ressurssidele.

b. Kasutatakse brauserit, mis isoleerib veebisaidid üksteisest autonoomsete protsesside või eraldi lõimedena. Pluginaid ja laiendusi käitatakse üksteisest isoleeritud aladel.

c. Brauseris on rakendatud ajakohasele W3C spetsifikatsioonidele vastav sisuturve (CSP-*Content Security Policy*).

d. Veebibrauser toetab Same-Origin Policy (SOP) ja Subresource Integrity funktsionaalsust.

APP.1.2.M2 Side krüpteerimine

a. Veebibrauser toetab transpordikihi turvaprotokolli TLS turvalist versiooni (2020 a. TLS 1.3).

b. TLS-i ebaturvalised versioonid on välja lülitatud.

c. Brauser toetab RFC 6797 kirjeldusele vastavat turvamehhanismi HSTS (HTTP Strict Transport Security).

APP.1.2.M3 Turvalised sertifikaadid

a. Brauser võimaldab väljastada usaldatavate juursertifikaadi väljastajate loendi ja võimaldab seda täiendada organisatsioonis kasutusele võetud sertifikaatidega.

b. Brauser toetab laiendvalideerimise sertifikaate (ingl *extended validation (EV) certificate*).

c. Juursertifikaate on võimalik lisada, muuta või kustutada ainult haldusõiguste olemasolul.

d. Sertifikaate on võimalik lokaalse veebibrauseri kaudu tühistada.

e. Brauser kontrollib avalike võtmete ja kehtivusaja abil serveri sertifikaatide kehtivust.

f. Brauser kontrollib serveri sertifikaadi olekut ja verifitseerib sertifikaadiahelat koos juursertifikaadiga.

g. Kasutaja jaoks on arusaadavalt ja hästi märgatavalt nähtav, kas andmevahetus on krüpteeritud või mitte. Vajadusel saab kasutaja brauseris serveri sertifikaati vaadata.

h. Brauser teavitab kasutajat sertifikaatide puudumisest või kehtetust olekust. Ühenduse loomine lõpetakse siis üksnes pärast kasutajalt selgesõnalise kinnituse saamist.

APP.1.2.M6 Paroolihalduri kasutamine veebibrauseris

a. Paroolihaldur loob veebibrauseris veebisaidi, kasutajanime ja parooli vahel unikaalse ja turvalise seose.

b. Paroole hoitakse paroolihalduris krüpteeritult. Juurdepääs paroolihaldurisse salvestatud paroolidele on võimalik üksnes pärast peaparooli (ingl *master password*) sisestamist.

c. Paroolihalduri abil autentimine rakendub üksnes käsiloleva seansi jaoks.

d. Kasutaja saab omi salvestatud paroole kustutada.

e. Paroolihalduri paroolide sünkroniseerimine pilvteenuse vahendusel on keelatud.

APP.1.2.M13 DNS-over-HTTPS protokolli kasutamine

a. Klientseadmetes kasutatavad brauserid toetavad DNS-over-HTTPS (DoH) protokolli kasutamist.

b. Kui DoH on kasutusele võetud, on klientseadmete veebibrauserites DoH kasutamine sisse lülitatud.

c. Organisatsioonisiseseks nimeteisenduseks kasutatav DNS-server toetab DNS-over-HTTPS protokolli.

3.3 Standardmeetmed

APP.1.2.M7 Andmete kaitse veebibrauseris [kasutaja]

a. Kolmandate poolte brauseriküpsised (ingl *browser cookie*) on blokeeritud. Kasutajal on võimalus salvestatud küpsiseid kustutada.

b. Andmesisestuse automaatjätkamine (ingl *autocompletion*) on desaktiveeritud. Kui seda funktsiooni siiski kasutatakse, saab kasutaja jätkuandmeid kustutada.

c. Kasutajal on võimalik kustutada brausimise ajalugu.
d. Brauseri sünkroniseerimine pilvteenusega on desaktiveeritud.
e. Tootja telemeetriafunktsioonid ja tõrketeadete automaatne edastamine on desaktiveeritud.
f. Ühendatud välisseadmed (nt mikrofon või veebikaamera) on vaikimisi brauseris desaktiveeritud.
g. Brauser võimaldab konfigureerida või blokeerida WebRTC-d, HSTS-i ja JavaScripti kasutamist.

3.4 Kõrgmeetmed

APP.1.2.M9 Isoleeritud brauserikeskkond (C-I)

a. Brauserit kasutatakse ainult isoleeritud keskkonnas (nt ReCoBS- *Remote-Controlled Browser System* või virtualiseeritud instants).

APP.1.2.M10 Brauseri privaatrežiim [kasutaja] (C-I)

a. Brauserit kasutatakse privaatrežiimis (*ingl private/incognito browsing mode*), milles andmeid püsivana kasutaja IT-süsteemi ei salvestata.
b. Brauser on konfigureeritud nii, et brauseri sulgemisel brausimise metaandmed kustutatakse.

APP.1.2.M11 Kahjursisu olemasolu kontroll (C)

a. Brausimisel tehakse veebilehtede kahjurvara- ja reputatsioonikontroll. Kahjulikuks liigitatud veebilehe külastamine blokeeritakse.
b. Veebilehtede kontroll toimub vastavuses andmekaitsealaste õigusaktidega.

APP.1.2.M12 Kahe brauseri strateegia (A)

a. Kui veebibrauseriga tekib lahenduseta turvaprobleeme, installitakse alternatiivseks kasutamiseks teise tootja turvaline brauser.

APP.1.4 Mobiilirakendused (äpid)

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed äriprotsessi toetavates mobiilirakendustes ehk äppides töödeldavate andmete kaitseks. Äppe käsitletakse päritolust (iseehitatud või mobiililirakenduste poest hangitud) sõltumata.

1.2 Vastutus

Mobiilirakenduste meetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Vastutav spetsialist.

1.3 Piirangud

Mobiilseadmete operatsioonisüsteemide iOS ja Android turvameetmeid käsitletakse moodulites SYS.3.2.3 *Organisatsiooni iOS* ja SYS.3.2.4 *Android*.

Mobiilseadmete keskhaldust käsitletakse moodulis SYS.3.2.2 *Mobiilseadmete haldus (MDM)*.

Äppide rakendusspetsiifilisi aspekte käsitletakse mooduligrupi APP (rakendused) moodulites APP.3.1 *Veebirakendused* ja APP.4.3 *Andmebaasisüsteemid*.

Rakenduste üldaspekte käsitlevad moodulid OPS.1.1.6 *Tarkvara testimine ja kinnitamine* ning APP.6 *Tarkvara üldiselt*.

2 Ohud

2.1 Ebasobiva mobiilirakenduse valimine

Kui mobiilirakenduse valimisel ei arvestata sobivust äriprotsessidega, võib rakendus hakata äriprotsessi takistama. Kui mobiilirakenduse tööks vajalikke tingimusi (nt mobiilsidevõrgu ühenduse kiirus või ühilduv riistvara) piisaval määral ei arvestata, ei pruugi rakendus nõuetekohaselt töötada. Mobiilirakendus võib pikemas perspektiivis osutuda kasutuks, kui tootja ei suuda tagada pikaajalist kasutusstabiilsust või kui ta rakendust piisavalt ei hoolda.

2.2 Liiga suured õigused

Operatsioonisüsteemide iOS ja Android mobiilirakendused vajavad funktsioonide ja teenuste toimimiseks laialdasi pääsu- ja kasutusõigusi. Kui kasutatakse mobiilirakendust, mis nõuab tööks laialdasemaid õigusi kui tegelikult vaja läheb, on lõppseadme andmete konfidentsiaalsus ja terviklus ohus. Äpid võivad informatsiooni (nt seadme asukoht, fotod, kontakt- ja kalendriandmed) edastada volitamata kolmandatele isikutele. Liigsed õigused mobiilirakenduses võivad kaasa tuua ka otsest rahalist kahju (nt seoses telefonikõnede, SMS-ide saatmise või mobiilirakenduste ostmisega).

2.3 Soovimatud funktsioonid mobiilirakendustes

Mobiilirakenduste installimisel kontrollimata või ebausaldusväärsest allikast on oht saada seadmesse koos rakendusega ka kahjurvara.

Ka mobiilirakenduste poe kaudu soetatud mobiilirakendused võivad sisaldada kahjurfunktsioone. Rakenduste kahjurvarakontroll ei pruugi kõiki kahjurfunktsioone avastada.

2.4 Tarkvara nõrkused ja vead mobiilirakendustes

Mobiilirakendus võib sisaldada turvanõrkusi. Teadaolevaid ja veel avalikustamata (nn nullpäeva) nõrkusi on võimalik ära kasutada seadme või selle võrguühenduste kaudu tervete IT-süsteemide ründamiseks. Paljude rakenduste uuendamine ja kasutajatugi lõpetatakse varsti pärast väljatöötamist. Kuna tuvastatud puudusi uuendite ja turvapaikadega ei kõrvaldata, jäävad nõrkused mobiilirakendusse alles.

2.5 Rakenduse andmete ebaturvaline lokaalne talletamine

Kui mobiilirakenduste seadmesse talletatud andmed (nt kasutajaprofiilid ja dokumendid) ei ole piisavalt turvatud, võivad neile juurde pääseda teised rakendused. Volitamata isikutel on neid andmeid lihtne lugeda (näiteks kui töötaja on oma seadme kaotanud). Lokaalselt talletatud andmeid andmevarunduskontseptsioonides tihti ei arvestata, mistõttu võivad need andmed lõppseadme kaotamisel või tõrke korral kaotsi minna.

2.6 Konfidentsiaalse teabe tuletamine metaandmetest

Mobiilirakendustega kogutakse hulgaliselt metaandmeid, millest osa võib olla konfidentsiaalne (nt telefoni- ja võrguühendused, liikumisandmed ja külastatud veebisaidid). Metaandmetest saab tuletada ka muud informatsiooni, nagu näiteks organisatsiooni korraldus, täpsed tegevuskohad ja isikkoosseis.

2.7 Konfidentsiaalsete andmete leke mobiilirakendusest

Mobiilseadmete operatsioonisüsteemid võimaldavad kasutada mobiilirakenduste ja välisseadmete vahel andmevahetuseks mitmeid liideseid. Ka kasutajal on andmete vahetamiseks mitmeid võimalusi (nt lokaalse mälukaardi, seadmekaamera või teiste rakenduste vahendusel). Mobiilirakenduse andmed võidakse saata pilvteenusesse. Tihti edastatakse andmeid mobiilirakenduse tarnija või mobiilseadme tootja serveri kaudu, kust kolmandatel osapooltel võib tekkida võimalus konfidentsiaalsetele andmetele juurdepääsuks.

Operatsioonisüsteemis kasutatakse kiirema andmepääsu saavutamiseks andmete ajutist salvestamist (puhverdamist). Konfidentsiaalsed andmed võivad lekkida või saab ründaja konfidentsiaalsele informatsioonile juurdepääsu.

2.8 Ebaturvaline ühendus tagasüsteemidega

Enamasti toimub andmeedastus mobiilseadmete ja tagasüsteemide (ingl *backend system*) vahel ebaturvaliste võrkude kaudu (mobiilsidevõrk, WLAN-võrk jms). Kui tagasüsteemidega ühendumiseks kasutatakse ebaturvalisi protokolle, saab andmeid pealt kuulata ja rikkuda.

2.9 Suhtlusteed väljaspool organisatsiooni taristut

Mobiilirakendustega on võimalik luua suhtlusteid ja organisatsioon ei suuda neid tuvastada ega kontrollida. Kasutaja saab mobiilseadmest andmete edastamiseks kasutada pilvteenuseid, mille kasutust organisatsioon ei kontrolli. Sotsiaalmeediateenuste tihe seotus mobiilirakendustega raskendab arusaamist, kas ja millal on andmeid lõppseadmest edastatud.

2.10 Sõltuvus taga- või välissüsteemidest ja -teenustest

Paljude mobiilirakenduste töö sõltub otseselt välissüsteemidest ja -teenustest. Ilma andmesideühenduseta töötavad paljud mobiilirakendused üksnes piiratult või ei saa neid üldse kasutada. Kui välisteenusega seotud andmesideühendus või teenus ise on kättesaamatu, on mobiilirakenduse käideldavus häiritud.

3 Meetmed

3.1 Elutsükkel

Kavandamine

APP.1.4.M1 Mobiilirakenduse nõuete analüüs

Evitus

APP.1.4.M3 Mobiilirakenduste turvaline levitamine

APP.1.4.M5 Mobiilirakenduste pääsuõiguste piiramine ja kontroll

Käitus

APP.1.4.M7 Mobiilirakenduste lokaalsete andmete turve

APP.1.4.M8 Andmelekete avastamine ja takistamine

APP.1.4.M16 Mobiilirakenduste haldus

Kõrvaldamine

APP.1.4.M12 Mobiilirakenduste turvaline desinstallimine

Lisanduvad kõrgmeetmed

APP.1.4.M14 Mitmikautentimine mobiilirakendustes

APP.1.4.M15 Mobiilirakenduste läbistustestimised

3.2 Põhimeetmed

APP.1.4.M1 Mobiilirakenduse nõuete analüüs [vastutav spetsialist]

a. Enne mobiilirakenduse kasutuselevõttu kaardistatakse äriprotsessidest tulenevad mobiilirakenduse nõuded.

b. Analüüsitakse mobiilirakenduse kasutuselevõtuga kaasnevaid riske ja tuvastatakse turvanõuded, arvestades töödeldavate andmete kaitsetarvet, IT-keskkonda ja õiguslikke raamtingimusi.

APP.1.4.M5 Mobiilirakenduste pääsuõiguste piiramine ja kontroll [vastutav spetsialist]

a. Enne mobiilirakenduse kasutuselevõttu kitsendatakse rakenduse pääsuõigused tööks minimaalselt vajalikeni.

b. Mobiilirakenduse turvaseadeid ei saa kasutajad ega rakendus iseseisvalt muuta. Kui see ei ole tehniliselt võimalik, kontrollitakse piirangute järgimist regulaarselt.

APP.1.4.M7 Mobiilirakenduste lokaalsete andmete turve

a. Mobiilirakendusele organisatsiooni sisedokumentidele juurdepääsu andmisel rakendatakse lokaalsete andmete kaitseks piisavaid meetmeid.

b. Pääsuvõtmeid hoitakse krüpteeritult.

c. Operatsioonisüsteem ei tee tundlike andmete vahesalvestusi teistesse talletuskohtadesse.

APP.1.4.M8 Andmelekete avastamine ja takistamine

a. Konfidentsiaalsete andmete edastamise vältimiseks analüüsitakse andmevahetust mobiilirakenduse testimisel (vt APP.1.4.M4 *Mobiilirakenduste testimine ja kasutuseks kinnitamine*).

b. Kontrollitakse, ega mobiilirakendus ei salvesta logi- või abifailidesse konfidentsiaalseid andmeid.

c. Mobiilirakenduse andmevahetuses piiratakse tundlike andmete vajaduseta väljastamist.

3.3 Standardmeetmed

APP.1.4.M3 Mobiilirakenduste turvaline levitamine

a. Mobiilirakendusi hangitakse üksnes turvalistest ja usaldusväärsetest allikatest.

b. Organisatsiooni siserakendusi, millega töödeldakse kaitset vajavat andmeid, levitatakse üksnes organisatsioonisisese äpipoe või mobiilseadmete halduse (MDM) kaudu.

APP.1.4.M12 Mobiilirakenduste turvaline desinstallimine

a. Mobiilirakenduse desinstallimisel kustutatakse kõik rakenduse failid, rakenduse poolt genereeritud failid ja rakendusega seotud ajutised andmed (nt puhvrid).
b. Mobiilirakenduse desinstallimisel kustutatakse rakenduse andmed välissüsteemides (nt pilvteenuses varundatu).

3.4 Kõrgmeetmed

APP.1.4.M14 Mitmikautentimine mobiilirakendustes (C-I)

a. Mobiilirakenduses kasutatakse autentimiseks mitut autentimistegurit. Mobiilirakenduse käitamiseks kasutavad seadmed toetavad mitmikautentimist.
b. Autentimistegurid on piisavalt võltsimatud. Biomeetriliste tuvastusmeetodite korral on analüüsitud, kas autentimiskindlus on võltsimiskatsete vältimiseks piisav.

APP.1.4.M15 Mobiilirakenduste läbistustestimised (C-I-A)

a. Enne mobiilirakenduse kasutuselevõttu viiakse läbi mobiilirakenduse läbistustestimine.
b. Turvanõrkuste avastamiseks kontrollitakse testimise käigus ka andmevahetusliideseid tagasüsteemidega ja lokaalset andmetalletust.
c. Läbistustestimisi korratakse mobiilirakenduse või mobiilseadme operatsioonisüsteemi suuremate muudatuste korral.

APP.1.4.M16 Mobiilirakenduste haldus (C-I-A)

a. Mobiilirakenduste seadistamiseks ja haldamiseks kasutatakse tsentraalset mobiilseadmete haldust.

APP.2: Kataloogiteenused

APP.2.1 Kataloogiteenus üldiselt

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed üldise kataloogiteenuse turvaliseks kasutamiseks ja kataloogiteenuse andmete kaitseks.

1.2 Vastutus

„Kataloogiteenus üldiselt“ meetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Andmekaitsespetsialist, vastutav spetsialist.

1.3 Piirangud

Moodul käsitleb kataloogiteenuste üldisi turvaaspekte. Meetmed tuntuimate kataloogiteenuste kaitseks on esitatud moodulites APP.2.2 *Active Directory Domain Services* ja APP.2.3 *OpenLDAP*.

Kataloogiteenust jagava serveri turvameetmed on esitatud mooduligrupis SYS.1 *Server*. Kataloogiteenuste pääsuõiguste halduses järgitakse moodulit ORP.4 *Identiteedi- ja õiguste haldus*.

Täiendavalt tuleb arvestada meetmeid mooduligrupist OPS.1.1 *IT-põhitööd*.

2 Ohud

2.1 Kataloogiteenuse rakendamise puuduv või piisamatu kavandamine

Kataloogiteenuse turvalisus sõltub suurel määral kataloogiteenust jagava serveri turvameetmetest. Kataloogiteenuse saab installida ja kataloogiteenust saab kasutada paljudes operatsioonisüsteemides. Väga heterogeense või keeruka kogulahenduse korral võib kataloogiteenusesse jääda turvanõrkusi, millele kavandamise käigus ei osatud tähelepanu pöörata. Haldustööde puuduliku kavandamise korral on olemas oht, et süsteemi hallatakse ebaturvaliselt või puudulikult.

2.2 Sektsioonimise ja dubleerimise väär või piisamatu rakendamine

Kui kataloogiteenuse andmestiku struktuuri sektsioonimist ja dubleerimist algselt mitte ette näha, siis seadistuse hilisem muutmine on küll võimalik, kuid võib kaasa tuua probleeme. Kui kataloogiteenuse andmestiku sektsioonimist ja dubleerimist kavandatakse puudulikult või piisamatult, võib see kaasa tuua andmekaotuse, vead andmetalletuses, kataloogiteenuse halva sooritusvõime või kataloogiteenuse tõrked.

2.3 Pääsuõiguste puudulik haldus

Kataloogiteenuse kaudu hallatavatele kasutajate ja rühmade pääsuõiguste puuduliku halduse tõttu (nt jättes vajalikud juurdepääsuõigused andmata) kaasnevad tõrked süsteemide igapäevases töös.

Liiga ulatuslikud pääsuõigused tekitavad turvanõrkusi.

Puudulik või ebaühtlane pääsuõiguste andmine kataloogiteenuses ohustab terve süsteemi turvalisust märkimisväärselt.Eksimus kataloogiteenuse haldamise õiguste määramisel võib ohustada kogu kataloogisüsteemi toimimist.

2.4 Kataloogiteenuse juurdepääsu väär konfiguratsioon

Kataloogiteenuse rakendamisel antakse juurdepääs kataloogiteenusele ka tavarakendustele (nt Interneti- või sisevõrgurakendused). Väära konfiguratsiooni tulemusena võimaldatakse kataloogiteenusele volitamata juurdepääs.

Kui autentimisandmeid edastatakse krüpteerimatult avatekstina, on võimalik andmeid luurata.

2.5 Kataloogiteenuse komponentide tõrked

Riistvara- ja tarkvaraprobleemidest tulenevad tehnilised rikked võivad kaasa tuua kataloogiteenuse katkestuse. Selle tagajärjel ei ole kataloogis hoitavad andmed ajutiselt juurdepääsetavad ja organisatsiooni äriprotsessid on häiritud. Äärmisel juhul võivad ka andmed kaotsi minna.

2.6 Kataloogiteenuse kahjustamine volitamata juurdepääsu kaudu

Kui ründajal õnnestub kataloogiteenusesse sisse murda, on tal võimalus kataloogiteenust ja sealseid andmeid kahjustada. Liiaste õiguste kaudu on võimalik saada volitamata juurdepääs võrguressurssidele ja teenustele, neid mõjutada või kahjustada.

Kataloogiteenuse turvalisust ohustab, kui kataloogiteenus ei nõua päringute esitamiseks autentimist. Anonüümsete päringutega saab hankida vähemalt osalist teavet kataloogiteenuse struktuuri ja sisu kohta. Ründaja saab kontrollimatut juurdepääsu kuritarvitada näiteks ummistusründe korraldamiseks.

2.7 Kataloogiteenuse väär konfigureerimine

Kataloogiteenuse arvukate funktsioonide konfigureerimisvead võivad viia lubamatu juurdepääsuni tervele kataloogiteenusele. Kui standardkonfiguratsiooni piisaval määral ei kontrollita ega kohandata, saab avateksti kujul edastatavaid autentimisandmeid ära kasutada edasisteks rünneteks.

3 Meetmed

3.1 Elutsükkel

Kavandamine

APP.2.1.M1 Kataloogiteenuse turvaeeskiri

APP.2.1.M2 Kataloogiteenuse kavandamine

APP.2.1.M8 Kataloogiteenuse sektsioonimine

APP.2.1.M15 Kataloogiteenuse migratsiooni turve

Soetus

APP.2.1.M9 Sobivate kataloogiteenuse komponentide valimine

Evitus

APP.2.1.M3 Kataloogiteenuse pääsuõiguste korraldus

APP.2.1.M11 Kataloogiteenuse juurdepääsu reguleerimine

Käitus

APP.2.1.M5 Kataloogiteenuse turvaline konfigureerimine

APP.2.1.M6 Kataloogiteenuse turvaline käitus

APP.2.1.M12 Kataloogiteenuse seire

APP.2.1.M13 Kataloogiteenuse andmevahetuse turve

APP.2.1.M17 Kaitsevajadusega pääsuteabe turve

APP.2.1.M18 Kataloogiteenuse dubleerimine

APP.2.1.M19 Kataloogiteenuse anonüümse juurdepääsu haldus

Kõrvaldamine

APP.2.1.M14 Kataloogiteenuse kõrvaldamise kord

Lisanduvad kõrgmeetmed

APP.2.1.M16 Eriolukorra tegevuskava koostamine kataloogiteenuse tõrgete puhuks

APP.2.1.M20 Kataloogiteenuse dubleerimise turve

APP.2.1.M21 Kataloogiteenuse kõrgkäideldavuse tagamine

3.2 Põhimeetmed

APP.2.1.M1 Kataloogiteenuse turvaeeskiri

a. On koostatud üldisele infoturvapoliitikale vastav kataloogiteenuse turvaeeskiri.

b. Kataloogiteenuse turvaeeskiri on kataloogiteenuse halduritele ja kasutajatele teatavaks tehtud.

APP.2.1.M2 Kataloogiteenuse kavandamine [andmekaitsespetsialist, vastutav spetsialist]

a. Kataloogiteenuse kavandamisel on lähtutud selle ühilduvusest kasutatavate rakendusega.

b. Kataloogiteenuse rakenduskavas on dokumenteeritud:

c. kataloogiteenuse struktuur;

d. ettenähtud kasutusviisidega sobiv objektiklasside ja atribuuditüüpide mudel;

e. vajadustel põhinev pääsuõiguste haldusmudel;

f. Isikuandmeid sisaldava kataloogiteenuse kavandamisel on kaasatud andmekaitsespetsialist.

g. On kavandatud meetmed takistamaks andmete volitamata kogumist kataloogiteenusest.

APP.2.1.M3 Kataloogiteenuse pääsuõiguste korraldus [vastutav spetsialist]

a. Kataloogiteenuse ja selle andmete haldustegevusi hoitakse omavahel lahus. Haldusülesanded dokumenteeritakse, ülesandeid täitvad isikud ei talitle konfliktsetes rollides.

b. Kasutajate ja haldurite pääsuõigused vastavad kataloogiteenuse turvaeeskirjale. Pääsuõigustega seotud tegevused on jälitatavad.

c. Mitme kataloogiteenusepuu liitmisel kontrollitakse tegelikke koondõigusi.

APP.2.1.M5 Kataloogiteenuse turvaline konfigureerimine

a. Kataloogiteenused ja kogu kataloogiteenuse taristu (server, klientarvutid, rakendused) konfigureeritakse turvaliselt.

b. Kataloogiteenuse konfiguratsiooni muudatustest teavitatakse kataloogiteenuse kasutajaid ennetavalt.

c. Enne konfiguratsioonimuudatusi varundatakse asjakohased andmed.

APP.2.1.M6 Kataloogiteenuse turvaline käitus

a. Kataloogiteenuse halduse ja käituse protsessid on dokumenteeritud.

b. Kataloogiteenuse halduseks kasutatakse spetsiaalset kasutajakontot. Halduskontosid ei kasutata tavapäraseks igapäevatööks.

c. Juurdepääs haldusinstrumentidele on tavakasutajate jaoks blokeeritud.

APP.2.1.M17 Kaitsevajadusega pääsuteabe turve

a. Juurdepääs kaitsevajadusega pääsuteavet sisaldavatele kataloogiteenuse atribuutidele (nt paroolid) on rangelt piiratud.

3.3 Standardmeetmed

APP.2.1.M8 Kataloogiteenuse sektsioonimine

a. Sektsioonimise kavandamisel on arvestatud kataloogiteenuse käideldavust ja kaitsetarvet.

b. Kataloogiteenuse sektsioonimine on kavandatud nii, et see piiraks turvaintsidentide mõju ja võimaldaks kataloogiteenuse taastet sektsioonhaaval.

APP.2.1.M9 Sobivate kataloogiteenuse komponentide valimine [vastutav spetsialist]

a. Kehtestatud valikukriteeriumite alusel on määratud kataloogiteenuse rakendamiseks sobivad komponendid (vt APP.6 *Tarkvara üldiselt*).

b. Kataloogiteenuse komponendid võimaldavad rakendada eelnevalt kataloogiteenuse otstarbe alusel määratletud turvanõudeid.

APP.2.1.M11 Kataloogiteenuse juurdepääsu reguleerimine

a. Kataloogiteenuse juurdepääs on konfigureeritud kataloogiteenuse turvapoliitika kohaselt.

b. Kataloogiteenuse kasutamisel üle Interneti on server kaitstud turvalüüsiga.

APP.2.1.M12 Kataloogiteenuse seire

a. Kataloogiteenuse logiandmeid analüüsitakse regulaarselt, tuginedes organisatsioonis kehtestatud poliitikatele ja määratud kriteeriumitele.

b. Kataloogiteenuse seire hõlmab ka servereid, kus kataloogiteenust kasutatakse.

APP.2.1.M13 Kataloogiteenuse andmevahetuse turve

a. Andmevahetus kataloogiteenuse serveri ja kliendi vahel on turvatud (krüpteeritud SSL/TLS protokolliga).

b. Juurdepääs kataloogiteenuse serverile Internetist on piiratud.

c. Juurdepääs andmetele lubatakse vaid vajadusepõhiselt.

d. Teenusekeskse arhitektuuri (ingl *service-oriented architecture*, SOA) kasutamisel teenuseregistri kaudu kontrollitakse kasutaja pääsuõiguste kehtivust.

APP.2.1.M14 Kataloogiteenuse kõrvaldamise kord [vastutav töötaja]

a. Kataloogiteenuse kasutamise lõpetamisel tagatakse vajalike õiguste ja andmete käideldavus, kõik muu kustutatakse.

b. Kasutajaid teavitatakse kataloogiteenuse kasutamise lõpetamisest ennetavalt.

c. Üksikute sektsioonide kõrvaldamisel ei mõjutata teiste sektsioonide käideldavust.

APP.2.1.M15 Kataloogiteenuse migratsiooni turve

a. Kataloogiteenuse migreerimiseks koostatakse eelnevalt migratsioonikava. Kataloogiteenuse skeemi kavandatud muudatused dokumenteeritakse.

b. Kui migreerimiseks on pääsuõigusi ajutiselt suurendatud, siis pärast migratsiooni lõppu korralised õigused taastatakse.

c. Uude kataloogisüsteemi üle viidud kasutajate pääsuõigused ajakohastatakse.

APP.2.1.M18 Kataloogiteenuse dubleerimine

a. Kataloogiteenuse dubleerimise kavandamisel määratakse dubleerimise eesmärgid ning koostatakse rakendusstsenaariumit ja võrgutopoloogiat kirjeldav tegevusplaan.

b. Kui eesmärgiks ei ole seatud kogu kataloogiteenuse kõrgkäideldavus, dubleeritakse ainult vajalikud kataloogiteenuse komponendid.

c. Dubleerimise rakendamisel on arvestatud piisava jõudlusega.

APP.2.1.M19 Kataloogiteenuse anonüümse juurdepääsu haldus

a. Kui anonüümsetele kasutajatele on kataloogipuu üksikutes sektsioonides vajalikud suuremad pääsuõigused, luuakse selleks spetsiaalne ajutine kasutajakonto (nn *proxy user*). Kui kontot enam ei kasutata, tühistatakse pääsuõigus kataloogiteenusele täies ulatuses.

b. Kataloogiteenuse otsingufunktsioon on piiratud, et vältida tundlike kataloogiandmete leket.

3.4 Kõrgmeetmed

APP.2.1.M16 Kataloogiteenuse avariikava (C-I-A)

a. Avariivalmenduse raames on kehtestatud ja dokumenteeritud organisatsiooni vajadustele vastav kataloogiteenuse avariikava.

b. Avariikavas sisalduvad kataloogiteenuse komponentide süsteemikonfiguratsioon ja taasteprotseduurid.

APP.2.1.M20 Kataloogiteenuse dubleerimise turve (C-I)

a. Konfidentsiaalse sisuga kataloogiteenuse dubleerimisel andmed krüpteeritakse rakendus- või transpordikihi tasemel (nt IPSec protokolliga).

b. Autentimiseks kasutatakse võimalikult turvalisi autentimismeetodeid.

APP.2.1.M21 Kataloogiteenuse kõrgkäideldavuse tagamine (A)

a. Kataloogiteenuse kõrgkäideldavuse tagamiseks on valitud sobiv strateegia (kas „Master-Master“ või „Master-Replica“ kordistamine).

b. On määratud, kuidas kataloogiteenus toimib erandjuhtudel, nt kui dubleeritud kataloogiteenuse osade vahel tekib sisuline vastuolu.

APP.2.2 Active Directory Domain Services

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed *Active Directory Domain Services* (AD DS) tavakasutuse turbeks olukorras, kus AD teenust kasutatakse Microsoft Windowsi süsteemidest (kliendid ja serverid) koosneva taristu ning keskse autentimis- ja autoriseerimislahenduse haldamiseks.

1.2 Vastutus

Active Directory Domain Service turvameetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Vastutav spetsialist.

1.3 Piirangud

Moodulit kohaldatakse kõigile Microsoft AD DS kataloogiteenustele, sh *Active Directory Lightweight Directory Services* (AD LDS).

Kataloogiteenuse üldised turbesoovitused on esitatud moodulis APP.2.1 *Kataloogiteenus üldiselt*.

AD DS rakendamine peab toimuma kooskõlas järgmiste moodulitega: ORP.4 *Identiteedi- ja õiguste haldus,* OPS.1.1.3 *Paiga- ja muudatuste haldus,* CON.3 *Andmevarunduse kontseptsioon,* OPS.1.2.2 *Arhiveerimine*, OPS.1.1.5 *Logimine*. Samuti mõjutab AD DS mooduleid OPS.1.1.2 *IT-süsteemide haldus*, OPS.1.2.5 *Kaughooldus,* DER.1 *Turvaintsidentide avastamine,* DER.2.1 *Turvaintsidentide käsitlus*, *DER.4 Avariihaldus* ja *APP.3.6 DNS-server*.

Moodulis ei käsitleta Windows serverite ja klientide operatsioonisüsteemide turvameetmeid (nt SYS.1.2.2 *Windows Server* või SYS.2.2.3 *Windows klient*) ning võrgutaristu haldust.

2 Ohud

2.1 Turvapiiride puudulik kavandamine

Kui AD DS üldstruktuuri (nn AD mets (ingl AD forest)) kuuluvate AD domeenide (ingl AD domain) turvapiire teadlikult ja hoolikalt ei kavandata, võib domeenide omavahelistest usaldusseoste tõttu saada ründe tulemusena kompromiteeritud kõik metsa kuuluvad domeenid ja neis olevad objektid, sealhulgas kõik kontod ja IT-süsteemid.

2.2 Usaldusseoste rohkus või lõtvus

AD domeenide ja metsade vahelised usaldusseoste tõttu on võimalik kontole anda juurdepääs teise AD domeeni või AD metsa ressurssidele. Kui AD metsade (ingl *AD forest*) ja AD domeenide (ingl *AD domain*) vaheliste usaldusseoste vajalikkust ja tüüpi regulaarselt ei hinnata ning kontrolliprotseduurid pole piisavad, siis võivad pääsuõigustega tekkida probleemid ning andmed võivad lekkida.

Normaalolekus aktiveeritud turvavõtmete (ingl *Security Identifier* - SID) filtreerimise desaktiveerimisel võivad tekkida raskesti avastatavad konfiguratsioonivead, mis võimaldavad liigseid pääsuõigusi ja nende kuritarvitamist. Sama kehtib valikautentimisest (ingl *selective authentication*) loobumise korral AD metsade vahelistes usaldusseostes.

2.3 Turvafunktsioonide puudumine pärandsüsteemides

Varasemate operatsioonisüsteemide kasutamine (primaarse) domeenikontrollerina või ajakohastamata domeeni funktsionaaltase (ingl Domain Functional Level- DFL) takistab nüüdisaegsete turvafunktsioonide kasutamist ja suurendab ebaturvaliste vaikeseadete kasutamise ohtu.

Ebaturvaliselt konfigureeritud domeen ohustab selles töödeldavaid andmeid ja võimaldab ründajal ründeid lihtsamalt ellu viia.

2.4 Liigsed rollid ja liigsete teenuste käitus domeenikontrolleris

Iga täiendav domeenikontrolleri teenus (v.a AD DS ja selleks tingimata vajalikud abiteenused, nagu DNS) lisab tsentraalsetele taristukomponentidele juurde turvanõrkusi, sh konfigureerimisvigu. Liigseid rolle ja lisandunud turvanõrkusi on võimalik kuritarvitada (nt andmete lubamatuks kopeerimiseks või muutmiseks).

2.5 Delegeeritud õiguste puudulik järelevalve ning dokumenteerimine

Kui organisatsioonis AD gruppide moodustamist ja nendele õiguste delegeerimist ei tehta süstemaatiliselt ja kavakohaselt, saavad kasutajad vajalikust ulatuslikumad pääsuõigused. Liigseid pääsuõigusi on võimalik kuritarvitada.

Vaikegruppide laialdasel kasutamisel ja nende õiguste delegeerimisel omaloodud gruppidele saadakse tulemuseks enamasti vajaminevast suuremad õigused.

2.6 Ebaturvaline autentimine

AD valdkonna autentimise pärandmehhanismid nagu näiteks NT LAN Manager (LM) ja NTLMv1, on tänapäeval ebaturvalised. Ründaja saab õigusi omandada ja kuritarvitada, ilma et tal oleks vaja kasutajaparoole teada, ära arvata või muul viisil murda.

2.7 Liigsete õigustega või ebaturvalised halduskontod

Rakendustarkvara tarnijate halduskontodele antakse tihti oma toodete testimise ja evitamise toetamiseks domeenihaldurite õigused, kuigi tööks on vaja tunduvalt kitsamaid õigusi. Halduskontodega seotud täiendavaid õigusi saavad ründajad domeenides edasiliikumiseks ära kasutada.

Nõrga turbega halduskonto tõttu (nt halduskonto on kaitstud nõrga parooliga) on võimalik domeen kompromiteerida. Näiteks saab ründaja Kerberose autentimisega taotleda TGS (*Ticket Granting Service*) autentimispileti ja halduskonto parooli jõuründega murda.

2.8 Korduvkasutatavad administraatori paroolid

Lokaalse konto kaudu saab süsteemi ka siis sisse logida, kui see ei ole domeeniga ühendatud. Kui mitmes süsteemis kasutatakse samu mandaate, saab süsteemiülem ka teistesse süsteemidesse sisse logida. See suurendab ohtu, et ründaja võib saada mõnest süsteemist suuremate õigustega domeenimandaadid ja neid kuritarvitada.

2.9 Ebaturvaline paroolide talletamine

Paroolid salvestatakse domeenikontrolleril paiknevasse AD-DS andmebaasi (ntds.dit). Sõltuvalt domeenikontrollerist võib olla kasutusel ilma „soolata“ (ingl salt) MD4 räsifunktsioon, mis ei vasta tänapäevastele krüptonõuetele. Nõrk räsifunktsioon võimaldab sõnastikründe (ingl *dictionary attack*) läbiviimist, seetõttu on volitamata juurdepääsu takistamine AD-DS salvestatud paroolidele kriitilise tähtsusega. AD DS-i laialdasest kasutusest tulenevalt on paroolide paljastamiseks loodud palju erinevaid ründevahendeid.

2.10 Ebapiisav domeenikontrollerite turve

AD-DS-i keskse andmebaasi (ntds.dit) koopia on kättesaadav kõigist domeenikontrolleritest. Samuti võib see sattuda volitamata kasutajatele kättesaadavaks tänu ebaturvalisele varundamisprotsessile. AD-DS keskse andmebaasi sattumine ründaja valdusesse võib viia paroolide paljastamise ja domeeni andmestiku kompromiteerimiseni. Samasugune oht esineb ka juhul, kui virtuaalne domeenikontroller on paigaldatud ebapiisavalt turvatud füüsilisesse virtualiseerimisserverisse. Ka virtualiseerimise halduskontodel võib olla AD DS-ile täielik juurdepääs.

2.11 AD halduri õigustes konto kasutamine domeeni klientides

Kui domeenis asuvasse serverisse või klientarvutisse logitakse sisse või kasutatakse teenuseid ülemääraselt kõrgete privileegidega kontodega, eksisteerib oht, et konkreetse serveri ründamisel on võimalik serveris säilitatud sisselogimisteabest (nt. Local Security Authority Subsystem - LSASS mälus) eraldada privilegeeritud konto pääsuandmed. Tulemusena võib

domeeni ühe serveri või kliendi kompromiteerimine viia kogu domeeni ja potentsiaalselt kogu AD metsa kompromiteerimiseni.

2.12 AD arvutiobjektide kontrollimatu lisamine Windows domeeni

AD DS vaikeseadistuse kehtides saab domeeni kasutaja lisada domeeni uusi arvuteid, vajamata selleks domeeni haldusõigusi. Lisatud IT-seadmel võivad olla lubatud pääsuõigused või funktsioonid, mida ründaja saab ära kasutada domeeni teiste komponentide ründamiseks.

IT-halduse protsess ei toimi, kuna arvutite ja IT-seadmete domeeni lisamisel ei ole järgitud kõiki ettenähtud protseduure, sh pole läbi viidud IT-süsteemide turbega seotud tegevusi.

2.13 Rakendusele omistatud õiguste ärakasutamine

Kui AD DS kontode lisamiseks kasutatakse tarkvaralisi rakendusi (nt Microsoft Exchange), on ründajal võimalik ära kasutada rakenduse turvanõrkusi, nt luua kõrgete privileegidega kasutajaid ning seeläbi rünnata tervet AD DS struktuuri (Microsoft Exchange turvanõrkus CVE-2019-0686, PrivExchange).

3 Meetmed

3.1 Elutsükkel

Kavandamine

APP.2.2.M1 AD DS kavandamine

APP.2.2.M3 Rühmapoliitikad tööks Windowsiga

Evitus

APP.2.2.M5 Domeenikontrolleri turvalisuse tõstmine

APP.2.2.M8 Turvalise kanali konfigureerimine Windowsis

APP.2.2.M9 Turvaline autentimine AD DS keskkonnas

Käitus

APP.2.2.M6 Usaldusseoste turvaline seadistamine

APP.2.2.M7 Active Directory turvaline haldus

APP.2.2.M16 AD DS kontode tugevdamine

APP.2.2.M17 AD metsa halduskontode kasutamise piiramine

APP.2.2.M18 AD arvutiobjektide domeeni lisamise piiramine

Avariivalmendus

APP.2.2.M12 Domeenikontrollerite andmete varundamine

Lisanduvad kõrgmeetmed

APP.2.2.M15 Domeenide halduse viimine eraldiseisvasse AD metsa

APP.2.2.M19 Virtualiseeritud domeenikontrollerite turvaline kasutamine

APP.2.2.M20 Organisatsiooniüksuste segmentimine

APP.2.2.M21 Mitmekihiline AD DS struktuurimudel

APP.2.2.M22 Halduskontode kasutuse ajaline piiramine

APP.2.2.M23 Pääsuõiguste ja võimalike ründevektorite regulaarne analüüs

3.2 Põhimeetmed

APP.2.2.M1 AD DS kavandamine [vastutav spetsialist]

a. AD DS struktuur vastab vähemalt Windows Server 2016 AD metsa ja domeenide funktsionaaltasemele.

b. On kehtestatud vajaduse- ja rollipõhine AD õiguste kontseptsioon ja õiguste delegeerimise kord.

c. AD DS kavandamisel on dokumenteeritud:
   - AD struktuur ning AD domeenide jaotus AD puudesse (ingl *AD tree*) ja AD metsadesse (ingl *AD forest*);
   - AD liidendusteenuse (ingl *Active Directory Federation Service*- ADFS) kasutamine ja usaldusseosed;
   - rühmapoliitikate rakendamise kontseptsioon;
   - kasutajate ja arvutite kuuluvus domeenidesse.

d. Iga domeeni kohta on otsustatud:
   - vajalikud AD objektid ja nende hierarhia;
   - arvuti- ja kasutajatüüpidest sõltuvad turvasätted;
   - rühmapoliitikad (ingl *Group Policy*);
   - vajaduspõhised AD andmete juurdepääsu subjektid ja liidesed;
   - automaatselt genereeritavad ja muud usaldusseosed.

e. Iga AD-objekti kohta dokumenteeritakse järgmised andmed:
   - nimetus ja asukoht AD puus;
   - otstarve;
   - AD-objektile kehtestatud halduspääsuõigused;
   - õiguste pärilikkuse konfiguratsioon;
   - seos rühmapoliitikaga.

APP.2.2.M3 Rühmapoliitikad tööks Windowsiga

a. Konfiguratsioonisätete (sh turvasätete) kogumiku rakendamine objektirühmadele toimub dokumenteeritud rühmapoliitikate alusel.

b. Rühmapoliitika objektide (ingl *Group Policy Object*, GPO) parameetrid määratakse AD kavandamisel koostatud rühmapoliitikate rakendamise kontseptsiooni alusel. Erandid dokumenteeritakse.

c. Kõikidele rühmapoliitika objektidele on määratud vajaduspõhised juurdepääsupiirangud.

APP.2.2.M5 Domeenikontrolleri turvalisuse tõstmine

a. Domeenikontrolleri (ingl *Domain Controller*, DC) vaikekontod on kaitstud piisavalt tugevate paroolidega ja neid kasutatakse üksnes avariikontodena.

b. Domeenikontrollerid on turvameetmetega kaitstud nii operatsioonisüsteemi kui AD tasemel.

c. Domeenikontrolleri logidele määratud suurus on vastavuses logimist ja infoturvasündmuste tuvastamist käsitlevatele poliitikatele ja eeskirjadele.

d. Domeenikontrollerisse tohivad lokaalselt sisse logida vaid domeenihaldurid. Tavakasutajate tegevused domeenikontrolleris on blokeeritud.

e. Domeenikontroller ei anna peale domeenikontrolleri jaoks vajalike standardteenuste (nt *Active Directory*, *Kerberos* ja DNS) lisaks rakendusteenuseid (nt DFS, DHCP).

f. Domeenikontroller ei jaga faile ühiskasutusse.

g. Domeenikontrollerit ei kasutata arvutitöökohana (Interneti ja väliste andmekandjate kasutamine on keelatud).

h. Muude operatsioonisüsteemide käivitamine domeenikontrolleris on blokeeritud.

i. Domeenikontrollerist tehakse regulaarselt varukoopiaid.

j. Domeenikontrolleri jaoks on koostatud taasteplaan. Ühe taastevõimalusena on võimalik domeenikontroller buutida AD taasterežiimis (ingl Directory Services Restore Mode, DSRM).

k. AD taasterežiim on kaitstud sobiva parooliga. Sellel režiimil tohib toiminguid teha ainult nelja silma põhimõtte kohaselt.

l. Domeenikontrollerit kaitstakse volitamata taaskäivituse eest.

APP.2.2.M6 Usaldusseoste turvaline seadistamine

a. AD domeenide ja AD metsade (ingl *AD forest*) usaldusseoseid analüüsitakse regulaarselt.

b. Kui domeen ei vaja kahesuunalisi usaldusseoseid teiste samasse AD metsa kuuluvate domeenidega, paigutatakse see domeen ümber eraldi AD metsa.

c. Domeenidevahelistes usaldusseostes filtreeritakse ja anonüümitakse õiguste andmed.

d. Usaldusseoste turbe tõstmiseks kasutatakse turvavõtmete (ingl *Security Identifier* - SID) põhist juurdepääsu filtreerimist.

e. Regulaarselt ajakohastatakse AD olulisemaid konfiguratsiooniparameetreid, sealhulgas vähemalt:
   - rühmapoliitika objektid;
   - usaldussuhted;
   - domeenikontrollerite struktuur;
   - dubleerimise topoloogia;
   - andmebaasi omadused;
   - domeenikontrolleris paigaldatud turvauuendid;
   - varuandmekandjad.

APP.2.2.M7 Active Directory turvaline haldus [vastutav spetsialist]

a. Teenusehalduskontosid haldavad üksnes teenusehaldurite rühma liikmed.

b. Enne konto lisamist eelmääratud AD DS kontorühma kontrollitakse, kas kõik rühmale antud õigused on kontoga seotud tegevuste jaoks tarvilikud.

c. Skeemihaldurite rühma (ingl „Schema-Admins“) lisatakse haldurid üksnes ajutiselt, skeemimuudatuste ajaks. Pärast skeemi muutmist liikmed eemaldatakse rühmast.

d. Haldurite rühmadesse (nt „Domain Admins“) mittekuuluvaid eelisõigustega kasutajakontosid luuakse ainult ajalise piiranguga ja vajaduse põhjenduse olemasolul.

e. Andmepääsude reguleerimiseks globaalses kataloogis ei kasutata domeenipõhiseid rühmi, vaid globaalseid või universaalseid rühmi.

APP.2.2.M16 AD DS kontode tugevdamine

a. AD DS vaikekontodele on seatud keerukad ja kordumatud paroolid.

b. Integreeritud „külalise“ (ingl „*Guest*“) konto on suletud.

c. Kasutajarühma „Igaüks“ (ingl „Everyone“) pääsuõigused on vajaduspõhiselt piiratud.

d. Eeliskontod (ingl *privileged accounts*) kuuluvad rühma „Protected Users“.

e. Teenusekontod kuuluvad rühma „Managed Service Accounts“.

f. Juurdepääs AD objektile *AdminSDHolder* on piiratud.

g. Kontosid kustutatakse ainult juhul, kui konto kasutamise ajaloo vaatamise ja logide hoidmise tähtajad möödunud.

APP.2.2.M17 AD metsa halduskontode kasutamise piiramine

a. Laialdaste pääsuõigustega AD metsa ja domeenide halduskontode kasutamine on lubatud ainult vajalikes IT-süsteemides.

b. Kasutajarühmadesse "Schema Admins", "Enterprise Admins" ja "Domain Admins" kuuluvad kontod saavad sisse logida ainult domeenikontrollerisse.

APP.2.2.M18 AD arvutiobjektide domeeni lisamise piiramine

a. AD arvutiobjekte (arvuteid ja teisi IT-seadmeid) saavad domeeni juurde lisada ainult vastavate halduskontode kasutajad.

3.3 Standardmeetmed

APP.2.2.M8 Turvalise kanali konfigureerimine Windowsis

a. Windowsis on tundlike andmete edastuseks konfigureeritud turvanõuetele ja rühmapoliitika parameetritele vastav turvaline ja krüpteeritud andmevahetuskanal (ingl *Secure Channel*).

b. Turvalise kanali kasutamine on aktiveeritud kõikides domeeni klientsüsteemides.

APP.2.2.M9 Turvaline autentimine AD DS keskkkonnas

a. AD keskkonnas kasutatakse võimalusel Kerberose autentimisprotokolli turvaseadistuses AES128_HMAC_SHA1 või AES256_HMAC_SHA1.

b. Ebaturvaline autentimine LM-i ja NTLMv1-i kaudu on blokeeritud. Kui pärandsüsteemide tõttu pole veel võimalik Kerberost kasutada, siis minnakse esmalt üle vähemalt NTLMv2-le ja koostatakse kava ning määratakse tähtajad Kerberose kasutuselevõtuks.

c. Domeenikontrollerite vaheline ning domeenikontrollerite ja domeeni klientarvutite vaheline SMB-liiklus on signeeritud. SMBv1 protokolli kasutamine on blokeeritud.

d. Anonüümne juurdepääs domeenikontrolleritele on blokeeritud.

e. LDAP sessioonid on signeeritud, kasutusele on võetud Channel Binding Token (CBT).

APP.2.2.M12 Domeenikontrolleri andmete varundamine

a. Domeenikontrolleri andmevarunduseks on loodud eraldi teenusehalduskontod, mille õigused kehtivad ainult ühes domeenis. Varundushaldurite rühma liikmete arv on piiratud miinimumini.

b. Pääsuõigusi *AdminSDHolder*-objektile (konteinerobjekt õiguste salvestamiseks) reguleeritakse võimalikult rangelt (vt APP.2.2.M7 *Active Directory turvaline haldus*).

c. Domeenikontrollerite andmeid varundatakse regulaarselt.

d. Domeenikontrolleritest varundatud andmeid kaitstakse samaväärsete turvameetmetega kui on kehtestatud domeenikontrollerite kaitseks.

e. Domeenikontrollerite andmete varundamise ja taaste protseduuride toimimist kontrollitakse regulaarselt. Domeenikontrollerite taastamisel eelistatakse varukoopiale teisest domeenikontrollerist andmete dubleerimist.

3.4 Kõrgmeetmed

APP.2.2.M15 Domeenide halduse viimine eraldiseisvasse AD metsa (C-I-A)

a. Domeenihalduse kontod ja IT-süsteemid on paigaldatud eraldiseisvasse AD metsa (ingl *AD forest*), millel on ühepoolne usaldusseos (töökeskkond usaldab halduskeskkonda).

b. Eelisõiguste täpseks haldamiseks ja eelistoimingute logimiseks kasutatakse täiendavaid tehnoloogiaid (nt *Privileged Access Management,* PAM).

APP.2.2.M19 Virtualiseeritud domeenikontrollerite turvaline kasutamine (C-I-A)

a. Virtualiseeritud domeenikontrollerid asuvad teistest virtuaalsetest IT-süsteemidest eraldiseisvas füüsilises hostis.

b. Virtualiseerimismasin, virtualiseerimise haldusega seotud IT-süsteemid ja virtualiseerimiskihi halduskontod asuvad virtualiseeritud domeenikontrollerist eraldiseisvas AD metsas.

APP.2.2.M20 Organisatsiooniüksuste segmentimine (C-I-A)

a. Infoturbe või muudel põhjustel sõltumatust vajavad organisatsiooniüksused (ingl *Organizational Unit* – OU) on paigutatud erinevatesse AD metsadesse.

APP.2.2.M21 Mitmekihiline AD DS struktuurimudel (C-I-A)

a. AD metsa struktuur on jagatud IT-süsteemide ja rakenduste kaitsevajadustest tulenevatesse eritasemelistesse kihtidesse.

b. Kõik AD metsa kontod, IT-süsteemid ja rakendused asuvad vajalike volituste ulatusest tulenevas AD metsa kihis.

c. Kõrgema kihi kontodel puudub õigus sisse logida madalama astme ressurssidesse.

d. Madalama kihi kontodel puudub kontroll kõrgema kihi kontode ja ressursside üle.

APP.2.2.M22 Halduskontode kasutuse ajaline piiramine (C-I-A)

a. Halduskontodele antakse haldustegevuste läbiviimiseks vajalikud volitused ainult tõendatud vajaduse alusel ja piiratud ajavahemikuks.

APP.2.2.M23 Pääsuõiguste ja võimalike ründevektorite regulaarne analüüs (C-I-A)

a. Organisatsioon analüüsib regulaarselt AD DS volitusstruktuuride ja kontode pääsuõiguste asjakohasust ja ulatust. Kui IT-süsteemi uuendi (ingl *update*) paigaldamine võib mõjutada AD DS-is määratud pääsuõigusi, tehakse vastav analüüs ka pärast IT-süsteemide uuendamist.

b. AD DS-iga integreeritud rakendustele (nt Microsoft Exchange) antud volitused on vähendatud minimaalselt vajalikuni.

c. Organisatsioon analüüsib AD DS-i konto ülevõtmisest tulenevaid AD domeeni või kogu metsa turvalisust ohustavaid ründevektoreid ning piirab nende realiseerumist.

d. Turvakriitiliste kontodega tehtavaid tegevusi seiratakse võimalike rünnete toimepaneku seisukohast.

4 Lisamaterjalid

4.1 Publikatsioonid

Lühend	Publikatsioon
[ADS]	Active Directory Security, https://adsecurity.org
[MS]	https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/active-directory-domeen-services https://docs.microsoft.com/de-de/previous-versions/windows/it-pro/windows-server-2003/cc759073(v=ws.10) https://docs.microsoft.com/de-de/previous-versions/windows/it-pro/windows-server-2003/cc755321(v=ws.10)

4.2 Rühmapoliitika turvasätete näidis

Allpool on esitatud turvasätted, mida saab kasutada rühmajuhendi turvasätete alusena. Esitatud väärtused tuleb igal juhul kohandada kohalike tingimustega. Rühmapoliitika kontseptsiooni raames jaotatakse üksikud väärtused erinevate rühmapoliitika objektide (GPO-de) vahel ära ja kohandatakse kasutusotstarbe kohaselt (nt serveri GPO, tööjaama GPO). Selle tulemuseks võivad olla üksikute kirjete erinevad väärtused.

Paroolijuhend

- paroolide ajaloo nõue: 6 salvestatud parooli
- paroolid peavad vastama keerukusnõuetele: aktiveeritud
- paroolide salvestamine iga domeenikasutaja jaoks reversiivse krüpteerimisega: desaktiveeritud
- parooli maksimaalne vanus: 180 päeva
- parooli minimaalne pikkus: 15 märki

· parooli minimaalne vanus: 1 päev

Konto blokeerimise juhend

· konto blokeerimise lävi: 3 ebaõnnestunud sisselogimiskatset

· konto blokeerimise kestus: 0 (märkus: konto on blokeeritud, kuni administraator blokeeringu tühistab)

· konto blokeerimisloenduri lähtestamiseks peab mööduma: 30 minutit

Kerberose juhend

· kasutaja sisselogimise piirangute kohustus: aktiveeritud

· kasutajapileti maksimaalne kehtivusaeg: 8 tundi

· teenusepileti maksimaalne kehtivusaeg: 60 minutit

· maksimaalne tolerants arvuti takti sünkroniseerimiseks: 5 minutit

· maksimaalne aeg, mille jooksul saab kasutajapiletit uuendada: 1 päev

Seirejuhend

· *Active Directory* andmepääsude seire: edukas, ebaõnnestunud

· sisselogimissündmuste seire: edukas, ebaõnnestunud

· sisselogimiskatsete seire: edukas, ebaõnnestunud

· kontode halduse seire: edukas, ebaõnnestunud

· objektide pääsukatsete seire: ebaõnnestunud

· protsesside toimimise seire: seiret ei toimu

· õiguste kasutamise seire: ebaõnnestunud

· juhendite muutmise seire: edukas, ebaõnnestunud

· süsteemisündmuste seire: edukas, ebaõnnestunud

Kasutajaõiguste määramine

· teenusena sisselogimine: määratud, kuid tühi

· süsteemiaja muutmine: administraator

· ajaplaneerimise prioriteedi tõstmine: administraator

· kvootide tõstmine: administraator

· sisselogimine pakktöötlustellimusena: määratud, kuid tühi

· pakktöötlustellimusena sisselogimisest keeldumine: määramata

· teenusena sisselogimisest keeldumine: määramata

· juurdepääs võrku sellest arvutist: igaüks, administraator, autenditud kasutaja, varunduse operaator

· läbiotsitava kontrollimise vahelejätmine: igaüks

· programmide silumine: määramata

· kasutamine operatsioonisüsteemi osana: määratud, kuid tühi

· arvuti eemaldamine dokist: administraator

- arvuti- ja kasutajakontode usaldamine delegeerimisotstarbeks: administraator
- volitustõendi asendamine protsessitasandil: määratud, kuid tühi
- saalimisfaili loomine: administraator
- süsteemi jõudluse profiili loomine: administraator
- üksikprotsessi profiili loomine: administraator
- volitustõendi objekti loomine: määratud, kuid tühi
- püsivalt ühiskasutusse antud objektide loomine: määratud, kuid tühi
- kaugsüsteemist juhitav väljalülitamine: administraator
- turvakontrollide loomine: määratud, kuid tühi
- süsteemi väljalülitamine: administraator
- tööjaamade lisamine domeeni: määratud, kuid tühi
- seadmedraiverite lisamine ja eemaldamine: administraator
- kohalik sisselogimine: administraator, varunduse operaator
- kohalikust sisselogimisest keeldumine: määramata
- failide ja kataloogide varundamine: varunduse operaator
- andmebaasi lehekülgede blokeerimine: määratud, kuid tühi
- kataloogiteenuse andmete sünkroniseerimine: määratud, kuid tühi
- failide ja objektide omandamine: administraator
- püsivara keskkonna muutujate muutmine: administraator
- seire- ja turvalogide haldamine: administraator
- failide ja kataloogide taastamine: administraator
- juurdepääsu keelamine võrgust arvutile: määramata

Turvamehhanismid

- administraatori ümbernimetamine: määramata
- kasutajalt parooli muutmise nõue enne parooli aegumist: 7 päeva
- printeridraiverite installimise keelamine kasutaja jaoks: aktiveeritud
- eelmiste sisselogimiste vahesalvestamise arv (kui domeenikontroller ei ole saadaval): 0 sisselogimist
- virtuaalse põhimälu saalimisfaili kustutamine süsteemi väljalülitamise korral: aktiveeritud
- NTFS-irdkandjate väljutamise lubamine: administraator
- kasutaja automaatne väljalogimine, kui sisselogimisaeg on ületatud (lokaalne): aktiveeritud
- kasutaja automaatne väljalogimine pärast sisselogimisaja lõppemist: aktiveeritud
- kliendi side digitaalne signeerimine (alati): desaktiveeritud
- kliendi side digitaalne signeerimine (võimaluse korral): aktiveeritud
- varundus- ja taasteõiguste kasutamise kontrollimine: desaktiveeritud
- külaliskonto ümbernimetamine: määramata

- süsteemi väljalülitamise lubamine ilma sisselogimiseta: desaktiveeritud
- LAN-i halduse autentimistasand: saada ainult NTLMv2-vastuseid \ keeldu LM-st
- tegevuseta ajavahemik kuni sessiooni lõpetamiseni: 15 minutit
- viimast kasutajanime ei näidata sisselogimisdialoogis: aktiveeritud
- teade kasutajale, kes soovib sisse logida: määramata
- teate pealkiri kasutajale, kes soovib sisse logida: määramata
- serveriside digitaalne signeerimine (alati): desaktiveeritud
- serveriside digitaalne signeerimine (võimaluse korral): aktiveeritud
- serveri operaatoritele plaanitud ülesannete käivitamise lubamine (ainult domeenikontrollerite jaoks): määramata
- turvaline kanal: turvalise kanali andmete digitaalne signeerimine (võimaluse korral): aktiveeritud
- turvaline kanal: turvalise kanali andmete digitaalne krüpteerimine (võimaluse korral): aktiveeritud
- turvaline kanal: turvalise kanali andmete digitaalne signeerimine või krüpteerimine (alati): aktiveeritud (märkus: sel juhul ei ole aegunud süsteemid sellega ühilduvad)
- turvaline kanal: tugeva seansivõtme nõue: aktiveeritud (märkus: sel juhul ei ole vananenud süsteemid sellega ühilduvad)
- globaalsete süsteemiobjektide (nt sümbolipõhiste otseteede) standardõiguste tugevdamine: aktiveeritud
- nõude CTRL+ALT+DEL desaktiveerimine sisselogimiseks: desaktiveeritud (märkus: st CTRL+ALT+DEL on vajalik)
- süsteemi kohene väljalülitamine, kui turvakontrolle ei saa enam logida: desaktiveeritud
- arvutikonto parooli süsteemihoolduse keelamine: desaktiveeritud
- krüpteerimata parooli saatmine, et luua ühendus kolmandate tootjate SMB-serveritega: desaktiveeritud
- tegutsemine signeerimata failide installimise korral (v.a draiverid): hoiata, kuid võimalda installimist
- tegutsemine signeerimata draiverite installimise korral: hoiata, kuid võimalda installimist
- tegutsemine kiipkaartide eemaldamise korral: arvuti sulgemine
- anonüümsete ühenduste täiendavad piirangud: andmepääsu keelamine, kui puudub selgesõnaline anonüümne põhjendus
- taastekonsool: automaatse administraatori sisselogimiste lubamine: desaktiveeritud
- taastekonsool: diskettide kopeerimise ning kõigile ketastele ja kataloogidele andmepääsu lubamine: desaktiveeritud
- CD-ROM-i draividele andmepääsu piiramine lokaalselt sisseloginud kasutajatele: aktiveeritud
- disketidraividele andmepääsu piiramine lokaalselt sisseloginud kasutajatele: aktiveeritud
- globaalsetele süsteemiobjektidele andmepääsu kontrollimine: desaktiveeritud

Sündmuste logi

- rakenduste logi säilitamine: määratama
- rakenduste logi säilitusmeetod: vajaduse korral sündmuste ülekirjutamine
- turvalogi säilitusmeetod: vajaduse korral sündmuste ülekirjutamine (märkus: suure kaitsetarbega valdkonnas valitakse järgmine säte: sündmuste ülekirjutamise keelamine (logi käsitsi puhastamine))
- süsteemilogi säilitusmeetod: vajaduse korral sündmuste ülekirjutamine
- külaliskonto andmepääsu piiramine rakenduste logile: aktiveeritud
- külaliskonto andmepääsu piiramine turvalogile: aktiveeritud
- külaliskonto andmepääsu piiramine süsteemilogile: aktiveeritud
- rakenduste logi maksimaalne maht: 30 080 kilobaiti
- turvalogi maksimaalne maht: 100 992 kilobaiti
- süsteemilogi maksimaalne maht: 30 080 kilobaiti
- turvalogi säilitamine: määramata
- süsteemi väljalülitamine turvalogi maksimaalse mahu saavutamise korral: desaktiveeritud (märkus: aktiveerida suure kaitsetarbega süsteemides)
- süsteemilogi säilitamine: määramata

APP.2.3 OpenLDAP

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed *OpenLDAP*il põhineva kataloogiteenuse turvaliseks kasutamiseks ja töödeldava teabe nõuetekohaseks kaitseks.

1.2 Vastutus

OpenLDAPi meetmete täitmise eest vastutab IT-talitus.

1.3 Piirangud

Moodulis lähtutakse *OpenLDAP* versioonist 2.4. Üldised turbesoovitused kataloogiteenuse jaoks on esitatud moodulis APP.2.1 *Kataloogiteenus üldiselt.*

OpenLDAP rakendamine peab toimuma kooskõlas järgmiste moodulitega: ORP.4 *Identiteedi- ja õiguste haldus,* OPS.1.1.3 *Paiga- ja muudatuste haldus,* CON.3 *Andmevarunduse kontseptsioon,* OPS.1.2.2 *Arhiveerimine*, OPS.1.1.5 *Logimine* ja OPS.1.1.2 *IT-süsteemide haldus*.

Haldusprotsesse (nt andmete varundamine, logimine ja paigahaldus) käsitletakse üksnes ulatuses kuivõrd need on seotud O*penLDAP*i erisustega.

2 Ohud

2.1 *OpenLDAP*i kavandamise puudumine või puudulikkus

Kui tagasüsteemid või seotud parameetrid valitakse vääralt, mõjutavad need soovimatult *OpenLDAP*i võimaldatavaid funktsioone.

Kui *OpenLDAP*i tagasüsteem (ingl *backend*) ja selle kataloogid on vääralt seadistatud, võib see *OpenLDAPi* funktsionaalsust tugevalt mõjutada.

*OpenLDAP*i funktsioneerimist takistab ülekatete (ingl *overlay*) puudulik kavandamine. Näiteks kui Slapd-serveri silumisfunktsiooni ja ülekatete revisjoni- ja pääsulogi plaanitakse piisamatult, siis ei logita kataloogiteenuse andmepöörduseid või seda tehakse puudulikult.

Kui *OpenLDAP*i andmete salvestamiseks kasutatakse võrgufailisüsteemi NFS (hajus failisüsteem), ei saa *OpenLDAP*i failifunktsioone (nt lukustusfunktsioon, mis blokeerib kataloogiteenuse andmebaasi, kui mitu kasutajat soovivad samaaegselt andmebaasi kirjutada) kasutada.

Kõik rakendused ei pruugi *OpenLDAP*iga ühilduda. Ka *OpenLDAP* versioonide vahel võivad tekkida ühilduvusprobleemid.

2.4 *OpenLDAP*i autonoomse ja *online*-juurdepääsu puudulik lahusus

*OpenLDAP*i *online*-juurdepääsuks kasutatakse protokolle LDAP ja slapd. Autonoomse süsteemi korral ühendutakse andmebaasifailidega otse või redigeeritakse ja eksporditakse LDIF faili. Autonoomse ja *online* juurdepääsu töörežiimide väär kasutamine tekitab erinevaid veaolukordi. Näiteks võib andmebaas taastamisel osutuda *OpenLDAPi* jaoks seostamatuks ja seda ei saa enam kasutada.

3 Meetmed

3.1 Elutsükkel

Kavandamine

APP.2.3.M1 *OpenLDAP*i rakendamise kavandamine

Evitus

APP.2.3.M3 *OpenLDAP*i turvaline konfiguratsioon

APP.2.3.M4 *OpenLDAP*i andmebaasi turvaline konfigureerimine

APP.2.3.M5 *OpenLDAP*i pääsuõiguste turvaline haldus

APP.2.3.M8 *OpenLDAP*i atribuutide piiramine

APP.2.3.M9 *OpenLDAP*i sektsioonimine ja dubleerimine

APP.2.3.M11 *OpenLDAP*i käituskeskkonna kitsendamine

Käitus

APP.2.3.M6 Turvaline autentimine *OpenLDAP*is

APP.2.3.M10 *OpenLDAP*i turvaline ajakohastamine

3.2 Põhimeetmed

APP.2.3.M1 OpenLDAPi rakendamise kavandamine

a. *OpenLDAP*i kavandamisel on arvestatud klientrakendustega, mida hakatakse kasutama ja mida on vaja tulevikus toetada.

b. *OpenLDAP*i kavandamisel arvestatakse vähemalt järgmist:
   - *OpenLDAP*i versiooni valik ja nõuded;
   - jõudlusnõuded;
   - rakenduste (nt aadressiraamat) konfigureerimine ja integreerimine *OpenLDAP*iga;
   - *OpenLDAP*i funktsioneerimiseks vajalikud tagasüsteemid (nt andmebaas) ja nende piirangud;
   - konfigureerimismeetodi valik (staatiline või veebikonfiguratsioon);
   - ülekatete piirangud ja ülekatete õige järjestuse tagamine.

APP.2.3.M3 OpenLDAPi turvaline konfiguratsioon

a. Slapd-server konfigureerimine (kas *slapd.conf* konfiguratsioonifaili või *slapd-config* veebikonfiguratsiooniga) on teostatud turvaliselt, konfigureerimiseks vajalikud haldusõigused on vaid volitatud kasutajatel.

b. *OpenLDAP*i konfigureerimisseadete (direktiivide) väärtusi kontrollitakse ja vajadusel kohandatakse enne nende esmast jõustamist.

c. Konfigureerimisel on arvestatud *OpenLDAP*i tagasüsteeme ja ülekatteid.

d. *OpenLDAP*i otsingupäringute jaoks on määratud sobivad aja- ja mahupiirangud.

e. Pärast iga muudatust Slapd-serveri konfiguratsioon kontrollitakse ja dokumenteeritakse.

APP.2.3.M4 OpenLDAPi andmebaasi turvaline konfigureerimine

a. Juurdepääs Slapd-serverile ja andmebaasifailidele on vaid selleks ette nähtud kontodel.

b. *OpenLDAP*i poolt kasutatava andmebaasi vaikeseadeid on kohandatud vastavalt kaitsetarbele.

APP.2.3.M5 OpenLDAPi pääsuõiguste turvaline haldus

a. Pääsuloendis on kasutaja iga tegevus hõlmatud asjakohase direktiiviga, mis seob kasutaja, talle lubatud sihtobjektid ja kasutamisõiguse ulatuse.

b. Pääsuloendite määramisel on arvesse võetud, et *OpenLDAPi* andmebaasidirektiivid (ingl *database directives*) kirjutavad üldised direktiivid (ingl gl*obal directives*) üle.

APP.2.3.M6 Turvaline autentimine OpenLDAPis

a. Kataloogiteenuse kasutajate eristamiseks on nõutav kasutajate autentimine, anonüümne juurdepääs on piiratud konfiguratsioonidirektiiviga *disallow bind_anon.*

b. Slapd-serveri ja sidepartneri vahelised autentimisandmed on krüpteeritud.

c. Serverid ja klientarvutid salvestavad paroole üksnes räsikujul, kasutades piisavalt murdmiskindlat algoritmi.

3.3 Standardmeetmed

APP.2.3.M8 OpenLDAPi atribuutide piiramine

a. *OpenLDAP*i atribuutide piiramiseks, väärtuste unikaalsuse ja viiteatribuutide tervikluse tagamiseks on kasutatud ülekatteid.

b. *OpenLDAP*i ülekatete kaudu seatud atribuudipiiranguid on rakendatud üksnes kasutajaandmetele.

APP.2.3.M9 OpenLDAPi sektsioonimine ja dubleerimine

a. OpenLDAP'i sektsioonimisel ja dubleerimisel on arvestatud turvavajadusi.

b. Kataloogiteenuse sektsioonimine alampuudeks on kavandatud ja ellu viidud vastavalt meetmele APP.2.1.M8 *Kataloogiteenuse sektsioonimine.*

c. Andmete sünkroniseerimine serverite vahel tehakse dubleerimisega. Dubleerimisrežiim on valitud vastavalt võrguühendusele ja käideldavusnõuetele.

APP.2.3.M10 OpenLDAPi turvaline ajakohastamine

a. Enne uue versiooni paigaldamist analüüsitakse, kas ja kuidas uus versioon mõjutab kasutusele võetud tagasüsteemide, tarkvarasõltuvuste ja ülekatete toimimist. Pärast uue versiooni paigaldamist testitakse tagasüsteemide ja ülekatete toimimist.

b. Haldurite endi koostatud skriptide toimimist kontrollitakse enne uue versiooni paigaldamist tootmiskeskkonda.

c. Pärast *OpenLDAP* ajakohastamist kontrollitakse konfiguratsiooni ja pääsuõigusi.

APP.2.3.M11 OpenLDAPi käituskeskkonna kitsendamine

a. Slapd-serveri tööks vajalikud konfiguratsioonifailid ja andmebaasid on piiratud käituskataloogiga.

b. Kui slapd-server on paigutatud konteinerisse, rakendatakse lisaks turvameetmeid moodulist SYS.1.6 *Konteinerdus*.

c. Kui slapd-server on paigutatud eraldi serverisse, on serveris kasutatud piisavaid tugevdusmeetmeid (ingl *hardening*).

3.4 Kõrgmeetmed

Selles moodulis kõrgmeetmed puuduvad.

APP.3: Võrguteenused

APP.3.1 Veebirakendused

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed veebirakenduste ja veebiteenuste turvaliseks tööks ning töödeldava teabe kaitseks.

1.2 Vastutus

„Veebirakendused“ meetmete täitmise eest vastutab IT-talitus.

Lisavastutajad
Hankeosakond, infoturbejuht.

1.3 Piirangud

Üldised meetmed tarkvara hankimiseks esitatakse moodulis APP.6 *Tarkvara üldiselt*.

Veebiserveri turbega seotud meetmed, sh veebisisu toimetamine ja avariihaldus, esitatakse moodulis APP.3.2 *Veebiserver.*

Veebirakenduste arendust käsitletakse moodulis CON.10 *Veebirakenduste arendus*.

Veebirakenduste logimist käsitletakse moodulis OPS.1.1.5 *Logimine*.

2 Ohud

2.1 Turvasündmuste logimise puudulikkus

Veebirakenduse turvasündmuste ebapiisaval logimisel ei ole võimalik hiljem turvasündmusi tuvastada ja nende tekkepõhjuseid välja selgitada. Ründed (nt veebirakenduse lubamatud konfiguratsioonimuudatused) võivad jääda märkamata. Puudulik logimine muudab keerukamaks ka nõrkuste tuvastamise ja kõrvaldamise.

2.2 Liigse taustainfo avaldamine veebirakendustes

Veebisaidid ja andmed, mida genereeritakse ja edastatakse veebirakenduste kaudu, võivad sisaldada informatsiooni taustsüsteemide kohta (nt IT-komponentide ja operatsioonisüsteemide versioonide andmed). See teave võib ründaja jaoks veebirakenduse sihtründe tegemise lihtsamaks muuta.

2.3 Veebirakenduse väärkasutus automatiseeritud lahendustega

Veebirakenduse funktsioonide kasutamise automatiseerimine võimaldab ründajal lühikese aja jooksul teha arvukalt ründekatseid. Näiteks korduva automaatse sisselogimisega on võimalik proovida ära arvata kehtivaid kasutajanime ja parooli kombinatsioone (jõurünne). Kui veebirakendus annab tagasisidet kasutajanime olemasolu kohta, on võimalik koostada kehtivate kasutajanimede loendeid. Korduvat ressursimahukate funktsioonide poole pöördumist (nt keerukad andmebaasipäringud) saab rakendustasemel ära kasutada ummistusrünnete tegemiseks.

2.4 Veebirakenduse autentimise ja seansihalduse puudulikkus

Veebirakenduse teatud funktsioone tohivad kasutada ainult selleks autoriseeritud kasutajad. Kui ründajal õnnestub puuduliku seansihalduse tõttu kindlaks teha autoriseeritud kasutaja seansi identifikaator, võib ta sellega saada juurdepääsu veebirakenduse kaitstud funktsioonidele ja ressurssidele. Seansipetteründe korral laseb ründaja kõigepealt veebirakendusel määrata seansi identifikaatori ja seejärel edastatakse see mõnele volitatud kasutajale (nt e-posti lingiga). Kui volitatud kasutaja kasutab seda linki ja veebirakenduses end ründaja edastatud seansi identifikaatoriga autendib, saab ka ründaja seejärel temale teadaoleva seansi identifikaatoriga veebirakendust rünnatud kasutaja turvakontekstis kasutada.

3 Meetmed

3.1 Elutsükkel

Kavandamine

APP.3.1.M8 Veebirakenduse turvaline arhitektuur

Soetus

APP.3.1.M9 Veebirakenduste hankimise kord

Evitus

APP.3.1.M4 Andmete ja sisu kasutamise piiramine

APP.3.1.M7 Kaitse veebirakenduste automatiseeritud kasutamise eest

APP.3.1.M11 Turvaline ühendus tagasüsteemidega

APP.3.1.M12 Veebirakenduste turvaline konfigureerimine

APP.3.1.M21 Veebirakenduste turvaline HTTP-konfiguratsioon

Käitus

APP.3.1.M1 Veebirakenduste autentimine

APP.3.1.M14 Konfidentsiaalsete andmete kaitse

APP.3.1.M22 Veebirakenduste läbivaatus ja läbistustestimine

Lisanduvad kõrgmeetmed

APP.3.1.M20 Veebitulemüürid

3.2 Põhimeetmed

APP.3.1.M1 Veebirakenduste autentimine

a. Veebirakenduse ressurssidele juurdepääs võimaldatakse ainult kasutaja autentimise kaudu.

b. Autentimisviisid on turvalised ja nende valik on dokumenteeritud.

c. Veebirakenduse kasutaja autentimisandmete klientarvutisse salvestamine saab toimuda ainult veebirakenduse kasutaja üheselt mõistetava nõusoleku alusel.

d. Veebirakenduses on määratud ebaõnnestunud sisselogimiskatsete lubatud arv. Pärast ebaõnnestunud sisselogimiskatsete lubatud arvu ületamist kasutaja juurdepääs tõkestatakse määratud ajaks.

APP.3.1.M4 Andmete ja sisu kasutamise piiramine

a. Veebirakendus väljastab kasutajatele üksnes ettenähtud ja lubatavaid andmeid ja sisu.

b. Veebirakenduse failide üleslaadimise funktsioon ning failide käivitamisõigused on piiratud. Kasutaja saab salvestada faile ainult ettemääratud asukohta.

c. Edasisuunamise funktsionaalsus kasutajatele on veebirakenduses piiratud.

d. Veebirakendusest edasisuunamise sihtkohad asuvad usaldusväärses domeenis. Kasutaja lahkumisel usaldatavast domeenist kasutajat teavitatakse.

APP.3.1.M7 Kaitse veebirakenduste automatiseeritud kasutamise eest

a. Veebirakendus on kaitstud volitamata automatiseeritud juurdepääsu eest.

b. Veebirakenduse RSS-söödete (ingl *RSS feed*) või teiste automatiseeritud funktsioonide olemasolul arvestatakse neid turvamehhanismide seadistamisel.

APP.3.1.M14 Konfidentsiaalsete andmete kaitse

a. Konfidentsiaalseid andmeid kaitstakse nende edastamisel piisavalt tugeva krüpteeringuga. Ka ühendusvigade korral ei kasutata krüpteeritud kanali asemel krüpteerimata kanalit.

b. Klientarvutisse ei salvestata ega ajutiselt puhverdata tundlikke andmeid.

c. Vormidel olevaid konfidentsiaalseid andmeid ei hoita brauseris avateksti kujul.

d. Veebirakenduse pääsuandmeid on serveris kaitstud piisavalt tugeva krüpteeringuga. Parooliandmetest hoitakse serveris ainult parooli räsi.

e. Veebirakenduse lähtekoodi kaitstakse lubamatu juurdepääsu eest.

3.3 Standardmeetmed

APP.3.1.M8 Veebirakenduse turvaline arhitektuur [hankeosakond, infoturbejuht]

a. Veebirakenduse kavandamisel on arvestatud turvaaspekte. Veebirakenduse turvamehhanismide kavandamisel on arvestatud nende võimekusega ka tulevikuvaates.

b. Võrguarhitektuur on mitmekihiline. Veebi-, rakenduse- ja andmekihi turvamehhanismid on üksteisest eraldatud.

c. Tarkvaraarhitektuuri kavandamisel on arvestatud, milliste komponentide jaoks milliseid turvamehhanisme rakendatakse, kuidas veebirakendus on olemasolevasse taristusse integreeritud ning milliseid krüpteerimisfunktsioone ja -protseduure kasutatakse.

d. Veebirakenduse tarkvaraarhitektuur toetab ja sidustab organisatsiooni äriprotsesse.

e. Veebirakenduse tarkvaraarhitektuur koos kõikide komponentide ja sõltuvustega on dokumenteeritud. Dokumentatsioonis on välja toodud ka rakendusevälised, kuid rakenduse tööks vajatavad komponendid.

APP.3.1.M9 Veebirakenduste hankimise kord [hankeosakond]

a. Veebirakenduse komponentide hankimiseks on kehtestatud nõuded tootele ja kokku lepitud hindamisskaala.

b. Veebirakenduste hankimisel on lisaks tarkvara hankimise üldistele aspektidele arvestatud vähemalt järgmist:
   - veebirakenduse sisendi valideerimine ja väljundi kodeerimine;
   - turvalised autentimisprotseduurid;
   - turvaline sessioonihaldus;
   - turvaliste krüptograafiliste mehhanismide kasutamine;
   - kasutajate pääsuõiguste haldus;
   - turvaline andmetalletus serveris;
   - piisav sündmuste logimine;
   - turvapaikade kättesaadavus ja paigaldamine;
   - kaitse veebirünnete vastu.

c. Kui veebirakenduse töötab välja teenuseandja, tagatakse teenuseandja turvanõuete rakendamine ja organisatsiooni juurdepääs lähtekoodile.

APP.3.1.M11 Turvaline ühendus tagasüsteemidega

a. Juurdepääs tagasüsteemidele on võimalik üksnes määratud liideste ja süsteemide kaudu ja minimaalselt vajalike õigustega.

b. Andmeliiklus kasutajate ja veebirakenduste või rakenduste ja teiste teenuste või taustsüsteemide vahel on reguleeritud turvalüüsidega.

c. Välisühenduse andmeliiklus on krüpteeritud ja toimub ainult autenditud sihtkohtade vahel.

APP.3.1.M12 Veebirakenduste turvaline konfigureerimine

a. Veebirakendus on konfigureeritud nii, et selle ressurssidele ja funktsioonidele on juurdepääs võimalik ainult määratud turvaliste sidekanalite kaudu.

b. Juurdepääs ebavajalikele ressurssidele ja funktsioonidele on veebirakenduses blokeeritud ja tarbetud HTTP-meetodid desaktiveeritud.

c. Küpsistele (ingl c*ookie*) on seatud atribuudid s*ecure ja SameSite.* Seansivõtme küpsisel on seatud atribuut *httponly*.

d. Konfigureerimisel on võimalik seadistada ja piirata järgmisi veebirakenduse omadusi:
   - märgikoodide (ingl *character encoding)* ja automaattõlke kasutamine;
   - üleliigse turvateabe avaldamist veateadetes ja vastussõnumites;
   - konfiguratsioonifailide hoidmine väljaspool juurkataloogi;
   - ebaõnnestunud juurdepääsukatsete lubatav arv.

APP.3.1.M21 Veebirakenduste turvaline HTTP-konfiguratsioon

a. Kaitseks klõpsurööv-rünnete (ingl *clickjacking*) ja skriptisüsti (ingl *cross-site scripting*) eest on veebirakenduse HTTP-vastusepäises säte *X-FRAME-OPTIONS: deny*.

b. Veebirakendus toetab brauseri sisuturbe standardit (Content Security Policy- CSP).

APP.3.1.M22 Veebirakenduste läbivaatus ja läbistustestimine [infoturbejuht]

a. Veebirakenduste turvalisust kontrollitakse ja testitakse regulaarselt.

b. Läbivaatuste ja läbistustestimiste tulemused dokumenteeritakse. Neid käsitletakse konfidentsiaalsetena ja säilitatakse turvaliselt.

c. Lahknevusi käsitletakse ja tulemustest teavitatakse infoturbejuhti.

3.4 Kõrgmeetmed

APP.3.1.M20 Veebitulemüürid (C-I-A)

a. Andmete filtreerimiseks kõrgematel protokollitasemetel kasutatakse veebitulemüüre (*ingl web application firewall* -WAF).

b. Veebitulemüüri konfiguratsioon on kohandatud kaitstava veebirakendusega.

c. Pärast veebirakenduse uuendamist kontrollitakse ja vajadusel muudetakse veebitulemüüri konfiguratsiooni.

4 Lisateave

Lühend	Publikatsioon
[ASVS]	OWASP Application Security Verification Standard v.4.0.3 https://github.com/OWASP/ASVS/tree/master/4.0/en

APP.3.2 Veebiserver

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed veebiserveri ja veebiserveri kaudu juurdepääsetava teabe kaitseks.

1.2 Vastutus

Veebiserveri meetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Vastavushaldur, vastutav spetsialist, haldusosakond.

1.3 Piirangud

Veebiserveri tarkvara majutava serveri turvaaspekte käsitletakse mooduligrupi SYS *IT-süsteemid* vastavates moodulites (vt SYS.1.1 *Server üldiselt* , SYS.1.3 *Linuxi ja Unixi server* või SYS.1.2.2 *Windows Server 2012*).

Veebiserveri integreerimine võrgu arhitektuuri ja tulemüüriga kaitsmine on esitatud moodulites NET.1.1 *Võrgu arhitektuur ja lahendus* ja NET.3.2 *Tulemüür*.

Dünaamilist sisu ja HTML-i täiendavaid funktsioone käsitleb moodul APP.3.1 *Veebirakendused*.

Krüptovõtmete turvalist haldust käsitleb moodul CON.1 *Krüptokontseptsioon*.

Kui veebiserveri puhul kasutatakse väliseid teenuseid, rakendatakse lisaks meetmeid moodulist OPS 2.3 *Väljasttellimine*.

Veebiserveri sündmuste logimist käsitletakse moodulis OPS.1.1.5 *Logimine*.

2 Ohud

2.1 Mainekaotus

Kui ründajatel õnnestub veebisaiti manipuleerida ja seda ümber kujundada ehk sodida (ingl *defacement*), võib kahjustuda organisatsiooni maine. Vale teabe (nt eksitava tootekirjelduse või poliitiliselt motiveeritud avalduse) avaldamine võib kaasa tuua organisatsiooni mainekaotuse avalikkuse ees.

2.2 Veebiserveri manipuleerimine

Ründaja, saades juurdepääsu veebiserverile, saab selles olevaid faile manipuleerida, muuta veebiserveri konfiguratsiooni ja veebisisu, käivitada täiendavaid teenuseid ning installida

kahjurvara. Ründaja võib näiteks kasutajatele allalaadimiseks mõeldud failid asendada kahjurvara sisaldavate failidega. Kui kahjurvara levitamiseks kasutatakse organisatsiooni veebiserverit, võib juhtuda, et veebiserveri usaldusväärsuse tase reputatsiooniteenustes langeb ja veebilehed ei ole enam kasutajaile kättesaadavad.

2.3 Hajus ummistusrünne

Ründajal on võimalik manipuleeritud serverit kasutada hajusa ummistusründe (ingl *distributed denial-of-service – attack,* DDoS) korraldamiseks. Hajusa ummistusründe tõttu võib veebiserver osaliselt või ka täielikult rivist välja langeda. Kasutaja jaoks on siis veebisait üksnes väga vaevaliselt kasutatav või juurdepääsematu. Paljude organisatsioonide (nt kellel on veebipoed) jaoks muutub selline tõrge kiiresti ärikriitiliseks.

2.4 Konfidentsiaalsete andmete leke

Paljudes veebiserverites kasutatakse endiselt aegunud krüpteerimisprotseduure, nagu näiteks RC4 ja SSL. Piisamatu autentimine ja nõrk krüpteerimine võivad viia selleni, et ründajad saavad klientarvutite ja serverite või serverite vahelist andmevahetust pealt kuulata ja muuta.

2.5 Õigusaktide nõuete rikkumine

Õigusaktide nõuete (eelkõige andmekaitse alaste) rikkumisel võivad kaasneda rahaline ja mainekahju. Samuti on oht rikkuda veebiserveri sisuga autoriõigusi (nt kui kasutatakse pilte, mille kasutamiseks puuduvad õigused).

2.6 Veebiserveri tõrgete kõrvaldamise puudulikkus

Veebiserveri töö ajal tekkivad tõrked mõjutavad veebiserveri käideldavust. Veebiserveri sisu edastamine on häiritud, kasutaja toimingud jäävad pooleli ning turvamehhanismid võivad lakata töötamast. Kui tõrgete juurpõhjustega järjepidevalt ei tegeleta, siis probleemid andmete turvalisusega jätkuvad.

3 Meetmed

3.1 Elutsükkel

Kavandamine

APP.3.2.M7 Veebisisu õiguspärasus

APP.3.2.M8 Veebiserveri rakendamise kava

APP.3.2.M9 Veebiserveri turvapoliitika

Soetus

APP.3.2.M10 Sobiv veebimajutaja

Evitus

APP.3.2.M1 Veebiserveri turvaline konfigureerimine

APP.3.2.M2 Veebiserveri failide kaitse

APP.3.2.M20 Kontaktisiku määramine

Käitus

APP.3.2.M3 Failide üles- ja allalaadimise turve

APP.3.2.M4 Sündmuste logimine

APP.3.2.M5 Autentimine

APP.3.2.M11 Krüpteerimine TLS abil

APP.3.2.M12 Vigade ja veateadete nõuetekohane käsitlus

APP.3.2.M13 Veebirobotite juurdepääsu piiramine

APP.3.2.M14 Tervikluse kontroll ja kaitse kahjurvara eest

APP.3.2.M16 Läbistustestimine ja läbivaatus

Lisanduvad kõrgmeetmed

APP.3.2.M15 Liiasus

APP.3.2.M18 Kaitse ummistusrünnete eest

3.2 Põhimeetmed

APP.3.2.M1 Veebiserveri turvaline konfigureerimine

a. Pärast veebiserveri installimist on loodud ja dokumenteeritud turvaline aluskonfiguratsioon.
b. Veebiserveri protsessi käitatakse minimaalsete õigustega kasutajakontoga.
c. Operatsioonisüsteemi poolse toe olemasolul käitatakse veebiserverit kapseldatud keskkonnas. Kui operatsioonisüsteem kapseldamist ei toeta, käitatakse igat veebiserverit eraldi virtuaalserveris või füüsiliselt eraldiseisvas serveris.
d. Veebiserveri teenusel puuduvad liigsed kirjutusõigused.
e. Veebiserveri tarbetud moodulid ja funktsioonid on desaktiveeritud.

APP.3.2.M2 Veebiserveri failide kaitse

a. Veebiserveri failid (eelkõige skriptid ja konfiguratsioonifailid) on kaitstud lubamatu lugemise ja muutmise eest.
b. Veebirakendustel on juurdepääs üksnes ettenähtud kataloogipuus (veebi juurkataloogis) olevatele failidele. Väljaspool veebikataloogi paiknevaid ressursse ei saa linkida ega nendega ühenduda. Katalooge esitavad funktsioonid on desaktiveeritud.
c. Failid, mida ei ole lubatud muuta, on kirjutuskaitsega.
d. Konfidentsiaalseid andmeid edastatakse ja salvestatakse krüpteeritult.

APP.3.2.M3 Failide üles- ja allalaadimise turve

a. Veebiserveris avaldatud faile kontrollitakse enne nende avaldamist kahjurvara puudumise suhtes.
b. Avaldatavad dokumendid puhastatakse enne nende avaldamist jääkteabest.
c. Alla laetud failid salvestatakse eraldi asukohta.
d. Kasutaja poolt serverisse üleslaaditavatele failidele on määratud mahupiirang ning on arvestatud piisava salvestusruumiga.

APP.3.2.M4 Sündmuste logimine

a. Veebiserveris logitakse vähemalt järgmisi sündmusi:
   - edukas juurdepääs ressurssidele;

- puudulike õiguste, puuduvate ressursside ja serveri vigade tõttu nurjunud juurdepääs ressurssidele;
- üldised veateated.

b. Logiandmeid analüüsitakse regulaarselt.

APP.3.2.M5 Autentimine

a. Klientarvutite autentimiseks veebiserveris kasutatakse krüpteeritud ühendust (vt APP.3.2.M11 *Krüpteerimine TLS abil*).

b. Parooliga autentimisel hoitakse parooliinfot serveris krüptograafiliselt kaitstult ja kaitstult lubamatu juurdepääsu eest.

APP.3.2.M7 Veebisisu avaldamise õiguspärasus [vastutav spetsialist, vastavushaldur]

a. Veebiserveri kaudu välistele pooltele sisu avaldamine on kooskõlas andmekaitse alase regulatsiooniga.

b. Veebisisu avaldamisel arvestatakse autoriõigustega.

APP.3.2.M11 Krüpteerimine TLS abil

a. Veebiserver võimaldab kõikide ühenduste krüpteerimist TLS abil. Välistes võrkudes kasutatakse andmeside kaitseks TLS-i ja protokolli HTTPS.

b. HTTPS-ühenduse korral kasutatakse HTTPS-i läbivalt, ilma eranditeta.

3.3 Standardmeetmed

APP.3.2.M8 Veebiserveri rakendamise kava

a. Veebiserveri rakendamiseks on koostatud kava, kus on dokumenteeritud veebiserveri kasutamise eesmärk, esitatavad andmed, kasutajate sihtrühm ja olemasolevasse IT-taristusse integreerimise protsess.

b. Veebiserveri tehnilise halduse ja veebisisu eest on määratud vastutajad.

APP.3.2.M9 Veebiserveri turvapoliitika

a. On kehtestatud ja dokumenteeritud veebiserveri turvapoliitika, mis määrab veebiserveri infoturbe meetmed ja vastutajad.

b. Veebiserveri turvapoliitikas on muuhulgas kirjeldatud:
- teabe hankimine teadaolevate turvanõrkuste kohta;
- veebiserveri turvameetmete rakendamine;
- turvaintsidentide käsitluse kord.

APP.3.2.M10 Sobiv veebimajutaja

a. Organisatsioonil on sõlmitud leping välise teenuseandjaga, kus on kokku lepitud teenuse majutusteenuse andmise viis, teenustase ja poolte turbealased kohustused.

b. Teenuseandja on enda IT-süsteemi kaitseks kasutusele võtnud tehnilised ja korralduslikud turvameetmed.

c. Teenuseandja on kohustatud IT-süsteemide tehniliste probleemide tekkimisel ning kliendisüsteemide ohtu sattumisel viivitamatult reageerima.

APP.3.2.M12 Vigade ja veateadete käsitluse kord

a. HTTP-teabest ja veateadetest ei ilmne veebiserveri tarkvarakomponentide nime, versiooni ega konfiguratsiooni.

b. Veebiserver edastab üksnes kasutaja teavitamiseks vajalikke rakendusekohaseid veateateid.

c. Vigade ja tõrgete korral lülitub veebiserver turvalisele ohutusrežiimile.

APP.3.2.M13 Veebirobotite juurdepääsu piiramine

a. Otsingurobotite juurdepääs veebisisule on robotikeelu protokolliga (*Robot Exclusion Protocol*) kitsendatud.

b. Veebiserveri sisu kaitsmiseks veebirobotite eest rakendatakse tehnilisi meetmeid (vt APP.3.2.M5 *Autentimine*).

APP.3.2.M14 Tervikluse kontroll ja kaitse kahjurvara eest

a. Lubamatute muudatuste avastamiseks kontrollitakse regulaarselt failide ja veebisisu terviklikkust.

b. Regulaarselt kontrollitakse kahjurvara esinemist failides.

APP.3.2.M16 Läbistustestimine ja läbivaatus

a. Veebiserveri turvalisust kontrollitakse regulaarsete läbistustestimiste (ingl *penetration testing*) ja korraliste läbivaatustega.

b. Testimise ja läbivaatuse tulemused dokumenteeritakse, neid hoitakse konfidentsiaalsena.

c. Tuvastatud lahknevusi käsitletakse, tulemusest teavitatakse infoturbejuhti.

APP.3.2.M20 Kontaktisiku määramine [haldusosakond]

a. Organisatsioonis on määratud kontaktisik veebiprobleemide lahendamiseks.

b. Organisatsioon on avaldanud organisatsioonivälistele kasutajatele kontaktandmed veebiprobleemidest teavitamiseks.

3.4 Kõrgmeetmed

APP.3.2.M15 Liiasus (A)

a. Veebiserverid ja nende ühendused muude IT-süsteemide ja Internetiga on dubleeritud.

APP.3.2.M18 Kaitse ummistusrünnete eest (A)

a. Ummistusrünnete avastamiseks rakendatakse veebiserveri pidevat seiret.

b. Kasutusel on meetmed ummistusrünnete tõrjeks ja leevendamiseks.

APP.3.3 Failiserver

1 Kirjeldus

1.1 Eesmärk

Esitada spetsiifilised meetmed failiserveri turvaliseks käitamiseks.

1.2 Vastutus

Failiserveri meetmete täitmise eest vastutab IT-talitus.

Lisavastutajad
Kasutaja.

1.3 Piirangud

Serveri turbe üldiseid aspekte käsitletakse moodulis SYS.1.1 Server üldiselt ja mooduligrupi SYS IT-süsteemid moodulites SYS.1.3 Unixi server või SYS.1.2.2 Windowsi server 2012.

Salvestussüsteemide ja salvestusvõrkude turbe meetmed on esitatud moodulis SYS.1.8 Salvestilahendused. Samuti ei käsitleta siin failiserveriteenuseid (nt Samba).

Failiserveri turbe tagamiseks on olulised pääsuõiguste korrektne haldus (vt ORP.4 Identiteedi ja õiguste haldus) ning andmevarunduse toimimine (vt CON.3 Andmevarunduse kontseptsioon).

2 Ohud

2.1 Failiserveri tõrge

Kui failiserveri tõrke tõttu pole kasutajatele ja rakendustele andmed või teenused saadaval, on organisatsiooni äriprotsessid oluliselt mõjutatud. See põhjustab organisatsioonile rahalist kahju ning mõjutab ka teiste organisatsioonide tegevust. Kui avariihalduse kontseptsioonis pole ette nähtud failiserveri kiiret taastamist, pikeneb katkestusaeg ja suurenevad sellega seotud kulud veelgi.

2.2 Failiserveri aladimensioneeritus

Kui failiserveri võrguühendus on aeglane või failiserveri salvestusmaht on ebapiisav, on keeruline tagada andmete nõutavat käideldavust. Lisaohuna võivad töötajad seetõttu eelistada oma andmete lokaalsesse arvutisse salvestamist. Kui andmetest hoitakse mitmeid erinevaid töökoopiaid, võib kannatada andmete konfidentsiaalsus ja terviklus. Puudub kindlus, mis toiminguid andmetega viimati tehti ja kes on andmete valdaja.

2.3 Salvestatud failide puudulik kontroll

Kui failiserver ei ole kahjurprogrammide eest piisaval määral turvatud, võib ründaja sinna märkamatult paigaldada kahjurvara. See võimaldab failiserveris hoitavaid andmeid lubamatult vaadata või neid manipuleerida. Kui failiserveri andmetele juurdepääsu omavaid seadmeid ja rakendusi on palju, võib kahjurtarkvara levida väga kiiresti üle organisatsiooni.

2.4 Pääsuõiguste kontseptsiooni puudumine või puudulikkus

Kui pääsuõiguseid ja failide ühiskasutust ei ole piisavalt kavandatud ega rakendatud, on võimalik tekkinud andmepääsunõrkusi failiserverisse volitamata juurdepääsu saamiseks ära kasutada. Ründaja saab andmeid vaadata, muuta, kustutada või kopeerida.

2.5 Struktureerimata andmehaldus

Kui andmehalduse kord puudub või töötajad ei pea sellest kinni, salvestatakse failiserverisse andmeid mittejälgitavalt ja koordineerimatult. See toob kaasa andmete paljususest tuleneva salvestusressursside raiskamise, volitamata juurdepääsu andmetele (nt kui faile hoitakse kataloogides või failisüsteemides, mis on volitamata isikutele kättesaadavad) või mittekooskõlaliste failiversioonide tekkimise.

2.6 Failiserveris talletatud andmete kaotus

Kui failiserver on paigutatud lihtsasti juurdepääsetavasse asukohta, on võimalik selle komponentidele ja serveris talletatud andmetele vahetult juurde pääseda. Ründajal on võimalik kõvaketas eemaldada või endaga kaasa võtta. Väiksemaid võrgusalvesteid on võimalik varastada koos neis talletatud andmetega.

Ka failiserveri mõne komponendi tõrge võib tekitada failiserveris andmekadu, eriti kui andmed kõvaketastel ei ole kaitstud RAID-lahendusega (ingl *redundant array of independent disks,* RAID) või kui andmetest ei ole tehtud äsja varukoopiat. Andmekadu võib põhjustada ka töötaja tähelepanematus failide kasutamisel, eriti nende hulgakaupa kustutamisel.

2.7 Lunavara

Lunavaraga (ingl ransomware) nakatumise korral IT-süsteemides olevad andmed krüpteeritakse ja lubatakse dekrüpteerida pärast lunaraha maksmist. Kuid isegi pärast lunaraha maksmist ei saa andmete tagasisaamises kindel olla.

Pärast viimast varundamist lisatud andmed võivad lunavara ründe tõttu kaotsi minna. Kui andmeid ei ole varundatud, võib lunavararünne halvimal juhul organisatsiooni tegevuse lõpetada.

Lunavara ei piirdu ainult nakatunud lokaalse IT-süsteemi salvestusruumiga, vaid võib levida edasi kasutaja kirjutusõigust omavatele võrguketastele. Isegi kui andmed on varundatud, tekib pikaajaline katkestus, mille vältel andmed ei ole kättesaadavad.

3 Meetmed

3.1 Elutsükkel

Kavandamine

APP.3.3.M15 Failiserveri eelanalüüs

Soetus

APP.3.3.M6 Failiserveri hankimise kord

APP.3.3.M7 Sobiva failisüsteemi valimine

Evitus

APP.3.3.M2 RAID-süsteem

APP.3.3.M3 Viirusetõrjeprogrammid

APP.3.3.M8 Struktureeritud andmetalletus

Käitus

APP.3.3.M9 Turvaline salvestihaldus

APP.3.3.M11 Kvootide rakendamine

Lisanduvad kõrgmeetmed

APP.3.3.M12 Andmestiku krüpteerimine

APP.3.3.M13 Dubleerimine teises asukohas

APP.3.3.M14 Veaparanduskoodide kasutamine

3.2 Põhimeetmed

APP.3.3.M2 RAID-süsteem

a. Organisatsioon on analüüsinud, kas ja millist RAID-süsteemi on failiserveris otstarbekas kasutada. RAIDi mittekasutamine on koos põhjendusega dokumenteeritud.

b. On otsustatud, kui kaua aega maksimaalselt võib võtta RAIDi ja andmete taaste.

c. Riistvaralise RAIDi kasutamise korral on serveris RAIDi kontroller dubleeritud ning kasutatakse kuumvahetatavaid (ingl *hot-swappable*) kõvakettaid.

APP.3.3.M3 Viirusetõrjeprogrammid

a. Andmete salvestamisel failiserverisse kontrollitakse andmeid kahjurtarkvara avastamiseks.

APP.3.3.M15 Failiserveri eelanalüüs

a. Failiserveri kasutusele võtmiseks on tehtud eelanalüüs, mis määratleb serveri otstarbele vajaliku funktsionaalsuse ja piirangud.

b. Serveri salvestusmaht on arvestatud piisava varuga, planeeritud andmevahetuskiirus ja ühenduvus vastavad serveri otstarbele.

c. Failiserverina ei kasutata tööjaama.

3.3 Standardmeetmed

APP.3.3.M6 Failiserveri hankimise kord

a. Failiserveri hankimiseks on koostatud failiserveri nõuete spetsifikatsioon, mille põhjal tooteid võrreldakse.

b. Failiserveri tarkvara ja käitatavad teenused on valitud lähtudes failiserveri kasutamise peamistest eesmärkidest (nt failide ühiskasutus, meedia voogedastus, kettatõmmiste varundus).

c. Failiserveri hankimisel on arvestatud selle sooritusvõimet, salvestusmahtu, andmevahetuskiirust ja kasutajate potentsiaalset arvu.

APP.3.3.M7 Sobiva failisüsteemi valimine

a. Kriteeriumid failisüsteemide sobivuse hindamiseks on esitatud failiserveri nõuete spetsifikatsioonis.

b. Transaktsioonide tagasivõtmiseks või uuesti käivitamiseks on failisüsteemis rakendatud päevikupidamise (ingl *journaling*) funktsioon.

c. Failisüsteemil on kaitsemehhanism mitme kasutaja või rakenduse samaaegse failimuutmise takistamiseks.

APP.3.3.M8 Struktureeritud andmehaldus [kasutaja]

a. Andmete talletuseks on välja töötatud kindel kataloogistruktuur.

b. Kasutajad on teadlikud andmetalletuse korrast, kaasa arvatud sellest, millised andmed salvestatakse lokaalselt ja millised failiserverisse.

c. Programmiandmeid ja tööfaile hoitakse eri kataloogides.

d. Struktureeritud andmehalduse nõuete täitmist kontrollitakse regulaarselt.

APP.3.3.M9 Turvaline salvestihaldus

a. Failiserveri ressursside üle peetakse arvestust.
b. Regulaarselt kontrollitakse, kas salvesti komponendid toimivad ettenähtud viisil. Tõrgete või mäluruumi lõppemise puhuks on olemas sobivad varukomponendid.
c. Andmesalvestite hierarhia (esimese, teise või kolmanda tasandi salvestid) olemasolul on koostatud (pool)automaatse salvestuse haldusprotseduurid.
d. Andmesalvestuse automaatika toimimist kontrollitakse regulaarselt.
e. Andmesalvestite turvasündmused (volitamata juurdepääsu katsed, pääsuõiguste muutmine) logitakse.

APP.3.3.M11 Kvootide rakendamine

a. Kasutajaile on failiserveris määratud mahupiirangud e kvoodid (ingl *quota*). Alternatiivse lahendusena hoiatatakse kasutajat kettamahu täitumisest ja omistatakse kirjutusõigus ainult süsteemiülemale.

APP.3.3.M14 Veaparanduskoodide kasutamine

a. Kasutusel on veaavastus- või veaparandusmeetodeid võimaldav failisüsteem, näiteks ZFS. Failiserveri hankimisel on arvestatud sellest tuleneva lisaruumi vajadusega.
b. Veaparanduskoodide kasutamisel arvestatakse, et selline vigade avastamine ja parandamine toimib üksnes piiratud määral.

3.4 Kõrgmeetmed

APP.3.3.M12 Andmestiku krüpteerimine (C-I-A)

a. Kõik failiserveris hoitavad andmed on kas riistvara või failisüsteemi tasemel krüpteeritud. Riistvaralise krüpteerimise korral kasutatakse ainult sertifitseeritud tooteid.
b. Viirusetõrje tarkvara suudab kontrollida ka krüpteeritud faile.

APP.3.3.M13 Dubleerimine teises asukohas (A)

a. Kõrgkäideldavuse vajaduse korral dubleeritakse andmed mitmetele seadmetele ja erinevatesse asukohtadesse.
b. Andmete dubleerimiseks on valitud sobiv dubleerimismehhanism.
c. Kasutatakse piisava täpsusega ajateenuseid.

APP.3.4 Samba

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed Samba protokollide ja meetodite turvaliseks kasutamiseks ja Samba andmete kaitseks.

1.2 Vastutus

Samba meetmete täitmise eest vastutab IT-talitus.

1.3 Piirangud

Sambat käitava Linuxi serveri turvameetmed on esitatud moodulites SYS.1.1 *Server üldiselt* ja SYS.1.3 *Linuxi ja Unixi server*.

Samba kaudu antavate prindi-, faili- ja kataloogiteenuste turvameetmed on kirjeldatud moodulites SYS.4.1 *Printer ja kontorikombain*, APP.3.3. *Failiserver*, APP.2.1. *Kataloogiteenus üldiselt* ja APP.3.6. *DNS-server,* APP.2.2 *Active Directory* ning APP.2.3 *OpenLDAP*).

Pääsuõiguste haldust käsitletakse moodulis ORP.4 Identiteedi ja õiguste haldus.

2 Ohud

2.1 Samba turvamata ühenduste pealtkuulamine

Kui failide edastamisel Linuxi serverite, Windowsi serverite ja klientide vahel kasutatakse turvamata protokolle, on Samba andmeühendusi võimalik püüda ja pealt kuulata. Nii saadud autentimis- ja kasutajaandmeid saab ründaja kuritarvitada organisatsiooni tundliku teabe varguseks.

2.2 Samba ebaturvalised vaikeseaded

Kui pärast Samba serveri installimist konfiguratsiooni turvalisemaks ei muudeta ning Samba käivitatakse konfiguratsioonifaili smb.conf vaikeseadetes, võib see kaasa tuua märkimisväärseid turvaprobleeme.

2.3 Samba lubamatu kasutamine või haldamine

Samba kasutamine või haldamine volitamata isikute poolt võimaldab konfidentsiaalsele teabele juurde pääseda, seda manipuleerida või põhjustada Samba teenuste tõrkeid. Konfiguratsioonivahendites nagu *Samba Web Administration Tool* (SWAT) ei ole tihti turvamehhanismide kasutamisele piisavat tähelepanu pööratud. Seetõttu rakendatakse neis nõrgemaid turvamehhanisme või puuduvad need üldse (näiteks ei toetata HTTPS-i).

2.4 Samba väär haldus

Kui süsteemiülemad ei tunne Samba ulatuslikku funktsionaalsust, Samba komponentide valikuid ja konfiguratsiooniseadeid piisavalt, võivad näiteks DNSi või kasutajaõiguste halduse konfigureerimisvead põhjustada volitamata isikute juurdepääsu serveri ressurssidele. Samuti võivad administreerimisvead põhjustada IT-süsteemide ja äriprotsesside katkestusi.

2.5 Andmekadu Sambas

Windowsi ja Unixi failisüsteemidel on erinevad omadused. Seetõttu ei ole tagatud, et Windowsis säilivad Unixi pääsuõigused. Tulemuseks võib olla volitamata juurdepääsu võimaldamisest tingitud andmekadu. Süsteemide erisuse tõttu võib kaduma minna ADSi (Alternate Data Streams) ja DOSi atribuutide andmed. Kui seda infot IT-süsteemides kasutatakse, võib operatsioonisüsteemide erinevuste tõttu tekkida tõrkeid äriprotsesside toimimises.

2.6 Andmete tervikluse kadu Sambas

Samba kasutamisel on oluline, et Samba TDB-vormingus (TDB - Trivial DataBase) hoitavad oluliste kasutusandmete andmebaasid oleksid terviklikud. Kui operatsioonisüsteem ei suuda neid andmebaase piisava jõudsusega käidelda, võivad Samba teenuste töös tekkida tõrked.

3 Meetmed

3.1 Elutsükkel

Kavandamine

APP.3.4.M1 Samba serveri rakendamise kava

APP.3.4.M4 Samba serveri NTFS-funktsioonide tagamine

Evitus

APP.3.4.M12 Samba serveri haldurite koolitus

APP.3.4.M2 Samba serveri turvaline aluskonfiguratsioon

APP.3.4.M3 Samba serveri operatsioonisüsteemi turvaline konfiguratsioon

APP.3.4.M5 Samba serveri juurdepääsu turvaline seadistus

APP.3.4.M6 Winbindi turvaline konfiguratsioon Samba keskkonnas

APP.3.4.M7 DNS-i turvaline konfiguratsioon Samba keskkonnas

APP.3.4.M8 LDAP turvaline konfiguratsioon Samba keskkonnas

APP.3.4.M9 Kerberose turvaline konfiguratsioon Samba keskkonnas

Käitus

APP.3.4.M10 Väliste programmide turvaline rakendamine Samba serveril

Avariivalmendus

APP.3.4.M13 Samba serveri oluliste süsteemikomponentide regulaarne varundus

Lisanduvad kõrgmeetmed

APP.3.3.M15 Samba andmepakettide krüpteerimine

3.2 Põhimeetmed

APP.3.4.M1 Samba serveri rakendamise kava

a. Enne Samba serveri kasutuselevõttu on otsustatud ja dokumenteeritud:
   - milliseid ülesandeid Samba server tulevikus täidab;
   - millisel tööviisil Samba töötab;
   - kuidas teostatakse autentimine;
   - milline peab olema Samba töökeskkond;
   - milliseid Samba ja muid komponente on selleks vaja.

b. On hoolikalt testitud järgmised Samba komponendid:
   - klastrilahendus CTDB (*Cluster Trivial Database*);
   - AD *(Active Directory)* teenused Linuxi ja Unixi süsteemidele;
   - AD autentimisprotseduur;
   - VFS (*Virtual File System*) moodulid ja nende rakendamise järjekord;
   - protokoll IPv6 Sambas.

APP.3.4.M2 Samba serveri turvaline aluskonfiguratsioon

a. Konfigureerimisel on pääsu reguleerimise ja serveri jõudlust mõjutavad sätted turvalisemaks muudetud.

b. Samba on konfigureeritud ühenduma ainult turvaliste hostide ja võrkudega.

c. Konfiguratsioonimuudatused, nende läbiviijad ja muudatuste põhjused dokumenteeritakse.

d. Iga muudatuse järel kontrollitakse süntaksi õigsust.

e. Lisatarkvara (nt SWAT) ei ole paigaldatud.

3.3 Standardmeetmed

APP.3.4.M3 Samba serveri operatsioonisüsteemi turvaline konfiguratsioon

a. TDB-vormingus andmebaase ei hoita partitsioonis, kus on kasutusel *ReiserFS* failisüsteem.

b. Ühiskasutuse (*Netlogon*) puhul ei ole volitamata kasutajatel võimalik ühiskasutuses olevaid faile muuta.

c. Samba serveri operatsioonisüsteem ning kasutatav failisüsteem toetavad failisüsteemi pääsuloendeid (ingl *access control list*, ACL).

d. SMB sõnumisigneerimise seaded vastavad kaitseala turvapoliitikale.

e. NT LAN Manageri (NTLM) või NTLMv2 nõrkuste ärakasutuse ja ülemäärase võrgukoormuse vältimiseks on kasutusel Kerberos.

APP.3.4.M4 NTFSi funktsioonide vältimine Samba serveris

a. Kui Samba versioonist tulenevalt kasutatakse NTFS ADSi andmevooge, siis tagatakse, et failisüsteemi objektid ei sisalda olulist ADS-infot enne objektide edastamist.

APP.3.4.M5 Samba serveri juurdepääsu turvaline seadistus

a. DOS-atribuutide vastendamiseks Linuxi failisüsteemis kasutatakse Samba vaikeparameetrite asemel failisüsteemi täiendatribuute (*Extended Attributes*).

b. Samba teenuse portide juurdepääs on lubatud ainult sisevõrgust.

c. Samba serveri pääsuõigusi ja logiandmeid kontrollitakse regulaarselt.

APP.3.4.M6 Winbindi turvaline konfiguratsioon Samba keskkonnas

a. Kui Windowsi domeeni kasutajate jaoks pole loodud kasutajakontosid serveri operatsioonisüsteemis, siis kasutatakse domeeni kasutajanimede Linuxi kasutajanimedeks teisendamiseks *winbind'i.* Seejuures välditakse konflikte lokaalsete Linuxi kasutajate ja domeenikasutajate vahel.

b. Autentimise toetamiseks kasutatakse PAM-pluginaid (*Pluggable Authentication Modules*).

APP.3.4.M7 DNS turvaline konfiguratsioon Samba keskkonnas

a. Samba rakendamisel DNS-serverina on selle konfiguratsiooni enne kasutuselevõttu testitud.

b. DNS on konfigureeritud Samba kasutusstsenaariumi kohaselt.

APP.3.4.M8 LDAP turvaline konfiguratsioon Samba keskkonnas

a. Kui Samba kasutajaid hallatakse LDAP-ga, on see hoolikalt kavandatud ja pääsuloendite (ACL) abil rakendatud.

APP.3.4.M9 Kerberose turvaline konfiguratsioon Samba keskkonnas

a. Autentimiseks Sambaga on rakendatud MIT või Heimdal Kerberos KDC (Key Distribution Center, KDC) koos Samba jaoks kohandatud Kerberose konfiguratsioonifailiga.

b. Kerberosega autentimisel asub keskne ajaserver lokaalsel domeenikontrolleril. NTP-teenuse ajapäringud on kättesaadavaks tehtud ainult volitatud klientidele.

c. Kerberose piletite krüptomehhanismid on piisavalt tugevad.

APP.3.4.M10 Väliste programmide turvaline rakendamine Samba serveris

a. Samba käivitab ainult kontrollitud ja usaldusväärseid väliseid programme.

APP.3.4.M12 Samba serveri haldurite koolitus

a. Samba serveri haldurid on läbinud koolituse Samba spetsiifiliste valdkondade, nt kasutajate autentimise, Windowsi ja Unixi kasutajaõiguste mudelite, aga ka NTFS-i pääsuloendite ja ADS-i alal.

APP.3.4.M13 Samba serveri oluliste süsteemikomponentide regulaarne varundus

a. Samba serveri taasteks vajalikud süsteemikomponendid ja tagasüsteemid on hõlmatud üleorganisatsioonilisse andmevarunduse kontseptsiooni.

b. Varundusse on kaasatud kõik TDB-failid.

3.4 Kõrgmeetmed

APP.3.4.M15 Samba andmepakettide krüpteerimine (C-I)

a. Samba andmepaketid krüpteeritakse protokolli SMB uuemates versioonides (alates SMB v3) sisalduvate meetoditega.

APP.3.6 DNS-server

1 Kirjeldus

1.1 Eesmärk

Esitada organisatsioonis rakendatavate siseste ja väliste DNS-serverite turvalise käitamise meetmed.

1.2 Vastutus

DNS-serveri meetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Haldusosakond.

1.3 Piirangud

Mooduli rakendamisel tuleb rakendada ka mooduli SYS.1.1 *Server üldiselt* ning sõltuvalt DNS-serveri operatsioonisüsteemist kas SYS.1.3 *Linuxi ja Unixi server* või SYS.1.2.2 *Windows Server 2012* meetmed.

2 Ohud

2.1 DNS-serveri tõrge

DNS-serveri tõrke korral ei saa organisatsiooni muud serverid ega kliendid enam aadresse teisendada. Ühendusi serverite vahel ei ole võimalik luua, organisatsioonisisesele serverile ei ole juurdepääsu ka välistel IT-süsteemidel (nt liikuvad töötajad, kliendid ja äripartnerid). Olulised äriprotsessid võivad olla häiritud.

2.2 DNS-serveri piisamatu suutlikkus

Kui DNS-server ei suuda pöördumisi piisava suutlikkusega töödelda, võivad sise- ja välisteenuste pöördusajad pikeneda, teenuste käideldavus on häiritud ja ründajal on lihtsam DNS-serverit teenusetõkestusründega (ingl *Denial of Service*, DoS) üle koormata.

2.3 DNSi rakendamise puudulik kavandamine

DNSi rakendamise puudulikust kavandamisest tingituna võivad tekkida turvanõrkused, mis võivad soodustada DNS-serveri vastu tehtavate rünnete õnnestumist. Kui DNSi võrguliiklust võimaldavad tulemüürireeglid on liiga leebed, võib see kaasa tuua volitamata juurdepääsu DNS-serverile. Ent kui reeglid on liiga piiravad, ei saa usaldatavad kliendid DNS-serverile päringuid esitada ja teenuste (nt e-post, FTP jne) kasutamine on häiritud.

2.4 Vigane domeeniinfo

Inimliku vea tulemusena luuakse semantiliselt ja/või süntaktiliselt vigane domeeniinfo. Viga tekib näiteks, kui hostinimega seostatakse vale IP-aadress, vajalikke andmeid pole sisestatud või kui on kasutatud keelatud märke. Kui nimeteisendused on rakendatud ebajärjekindlalt, võib see kaasa tuua vigu neid andmeid kasutavates teenustes, sõltuvalt sellest, millist allikat aadressi teisenduseks kasutatakse.

2.5 DNS-serveri väär konfiguratsioon

Vaikeseadete muutmata jätmine või konfigureerimisel tehtud vead võivad põhjustada DNS-serveri turvanõrkusi või häireid serveri töös. Kui DNS-server on konfigureeritud vastu võtma sisevõrgust rekursiivseid päringuid ilma piiranguteta, võib see suurema koormuse tõttu mõjutada oluliselt serveri käideldavust. DNS-serveri konfiguratsioonivead muudavad serveri avatuks DNSi peegeldusründele (ingl *DNS reflection attack*).

Kui DNS-tsoonitransaktsioone ei ole piiratud kindlate DNS-serveritega, saab iga host, millel on võimalus välisvõrgu DNS-serverile päring esitada, nende serverite domeeniinfot lugeda. See võib oluliselt lihtsustada serveri hilisemat ründamist.

2.6 DNSi manipuleerimine

DNS-pettega (ingl *DNS spoofing*, *DNS cache poisoning*) püütakse saavutada olukord, kus rünnatav server salvestab IP-aadresside ja nimede vahel väärad seosed. Seejuures kasutatakse ära asjaolu, et DNS-serverid salvestavad domeeniteabe teatud ajaks vahemällu. Kui päringud esitatakse manipuleeritud DNS-serverile, saadab see vastuseks võltsitud andmeid. Klientseade salvestab vastuse enda vahemällu, mistõttu ka see on „mürgitatud“. Kui *DNS resolver* esitab manipuleeritud aadressi kohta päringu, küsitakse seda mõnest teisest DNS-

serverist alles pärast seda, kui andmete eluiga (ingl *time to live*, TTL) on lõppenud. Nii on võimalik, et manipuleeritud DNSi informatsioon säilib pikka aega, isegi kui esmalt rünnatud DNS-serveris on vead juba parandatud.

Kui ründajal õnnestub manipuleerida domeeni nimeteisendust, mõjutab see automaatselt ka kõiki alamdomeene. DNS-petteid tehakse sageli eesmärgiga suunata päringud pahatahtlikesse serveritesse.

2.7 DNSi kaaperdamine

DNSi kaaperdamine (ingl DNS hijacking, DNS redirection) on ründemeetod, mida kasutatakse DNS-serverite ja resolverite vahelise suhtluse juhtimiseks läbi ründaja IT-süsteemi. Selle vahendusründega saab ründaja pealt kuulata ja salvestada serverite vahelist suhtlust. Palju suurem oht on aga see, et ründaja saab mõlema suhtluspartneri liiklust oma tahtmise järgi muuta. Kui pärast DNS-i kaaperdusrünnet saadetakse kliendi IT-süsteemi DNS-resolverilt päring DNS-serverile, saab ründaja väheste küsijate jaoks ning piiratud tingimustel nime ja IP-aadressi vahelisi seoseid muuta. DNS-petet saab kombineerida ka muude rünnetega (eriti õngitsemisega).

2.8 DNSi ummistusrünne

DNS-serveri ummistusründe korral saadetakse serverile nii palju päringuid, et võrguühendus või DNS-server ise koormatakse üle. Suure hulga päringute saatmiseks korraga koostab päringud tavaliselt bottnett (ingl botnet). Ülekoormatud DNS-server ei saa enam päringutele vastata.

2.9 DNSi peegeldusrünne (DNS-dublee)

DNS-i peegeldusrünne (ingl *DNS reflection*) on ummistusrünne, mille sihtmärk ei ole DNS-server, millele päringuid saadetakse, vaid päringu saatja. Selle ründe korral kasutatakse ära asjaolu, et teatud päringud tekitavad suhteliselt suure hulga vastuseandmeid. Seejuures on võimalik saavutada enam kui 100-kordne võimendustegur. Vastuste arvu ja mahu tõttu koormatakse võrku või arvutit maksimaalse jõudluspiirini. Ründe sihtmärgiks saavad olla erinevad tehnilised IT-komponendid. DNSi peegeldusründe läbiviimist lihtsustavad välisvõrgu DNS-resolverid.

3 Meetmed

3.1 Elutsükkel

Kavandamine

APP.3.6.M1 DNSi rakendamise kava

APP.3.6.M8 Domeeninimede haldus

APP.3.6.M11 DNS-serveri piisav dimensioneerimine

APP.3.6.M17 Protokollilaienduse DNSSEC rakendamine

Soetus

APP.3.6.M10 DNS-serveriks sobiv server

Evitus

APP.3.6.M3 Eraldi DNS-serverid sise- ja välispäringutele

APP.3.6.M4 DNS-serveri turvaline aluskonfiguratsioon

APP.3.6.M6 Dünaamiliste DNS-uuendite turve

APP.3.6.M13 Domeeniteabe nähtavuse piiramine

APP.3.6.M14 DNS-serverite eraldamine

Käitus

APP.3.6.M7 DNS-serveri seire

APP.3.6.M15 Logiandmete analüüs

APP.3.6.M16 DNS-serveri õige paigutus P-A-P arhitektuuris

APP.3.6.M18 Tsoonitransaktsiooni turbe tugevdamine

Kõrvaldamine

APP.3.6.M19 DNS-serveri turvaline kasutuselt kõrvaldamine

Avariivalmendus

APP.3.6.M2 DNS-serveri dubleerimine

APP.3.6.M9 DNS-serveri avariikava

Lisanduvad kõrgmeetmed

APP.3.6.M20 Avariikava teostatavuse kontroll

APP.3.6.M21 DNS-primaarserveri peitmine

APP.3.6.M22 DNS-teenuste sidumine mitme tarnijaga

3.2 Põhimeetmed

APP.3.6.M1 DNSi rakendamise kava

a. DNSi rakendamise kavandamisel on otsustatud ja dokumenteeritud:
   - DNS teenuse ülesehitus;
   - kaitstav domeeniinfo;
   - DNS-serverite integreerimisviis;
   - DNS-teenusega seotud kasutajarollid.

APP.3.6.M2 DNS-serveri dubleerimine

a. DNSi infot kuulutav server on dubleeritud teise DNS-serveriga.

APP.3.6.M3 Eraldi DNS-serverid sise- ja välispäringutele

a. DNSi infot kuulutav server (ingl *DNS advertiser*) ja DNSi infot lahendav server e. DNS-resolver (ingl *DNS resolver*) on füüsiliselt eraldiseisvates serverites.

b. Sisemised IT-süsteemid kasutavad nimeteisenduseks organisatsioonisiseseid DNS-resolvereid.

APP.3.6.M4 DNS-serveri turvaline aluskonfiguratsioon

a. Sisevõrku teenindav DNS-server on konfigureeritud töötlema ainult sisevõrgust saadetud päringuid. Päringute saatmisel kasutatakse juhuslikke lähteporte.

b. Kui vigast domeeniinfot edastavad DNS-serverid on teada, tõkestatakse neile juurdepääs.

c. DNSi infot kuulutav server on konfigureeritud käsitlema Internetist tulevaid päringuid iteratiivselt.

d. Tsooniinfo edastamine on lubatud üksnes primaarserveri ja sekundaarserveri(te) vahel ning piiratud IP aadressi põhiselt.

e. DNS-serveri toote versiooninumber on varjatud.

APP.3.6.M6 Dünaamiliste DNS-uuendite turve

a. Domeeniinfot sise-DNS-serverites saavad muuta ainult selleks volitatud IT-süsteemid.

b. On määratud, millist domeeniinfot saavad IT-süsteemid muuta.

APP.3.6.M7 DNS-serveri seire

a. DNS-serverit seiratakse pidevalt tõrgete või anomaaliate avastamiseks.

b. Seiratakse DNS-serveri koormust, et ülekoormuse korral suurendada riistvara jõudlust.

c. DNS-serveris logitakse vähemalt järgmisi turvasündmusi:

- ebaõnnestunud DNS-päringud;
- EDNS (Extension Mechanisms for DNS) vead;
- kehtetud ja ebaõnnestunud tsoonitransaktsioonid.

APP.3.6.M8 Domeeninimede haldus [haldusosakond]

a. Organisatsiooni domeenide registreeringuid on regulaarselt ja aegsasti pikendatud.

b. On määratud Interneti domeeninimede halduse eest vastutav töötaja.

c. Organisatsioonil on kontroll enda registreeritud domeenide üle ka siis, kui domeenihalduseks kasutatakse teenuseandjat.

APP.3.6.M9 DNS-serveri avariikava

a. DNS-serveri jaoks on koostatud avariikava, mis on kooskõlas organisatsiooni olemasolevate avariikavade ja jätkusuutlikkusplaaniga (vt DER.4 *Avariihaldus*)

b. Avariikava sisaldab tsooni- ja konfiguratsioonifailide varunduse protseduuri, mis on integreeritud organisatsiooni olemasolevasse andmevarunduse kontseptsiooni.

c. Avariikava sisaldab ka DNS-serveri taasteplaani.

3.3 Standardmeetmed

APP.3.6.M10 DNS-serveriks sobiv server

a. Valitud DNS-serveri lahenduse kasutamine on end praktikas piisavalt õigustanud.

b. DNS-server vastab kehtivale RFC-standardile.

c. DNS-server toetab süntaktiliselt õigete tsoonifailide (ingl *master file*) loomist.

APP.3.6.M11 DNS-serveri piisav dimensioneerimine

a. DNS-serveri ressurss tagab funktsiooni täitmiseks piisava jõudluse.

b. DNS-serverit kasutatakse üksnes DNS-serveri teenuse käitamiseks.

c. DNS-serveri võrguühendus on piisava läbilaskevõimega.

APP.3.6.M13 Domeeniteabe nähtavuse piiramine

a. Sama domeeninime kasutamisel on domeeni nimeruum selgelt jaotatud avalikuks ja organisatsioonisiseseks osaks.

b. Avalik osa sisaldab ainult sellist domeeniinfot, mida on vaja väljast juurdepääsetavate teenuste jaoks.

c. Avalikku IP-aadressi omavate sisevõrgu IT-süsteemide sisemisi DNS-nimesid ei saa välisvõrgust lahendada.

APP.3.6.M14 DNS-serverite eraldamine

a. Primaarne ja sekundaarne DNSi infot kuulutav server on paigutatud eri võrgusegmentidesse.

APP.3.6.M15 Logiandmete analüüs

a. DNS-serveri ja selle operatsioonisüsteemi logifaile kontrollitakse ja analüüsitakse regulaarselt.

b. Analüüsitakse vähemalt järgmisi logiandmeid:
   - DNS-päringute arv;
   - ebaõnnestunud DNS-päringute arv ja vigade põhjused;
   - ebaõnnestunud DNS-päringute suhtarv ja selle dünaamika;
   - ebaõnnestunud tsoonitransaktsioonide põhjused.

APP.3.6.M16 DNS-serveri õige paigutus P-A-P arhitektuuris

a. DNSi infot kuulutava serveri ja DNSi infot lahendava serveri vaheline liiklus on filtreeritud P-A-P ahitektuuri (*packet filter – application level gateway – packet filter, P-A-P*) paketifiltrite ja rakenduslüüsiga (ingl *application level gateway*, ALG).

b. DNS-serverite vahel on võimalik ainult DNS-liiklus.

c. Kui domeeninime haldab väline teenuseandja, avaldatakse talle ainult minimaalne vajalik domeeniinfo.

APP.3.6.M17 Protokollilaienduse DNSSEC rakendamine

a. Kõigis DNS-serverites on aktiveeritud DNS-i protokollilaiendus DNSSEC.

b. Võtmesigneerimisvõtmeid (ingl *Key Signing Key*, KSK) ja tsoonisigneerimisvõtit (ingl *Zone Signing Key*, ZSK) hallatakse turvaliselt ning vahetatakse regulaarselt või võtme paljastumisel.

APP.3.6.M18 Tsoonitransaktsiooni turbe tugevdamine

a. Tsoonitransaktsiooni turbeks kasutatakse transaktsioonisignatuure (ingl *Transaction Signatures*, TSIG).

APP.3.6.M19 DNS-serveri turvaline kasutuselt kõrvaldamine

a. DNS-serveri kasutuselt kõrvaldamisel kustutatakse serveri salvestuskandjad turvaliselt.

b. DNS-serveri kõrvaldamisel kustutatakse vastava serveri nimi ja IP-aadress kõigist konfiguratsioonifailidest nii organisatsioonis kui teenuseandjate juures.

3.4 Kõrgmeetmed

APP.3.6.M20 Avariikava teostatavuse kontroll (A)

a. Regulaarselt kontrollitakse, kas avariiolukorra tegevuskava on teostatav.

APP.3.6.M21 DNS-primaarserveri peitmine (C-I-A)

a. DNSi infot kuulutav välisvõrgu primaarserver kasutab primaaripeite (ingl *hidden master*) võtet, nii et see server pole DNS-tsooniandmetes nähtav ega väljast kättesaadav.

APP.3.6.M22 DNS-teenuste sidumine mitme tarnijaga (I-A)

a. Domeeninime registreerimisel on määratud vähemalt kaks välisvõrgu DNS-nimeserverit (primaarne ja sekundaarne).

b. Primaarne ja sekundaarne DNS-server asuvad eri võrkudes ja on ühendatud erinevate teenuseandjate kaudu.

4 Lisateave

Lühend	Publikatsioon
[NIST]	NIST Special Publication 800-81-2 „Secure Domain Name System (DNS) – Deployment Guide“
[RFC]	RFC 1034 „Domain Names – Concepts and Facilities“

APP.4: Ärirakendused

APP.4.3 Andmebaasisüsteemid

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed relatsioonandmebaasisüsteemide turvaliseks kavandamiseks, rajamiseks ja käitamiseks ning andmebaasides töödeldava teabe kaitseks.

1.2 Vastutus

Relatsioonandmebaasisüsteemide meetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Arendaja, vastutav spetsialist.

1.3 Piirangud

Moodul ei käsitle mitterelatsiooniliste andmebaasisüsteemide turvameetmeid. Moodul ei käsitle rakenduste turvalist arendust, andmebaasi struktuuri ja juurdepääsuga seotud turvameetmeid. Samuti ei ole moodulis käsitletud andmebaasiserveri operatsioonisüsteemi ja

riistvara turvameetmeid, need on esitatud SYS mooduligrupi moodulites SYS.1.3 Linuxi ja Unixi server või SYS.1.2.2 Windows Server 2012.

Täiendavalt rakendatakse relatsioonandmebaasidele meetmeid moodulitest ORP.4 Identiteedi ja õiguste haldus, OPS.1.1.3 Paiga- ja muudatuste haldus, CON.3 Andmevarunduse kontseptsioon, OPS.1.1.2 IT-süsteemide haldus ja OPS.1.1.5 Logimine.

2 Ohud

2.1 Süsteemiressursside ebapiisavus

Kui andmebaasihalduse süsteemi (ingl *database management system,* DBMS) käitava riistvara võimekus ja ressursid on ebapiisavad, võivad andmebaasis tekkida tõrked (nt ei saa andmeid enam salvestada). Samuti võivad süsteemiressursid olla tipptundidel ülekoormatud, mistõttu rakendused töötavad aeglaselt või lakkavad toimimast.

2.2 Vaikekontode kasutuselejätt

Andmebaasihalduse süsteemi esmasel paigaldamisel ei ole kasutaja- ega halduskontod sageli üldse kaitstud või on need kaitstud avalikult teadaolevate paroolidega. Sellega kaasneb kontode kuritarvitamise oht (nt saab ründaja andmebaasihalduse süsteemi kasutaja või koguni süsteemiülemana sisse logida). Seejärel saab ründaja konfiguratsiooni või salvestatud andmeid lugeda, manipuleerida või kustutada.

2.3 Krüpteerimata andmevahetus

Tüüpseadistuses ei kasuta paljud andmebaasihalduse süsteemid andmebaasiga ühendumiseks krüpteerimist. Kui rakenduste ja andmebaaside vaheline suhtlus on krüpteerimata, saab autentimisandmeid ja edastatavaid andmeid lugeda või manipuleerida.

2.4 Andmekadu andmebaasis

Andmebaasist võivad andmed kaotsi minna riist- ja tarkvaravigade ning inimliku eksituse tõttu. Kuna andmebaasides talletatakse enamasti rakenduste käitamiseks olulist informatsiooni, võib see teenuste andmise või terve äriprotsessi katkestada.

2.5 Andmete tervikluse kadu

Andmebaasisüsteemis talletatud andmete terviklust võivad kahjustada vääralt konfigureeritud andmebaasid, tarkvaravead või andmete manipuleerimine. Kui tervikluse kahjustumist ei märgata või märgatakse liiga hilja, võib see organisatsiooni põhiprotsesse suurel määral takistada.

Kui tabelite viitetervikluse nõuet pole andmebaasi projekteerimisel järgitud, võivad andmebaasi sattuda väärad andmed. Kui tegu on kriitiliste andmetega (nt raamatupidamisandmed või tööstussüsteemi juhtandmed), siis võib aja jooksul tekkida sellest ulatuslik kahju.

2.6 SQL-süst

SQL-süst (ingl SQL injection) on sageli kasutatav andmebaaside ründemeetod. Kui rakendusel on juurdepääs SQL-andmebaasis talletatud andmetele ning sisendandmeid piisavalt ei valideerita, on ründajal võimalik käivitada rakenduse halduskonto õigustes oma SQL-käske, mis lihtsustavad andmete lugemist ja manipuleerimist. Ründaja saab lisada uusi andmeid või käivitada süsteemikäske.

2.7 Andmebaasihalduse süsteemi ebaturvaline konfiguratsioon

Sageli on andmebaasisüsteemi tüüpkonfiguratsioonis aktiveeritud ebavajalikud funktsioonid, mis lihtsustavad ründajal andmebaasis hoitavaid andmeid lugeda või manipuleerida. Näiteks võib ründaja kasutada tüüpinstallatsiooni käigus paigaldatud, kuid organisatsioonis mittekasutatavat rakendusliidest, et hallata andmebaasihalduse süsteemi ilma autentimata. Nii saab ta volitamata juurdepääsu organisatsiooni andmebaasidele.

2.8 Kahjurvara ja ebaturvalised skriptid

Paljudes andmebaasihalduse süsteemides saab toiminguid automatiseerida andmebaasiskriptide ja andmebaasi trigerite abil, mida andmebaasi kontekstis (nt PL/SQL-ga) käivitatakse. Skriptide kontrollimatu kasutuse ja organisatsiooni tarkvaraarenduse nõuetega vastuolu korral satub ohtu andmete turvalisus.

Ründaja saab kahjurprogrammidega või andmebaasiskriptidega manipuleerida andmebaasi (nt selle andmesõnastikku (ingl data dictionary)). Lisaks on seda tüüpi ründeid ja kasutajavigu keeruline märgata.

3 Meetmed

3.1 Elutsükkel

Kavandamine

APP.4.3.M1 Andmebaasisüsteemi turvaeeskiri

Evitus

APP.4.3.M4 Uute andmebaaside kasutuselevõtu reguleerimine

APP.4.3.M11 Riistvara dimensioneerimine

APP.4.3.M12 Andmebaasihalduse süsteemi tüüpkonfiguratsioon

APP.4.3.M16 Andmebaasiühenduste krüpteerimine

Käitus

APP.4.3.M3 Andmebaasihalduse süsteemi turvalisuse tõstmine

APP.4.3.M13 Andmebaasilinkide kitsendav korraldus

APP.4.3.M17 Andmete laadimise või migratsiooni korraldus

APP.4.3.M18 Andmebaasihalduse süsteemi järelevalve

APP.4.3.M19 Mittekvaliteetsete skriptide vältimine

APP.4.3.M20 Regulaarne läbivaatus

Avariivalmendus

APP.4.3.M9 Andmebaasisüsteemi varundamine

Lisanduvad kõrgmeetmed

APP.4.3.M21 Andmebaasi turbe instrumentide

APP.4.3.M22 Avariivalmendus

APP.4.3.M23 Arhiveerimine

APP.4.3.M24 Krüpteerimine andmebaasis

APP.4.3.M25 Andmebaasisüsteemi turvaaudit

3.2 Põhimeetmed

APP.4.3.M1 Andmebaasisüsteemi turvaeeskiri

a. Organisatsiooni üldise infoturvapoliitika põhjal on koostatud andmebaasisüsteemi turvaeeskiri, mis esitab andmebaaside turvalise kasutuse nõuded.

b. Andmebaaside halduse valdkonna vastutajad tunnevad andmebaasisüsteemi turvaeeskirja ja järgivad seda oma töös.

c. Eeskirja nõuetest kõrvale kaldumine dokumenteeritakse ja sellest teavitatakse infoturbejuhti.

d. Andmebaasisüsteemi turvaeeskirja järgimist kontrollitakse regulaarselt, tulemused dokumenteeritakse.

APP.4.3.M3 Andmebaasihalduse süsteemi turvalisuse tõstmine

a. Andmebaasihalduse süsteemi tugevdamise meetmetest on koostatud kontroll-loend.

b. Tugevdusmeetmete rakendamist ja meetmete ajakohasust kontrollitakse regulaarselt, vajadusel korrigeeritakse kontroll-loendit.

c. Andmebaasi paroole ei ole talletatud avatekstina.

APP.4.3.M4 Uute andmebaaside kasutuselevõtu reguleerimine

a. Andmebaaside loomiseks ja kasutuselevõtuks on kehtestatud protseduur.

b. Teave kasutuselevõetava andmebaasi kohta dokumenteeritakse kokkulepitud kujul.

APP.4.3.M9 Andmebaasisüsteemi varundamine

a. Andmebaasisüsteemi ja selles olevaid andmeid varundatakse regulaarselt.

b. Andmebaasisüsteemi varundatakse ka enne andmebaasi loomist, kasutades selleks ette nähtud utiliiti.

c. Andmebaasi taastamise parameetrid määratakse olenevalt andmete kaitsetarbest (vt CON.3 *Andmevarunduse kontseptsioon*).

d. Andmevarunduseks kavandatud mahtude ületamisel kaalutakse andmevarunduse kontseptsiooni (nt võtta kasutusele inkrementvarundus) muutust.

3.3 Standardmeetmed

APP.4.3.M11 Riistvara dimensioneerimine [vastutav spetsialist]

a. Andmebaasihalduse süsteem installitakse piisava ressursivaruga riistvarale.

b. Riistvara dimensioneerimisel on arvestatud eeldatavat nõuete ja mahtude suurenemist plaanitud kasutusaja vältel.

c. Ressursside kasutust seiratakse. Ressursipuudust on võimalik aegsasti märgata ja lahendada.

APP.4.3.M12 Andmebaasihalduse süsteemi tüüpkonfiguratsioon

a. Andmebaasihalduse süsteemide jaoks on koostatud ühtne tüüpkonfiguratsioon.

b. Tüüpkonfiguratsioonist kõrvalekalded kinnitatakse infoturbe juhi poolt ja dokumenteeritakse.

c. Andmebaasihalduse tüüpkonfiguratsiooni kontrollitakse ja vajadusel kohandatakse regulaarselt.

APP.4.3.M13 Lingitud andmebaaside piirangud

a. Andmebaasilinkide (ingl *database links, DB links*) loomise õigused on ainult määratud isikutel.
b. Andmebaasilingid on dokumenteeritud ja neid kontrollitakse regulaarselt.
c. Avalike andmebaasilinkide asemel on eelistatud privaatseid andmebaasilinke (link on kasutatav kasutajakontoga, mille õigustega link loodi).
d. Andmebaasilinke arvestatakse andmebaasisüsteemi varundamisel (vt APP.4.3.M9 *Andmebaasisüsteemi varundamine*).

APP.4.3.M16 Andmebaasiühenduste krüpteerimine

a. Andmebaasisüsteem on konfigureeritud kõiki andmebaasiühendusi krüpteerima.
b. Krüpteerimisprotseduurid ja krüptomehhanismid vastavad kaitsetarbele (vt CON.1 *Krüptokontseptsioon*).

APP.4.3.M17 Andmete laadimise ja migratsiooni korraldus [vastutav spetsialist]

a. On koostatud protseduurid andmete laadimiseks ja migreerimiseks andmebaasi.
b. Pärast laadimist või migreerimist kontrollitakse üleviidud andmete terviklust.

APP.4.3.M18 Andmebaasisüsteemi seire

a. On määratletud andmebaasihalduse süsteemi turvalise käituse jaoks olulised parameetrid, sündmused ja olekud.
b. Rakendusekohased parameetrid, sündmused ja nende läviväärtused kooskõlastatakse rakenduste eest vastutajatega (vt APP.4.3.*M11 Riistvara dimensioneerimine*).
c. Määratletud parameetreid ja sündmusi seiratakse, neile seatud läviväärtuste ületamisel teavitatakse vastutajaid.

APP.4.3.M19 Mittekvaliteetsete skriptide vältimine [arendaja]

a. Andmebaasiskriptide arendamisele on kehtestatud kvaliteedikriteeriumid (vt APP.7 *Tellimustarkvara arendus*).
b. Enne andmebaasiskripti rakendamist viiakse läbi funktsionaaltestid, tulemused dokumenteeritakse.

APP.4.3.M20 Regulaarne läbivaatus

a. Regulaarselt kontrollitakse andmebaasisüsteemi iga komponendi turvameetmete rakendamist.
b. Ülevaatuse käigus kontrollitakse, kas:
   - dokumenteeritud seis vastab hetkeseisule;
   - andmebaasihalduse süsteemi konfiguratsioon vastab dokumenteeritud tüüpkonfiguratsioonile;
   - andmebaasiskriptid on vajalikud ja vastavad organisatsiooni kvaliteedistandardile;
   - andmebaasihalduse süsteemi logide anomaaliatele on reageeritud (vt DER.1 *Turvaintsidentide avastamine*).

c. Läbivaatuste tulemused on dokumenteeritud.

d. Lahknevusi käsitletakse kehtestatud korra kohaselt.

3.4 Kõrgmeetmed

APP.4.3.M21 Andmebaasi turbe instrumendid (C-I)

a. Andmebaaside kaitseks kasutatakse täiendavaid turvatooteid, mis võimaldavad:
   - koostada andmebaaside turbe aruandlust;
   - lisavõimalusi andmebaasi konfigureerimiseks ja õiguste halduseks;
   - avastada (nt jõurünne kasutajakontole, SQL-süst) ja vältida ründeid;
   - toetada auditi läbiviimist (nt konfiguratsiooni turvalisuse kontrollimiseks).

APP.4.3.M22 Avariivalmendus (C-I-A)

a. Andmebaasisüsteemi intsidendi puhul käitumiseks ning andmebaaside tavapärase seisundi taastamiseks on koostatud avariikava.

b. Andmebaasihalduse avariikava määrab avariihalduse protseduurid, teatamisteed, nõutavad teavitusajad, vajalikud ressursid ja vastutajad (vt DER.4 *Avariihaldus*).

c. Avariikavas on arvestatud kõigi andmebaasist sõltuvate IT-süsteemide vajadustega.

APP.4.3.M23 Arhiveerimine (I-A)

a. Andmebaasisüsteemi andmete arhiveerimiseks on koostatud andmebaasisüsteemi arhiveerimiskava.

b. Arhiveerimiskavas on määratletud arhiveerimise meetodid, arhiveerimisvälbad ja arhiveeritud andmete säilitustähtajad.

c. Arhiveeritud andmete taastamist harjutatakse regulaarselt, tulemused dokumenteeritakse.

APP.4.3.M24 Krüpteerimine andmebaasis (C)

a. Andmebaasis hoitavad andmed on krüpteeritud (vt CON.1 *Krüptokontseptsioon*).

b. Andmebaasi krüpteerimisel on täiendavalt arvestatud järgmiste teguritega:
   - mõju sooritusvõimele;
   - võtmehaldusprotsessid ja -meetmete rakendatavus;
   - mõju andmevarundusele ja taastele;
   - mõju funktsionaalsusele (nt sorteerimise kasutamisele).

APP.4.3.M25 Andmebaasisüsteemi turvaaudit (C-I-A)

a. Andmebaasisüsteemide turvameetmete rakendamist auditeeritakse regulaarselt.

b. Auditi läbiviimisel arvestatakse andmebaasitaristu (nt kataloogiteenuste) ja andmebaasihalduse süsteemi tootespetsiifilisi, tehnilisi ja rakenduslikke aspekte.

APP.4.4 Kubernetes

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed konteinerduse (ingl *containerization*) automatiseerimiseks ja halduseks ning andmete kaitseks Kubernetese klastris (ingl *cluster*). Kubernetese klaster koosneb konteineri käituskeskkonda (ingl *runtime*) sisaldavatest sõlmedest (ingl *node*). Väiksem Kubernetese orkestreeritav (ingl *orchestration*) objekt on ühes operatsioonisüsteemis installitud konteiner (ingl *container*) või konteinerite grupp (edaspidi nimetatud kui *pod*).

Kubernetes on *de facto* standardlahendus konteinerite orkestreerimiseks nii avalikus kui privaatpilves.

1.2 Vastutus

Kubernetese turvameetmete rakendamise eest vastutab IT-talitus.

Lisavastutajad

Lisavastutajad puuduvad.

1.3 Piirangud

Moodul käsitleb Kubernetese kasutuselevõtu, rakendamise ja haldusega seotud meetmeid, sh meetmeid spetsialiseeritud riistvarakomponentide, nt CNI (Container Network Interface) ja CSI (Container Storage Interface) tarbeks.

Antud mooduli meetmeid käsitletakse alati koos meetmetega moodulist SYS.1.6 *Konteinerdus*.

Meetmete rakendamisel ei ole oluline, millist konteineri käituskeskkonda (nt Docker, r*unC*, *containerd*, Windows Container) kasutatakse.

Kubernetese klastris töötavate IT-teenuste turvameetmed on esitatud vastavaid teenuseid käsitlevates moodulites (nt APP.3.2 *Veebiserver*).

2 Ohud

2.1 Vead autentimisel ja volitamisel Kubernetese juhttasandil

Kubernetese juhttasand (ingl Control Plane) sisaldab Kubernetese sõlmede (ingl node), käituskeskkondade (ingl runtime) ja klastrite (ingl cluster) orkestreerimiseks kasutatavaid rakendusi. Tööks Kubernetese juhttasandil on vajalik juurdepääs administraatoriõigustes (eelispääs). Eelispääsud on enamasti realiseeritud selleks määratud võrguportide või Unix Socket'i kaudu.

Sageli on autentimis- ja krüptomehhanismid turvaliseks andmevahetuseks olemas, kuid neid pole vaikeseadistuses ega hilisema konfigureerimise käigus aktiveeritud. Kui ründaja saab juurdepääsu sõlmele või võrguühendusele, võib ta kasutada piisava kaitseta eelispääsu andmete turvalisust ohustavate süsteemikäskude edastamiseks.

2.2 *Pod*'i identsustõendi konfidentsiaalsuse kadu

Pod'id vajavad Kubernetese juhtasandiga suhtlemiseks identsustõendit (ingl *token*). *Pod'*i ründamise tagajärjel võib identsustõend sattuda ründaja valdusesse. Seejärel on ründajal

võimalik luua ühendus Kubernetese juhttasandiga ja piisavate volituste olemasolul teha juhttasandi seadistuses või orkestreerimises volitamata muudatusi.

2.3 Pod’i põhjustatud ressursikonflikt

Üks *pod* võib ressursikonflikti tulemusena üle koormata sõlme, millel *pod* asub või takistada kogu Kubernetese orkestreerimist. Ressursikonflikt võib ohustada kõigi teiste *pod*’ide kättesaadavust antud *pod’*ist või takistada sõlme tavapärast toimimist.

2.4 Volitamata muudatused Kubernetese klastris

Automatiseerimiseks CI/CD (Continuous Integration / Continuous Delivery) tööriistade abil on vajalik tööriistadele anda klastris tegutsemiseks eelisõigused. Eelisõiguste kasutamisega kaasneb oht Kubernetese klastris volitamata muudatuste tegemiseks. Näiteks paigaldab arendaja klastrisse rakenduse uue versiooni, mida pole piisavalt testitud või mis ei ole korrakohaselt kasutuseks kinnitatud.

Kui CI/CD keskkonnas on jagatud liigseid pääsuõigusi, on oht, et volitamata kasutaja või kahjurvara saab juurdepääsu klastris olevatele andmetele. See võimaldab ründajal rakenduste andmeid muuta või kustutada.

2.5 Volitamata juurdepääs *pod*’ile

Kõik *pod*’id on võimelised suhtlema üksteisega, klastris olevate sõlmedega ja muude IT-süsteemidega. Kahjurvara või ründaja saab andmevahetuspiirangute puudumist kasutada Kubernetese juhttasandi, teiste *pod*’ide või sõlmede ründamiseks.

Kui klastri *pod*’ile saadakse volitamata juurdepääs väljaspoolt klastrit, on võimalik rünnata teenuseid, mis peaksid tegelikult olema juurdepääsetavad ainult klastri sees. Oht on suurem kui kui välise juurdepääsuta teenustes on turvanõrkuse olemasolu lubatav või sisekasutuseks mõeldud teenuste turvauuendeid paigaldatakse ebaregulaarselt.

3 Meetmed

3.1 Elutsükkel

Kavandamine

APP.4.4.M1 Rakenduste eraldatuse kavandamine

APP.4.4.M2 Rakenduste arenduse automatiseerimine CI/CD abil

APP.4.4.M3 Kubernetese identiteedi- ja õiguste halduse kavandamine

Evitus

APP.4.4.M4 Pod’ide eraldamine

APP.4.4.M7 Kubernetese võrkude eraldamine

Käitus

APP.4.4.M5 Klastri andmete varundamine

APP.4.4.M8 Kubernetese konfiguratsioonifailide turve

APP.4.4.M9 Kubernetese teenusekontode turve

APP.4.4.M10 Automatiseerimisprotsessi turve

APP.4.4.M11 Konteinerite kasutuse seire

APP.4.4.M12 Taristurakenduste turve

Lisanduvad kõrgmeetmed

APP.4.4.M13 Automaatsed konfiguratsiooniauditid

APP.4.4.M14 Spetsialiseeritud sõlmede kasutamine

APP.4.4.M15 Rakenduste eraldamine sõlme ja klastri tasemel

APP.4.4.M16 Kubernetese operaatorite kasutamine

APP.4.4.M17 Sõlmede atesteerimine

APP.4.4.M18 Mikrosegmenteerimine

APP.4.4.M19 Kubernetese kõrgkäideldavuse tagamine

APP.4.4.M20 Juhttasandi salvestusruumi krüpteerimine

APP.4.4.M21 Pod'ide perioodiline taaskäivitamine

3.2 Põhimeetmed

APP.4.4.M1 Rakenduste eraldatuse kavandamine

a. Enne rakenduste käidukeskkonda paigaldamist on kavandatud, kuidas *pod*'i paigaldatav rakendus eraldatakse teistest rakendustest ning oma test- ja arenduskeskkondadest.

b. Lähtuvalt rakenduste kaitsetarbest ja võimalikest riskidest on määratud nimeruumide (ingl *namespace*), metasiltide (ingl *meta tag*), klastrite ja võrkude arhitektuur ning otsustatud virtuaalserverite kasutusvajadus.

c. Kavandamise käigus on koostatud võrgu, CPU ja püsimälu eraldamise reeglid.

d. Rakenduste eraldamine vastab organisatsiooni üldisele võrguarhitektuurile ja võrgu tsoneerimise põhimõtetele.

e. Iga rakendus ja kõik rakendusega seotud programmid on kavandatud töötama oma Kubernetese nimeruumis.

f. Ühes Kubernetese klastris on ainult ühesuguse kaitsetarbega ja sarnaste võimalike ründevektoritega rakendused.

APP.4.4.M2 Rakenduste arenduse automatiseerimine CI/CD abil

a. Kubernetese rakenduste arenduse automatiseerimine CI/CD (Continuous Integration / Continuous Delivery) abil hõlmab kogu rakenduse elutsüklit alates selle kavandamisest kuni kasutuselt eemaldamiseni (sh arendust, testimist, käitamist, seiret ja uuenduste paigaldamist).

b. CI/CD kavandamisel on määratud vajalikud rollid ning ja minimaalselt vajalikud õigused/ volitused.

c. Automatiseerimise kavandamisel on määratud, kuidas kaitstakse Kubernetese rakendustes töödeldavaid andmeid.

APP.4.4.M3 Kubernetese identiteedi- ja õiguste halduse kavandamine

a. Kõik Kubernetese ja juhttasandi (ingl *Control Plane*) rakenduste kasutajad autenditakse. Kubernetese kasutajatele antud volitused võimaldavad teha ainult tööülesande täitmiseks vajalikke toiminguid.

b. Automatiseeritud keskkonnas kasutatav tarkvara autenditakse ja tarkvarale on antud ainult vajalikud volitused. Autentimine ja volitamine toimub olenemata sellest, kas toimingud toimuvad kliendi, veebiliidese või rakendusliidese (API) kaudu.

c. Kubernetese haldustoimingud on lubatud ainult isikustatud kasutajatele, anonüümsed toimingud on keelatud. Automatiseerimisprotsesse saab määrata ja muuta ainult kitsas töötajate ring.

d. Kubernetese salvestusruume (*Persistent Volumes*) saavad luua või muuta ainult selleks määratud haldurid.

APP.4.4.M4 Pod'ide eraldamine

a. Sõlme (ingl *node) o*peratsioonisüsteemi tuumas on rakendatud isoleerimismehhanismid *pod*'ide ressursikasutuse (nt Linuxi nimeruumid ja cgroups) nähtavuse piiramiseks.

b. Pod'ide eraldamine hõlmab vähemalt protsessi ID-sid, protsessidevahelist andmevahetust, kasutaja ID-sid, failisüsteemi ja võrku (sh hostinime).

APP.4.4.M5 Klastri andmete varundamine

a. Klastri andmeid varundatakse perioodiliselt. Varukoopia sisaldab vähemalt järgmist:
   - salvestusruum (*Persistent Volumes*);
   - Kubernetese ja teiste juhttasandi programmide konfiguratsioonifailid;
   - Kubernetese klastri olekuteave (sh laiendused);
   - konfiguratsiooniandmebaasid (eriti *etcd*);
   - kõik taristurakendused, mis on vajalikud klastri ja selles sisalduvate teenuste toimimiseks;
   - koodi- ja tõmmiseregistrite (ingl *image registries*) andmed.

b. Võimalusel on varundatud ka rakenduste käituse hetktõmmised (ingl *snapshot*), kuid hetktõmmised ei saa olla ainukeseks varundusmeetodiks.

3.3 Standardmeetmed

APP.4.4.M6 Pod'ide turvaline lähtestamine

a. *Pod*'i rakenduse lähtestamine tehakse spetsiaalses *init* konteineris.

b. Rakenduse lähtestamine lõpetab kõik pooleliolevad protsessid. Kubernetese muud konteinerid käivitatakse alles pärast rakenduse edukat lähtestamist.

APP.4.4.M7 Kubernetese võrkude eraldamine

a. Sõlmede haldusvõrgud, juhttasandi ja rakenduseteenuste üksikvõrgud on eraldatud.

b. Pod'ide võrgus on avatud ainult *pod*'i tööks vajaminevad pordid.

c. Kui Kubernetese klastris on mitmeid rakendusi, on Kubernetese nimeruumide vahelised võrguühendused vaikeseadistusena blokeeritud. Tööks vajalikud võrguühendused lisatakse lubatud loendisse (ingl *whitelisting*) vastava vajaduse tekkimisel.

d. Sõlmede, käituskeskkonna ja Kubernetese (sh selle laiendused) haldamiseks vajalikud võrgupordid on juurdepääsetavad ainult haldusvõrgust ja selleks määratud *pod*'idest.

e. Kubernetese CNI-de (Container Network Interface) haldamise ja võrgureeglite muutmise õigused on ainult selleks määratud halduritel.

APP.4.4.M8 Kubernetese konfiguratsioonifailide turve

a. Kubernetese klastri konfiguratsioonifailid (sh kõigi laienduste ja rakenduste seadistused) on varustatud versiooninumbrite ja selgitustega.

b. Konfiguratsioonifailide halduseks kasutatava tarkvara juurdepääsuõigused on võimalikult piiratud. Eriti hoolikalt on reguleeritud juhttasandi konfiguratsioonifailide lugemis- ja kirjutamisõigused.

APP.4.4.M9 Kubernetese teenusekontode turve

a. Pod'is ei kasutata vaikeseadistuses määratletud teenusekontot (ingl *service account*), selle konto õigused on eemaldatud.

b. Erinevate rakenduste pod'idele on loodud eraldi teenusekontod. Teenusekontode õigused on piiratud minimaalselt vajalike õigusteni.

c. Teenusekontot mittevajaval *pod*'il teenusekonto puudub. Sellised *pod*'id kasutavad Kubernetese juhtasandiga suhtlemiseks identsustõendit (ingl *token*).

d. Eeliskasutaja õigustega teenusekontosid kasutatakse ainult juhttasandi ning eeliskontot tingimata vajavates *pod*'ides.

e. Automatiseerimisrakendused kasutavad identsustõendit isegi juhul kui sarnase ülesande täitmiseks saaks kasutada ühist teenusekontot.

APP.4.4.M10 Automatiseerimisprotsessi turve

a. Kõik automatiseerimistarkvara protsessid, sh CI/CD ja selle andmekonveierid (ingl *pipeline*), töötavad ainult minimaalselt vajalikes õigustes.

b. Automatiseerimistarkvara kaudu *pod*'i konfiguratsiooni muutmine või *pod*'i käivitamine on lubatud ainult selleks määratud kasutajatele.

APP.4.4.M11 Konteinerite kasutuse seire

a. *Pod*'i konteinerite jaoks on määratud ja seadistatud konteinerite käitamise seisundikontrollid (ingl *health check*) ja rakenduse või teenuse jaoks sobiv kontrollide läbiviimise regulaarsus.

b. Seisundikontrolli tulemustest lähtuvalt on Kubernetes võimeline pod'e sulgema või taaskäivitama.

APP.4.4.M12 Taristurakenduste turve

a. Juhul kui automatiseerimisel, kõvaketta halduses või konfiguratsioonifailide varundamisel kasutatakse tõmmiseid (ingl *image*), on arvestatud vähemalt järgmisega:
   - isikustatud kontode ja teenusekontode pääsuõigused;
   - andmevahetuse krüpteerimine;
   - andmeside krüpteerimine kõigis võrguportides;
   - minimaalselt vajalikud volitused kasutajatele ja teenusekontodele;
   - muudatuste logimine;
   - regulaarne andmevarundus.

3.4 Kõrgmeetmed

APP.4.4.M13 Automaatsed konfiguratsiooniauditid (C-I-A)

a. Sõlmede, Kubernetese ja rakendusi sisaldavate *pod*'ide seadistuse kontrolliks on loodud automaatkontrollid, mis võrdlevad tegelikke seadeid määratud loendite ja võrdlusnäitajatega.

b. On loodud reeglid Kubernetese klastriga sobivate audititööriistade kasutamiseks.

APP.4.4.M14 Spetsialiseeritud sõlmede kasutamine (C-I-A)

a. Kubernetese klastris on loodud spetsialiseeritud ülesande täitmiseks loodud sõlmed (ingl *node*), millel töötavad ainult spetsialiseeritud ülesande täitmiseks kavandatud *pod*'id.

b. Rakenduste sissetulev ja väljaminev andmevahetus teiste võrkudega on reguleeritud eelseadistatud eriotstarbeliste sõlmedega (ingl *bastion node*).

c. Juhttasandi (ingl *Control Plane*) pod'id asuvad nn haldussõlmedes (ingl *management node*). Kogu andmevahetus juhttasandiga on viidud läbi haldusõlmede.

d. Varundusteenustele spetsialiseeritud pod'id on koondatud varundussõlmedesse (ingl *storage node*).

APP.4.4.M15 Rakenduste eraldamine sõlme ja klastri tasemel (C-I-A)

a. Väga kõrge kaitsetarbega rakendused on paigutatud eraldatud Kubernetese klastrisse või sõlmedesse, mis pole teistele rakendustele kättesaadavad.

APP.4.4.M16 Kubernetese operaatorite kasutamine (C-I-A)

a. Kriitiliste rakenduste ja juhttasandi programmide tööülesanded on automatiseeritud Kubernetese operaatoriga (ingl *operator*).

APP.4.4.M17 Sõlmede atesteerimine (C-I-A)

a. Sõlmed esitavad juhttasandile krüptograafiliselt ja eelistatavalt TPM-iga (Trusted Platform Module) kontrollitud turvalise oleku tõendeid.

b. Juhttasand aktsepteerib ainult kastri sõlmi, mis on oma turvalisust edukalt demonstreerinud.

APP.4.4.M18 Mikrosegmenteerimine (C-I)

a. *Pod*'ide vaheline suhtlus Kubernetese nimeruumis on lubatud ainult määratud võrguportide kaudu. Mittevajalikud andmeühendused on Kubernetese CNI-s kehtestatud reeglitega keelatud.

b. CNI reeglites on üheselt määratletud andmeühenduse allikad ja sihtkohad ning andmevahetuse filtreerimine kas teenuse nime, metaandmete, teenusekontode või sertifikaadipõhise autentimise alusel.

c. Mikrosegmenteerimiseks kasutatud kriteeriume saavad muuta ainult selleks volitatud isikud ja haldusteenused.

APP.4.4.M19 Kubernetese kõrgkäideldavuse tagamine (A)

a. Ühes lokatsioonis ilmneva tõrke või katkestuse korral jätkavad klastrid ja seega ka pod'ide rakendused tööd ilma märgatava katkestuseta või on võimalik lühikese aja jooksul taaskäivitada rakendused teises lokatsioonis.

b. Rakenduste taaskäivitamiseks teises lokatsioonis on ette valmistatud kõik vajalikud konfiguratsioonifailid, tõmmised, kasutajakontod, võrguühendused ja muud tööks vajalikud ressursid, sh tööks vajalik riistvara.

c. Klastri kõrgkäideldavuse tagamiseks on Kubernetese juhttasand, klastrite riistvara, *pod*'id ja rakendused jaotatud erinevate lokatsioonide vahel selliselt, et nt riistvara rike ega tulekahju ei põhjustaks rakenduse käideldavuskadu.

d. Klastri, pod'ide ja rakenduste koostöö kontrollimiseks viiakse läbi regulaarseid, süsteemirikkeid simuleerivaid teste.

APP.4.4.M20 Juhttasandi salvestusruumi krüpteerimine (C)

a. Juhttasandi püsivate andmetega failisüsteemid (eriti *etcd*) ja rakendusteenused on krüpteeritud.

APP.4.4.M21 Pod'ide perioodiline taaskäivitamine (C-I-A)

a. Kõrgendatud välise sekkumise ohu ja väga kõrge kaitsetarbe puhul rakendatakse *pod*'ide regulaarset seiskamist ja taaskäivitamist (ingl *restart*). Soovitatav on, et *pod* 'i pidev tööaeg on väiksem kui 24 tundi.

b. Taaskäivituse ajal on tagatud pod'i rakenduste käideldavus.

4 Lisateave

Lühend	Publikatsioon
[NIST]	NIST Special Publication 800-190 "Application Container Security Guide", https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-190.pdf
[CIS]	CIS Kubernetes Benchmark, https://www.cisecurity.org/benchmark/kubernetes/
[OCI]	Open Container Initiative, https://www.opencontainers.org/
[CNCF]	Cloud Native Computing Fountation, https://www.cncf.io/

APP.5: Rühmatarkvara

APP.5.2 Microsoft Exchange ja Outlook

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed keskmiste ja suurte organisatsioonide jaoks ette nähtud rühmatarkvaralahenduste Microsoft Exchange'i ja Outlooki turvaliseks kasutamiseks.

1.2 Vastutus

Microsoft Exchange'i ja Outlooki meetmete täitmise eest vastutab IT-talitus.

1.3 Piirangud

Moodulis esitatavad meetmed täiendavad mooduli APP.5.3 *E-posti server ja klient üldiselt* meetmeid *Microsoft Exchange* süsteemis.

Serveriplatvormi, operatsioonisüsteemi ja kliente käsitlevad meetmed on esitatud moodulites SYS.1.1 *Server üldiselt* ja SYS.2.1 *Klientarvuti üldiselt* ning operatsioonisüsteeme käsitlevates moodulites.

2 Ohud

2.1 *Microsoft Exchange*'i ja *Outlooki* puuduv või puudulik rakendamise kord

Kui *Microsoft Exchange*'i *ja Outlooki* jaoks pole kehtestatud selle rakendamise korda, võidakse teha haldusvigu. Näiteks kui *Microsoft Exchange* integreeritakse *Active Directory*'ga vääralt, võivad andmed osaliselt või täielikult minna kaduma. Sama kehtib siis, kui postkastide andmebaase kustutatakse koordineerimata viisil.

Kui *Microsoft Outlooki* klientide juurdepääs *Microsoft Exchange*'i serverile on piiramata, on võimalik saada juurdepääs konfidentsiaalsetele andmetele.

2.2 *Microsoft Exchange*'i väär migreerimine

Kui uuele *Microsoft Exchange*'i serveri versioonile migreerimine ei ole hoolikalt kavandatud ega ellu viidud, võivad ilmneda konfigureerimisseadete muutumisest ja vigastest logimisseadetest põhjustatud probleemid. Migreerimise vead võivad häirida infovahetust organisatsiooni sees ning suhtlust klientide ja partneritega.

Uued operatsioonisüsteemid toovad kaasa muutuvad nõuded kataloogiteenustele ja domeenikontseptsioonile. Need omakorda võivad mõjutada *Microsoft Exchange'*i funktsioneerimist.

2.3 *Microsoft Exchange*'i lubamatu brauseripääs

Microsoft Exchange'i serveri püsikomponendi Internet Information Services (IIS), mida kasutatakse meilikontodele juurdepääsu saamiseks brauseri vahendusel, konfigureerimisvigu saab ründaja ära kasutada sisevõrku pääsemiseks.

Kui brauser võimaldab juurdepääsu ka e-kirjadele, saab ründaja ilma otsese juurdepääsuta organisatsiooni võrgule lugeda e-kirju, luurata e-posti aadresse ning saata rämpsposti.

2.4 Muude süsteemide lubamatu sidumine *Microsoft Exchange*'iga

Kui *Microsoft Exchange*'i migreerimise käigus väliste süsteemidega suhtlemiseks mõeldud konnektoritega ei arvestata, võivad olemasolevad konnektorid osutuda migreeritud *Microsoft Exchange*'i versioonidega ühildumatuks. Nii võivad e-kirjad kaduma minna või saab neid soovimatult muuta.

Väljaspool homogeenset Microsofti keskkonda ei saa tagada *Microsoft Exchange*'i süsteemiga mitteseotud turvasätete kehtivust. Sama kehtib *Microsoft Exchange*'is määratud Windowsi serveri turvaparameetrite kohta. Asjatundmatult seotud võõrad süsteemid võivad põhjustada andmekadu või süsteemi mittetöötamist.

2.5 *Microsoft Exchange*'i ja Outlooki pääsuõiguste väär haldus

Kui Outlooki kliendi juurdepääsuõigusi või Microsoft Exchange'is talletatud andmete juurdepääsuõigusi määratakse ja hallatakse vääralt, võivad tekkida turvanõrkused. Kui peale vajalike õiguste antakse kasutajatele liigseid õigusi, luuakse nii volitamata juurdepääs konfidentsiaalsele teabele.

2.6 *Microsoft Exchange*'i väär konfiguratsioon

Vääralt konfigureeritud süsteemid on Microsoft Exchange edukate rünnete levinum põhjus. Microsoft Exchange'i süsteemi keerukuse tõttu võivad mitmesugused konfigureerimisseaded ja üksteist mõjutavad parameetrid põhjustada erinevaid turvaprobleeme.

Võimalikud konfigureerimisvead on näiteks Microsoft Exchange'i komponentide installimine ja käitamine sobimatutes süsteemides, andmevahetuse krüpteerimata jätmine, Microsoft Exchange'i kliendi ebapiisavad juurdepääsud serverile ning õiguste väär määramine Microsoft Exchange'i andmebaasi loomise või lähtestamise korral.

2.7 *Outlooki* väär konfiguratsioon

Outlooki konfigureerimisvead, näiteks kasutajale liigsete juurdepääsuõiguste andmine, tekitavad erinevaid turvaprobleeme. Vääralt valitud suhtlusprotokoll võib põhjustada spetsiifilisi turvanõrkusi. Samuti on võimalik *Outlooki* e-kirjade krüpteerimiseks ja allkirjastamiseks kasutatava privaatvõtme kompromiteerimine. Kui krüpteerimist kasutatakse võrgutasemel (nt IPSeci või TLS-i kaudu), võivad krüpteerimismehhanismid vääralt konfigureeritud kliendi korral osutuda mittetoimivaks.

2.8 *Outlookile* lisatud makrode ja programmiliideste tõrked ja väärkasutus

Outlooki kui tuntud grupitöövahendit saab kuritarvitada kahjurtarkvara levitamiseks. Outlooki makrode kaudu levitatav kahjurtarkvara võimaldab andmetele juurde pääseda, neid muuta või kustutada.

Makrodes tehtud vigade või tahtlike manipulatsioonide tulemusel (nt kui makro arvutusvea tõttu arvutatakse valesid väärtusi) võib organisatsioon vastu võtta vääraid ja ebamajanduslikke juhtimisotsuseid. Halvasti koostatud makro võib automaatselt andmeid lekitada ja neid volitamata kasutajatele kättesaadavaks teha.

3 Meetmed

3.1 Elutsükkel

Kavandamine

APP.5.2.M1 *Microsoft Exchange'*i ja *Outlooki* rakendamise kava

APP.5.2.M2 *Microsoft Exchange*'iga sobiv taristu

Evitus

APP.5.2.M3 *Microsoft Exchange*'i pääsuõiguste haldus

APP.5.2.M7 *Microsoft Exchange*'i migreerimise kord

APP.5.2.M9 *Microsoft Exchange*'i serveri turvaline konfiguratsioon

APP.5.2.M10 *Outlooki* turvaline konfiguratsioon

Käitus

APP.5.2.M5 *Microsoft Exchange*'i varundus

APP.5.2.M11 *Microsoft Exchange*'i ühenduste turve

APP.5.2.M12 *Outlook Anywhere*, *MAPI over HTTP* ja *Outlook Web App* kasutamise turve

Lisanduvad kõrgmeetmed

APP.5.2.M17 *Microsoft Exchange*'i süsteemi andmebaaside krüpteerimine

3.2 Põhimeetmed

APP.5.2.M1 Microsoft Exchange'i ja Outlooki rakendamise kava

a. *Microsoft Exchange*'i ja *Outlooki* rakendamise kava koostamisel on arvestatud vähemalt järgmist:
   - meilitaristu struktuur;
   - *Microsoft Exchange*'iga ühenduvad klient- ja serversüsteemid;
   - funktsioonilaienduste kasutamine;
   - kasutatavad protokollid.

APP.5.2.M2 Microsoft Exchange'iga sobiv taristu

a. Rakendamise kavale tuginedes on valitud sobivad *Microsoft Exchange*'i taristu komponendid, loodud taristu struktuur ja otsustatud, millises järjekorras taristu teostatakse.

b. On tehtud põhjendatud valik pilv- ja lokaalteenuse vahel.

APP.5.2.M3 Microsoft Exchange'i pääsuõiguste haldus

a. *Microsoft Exchange*'i taristu süsteemide jaoks on koostatud ja dokumenteeritud pääsuõiguste kontseptsioon.

b. IT-talitus kasutab *Microsoft Exchange*'i poole pöördumiseks serveripoolseid kasutajaprofiile.

c. NTFS tüüpõigused on seatud nii, et *Microsoft Exchange*'i kataloogi juurdepääs on ainult volitatud halduritel ja vajalikel süsteemikontodel.

APP.5.2.M5 Microsoft Exchange'i varundus

a. *Microsoft Exchange*'i andmeid varundatakse perioodiliselt.

b. *Microsoft Exchange*'i andmebaase varundatakse lisaks veel enne uuendite installimist ja enne konfiguratsiooni muudatusi.

c. Kustutatud *Microsoft Exchange*'i objektid eemaldatakse andmebaasist lõplikult alles pärast määratud aja möödumist.

3.3 Standardmeetmed

APP.5.2.M7 Microsoft Exchange'i migreerimise kord

a. Migreerimise etapid on hoolikalt kavandatud ja dokumenteeritud. Migreerimise kavas on arvestatud postkastide, objektide, turvapoliitikate, *Active Directory* ülesehituse,

meilisüsteemide ning *Microsoft Exchange*'i ja *Outlooki* versioonide funktsioonide erinevustega.

b. Enne installimist töökeskkonda on uut süsteemi testitud eraldi testimisvõrgus. Testimise tulemused on dokumenteeritud.

APP.5.2.M9 Microsoft Exchange'i serveri turvaline konfiguratsioon

a. *Microsoft Exchange'*i serverid on konfigureeritud vastavalt e-posti turvaeeskirja nõuetele (vt APP.5.3.M6 *E-posti turvaeeskiri*).

b. *Microsoft Exchange'*i konnektorite konfiguratsioon on turvaline. Konnektorite konfiguratsiooni muudatused dokumenteeritakse.

c. *Microsoft Exchange*'i tegevuste logimine on aktiveeritud.

d. Funktsioonilaienduste (nt *Microsoft Exchange ActiveSync*, pordi peegeldamine, spämmifilter, *Outlook Web App* või lekketõrje) kasutuselevõtul on arvestatud nende turvaaspekte.

APP.5.2.M10 Outlooki turvaline konfiguratsioon

a. Igale kasutajale on loodud oma *Outlooki* profiil koos kasutajaspetsiifiliste seadetega.

b. Kasutaja saab muuta vaid selleks spetsiaalselt lubatud seadeid (nt kirja jaluse seadmine, eemaloleku funktsiooni aktiveerimine).

c. Suhtluse teisele osapoolele ei esitata üleliigset (nt e-kirja avamise automaatteavitus) ja siseinfot paljastavat (nt organisatsiooni struktuur) teavet.

APP.5.2.M11 Microsoft Exchange'i ühenduste turve

a. On määratud ja dokumenteeritud, milliste turvamehhanismidega suhtlust *Microsoft Exchange*'i süsteemidega kaitstakse.

b. On rakendatud meetmed järgmiste komponentide kaitseks:

- haldusliidesed;
- klient-server-suhtlus;
- olemasolevad *WebDAV*-liidesed;
- serveritevaheline suhtlus ja sõnumside;
- avaliku võtme taristu (ingl *Public Key Infrastructure*, PKI), millel *Outlooki* e-kirjade krüpteerimine põhineb (S/MIME).

APP.5.2.M12 Outlook Anywhere, MAPI over HTTP ja Outlook Web App kasutamise turve

a. *Outlook Anywhere*, *MAPI over HTTP* ja *Outlook Web App* on konfigureeritud vastavalt organisatsiooni turvanõuetele ja Microsoft Exchange'i turvaeeskirjale.

b. *Microsoft Exchange*'i juurdepääs Interneti kaudu on antud ainult põhjendatud vajaduse alusel määratud kasutajatele.

3.4 Kõrgmeetmed

APP.5.2.M17 Microsoft Exchange'i süsteemi andmebaaside krüpteerimine (C)

a. On dokumenteeritud juhend PST-failide ja *Managed Store*'i krüpteerimiseks.

b. Kasutajaid on koolitatud PST-failide krüpteerimise ja turvamehhanismide kasutamise alal.

c. Lokaalse arvuti PST-failis hoitavate e-kirjade turbe tagamiseks kasutatakse kas failisüsteemi põhist krüpteeringut (nt *Encrypting File System*, EFS) või kõvaketta krüpteerimist (nt *Windows BitLocker*).

APP.5.3 E-posti server ja klient üldiselt

1 Kirjeldus

1.1 Eesmärk

Esitada üldised meetmed e-posti serveris ja e-posti klientides töödeldavate andmete kaitseks.

1.2 Vastutus

„E-posti server ja klient üldiselt“ meetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Kasutaja, ülemus.

1.3 Piirangud

Moodulis esitatakse üldised meetmed e-posti serveri ja klientide kaitseks. Moodulis ei käsitleta rühmatarkvara muud funktsionaalsust (nt kalender ja kontaktihaldus) ning pilvteenusena kasutatavat rühmatarkvara (nt Microsoft 365, Google G Suite).

Serveriplatvormi, operatsioonisüsteemi ja kliente käsitlevad meetmed on esitatud moodulites SYS.1.1 *Server üldiselt* ja SYS.2.1 *Klientarvuti üldiselt* ning operatsioonisüsteeme käsitlevates moodulites. Logimist käsitletakse moodulis OPS.1.1.5 *Logimine* ja varundamist moodulis CON.3 *Andmevarunduse kontseptsioon*.

2 Ohud

2.1 E-posti kasutamise puudulik kavandamine

Kui e-posti teenuse rakendamisel ei järgita protseduure ja korralduslikke ning tehnilisi eeskirju, võib sellest tulenev määramatus põhjustada vääraid seadeid, programmeerimisvigu ja (organisatsioonisiseseid/-väliseid) ründeid. Kui tehnilised ja organisatoorsed turvameetmed on jäänud rakendamata, suureneb e-kirjaga saadud kahjurvaraga nakatumise ning väliste rünnete õnnestumise oht.

2.2 E-posti serveri ja klientide väär seadistamine

E-posti taristu ja tarkvara seadistuse keerukusest tingituna ning mitmete parameetrite koosmõjul võivad tekkida olukorrad, kus turvakriitilisi seadeid (nt üksikute andmete krüpteerimine või õiguste piiramine) on eiratud. Turvakriitiliste parameetrite eiramine võib põhjustada andmete käideldavuse, autentsuse ja konfidentsiaalsuse kadu. E-posti serveri seadistusviga võib põhjustada e-kirjade serverisse „kinnijäämist“, sõnum ei jõua ettenähtud aadressile. Turvanõrkustega e-posti serverit võib ründaja kasutada rämpsposti levitamiseks. Tihti jäetakse e-posti serveris kontrollimata, kas kiri on tegelikult tulnud sellelt serverilt, mida kirja saatja aadressi järgi võib eeldada.

2.3 E-posti ebausaldusväärsus

Kuigi e-posti sõnumivahetus on üldjuhul kasutajatele mugav ja kiire viis andmeid vahetada, pole see alati usaldusväärne. Näiteks võivad saadetud sõnumid viibida või kaduma minna vääralt seadistatud e-posti serveri või sidekanalite häire tõttu. Legitiimsed sõnumid võivad teinekord jääda kinni rämpsposti filtritesse, samuti võib e-kiri kaotsi minna, kui saaja aadress pole õigesti sisestatud. Halvimal juhul võidakse konfidentsiaalne teave saata kogemata valele adressaadile. Ründaja võib krüptograafiliselt kaitsmata e-posti sõnumivahetusele juurde pääseda ja vestlusi sihipäraselt pealt kuulata.

2.4 Kahjurvara levitamine

Ründaja võib e-posti kasutada kahjurvara levitamiseks ja arvutite ning IT-süsteemide teadlikuks nakatamiseks. Kahjurkoodi on võimalik peita e-kirja sisusse. Kui e-posti klient ei ole turvaliseks seadistatud, võib kahjurkood käivituda kohe pärast kirja avamist. Teine võimalus kahjurvara levitamiseks on peita see e-kirjale lisatud failimanusesse. Kahjurvara aktiveerub kohe pärast e-kirjale lisatud faili avamist. Ründaja võib niimoodi käivitada lunavara (ingl ransomware) ründe või kasutada nakatunud arvuteid võrguliikluse pealtkuulamiseks ja andmete varastamiseks.

2.5 Suhtlusrünne

E-posti teel läbiviidav suhtlusrünne (ingl social engineering) kasutab ära töötajate inimlikke omadusi (nt abivalmidus, usaldus, tähelepanematus või autoriteedist lugupidamine), et saavutada lubamatu juurdepääs teabele või mõjutada töötajat käituma ründajale sobival viisil. Tihti põhineb e-posti suhtlusrünne identiteedivargusel, mille käigus ründaja on algselt kaaperdanud kirjavahetuse ning suhtleb nüüd teise osapoolega eesmärgiga raha välja petta. Kui töötajaid ei ole koolitatud suhtlusrünnet ära tundma ja vältima, on suhtlusründe oht suurem.

2.6 E-kirjade volitamata lugemine ja manipuleerimine

Ilma krüpteerimata e-kirjavahetust on võimalik ründajal üle võtta ja seeläbi saada juurdepääs konfidentsiaalsele teabele. Ründajal on võimalik digiallkirjastamata materjali manipuleerida või lisada e-kirjale kahjurvara.

3 Meetmed

3.1 Elutsükkel

Kavandamine

APP.5.3.M6 E-posti turvaeeskiri

Evitus

APP.5.3.M1 E-posti kliendi turvaline konfiguratsioon

APP.5.3.M2 E-posti serveri turvaline käitus

APP.5.3.M5 E-kirjade vastuvõtja asendamise kord

APP.5.3.M7 Kasutaja koolitus e-posti turbe alal

APP.5.3.M9 Laiendatud turvameetmed e-posti serveril

Käitus

APP.5.3.M3 E-kirjade varundus ja arhiveerimine

APP.5.3.M4 E-posti serveri spämmi- ja viirusetõrje

APP.5.3.M8 Kasutaja spämmikäsitlus

Lisanduvad kõrgmeetmed

APP.5.3.M10 Otspunktkrüpteerimine ja digiallkirjastamine

APP.5.3.M11 E-posti serveri liiasus

APP.5.3.M12 Mustade nimekirjade seire

APP.5.3.M13 TLS-raportid

3.2 Põhimeetmed

APP.5.3.M1 E-posti kliendi turvaline konfiguratsioon

a. Organisatsioon on e-posti klientidele kehtestanud turvalise lubatava konfiguratsiooni.
b. Kasutajale antakse klientprogramm turvalise konfiguratsiooniga. Kasutajal on konfiguratsiooni muutmine keelatud või tehniliselt tõkestatud.
c. Enne manuste avamist lõppkasutaja poolt kontrollib süsteem manuseid kahjurvaratõrje programmiga.
d. Kliendi konfiguratsioon ei võimalda HTML-vormis saadetud e-kirjades koodi automaatset interpreteerimist.
e. Manusfailide automaatne eelvaatefunktsioon on kliendi konfiguratsioonis keelatud.
f. E-kirjade automaatne filtreerimine ja automaatne edasisaatmise on lubatud ainult põhjendatud juhtudel.
g. Ebaturvalistes ja avalikes võrkudes tohib e-posti serveriga ühenduda ainult läbi turvatud andmesidekanali (nt VPN).

APP.5.3.M2 E-posti serveri turvaline käitus

a. IT-talitus rakendab meetmeid ummistusrünnete tõrjeks.
b. E-posti serveri ja klientide vaheline andmeside nii sise- kui välisvõrgus on krüpteeritud.
c. E-kirjade edasisaatmine ebaturvaliste ning krüpteerimata andmesideühenduste kaudu on keelatud.
d. On koostatud kirjalik loend konkreetses e-posti serveris lubatud protokollidest ja teenustest.
e. Meiliserveri kasutus spämmi vahendamiseks on välistatud.
f. Meiliserveri postkastidele on seatud mahupiirang.

APP.5.3.M3 E-kirjade andmevarundus ja arhiveerimine

a. E-kirjade varundamine ja arhiveerimine toimub kehtestatud korra alusel.
b. E-posti serveris olevaid andmeid varundatakse regulaarselt.
c. Varundatud ja arhiveeritud e-kirju hoitakse turvaliselt.
d. Kasutajaid on teavitatud, kas ja kuidas varundatakse klientarvutis paikneva e-posti kliendi andmeid.

APP.5.3.M4 E-posti serveri spämmi- ja viirusetõrje

a. Kesksel e-posti serveril rakendatakse skaneerimisprogrammi koos viirusetõrje tarkvaraga, millega sisenevas ja väljuvas meilis ja meilimanustes avastada spämmi ja kahjursisu.

b. Kui meiliskanner ei ole võimeline krüpteeritud e-kirju skaneerimiseks dekrüpteerima, on rakendatud kompenseerivaid turvameetmeid.

c. Meiliskanneri kasutamisest on teavitatud töötajaid ja andmekaitsespetsialisti.

3.3 Standardmeetmed

APP.5.3.M5 E-kirjade vastuvõtja asendamise kord [ülemus]

a. Kui töötaja tööülesannetest moodustab olulise osa e-kirjade vastuvõtmine ja töötlemine, on töötajale e-kirjade vastuvõtmiseks määratud asendaja.

b. Asendajale antakse juurdepääs asendatava isiku postkastile või suunatakse e-kirjad asendajale ainult kooskõlas kehtiva isikuandmete kaitse regulatsiooniga.

c. Asendatavat isikut teavitatakse eelnevalt suunamise aktiveerimisest.

d. E-kirja automaatvastuse funktsioonide turvaliseks kasutamiseks on koostatud kirjalikud juhised. Siseteabe edastamine automaatvastuse funktsiooniga on keelatud.

APP.5.3.M6 E-posti turvaeeskiri

a. Organisatsioon on koostanud e-posti turvaliseks kasutamiseks turvaeeskirja, mis on kooskõlas organisatsiooni infoturvapoliitikaga.

b. Kasutajaid ja haldureid teavitatakse e-posti kasutamise uutest või muudetud turvanõuetest.

c. Eeskirja rakendamist kontrollitakse regulaarselt.

d. E-posti turvaeeskiri sisaldab kasutajate tarbeks vähemalt:
   - millised on e-posti serveri ja klientide pääsuõigused;
   - kuidas edastatud ja vastu võetud e-kirju kaitstakse;
   - kuidas tagatakse e-kirjade terviklus;
   - kuidas hallatakse meiliaadresse ja meililiste;
   - kas ja kuidas on e-posti kasutamine lubatud eraotstarbeks;
   - kuidas hallatakse lahkuvate töötajate postkaste;
   - kas ja kuidas on lubatud veebimeili rakenduse kasutamine;
   - kuidas käsitleda meilimanuseid;
   - kas lubatakse e-kirja vaadet HTML-režiimis.

e. Haldurite tarbeks on koostatud täiendavad juhised, mis määratlevad:
   - kuidas konfigureeritakse e-posti serveri ja kliendi komponente;
   - kuidas toimub teiste serverite juurdepääs e-posti serverile;
   - millistelt töökohtadelt ja mis viisil on e-posti serveri haldus lubatud.

APP.5.3.M7 Kasutajate koolitus rühmatarkvara kliendi turbe alal

a. Kasutajaid on koolitatud e-posti kliendiga töötama turvaliselt.

b. Kasutajaid on teavitatud ohtudest seoses e-posti teenuse kasutamisega, sealhulgas õngitsuskirjade ja võltsitud saatjaaadressiga e-kirjadega seonduvatest ohtudest.

c. Kasutajaid on hoiatatud ahelkirjade saatmise ning mittevajalikes meililistides osalemise ohtudest.

APP.5.3.M8 Kasutajate spämmikäsitlus [kasutaja]

a. Kasutajad on kohustatud tundmatult saatjalt saadetud soovimatuid e-kirju ignoreerima ja need kustutama. Sellisele e-kirjale on keelatud vastata ning e-kirjades olevaid linke ja manuseid on keelatud avada.

b. E-posti serveris on kasutusele võetud tsentraalselt hallatav spämmifilter.

APP.5.3.M9 Laiendatud turvameetmed e-posti serveril

a. E-posti serveril rakendatakse e-kirja saatnud serveri ehtsuse kontrollimise ja autentimise mehhanisme SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) ja DMARC (Domain-based Message Authentication, Reporting and Conformance).

b. SPF SoftFail („~“) parameetrit kasutatakse ainult testimisotstarbel.

c. DMARC on seadistatud tõrke korral e-kirju tagasi lükkama.

d. DMARC ründetuvastusraporteid vaadatakse üle regulaarselt.

e. E-posti serverite vahelise andmeside kaitseks on rakendatud MTA-STS ja/või DANE turvamehhanismid.

3.4 Kõrgmeetmed

APP.5.3.M10 Otspunktkrüpteerimine ja digiallkirjastamine (C)

a. Organisatsioon kasutab andmevahetuse kaitseks otspunktkrüpteerimist (ingl *end-to-end encryption*) ja digisignatuure (ingl *digital signature*).

b. Krüpteerimiseks ja digiallkirjastamiseks kasutatakse piisavat turvalisust tagavaid protokolle (vt CON.1 *Krüptokontseptsioon*).

APP.5.3.M11 E-posti serveri liiasus (A)

a. E-posti serverid on rakendatud liiasusega, samaaegselt on kasutuses mitu e-posti serverit.

b. On kindlaks määratud ja rakendatud reeglid e-posti serverite omavaheliseks sünkroonimiseks.

APP.5.3.M12 Mustade nimekirjade seire (A)

a. Regulaarselt jälgitakse, kas organisatsiooni e-posti servereid pole lisatud avalikesse, spämmilevitamise kahtlusega serveriaadresside mustadesse nimekirjadesse (ingl *blacklist*).

APP.5.3.M13 TLS-raportid (C-I-A)

a. Organisatsioon kasutab võimalikest krüpteerimistõrgetest teada saamiseks TLS-raportit (TLS-RPT).

b. Võimalusel jagatakse TLS-raporti andmeid teiste seotud osapooltega.

APP.5.4 Ühendatud side- ja koostöölahendused (UCC)

1 Kirjeldus

1.1 Eesmärk

Esitada üldised meetmed ühendatud side- ja koostöölahenduste (ingl *Unified Communications and Collaborations*, UCC) turvaliseks kasutamiseks. UCC-lahendused kombineerivad endas telefoni- ja sõnumiside, videokonverentsi, ekraanijagamise, grupitöö ja failiedastuse vahendeid.

1.2 Vastutus

„Ühendatud side- ja koostöölahendused (UCC)“ meetmete täitmise eest vastutab IT-talitus.

Lisavastutajad
Lisavastutajad puuduvad.

1.3 Piirangud

Kuna UCC-teenused vajavad toimimiseks turvalisi andmesideühendusi, tuleb koos antud mooduliga rakendada meetmed moodulitest NET.1.1 *Võrgu arhitektuur ja lahendus* ja NET.3.2 *Tulemüür.*

UCC taristut (serveriplatvormi, operatsioonisüsteemi ja kliente) käsitlevad meetmed on esitatud moodulites SYS.1.1 *Server üldiselt*, SYS.2.1 *Klientarvuti üldiselt* ja operatsioonisüsteeme käsitlevates moodulites. Ühiskasutatavate failide turvalist talletamist käsitletakse moodulis APP.3.3 *Failiserver*.

Pilvteenusena kasutatavale UCC-lahendusele kohalduvad täiendavalt meetmed moodulist OPS.2.2 *Pilvteenuste kasutamine*.

E-posti teenuseid ei loeta UCC-teenusteks, neile rakenduvad meetmed moodulist APP.5.3 *E-posti server ja klient üldiselt.*

2 Ohud

2.1 UCC teenuste ebapiisav käideldavus

Andmesidevõrgu kvaliteet mõjutab otseselt UCC-teenuste kvaliteeti ja käideldavust. Andmesidevõrgu või internetiühenduse häired põhjustavad UCC sessiooni katkemist, häireid videopildi toimimises või kasutajatevahelises kommunikatsioonis.

Kui UCC-teenuseid kasutatakse kriitiliste IT-süsteemide taastamise koordineerimiseks, võib süsteemide omavaheline sõltuvus tekitada katkestusi ka teiste kriitiliste IT-süsteemide töös. Kuna ilma töötava andmesideta pole ka UCC-teenused kasutatavad, pole võimalik ettenähtud viisil andmesidevõrku (ja teisi kriitilisi IT-süsteeme) taastada.

Kasutades UCC -lahendust pilvteenusena, sõltub teenuse käideldavus täiendavalt ka teenuseandja tegevustest ja tema poolt rakendatud infoturbe meetmete toimimisest. Sarnane risk on seotud autentimisteenustega, mida kasutajad kasutavad UCC-teenustesse sisselogimiseks. Kui autentimisteenus ei tööta, ei saa UCC-teenuseid kasutada.

2.2 Vead UCC kasutuselevõtu kavandamisel

UCC-teenuste kasutajate arvu ja kasutusintensiivsuse valearvestus võib mõjutada teenuse kvaliteeti (kui teenuse kasutajaid on oodatust rohkem) või teenusega seotud kulusid (kui teenuse kasutajaid on oodatust vähem).

Sõltuvalt kasutatavatest UCC-teenustest võivad UCC-komponentide nõuded andmesidevõrgu läbilaskevõimele ja kvaliteedile suurel määral erineda. Andmeside nõuded sisevõrgus peetavale kõnesidele on teised kui pilvteenuse kasutamiseks vajalikule internetiühendusele. Kui andmesidevõrgud kõiki vajalikke UCC-teenuseid ei toeta, ei saa UCC-teenused vajalikul määral kasutada.

Videoside ja sellega seotud pilditöötluse funktsioonid eeldavad seda kasutatavatelt klientseadmetelt kõrget tehnilist võimekust. Kui klientseade ei ole pilditöötluseks piisavalt võimas, kannatab oluliselt kasutajakogemus. Halvemal juhul ei saa üht osa organisatsiooni klientseadmetest videosideks kasutada.

2.3 UCC-lahenduse väär seadistamine

UCC- lahenduse seadistamine toimub tavaliselt klientarvutis ja seda teeb kasutaja ise. Erinevad lõppkasutajaseadmed (peakomplektid, mikrofonid jne) võivad vajada erinevat seadistust. Konfigureerimisel tehtud vea tõttu ei pruugi kasutaja olla koosolekul kuuldav ja nähtav või ei kuule ta ise teisi osalejaid.

Kui koosolekuruumi paigaldatud sideseade võtab sissetulevad sidetaotlused automaatselt vastu, võidakse teisele poolele tahtmatult avaldada konfidentsiaalset teavet.

UCC-teenuste kasutamine võib olla häiritud kui sideseade ei ole korrektselt ühendatud organisatsiooni sisevõrku. Väärad marsruutimisseaded võivad kaasa tuua UCC-teenuse kvaliteedi languse.

Kui paljud osalejatega koosolekul osalejate identiteeti ei kontrollita ning osalejate õigusi piisavalt ei piirata, on koosolekut keeruline läbi viia. Samuti võivad koosolekul osalejad saada volitamata juurdepääsu koosoleku materjalidele.

2.4 UCC-lahenduse haldusõiguste väärkasutamine

UCC-lahenduse halduril on laialdased võimalused UCC-lahenduse kasutamisvõimalusi muuta. Haldusõiguste väärkasutamisel või vähesest teadlikkusest tehtud haldusvigadel võivad olla rasked tagajärjed. Näiteks saab haldur piiratud ligipääsuga vestlused või failijagamiskeskkonnad teha kättesaadavaks kõigile UCC-teenuse kasutajatele.

2.5 Konfidentsiaalse teabe leke

Erinevatel UCC-lahendustel on erinevad kasutajaliidesed (ingl user interface). Samuti võivad mõneti erineda sama UCC-lahenduse rakenduse ja veebiliidese kasutamine. Kasutaja võib hooletusvea tõttu jagada tahtmatult oma ekraanipilti, mis sisaldab konfidentsiaalset teavet või unustada sisse mikrofoni, mistõttu kõik kuulevad pealt kasutaja privaatset vestlust.

Samuti on võimalik, et osalejatele ühiskasutuseks mõeldud materjalidele antakse kogemata juurdepääs ka selleks volitamata isikule.

Paljud UCC-lahendused salvestavad vestluseid ja muid andmeid pilve. Nii võib juhtuda et kõrge kaitsetarbega teave salvestatakse teadmata asukohaga pilvteenuse tarnija serverisse. See võib tähendada vastuolu seadusandlusest tulenevate nõuetega.

Ühisesse failijagamiskeskkonda uusi kasutajaid lisades unustatakse tihti tõsiasi, et uus kasutaja pääseb muuhulgas ligi ka kõigile sinna keskkonda eelnevalt salvestatud failidele.

2.6 Isikuandmete loata avalikustamine

UCC-teenused koguvad kasutajakohaseid andmeid ja loovad kasutajaprofiile, mida kuvatakse ka teistele kasutajatele. See võib põhjustada isikuandmete avalikustamise, kuna võimaldab teha järeldusi nii isiku tööaja kasutuse, töötulemuste kui isiklike suhete kohta. Isegi kasutaja hetke staatuste või kättesaadavuse nägemine võib tähendada kasutaja isikuandmete loata jagamist.

Kui keegi osaleb virtuaalsel koosolekul kodukontorist, võib videopildi taustal olla nähtaval osaleja isiklikud esemed, näha taustal toimetavaid inimesi või kuulda privaatse keskkonna taustahelisid.

2.7 UCC-lahenduse ressursihalduse probleemid

UCC-lahenduste toimimine sõltub arvuti IT-komponentide toimimisest. Erinevad UCC-lahendused kasutavad sageli samasid operatsioonisüsteemi poolt jagatud ressursse. Tihti juhtub, et kasutaja ei saa samaaegselt mitme UCC-lahendusega (nt telefonirakendus ja videokonverentsirakendus) töötada, kuna üks rakendus võtab kasutusele ja blokeerib teiste rakenduste eest vajalikud ressursid, nt suhtlemiseks vajaliku peakomplekti.

Mõnel UCC-lahendusel on väga kõrged ressursinõuded, mis võivad põhjustada klientseadme ülekoormust ja ülekuumenemist. Seda eriti juhul, kui taustal töötab paralleelselt mitmeid videokonverentsirakendusi.

2.8 Kasutaja arvuti lubamatu ülevõtmine

UCC-lahendused võivad sisaldada funktsionaalsust kasutaja arvuti juhtimise (nt hiirekursori liigutamise) üleandmiseks teisele osapoolele. Samas puudub ekraani üleandjal võimalus arvuti juhtimist ise tagasi võtta ning ta kaotab kontrolli edasiste toimingute üle. Selle tulemusena võivad vestluses osalejad saada juurdepääsu rakendustele ja andmetele, mida ekraani üleandja ei soovi teistega jagada.

2.9 Valeidentideedi kasutamine

Pahatahtlikul kasutajal on konfidentsiaalse teabe hankimiseks või edasiste rünnete kavandamiseks võimalik teeselda usaldusväärset suhtluspartnerit ning osaleda koosolekutel või videokonverentsidel, kasutades selleks valeidentiteeti. Tihti on see võimalik siis, kui koosolekul osaleb suurem hulk inimesi ning koosoleku alguses kõigile osalejatele enda tutvustamiseks sõna ei anda.

Ründajal on võimalik jagada läbi vestluskanalite hüperlinke kahjulikule sisule. Kuna tavakasutaja jaoks on UCC-teenus suurema usaldusväärsusega platvorm kui e-kiri, on UCC-teenuse kasutaja sotsiaalsele manipuleerimisele ning suhtlusrünnetele (ingl *social engineering*) võrreldes e-posti teenusega vastuvõtlikum.

Ründaja saab usalduse tõstmiseks suhtluskeskkonnas manipuleerida oma kuvatavaid nimesid, häält või välimust. Näiteks võib ründaja teeselda ülemust, et saada otse vestluse kaudu konfidentsiaalset teavet või nõutada konfidentsiaalseid dokumente.

3 Meetmed

3.1 Elutsükkel

Kavandamine

APP.5.4.M1 UCC-teenuste kasutuselevõtu kavandamine

Evitus

APP.5.4.M2 UCC-teenuste kasutuselevõtule eelnev võrgulahenduse kontroll

APP.5.4.M3 UCC-teenuste testimine

APP.5.4.M4 Tarbetute funktsioonide ja teenuste desaktiveerimine

Käitus

APP.5.4.M5 UCC rollide ja pääsuõiguste määramise põhimõtted

APP.5.4.M6 UCC andmevahetuse krüpteerimine

APP.5.4.M7 UCC-teenuste turvalise kasutamise kord

APP.5.4.M8 Seansipiirikontrolleri (SBC) rakendamine

APP.5.4.M9 UCC turvaline seadistus

APP.5.4.M10 Edastatava teabe sisupõhine piiramine

Lisanduvad kõrgmeetmed

APP.5.4.M11 UCC-teenuste kõrgkäideldavuse tagamine

APP.5.4.M12 UCC-teenuste lisamine avariihaldusplaani

APP.5.4.M13 SIP magistraalliinide turvaline haldus

APP.5.4.M14 UCC andmeside otspunktkrüpteerimine

APP.5.4.M15 Tehisintellekti kasutavate funktsioonide piiramine

APP.5.4.M16 Seansipiirikontrolleri (SBC) rakendamine teistes võrgulüüsides

APP.5.4.M17 UCC-teenuste kasutuse piiramine

APP.5.4.M18 UCC-komponentide integreerimine turvaseiresse

3.2 Põhimeetmed

APP.5.4.M1 UCC-teenuste kasutuselevõtu kavandamine

a. Organisatsioon on analüüsinud UCC-teenuste kasutamise vajadust ning UCC-teenustega kaasnevaid organisatoorseid ning tehnilisi mõjusid organisatsiooni eesmärkide saavutamisele.

b. Organisatsioon on koostanud UCC-teenuste kasutuselevõtu kava, mis kirjeldab vähemalt järgmist:
   - eesmärgid, mida tahetakse UCC-teenuste kasutuselevõtuga saavutada;
   - funktsionaalsed nõuded (nii UCC-lahendusele tervikuna kui üksikutele teenustele);
   - UCC-teenustele kohalduvad infoturbe nõuded;
   - UCC-teenuste kaudu edastatav lubatav teave ja andmespetsifikatsioonid;
   - organisatsiooni nõuetele vastavate UCC-teenuste loetelu;
   - UCC ja teiste IT-teenuste omavahelise sõltuvuse analüüs;
   - muudatused organisatsiooni töökorralduses seoses UCC-teenuste kasutuselevõtuga.

c. Organisatsioon on koostanud juhendi UCC-komponentide integreerimiseks organisatsiooni IT-süsteemide ja IT-taristuga.

d. Organisatsioon on analüüsinud, kas UCC-komponendid paigutada eraldiseisvasse võrgusegmenti ning kuidas lahendada UCC-komponentide liidestamine teiste rakendustega.

APP.5.4.M2 UCC-teenuste kasutuselevõtule eelnev võrgulahenduse kontroll

a. UCC-teenuste kasutusvalmiduse hindamisel arvestatakse järgmiseid võrgutehnilisi aspekte:
   - UCC-spetsiifilised jõudlusparameetrid - lubatav paketikadu (ingl *packet loss*), faasivärin (ingl *jitter*) ja latentsusaeg (ingl *latency*);
   - videokonverentside läbiviimiseks piisava võrgu läbilaskevõime (ingl *bandwidth*) olemasolu;
   - statsionaarsete lõppseadmete toimimiseks vajalik Ethernet-toite (ingl *Power over Ethernet*, PoE);
   - WLAN sideühenduse võimalus mobiilseadmetele.
b. Enne UCC-teenuste kasutuselevõttu kontrollitakse võrgu vastavust UCC-spetsiifilistele jõudlusparameetritele ning koostakse kava leitud puuduste kõrvaldamiseks.
c. Täiendavate UCC-teenuste lisandumisel vaadatakse eeltoodud tehnilised aspektid uuesti üle.

APP.5.4.M3 UCC-teenuste testimine

a. Enne UCC-teenuste kasutuselevõttu testitakse, kas UCC-komponendid töötavad ettenähtud funktsionaalsusega ning ilma tõrgeteta.
b. UCC-teenuste testimisel osalevad ka lõppkasutajad, kes testivad UCC-teenuste koostoimet töötamisel koos teiste rakendustega.
c. Testimist korratakse, kui UCC-teenuseid muudetakse või lisatakse täiendavaid teenuseid.

APP.5.4.M4 Tarbetute funktsioonide ja teenuste desaktiveerimine

a. Kasutatavad UCC-teenused vastavad määratletud eesmärkidele ning teenuseid kasutatakse väiksema vajaliku hulga funktsioonidega.
b. Funktsionaalsuse piiramisel on arvestatud UCC-komponentide võimalikke koostoimeid.
c. Võimalusel desaktiveeritakse või piiratakse järgmiste funktsioonide kasutamist:
   - UCC-komponendi teostatav isikuandmete töötlus ja salvestamine;
   - kasutajate ja UCC-teenuste juurdepääs isikuandmetele;
   - organisatsioonivälistе isikute juurdepääs potentsiaalselt tundlikku teavet sisaldavatele UCC-teenustele (nt tekstsuhtlus, kasutaja olekustaatus, ühiskasutatav salvestusruum);
   - andmete ja failide saatmine organisatsioonivälistesse UCC-teenustesse.
d. Isikutevaheliste vestlusega seotud logiandmeid kogutakse ja säilitatakse ainult minimaalselt vajalikul määral.
e. On olemas ülevaade, millised kasutajad ja UCC-komponendid omavad juurdepääsu logiandmetele. Vajadusel piiratakse juurdepääs ja/või desaktiveeritakse vastavad UCC-teenuse funktsioonid.

APP.5.4.M5 UCC rollide ja pääsuõiguste määramise põhimõtted

a. Organisatsioonis kehtestatud rollide ja pääsuõiguste halduse korda on täiendatud UCC-spetsiifiliste rollide ja volitustega. Rollide määramisel on arvestatud kõikide (sh organisatsioonivälise) kasutajagruppidega.

b. Pääsuõiguste andmisel on arvestatud järgmisi aspekte:
   - minimaalselt vajalikud pääsuõigused UCC-teenuste sihipäraseks kasutamiseks;
   - vajalikud pääsuõigused UCC-teenuste seadistamiseks ja seadistuse muutmiseks;
   - UCC-teenuste erifunktsioonide (nt vestluste salvestamine) aktiveerimise õigused.

c. Tavakasutajatele antud pääsuõigused on piiratud vajaliku miinimumini.

d. UCC-teenuste erifunktsioonide kasutamise õigus on ainult selleks volitatud kasutajatel.

e. Kasutajate pääsuõiguste minimaalsuse põhimõtte järgimist ja kasutajatele antud pääsuõiguste asjakohasust UCC-teenustes kontrollitakse regulaarselt. Täiendavalt kontrollitakse pääsuõigusi pärast UCC-teenustes muudatuste tegemist. Vajadusel pääsuõigused ajakohastatakse.

APP.5.4.M6 UCC andmevahetuse krüpteerimine

a. Ebausaldusväärsete võrkude (nt Internet) kaudu edastav UCC andmeside on krüpteeritud.

b. Kui UCC andmeside krüpteerimine ei ole võimalik, on organisatsioon selgelt määratlenud teabe liigid, mille edastamine ühendatud side- ja koostöölahenduste kaudu on keelatud.

c. Erinevate UCC-lahenduste vahelise andmevahetuse puhul on määratud, mis andmeid tohib edastada ainult eelnevalt krüpteerituna (nt failide edastamine).

d. UCC-lahenduse failihoidlasse salvestatud konfidentsiaalseid andmeid (sh isikuandmeid) sisaldavad failid on krüpteeritud turvaliste krüpteerimismehhanismidega. Krüpteerimise nõue kehtib nii organisatsioonisisese failirepositooriumi kui UCC-teenuse tarnija pilve salvestatavate failide puhul.

e. UCC-lahenduse kasutajatel on võimalik veenduda, et andmeside on turvaliselt krüpteeritud.

APP.5.4.M7 UCC-teenuste turvalise kasutamise kord

a. Kasutajad on teadlikud, kuidas UCC-teenuseid turvaliselt kasutada, seda ka välise osapoole algatatud vestluste või videokonverentside puhul.

b. Kasutajaid on teavitatud, millised UCC-lahenduse funktsioonid (nt jagatud PIN-koodi sisestamine, osapoolte turvaline autentimine) aitavad enda algatatud vestlusi või videokonverentse turvalisemaks muuta.

c. UCC videokonverentsi või veebikoosoleku algatamisel lepitakse kokku järgnevad turvaaspektid:
   - osalejate valik vastavalt vestluse sisule ja eesmärkidele;
   - kõigi osalejate tõsikindel tuvastamine;
   - modereerimisõiguste määramine ainult valitud kasutajatele;
   - videokonverentsi või vestluse salvestamise kord;
   - koosolekuruumide konverentsiseadmete kasutamise kord.

3.3 Standardmeetmed

APP.5.4.M8 Seansipiirikontrolleri (SBC) rakendamine

a. UCC meediumivoogude ülekandmisel madalama usaldusväärsusega võrku on lüüsis (ingl *gateway*) aktiveeritud seansipiirikontroller (ingl *sessioon border controller*, SBC). Eelkõige on see tähtis UCC kõneteenuste kasutamisel.

b. SBC toimib krüpteerimise otspunktina ja filtreerib signaalimist ning meediavoogude ülekannet.

APP.5.4.M9 UCC turvaline seadistus

a. UCC seadistamisel on kaalutud järgmiste täiendavate turvameetmete rakendamist:
   - signaalimise ja meediavoogude krüpteerimine ka usaldusväärsetel edastusteedel;
   - salvestatud andmete täiendavad kaitsemeetmed ning vestluste salvestistele juurdepääsuõiguste piiramine;
   - UCC-teenuste lubamine ainult sisekasutajatele;
   - kasutajate hetkestaatuse teabe edastamise blokeerimine;

b. Salvestatud andmed on krüpteeritud ja on juurdepääsetavad ainult volitatud kasutajale pärast turvalist autentimist.

c. Klientarvutites on sõnumiside rakendused turvaliseks kasutamiseks eelseadistatud. Kahjulike linkide tuvastamiseks skaneeritakse tekstipõhiseid vestlusi kahjurvaratõrje rakendusega.

APP.5.4.M10 Edastatava teabe sisupõhine piiramine

a. Organisatsioon on hoolikalt kaalunud, kas vestluse sisu (automaatse) hindamise ja piiramise meetme rakendamine on proportsionaalne, arvestades kaitsetarvet ja reaalseid andmekaitse vajadusi.

b. Teabe sisupõhist piiramist on võimalik vajadusel desaktiveerida kas täielikult või ühe konkreetse vestluse kaupa.

c. On võetud vastu teadlik otsus, kas sisu hindamisel lubada tehisintellekti (ingl *artificial intelligence*, AI) kasutavad teenused ning sõnumisisu saatmine pilvteenuse tarnijale.

d. UCC-teenuse kasutajaid on sisupõhisest piiramisest ja vestluse sisu analüüsimisest eelnevalt teavitatud ning nad on andnud selleks selgesõnalise ja üheselt mõistetava nõusoleku.

e. Vestluste hindamise käigus tekkinud andmestik on kaitstud volitamata juurdepääsu eest.

3.4 Kõrgmeetmed

APP.5.4.M11 UCC-teenuste kõrgkäideldavuse tagamine

a. UCC-teenuste käideldavuse tõstmiseks rakendatakse järgmisi tehnilisi meetmeid:
   - keskserverite ja kesksete teenuste liiasuse (ingl *redundancy*) tagamine;
   - CAC (Call Admission Control) kasutamine telefoni- ja videoteenuste kvaliteedi tõstmiseks;
   - iseseisvalt toimivate, ilma oluliste sõltuvusteta UCC-teenuste kasutamine.

b. Pilvepõhiste UCC-teenuste kasutamisel on pilveteenuse andja ja interneti tarnija (ingl *Internet Service Provider*, ISP) vahelised võrguühendused kavandatud toimima liiasusega ja tõrkekindlalt.

c. VoIP telefoniside kasutamisel tagab SIP-teenuse tarnija oma sidevõrkude kõrgkäideldavuse.

d. UCC-teenuste käideldavust seiratakse ja mõõdetakse pidevalt.

APP.5.4.M12 UCC-teenuste lisamine avariihaldusplaani

a. UCC-teenustele on teostatud äritoime analüüs (ingl Business Impact Analysis, BIA) ning otsustatud, milliseid UCC-teenuseid käsitletakse avariikontseptsioonis (vt DER.4.M7 *Avariikontseptsioon*).

b. Iga UCC-teenuse jaoks on määratud alternatiivlahendus, mida kasutatakse juhul, kui teenus ei ole kättesaadav. Eelkõige on kasutajatele tagatud hädaabikõne võimalus.

c. Keerulisemat seadistust (nt võrgukonfiguratsiooni muudatused või marsruutimise muutmine telefoniteenuse tarnija juures) vajavatele või teistest teenustest sõltuvatele UCC-teenustele on koostatud detailsed taasteplaanid.

APP.5.4.M13 SIP magistraalliinide turvaline haldus

a. SIP magistraalliinide (ingl *SIP trunk*) haldamisel rakendatakse nelja silma põhimõtet järgmiste muudatuste tegemisel:

- muudatused marsruutimise seadistuses;
- muudatused CAC (Call Admission Control) parameetrites;
- krüpteerimise seadistused (nii sisevõrgus kui teenusetarnija võrgu suunas);
- muudatused turvaseadistustes, nt andmete kohaliku salvestamise seadistamine.

APP.5.4.M14 UCC andmeside otspunktkrüpteerimine

a. Osavõtjaid ühendav meediavoog ja signaalimine on turvaliselt otspunktkrüpteeritud (ingl *end-to-end encryption*).

b. Otspunktkrüpteerimata andmeside (nt juhul kui erinevate UCC-lahenduste vaheline suhtlus otspunktkrüpteerimist ei võimalda) kasutamine UCC-teenustes on keelatud.

APP.5.4.M15 Tehisintellekti kasutavate funktsioonide piiramine

a. Tehisintellekti (ingl *artificial intelligence*, AI) kasutamine UCC-teenustes on desaktiveeritud või piiratud miinimumini.

b. Kui AI-d pole võimalik keskselt desaktiveerida, on kasutajatel kohustus vestluse alguses AI funktsioonid välja lülitada.

APP.5.4.M16 Seansipiirikontrolleri (SBC) rakendamine teistes võrgulüüsides

a. Seansipiirikontrollerid (ingl *sessioon border controller*, SBC) rakendatakse ka sisevõrgu lüüsides. Eriti oluline on see erinevate kaitsenõuetega võrgusegmentide vahelises UCC andmesides.

b. Sisevõrgu segmentide vahelises andmesides on SBC krüpteerimismehhanismid rakendatud.

APP.5.4.M17 UCC-teenuste kasutuse piiramine

a. UCC-teenuste piiramiseks kasutatakse järgnevaid meetmeid:

- edastatava teabe sisust ja kaitsenõuetest tulenev teenuste lubamine/keelamine;
- kasutajate mitmikautentimine (ingl *multifactor authentication*, MFA);
- organisatsioonivälistе kasutajate blokeerimine;
- metaandmete salvestamise desaktiveerimine;
- sideandmete nähtavuse piiramine halduritel.

b. Vajadusel kasutatakse UCC-lahendustes täiendavaid tehnilisi ja/või organisatoorseid turvameetmeid (nt igakordne PIN-koodi või parooli sisestamine).

APP.5.4.M18 UCC-komponentide integreerimine turvaseiresse

a. Olulised UCC-komponendid (nt UCC juhtseadmed, SBCd, krüpteerimisseadmed) on integreeritud pidevasse turvaseiresse.

b. Kui organisatsioon kasutab turvasündmuste tuvastamiseks ja nendest teavitamiseks reaalajalisi automatiseeritud kontrollsüsteeme, on järelevalve alla võetud ka olulised UCC-komponendid.

APP.6 Tarkvara üldiselt

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed tarkvara ja tarkvaraga töödeldavate andmete turbe tagamiseks, sh meetmed tarkvara kasutuselevõtuks, hankimiseks, kasutamiseks ja kasutuselt kõrvaldamiseks. Tarkvara all mõistetakse antud moodulis kõiki tarkvaratooteid (nt operatsioonisüsteemid, kontoritarkvara, finantstarkvara, dokumendihalduse süsteem).

1.2 Vastutus

„Tarkvara üldiselt“ meetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Hankeosakond, vastutav spetsialist.

1.3 Piirangud

Moodulis käsitletakse tarkvara tüüpprotseduure üldistatud elutsükli vältel. Moodul ei kohandu suletud süsteemide (nt. IoT ja võrguseadmete) tarkvarale. Lisaks sellele moodulile rakendatakse tarkvarale meetmeid moodulitest OPS.1.1.3 *Paiga-ja muudatusehaldus*, OPS.1.1.6 *Tarkvara testimine ja kasutuselevõtt* ja tootespetsiifilistest APP moodulitest.

2 Ohud

2.1 Sobimatu tarkvara valimine

Organisatsiooni vajadustele sobimatu tarkvara valimine mõjutab negatiivselt äriprotsesse. Näiteks ei pruugi uus tarkvara ühilduda olemasolevate IT-süsteemidega või esineb puudujääke tarkvara funktsionaalsuses või sooritusvõimes. Kui tarkvara ei vasta

organisatsioonis kehtestatud turvanõuetele, tekib oht tarkvaraga töödeldavate andmete avalikuks tulemiseks või manipuleerimiseks.

2.2 Konfiguratsiooniveast põhjustatud andmekaotus

Kui tarkvara on vääralt konfigureeritud, võidakse tahtmatult paljastada tundlikku teavet. Näiteks sünkroonitakse andmeid tarkvaratootja pilveteenusega, sest konfigureerimisel jäi vastav seadistus desaktiveerimata. Konfiguratsioonivead võivad kaasa tuua vastuolu õigusaktidega, rahalise kahju või mainekao.

2.3 Tarkvara soetamine ebausaldusväärsest allikast

Kui tarkvara või selle uuendeid hangitakse ebausaldusväärsetest allikatest, võib soovitud tarkvara asemel saada rikutud või tahtlikult muudetud tarkvarakoopia. Sellise tarkvara installimisel organisatsiooni arvutitesse võib levida kahjurvara ja/või tarkvara ei pruugi toimida eeldatud viisil.

2.4 Puudulikust hooldusest tingitud turvanõrkused

Tarkvara turvanõrkusi võib ilmneda kogu tarkvara kasutusaja vältel. Kui turvanõrkusi võimalikult kiiresti ei kõrvaldata, satuvad ohtu tarkvaraga töödeldavad andmed. Kui tarkvara tootja ei taga uuendite ja turvapaikade väljastamist või kui tarkvara hoolduseks ei ole sõlmitud hooldusleping, võib ründaja tarkvaras olevaid turvanõrkusi ära kasutada võrku tungimiseks või andmete varastamiseks.

2.5 Tarkvara väärkasutamisest tulenev andmekaotus

Tarkvaras sisalduvate funktsioonide väära kasutamise korral võivad töötajad ekslikult andmeid kustutada või kasutuskõlbmatuks muuta. Näiteks krüpteerimisfunktsiooni valesti kasutamisel võivad andmed olla endiselt alles, kuid neid ei õnnestu enam dekrüpteerida.

2.6 Ressursipuudus tarkvara kasutamisel

Kui olemasolevas IT-taristus pole tarkvara käitamiseks piisavalt ressursse, võib tarkvara käideldavus olla tugevalt häiritud. Suurenevad tarkvara pöördus- ja ooteajad mõjutavad negatiivselt äriprotsesside toimimist.

2.7 Tarkvara sobimatus kasutajate vajadustega

Kui hangitud tarkvara funktsionaalsus ei vasta tegelikele vajadustele (nt vormingud ei ühildu kasutusel olevate rakendustega), võib organisatsiooni töö olla oluliselt häiritud. Ka juhul kui tarkvara funktsionaalsus on piisav, kuid kasutajaliides pole kasutajasõbralik, võivad kasutajad loobuda tarkvara kasutamisest ja otsida selle asemel alternatiivseid lahendusi. See soodustab organisatsioonis illegaalse või ainult personaalseks kasutuseks lubatud tarkvara kasutamist.

3 Meetmed

3.1 Elutsükkel

Kavandamine

APP.6.M1 Tarkvara kasutuselevõtu kavandamine

APP.6.M2 Tarkvarale esitatavate nõuete loend

Soetus

APP.6.M3 Tarkvara turvaline hankimine

APP.6.M7 Sobiva tarkvara valimine

APP.6.M11 Tarkvara lisandmoodulite ja pluginite haldus

Evitus

APP.6.M4 Tarkvara installimise ja seadistamise kord

APP.6.M5 Tarkvara turvaline installimine

APP.6.M8 Installimeedia turvaline kasutamine

Käitus

APP.6.M6 Täiendavad tarkvara turvafunktsioonid

APP.6.M9 Tarkvara inventuur

APP.6.M10 Tarkvara turvajuhend

Kõrvaldamine

APP.6.M12 Tarkvara kasutusest kõrvaldamine

APP.6.M13 Tarkvara turvaline desinstallimine

Lisanduvad kõrgmeetmed

APP.6.M14 Sertifitseeritud tarkvara kasutamine

3.2 Põhimeetmed

APP.6.M1 Tarkvara kasutuselevõtu kavandamine [vastutav spetsialist]

a. Tarkvara kasutuselevõtu kavandamise käigus on kirjeldatud:
   - tarkvara kasutamise eesmärk;
   - andmed, mida tarkvaraga töödeldakse;
   - riistvara ja IT-süsteemid, millel tarkvara kasutatakse;
   - tarkvara liidestus ja lõimimine olemasolevate rakendustega;
   - välise toe vajadus tarkvara juurutamisel ja käigushoidmisel.

b. Tarkvara kasutuselevõtu kavandamisel on arvestatud infoturbe aspekte ja turvanõudeid, millele tarkvara peab vastama.

c. Tüüptarkvara kasutuselevõtuks määratakse vajalikud kooskõlastused ning vastutajad, kes:
   - koostavad nõuete loendi;
   - valivad tarkvaratoote;
   - testivad tarkvara;
   - installivad tarkvaratoote.

APP.6.M2 Tarkvarale esitatavate nõuete loend [vastutav spetsialist]

a. Tarkvara kasutuselevõtu kavandamise tulemite põhjal on koostatud ja kinnitatud tarkvarale esitavate nõuete loend.

b. Tarkvarale esitatavate nõuete loend sisaldab nii tarkvara funktsionaalseid kui mittefunktsionaalseid (sh infoturbe) nõudeid.

c. Mittefunktsionaalsete nõuetena kirjeldatakse:
   - rakenduse keskkond, sh platvorm, välisseadmed, liidestus;

- ühilduvus muude komponentidega, sh migratsiooni tugi ja tagasiühilduvus;
- jõudlusnõuded;
- koostalitlusnõuded;
- usaldatavusnõuded, sh stabiilsus-, veakindlus- ja veatõrjenõuded;
- vastavus standarditele ja sise-eeskirjadele;
- kasutatavusnõuded, sh kasutamise hõlpsus, arusaadavus, õpitavus;
- kulude ülapiir;
- nõuded dokumentatsioonile;
- nõuded tarkvara kvaliteedile.

d. Turvanõuetena kirjeldatakse:
   - identifitseerimine ja autentimine;
   - pääsu reguleerimine;
   - asitõendite turve;
   - logimisnõuded;
   - rikkumiskindlus;
   - usaldatavus;
   - turvaline andmeedastus;
   - andmevarundus;
   - krüpteerimine;
   - andmetervikluse tagamise funktsioonid.
e. Tarkvarale esitatavad nõuded on kooskõlas isikuandmete kaitse alase regulatsiooni ja teiste asjassepuutuvate õigusaktidega.
f. Tarkvarale esitatavate nõuete loend on organisatsioonisiseselt kooskõlastatud kõigi mõjutatud üksuste ja seotud osapooltega.

APP.6.M3 Tarkvara turvaline hankimine [hankeosakond]

a. Tarkvara hankimisel lähtutakse tarkvarale esitatavate nõuete loendis (vt APP.6.M2 *Tarkvarale esitatavate nõuete loend*) esitatud tingimustest.
b. Tarkvara hangitakse ainult usaldusväärsetest allikatest. Hangitud tarkvara autentsus ja terviklus on tõendatav.
c. Tarkvara kogu eeldatava eluea jooksul on tagatud tarkvarale tootja tugi ja turvapaikade olemasolu.

APP.6.M4 Tarkvara installimise ja seadistamise kord [vastutav spetsialist]

a. Tarkvara installimisel ja seadistamisel järgitakse järgmisi põhimõtteid:
   - tarkvara installitakse ja käitatakse ainult vajaliku funktsionaalsuse ulatuses, tarbetud teenused ja funktsioonid desinstallitakse või lülitatakse välja;
   - tarkvara käitatakse minimaalselt vajalike pääsuõigustega;
   - tarkvara ei sisalda üleliigseid andmeid, sh isikuandmeid.

b. Tarkvara uuendid ja turvapaigad paigaldatakse enne tarkvara käidukeskkonnas kasutusele võtmist.
c. Tarkvara installimiseks koostatakse installijuhend, mis sisaldab kõiki käsitsi tehtavaid installisamme, sh installimise käigus tehtavaid konfiguratsioonimuudatusi.
d. Installiprotseduure viivad läbi selleks volitatud IT-talituse töötajad.
e. Enne tarkvara installimist veendutakse installipaketi autentsuses ja tervikluses, kasutades selleks tarkvara väljastaja poolt antud digiallkirja või failiräsi teavet.
f. Tarkvara tüüpkonfiguratsioon ja selles tehtud muutused dokumenteeritakse.
g. Enne ja pärast tarkvara installimist tehakse kõigist mõjutatud IT-süsteemidest täielik andmevarundus.

APP.6.M5 Tarkvara turvaline installimine

a. Tüüptarkvara installitakse ja konfigureeritakse installijuhendi kohaselt (vt APP.6.M4 *Tarkvara installimise ja seadistamise kord*).
b. Installitakse ainult eelnevalt testitud ja kasutuselevõtuks kinnitatud tarkvara.
c. Installiprotseduure viivad läbi selleks volitatud IT-talituse töötajad.
d. Juhendist lahknevused kooskõlastatakse vastutava IT-talituse töötaja ja kasutuselevõttu kinnitava osapoolega.

3.3 Standardmeetmed

APP.6.M6 Täiendavad tarkvara turvafunktsioonid

a. Suure kaitsetarbe korral hinnatakse kasutusele võetud tarkvara turvafunktsioonide piisavust, võimalusel tehakse seda nõuete määramise ja tarkvaratoote valimise käigus.
b. Täiendavate turvafunktsioonidena kaalutakse vähemalt järgmist:
    - logiandmete turbe tugevdamine;
    - tarkvara käitava riistvara ja operatsioonisüsteemi tugevdamine (ingl *hardening*);
    - andmevahetuse krüpteerimismehhanismide tugevdamine;
    - pääsuõiguste detailsem astmestus.

APP.6.M7 Sobiva tarkvara valimine [vastutav spetsialist, hankeosakond]

a. Saadaolevaid tarkvaratooteid analüüsitakse ja võrreldakse nõuete loendi alusel (vt APP.6.M2 *Tarkvarale esitatavate nõuete loend*), kasutades sobivat võrdlusskaalat.
b. Kui sobivaid tarkvaratooteid on rohkem kui üks, analüüsitakse täiendavalt toote kasutajate maksimaalset arvu, tootearvustusi ning tootega kaasnevaid kulusid (nt koolitusteks, migratsiooniks ja käitamiseks).
c. Sobiv toode valitakse koostöös taotluse esitanud üksuse juhiga eelneva hindamise ja toote testimise tulemuste põhjal.

APP.6.M8 Installimeedia turvaline kasutamine

a. Installimeediast on tehtud varukoopia, võimalusel kasutatakse korduvatel installimistel varukoopiat.
b. Installimeediat hoitakse kaitstuna volitamata juurdepääsu eest. Volitatud töötajate jaoks on installimeedia juurdepääsetav.

c. Vajaduse korral on võimalik installifaile tootja repositooriumist (nt äpipoest) uuesti allalaadida.

d. Tarkvara konfiguratsioonifailidest on tehtud varukoopia, seadistamistegevused on dokumenteeritud.

e. Tarkvara taaspaigaldamine on integreeritud organisatsiooni andmevarunduskontseptsiooni.

APP.6.M9 Tarkvara inventuur

a. Kasutatavad tarkvaratooted on arvele võetud inventuuri nimekirja.

b. Tarkvara inventuuri nimekirjas on esitatud tarkvara nimetus, litsentsitüüp, litsentside arv ja litsentsi kehtivusaeg.

c. Tarkvara tohib kasutada ainult juhul, kui kasutamine vastab tarkvara litsentsitingimustele.

d. Tüüptarkvarast erinevate tarkvaratoodete puhul on inventuuri nimekirjas märgitud tarkvara kasutamise põhjus.

e. Tarkvara inventuuri nimekirja vaadatakse üle ja uuendatakse regulaarselt. Samuti uuendatakse nimekirja võimalikult kohe pärast uue tarkvara lisandumist.

APP.6.M10 Tarkvara turvajuhend

a. Nõuded tarkvara turvaliseks seadistamiseks ja kasutamiseks on koondatud tarkvara turvajuhendisse.

b. Asjakohased välised osapooled ja organisatsiooni töötajad järgivad tarkvara turvajuhendit igapäevaste tööülesannete täitmisel.

c. Tarkvara turvajuhendi täitmist kontrollitakse pisteliselt.

APP.6.M11 Tarkvara lisandmoodulite ja pluginite haldus

a. On lubatud ainult tarkvara eesmärgipäraseks käitamiseks vajalike lisandmoodulite ja pluginite kasutamine.

b. Üleliigsed lisandmoodulid ja pluginid on desinstallitud või desaktiveeritud.

APP.6.M12 Tarkvara kasutusest kõrvaldamine [vastutav spetsialist]

a. On koostatud üksikasjalikke tegevusi ning tegevuste eest vastutajaid sisaldav juhend tarkvara turvaliseks kõrvaldamiseks.

b. Kui tarkvara kasutusest kõrvaldamise tõttu muutuvad töötajate igapäevased tööülesanded, teavitatakse sellest töötajaid piisavalt ette ning tagatakse töötajatele vajalik väljaõpe.

APP.6.M13 Tarkvara turvaline desinstallimine

a. Tarkvara desinstallimisel eemaldatakse kõik failid, mis tarkvara kasutamiseks IT-süsteemis loodi ning kustutatakse süsteemifailidest kõik eemaldatava tarkvaraga seotud kirjed.

b. Desinstallimise käigus tehtud süsteemimuudatused dokumenteeritakse (käsitsi või spetsiaalsete programmide abil).

3.4 Kõrgmeetmed

APP.6.M14 Sertifitseeritud tarkvara kasutamine (C-I-A)

a. Tarkvara hankimisel hinnatakse, kas tootja, tarnija või teenuseandja kinnitused rakendatud turvafunktsioonide kohta on piisavalt usaldusväärsed.

b. Kui nõutava funktsionaalsusega ning sertifitseeritud tarkvaratooteid on mitmeid, hinnatakse toote täiendavaid turvamehhanisme ning nende vastavust kaitsetarbele.
c. Kui turul puudub sobiv sertifitseeritud toode, kaitstakse tarkvara käidukeskkonda täiendavate turvameetmetega.

APP.7 Tellimustarkvara arendus

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed organisatsiooni individuaalseks kasutusotstarbeks välja töötatud või organisatsiooni tarbeks oluliselt kohandatud rakenduste kavandamiseks, hankimiseks, evitamiseks, kasutamiseks ja kasutuselt kõrvaldamiseks.

1.2 Vastutus

Tellimustarkvara arenduse meetmete täitmise eest vastutab vastutav spetsialist.

Lisavastutajad

Hankeosakond, IT-talitus.

1.3 Piirangud

Moodulis vaadeldakse tarkvara kavandamist, tellimist, kasutuselevõttu, käitamist ja kasutusest eemaldamist tellija aspektist.

Tarkvaraarendust arendaja vaates ning seonduvaid turvameetmeid käsitletakse moodulis CON.8 *Tarkvaraarendus*. Lisaks sellele moodulile rakendatakse tarkvarale meetmeid moodulist OPS.1.1.6 *Tarkvara testimine ja kasutuselevõtt* ja tootespetsiifilistest APP moodulitest.

2 Ohud

2.1 Puudulikud sätted lepingus välise teenuseandjaga

Kui välise teenuseandjaga sõlmitud lepingus on osapoolte tegevused kirjeldatud puudulikult või ebaselgelt, võivad turvameetmed kas isikute teadmatuse, puuduva kvalifikatsiooni või puuduvate ressursside tõttu jääda rakendamata. Näiteks võivad õigusaktidest tulenevad nõuded tarkvarale jääda täitmata, kui vastava funktsionaalsuse arendamist pole kokku lepitud teenuseandjaga sõlmitud lepingus.

2.2 Ebaturvaline tarkvaraarhitektuur

Kui rakenduses on kasutatud alamprogramme, mooduleid ja protokolle, mille nõutud turvatase üksikult võetuna on madalam kui tervikrakendusel, võivad rakenduses esineda olulised turvanõrkused.

Kui tarkvara programmimoodulid ja protokollid on kavandatud töötamiseks isoleeritud keskkonnas, siis võib tarkvara ühendamisel Internetiga tekkida erinevaid turvaprobleeme. Tarkvara nõrkuse ärakasutamisel või tarkvara vea ilmnemisel ei pruugi ettenähtud turvamehhanismid plaanipäraselt toimida. Tarkvaraarhitektuuri turvanõrkuste tõttu võib ründaja leida võimaluse turvamehhanismidest möödumiseks.

2.3 Dokumenteerimata funktsioonid

Rakendus võib sisaldada tavakasutajale mitteteadaolevaid ning dokumenteerimata funktsioone. Selliseid peidetud funktsioone võib ründaja ära kasutada olemasolevatest tavakasutajatele suunatud turvamehhanismidest möödumiseks.

2.4 Turvameetmete puudumine või puudulikkus rakenduses

Sobivate turvameetmete puudumine rakenduses teeb rakenduse andmed ründajale hõlpsasti juurdepääsetavaks. Turvameetmete puudulikkus võib olla tingitud ebapiisavast projektieelarvest või liiga kiirest arenduse ajagraafikust.

Turvamehhanismid ja -funktsioonid, mis peavad tagama rakenduses töödeldavate andmete turvalisuse, võivad olla lihtsama kasutamise huvides välja lülitatud.

2.5 Puudulik kontroll tarkvara arenduse üle

Kui tellija pole võimeline kontrollima, kas kokku lepitud funktsionaalsus (sh turvafunktsionaalsus) on rakenduses realiseeritud, eksisteerib oht, et rakendus võetakse vastu koos rakenduses sisalduvate turvanõrkustega.

Kui tarkvara arenduses suunatakse kogu ressurss ärilise funktsionaalsuse täiustamisele, kannatab selle tõttu tarkvara turvafunktsionaalsus. Rakenduse turvafunktsioonid on algelised ja võivad sisaldada nõrkusi, mida ründaja saab ära kasutada.

2.6 Ebapädev tarkvaraarendaja

Valitud tarkvaraarendajal võivad puududa konkreetse programmeerimiskeele või -raamistiku osas vajalikud tehnilised teadmised. Samuti ei oska arendaja arvestada kõiki IT-taristu ja käidukeskkonnaga seonduvaid üksikasju. Piisavate kogemuste puudumisel võib arendaja teha vigu, mis muidu oleksid välditavad.

Ebareaalse ajaplaani või kuluhinnangute tõttu võib arendaja sattuda suure surve alla, mistõttu kannatab tarkvara kvaliteet. Arendaja ei ole eraldanud piisavalt aega ja inimressurssi turvafunktsionaalsuse arendamisele.

3 Meetmed

3.1 Elutsükkel

Kavandamine

APP.7.M1 Tellimustarkvara arendusprojekti kavandamine

APP.7.M2 Tarkvaraarenduse turvanõuete määramine

APP.7.M3 Tarkvara käidunõuete määramine

APP.7.M4 Tellimustarkvara nõuete määramine

APP.7.M6 Tellimustarkvara nõuete põhjalik dokumenteerimine

Evitus

APP.7.M7 Tellimustarkvara turvaline hankimine

Käitus

APP.7.M5 Tarkvaraarendusprojekti seire

APP.7.M8 Töötajate kaasamine tarkvara varajasse testimisse

Lisanduvad kõrgmeetmed

APP.7.M9 Usaldatav deponeerimine

APP.7.M10 Sertifitseeritud tarkvaraarendaja kasutamine

3.2 Põhimeetmed

APP.7.M1 Tellimustarkvara arendusprojekti kavandamine

a. Tarkvara arendusprojekti juhtimiseks ja koordineerimiseks on määratud vastutav osapool (tellija või arendaja) ja projektijuht.

b. Organisatsioon on teostanud esmase analüüsi ja määranud tellimustarkvara raamtingimused, sealhulgas:

- äriprotsessid, mida rakendus toetab;
- töödeldavad andmed ja nende kaitsetarve;
- õiguslikud raamtingimused;
- IT-süsteemid, millega rakendus andmeid vahetab;
- vajalikud rollid ja pääsuõigused.

c. Arendusprojekti läbiviimiseks on kinnitatud tarkvaraarenduse metoodika ja projektijuhtimise mudel.

d. Tellimustarkvara arendusprojektil on kindlaksmääratud tulem, eelarve ja teostusaeg.

APP.7.M2 Tarkvaraarenduse turvanõuete määramine

a. Organisatsioon on kinnitanud arendusprotsessi korralduslikud ja tehnilised turvanõuded.

b. Arenduskeskkond ja selle turvameetmed valitakse lähtuvalt tarkvaraarenduse turvanõuetest ja andmete kaitsetarbest.

APP.7.M3 Tarkvara käidunõuete määramine [IT-talitus]

a. IT-talitus on koostanud tellimustarkvara käitamiseks nõutava riist- ja tarkvara spetsifikatsiooni:

- riistvaraplatvorm (sh server ja salvestusseadmed);
- tarkvara (sh operatsioonisüsteem ja andmebaas);
- süsteemiressursid (sh nõuded protsessorile, muutmälule ja salvestusmahule).

b. Tarkvara lõimimiseks teiste IT-süsteemidega on koostatud liidestuse spetsifikatsioon.

APP.7.M4 Tellimustarkvara nõuete määramine [hankeosakond]

a. Tellimustarkvara hankimiseks on määratud järgnevad nõuded:

- organisatsiooni ärinõuetest ja õigusaktidest tulenevad tarkvara funktsionaalsed nõuded;
- tarkvarale esitatavad nõuded (vt APP.6.M2 *Tarkvarale esitatavate nõuete loend*);
- arendusprotsessi turvanõuded (vt APP.7.M2 *Tarkvaraarenduse turvanõuete määramine*);
- tarkvara tehnilised nõuded (vt APP.7.M3 *Tarkvara käidunõuete määramine*).

3.3 Standardmeetmed

APP.7.M5 Tarkvaraarendusprojekti seire

a. Tellimustarkvara arendamisel järgitakse kokku lepitud ja kinnitatud tarkvaraarenduse metoodikat ja projektijuhtimise mudelit.

b. Tarkvara arendusprojekt sisaldab riski- ja kvaliteedihaldust.

c. Arendusprojekti riski-ja kvaliteedihalduses osalevad töötajad ja välised arendajad on piisavalt kvalifitseeritud.

d. Tarkvaraarenduse metoodika ja projektijuhtimise mudelis ettenähtud kontrolltegevusi viiakse läbi kogu tellimustarkvara elutsükli jooksul.

APP.7.M6 Tellimustarkvara nõuete põhjalik dokumenteerimine

a. Rakendusele esitatud ärinõuded ja nende teostus (nt töövood, dialoogid, parandusmallid, andmestruktuurid) on esitatud rakenduse funktsionaalsete nõuetena.

b. Mittefunktsionaalsete nõuetena on dokumenteeritud vähemalt järgnevad rakendusele esitatavad nõuded:
   - kvaliteedinõuded (kasutatavus, usaldatavus, sooritusvõime);
   - arhitektuuri- ja IT-taristu nõuded, mille jaoks rakendus välja töötatakse;
   - liidestusnõuded;
   - rakenduse dokumentatsioon (nt modelleerimine UML-is);
   - rakenduse testimise nõuded;
   - turvafunktsioonide nõuded.

c. Rakenduse andmete suure kaitsetarbe puhul on dokumenteeritud ka järgmised turvanõuded:
   - krüptomehhanismide kasutamise nõuded (vt CON.1 *Krüptokontseptsioon*);
   - andmevarunduse nõuded (vt CON.3 *Andmevarunduse kontseptsioon*);
   - arhiveerimise nõuded (vt OPS.1.2.2 *Arhiveerimine*);
   - logimisnõuded (vt OPS.1.1.5 *Logimine*).

d. Pärast tarkvaramuudatuste ja funktsionaalsete uuendite installimist kontrollitakse nõuetele vastavust ning vajadusel uuendatakse tarkvara nõuete dokumentatsiooni.

APP.7.M7 Tellimustarkvara turvaline hankimine

a. Tellimustarkvara arendaja esitab pakkumuse koosseisus ka sobiva tarkvaraarendus- ja projektihaldusmetoodika.

b. Tarkvara avalikud hankedokumendid ei paljasta liigselt plaanitava tarkvara turvaarhitektuuri.

c. Organisatsioon on loonud protsessid ja määranud vastutajad tehtud pakkumuste hankedokumentatsioonile vastavuse hindamiseks.

APP.7.M8 Töötajate kaasamine tarkvara varajasse testimisse

a. Organisatsiooni töötajad on tarkvara testimisse kaasatud võimalikult varajases tarkvaraarenduse etapis.

b. Arendaja tagab testimise käigus ilmnenud vigade kõrvaldamiseks ja parendusettepanekute realiseerimiseks piisava ajavaru.

3.4 Kõrgmeetmed

APP.7.M9 Usaldatav deponeerimine (A)

a. Ärikriitilise tellimustarkvara puhul on otsustatud, kas tarkvara on vaja kindlustada tarkvara toe katkemise vastu.

b. On kaalutud tarkvara lähtekoodi jm olulise materjali usaldatavale hoiule andmise (ingl *escrow*) vajadust. Hoiustusleping sisaldab vähemalt järgnevat:

- hoiustatud materjali väljastusõigused ja tingimused;
- hoiustatud materjali verifitseerimine;
- hoiustatud materjali asjakohane säilitus ja turve;
- hoiustatud materjali uuendamise kord.

APP.7.M10 Sertifitseeritud tarkvaraarendaja kasutamine (C-I-A)

a. Turvakriitilise tellimustarkvara arendamisel kasutatakse turbehalduse ja tarkvaraarenduse valdkonnas sertifitseeritud tarkvaraarendusettevõtteid.

b. Tarkvara arenduspartneri valikul hinnatakse, kas arendaja kinnitused omandatud sertifikaatide ja rakendatud turvafunktsioonide kohta on piisavalt usaldusväärsed.

APP.EE: Eesti rakendused

APP.EE.1 X-tee andmeteenus

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed X-tee andmeteenuse andja või -tarbija kaitseks.

X-tee turvaserveriga liidestatud IT-süsteemid ei tohi ohustada X-tee taristut ega sattuda X-teega liidestatuse tõttu ise haavatavasse olukorda. Samuti peab andmete liikumine erinevate organisatsioonide ja üksuste vahel baseeruma selgetel õiguslikel alustel.

1.2 Vastutus

X-tee andmeteenuse tarbimise meetmete täitmise eest vastutab vastutav spetsialist.

Lisavastutajad

IT talitus, andmekaitse spetsialist.

1.3 Piirangud

X-tee turvaserveri omaniku meetmed on esitatud moodulis SYS.EE.1 *X-tee turvaserver*.

Turvaserveri kasutamise ja andmeteenuste kokkulepped toetuvad moodulitele CON.9 *Teabevahetus* ning OPS.3.2 *Teenuseandja infoturve*.

Lisaks sellele moodulile rakendatakse tarkvarale meetmeid moodulist OPS.1.1.6 Tarkvara testimine ja kasutuselevõtt ja tootespetsiifilistest APP moodulitest.

2 Ohud

2.1 Andmeteenuse andmete väärkasutus

X-tee andmeteenusega vahendatakse ja säilitatakse nii teenuseandjate kui -tarbijate andmeid. Andmete väärkasutus, leke või volitamata muutmine mõjutab andmeteenuse osapooli ning andmeomanikke (sh eraisikuid).

2.2 Turvaserveri seadistusvead

Vead suhtluses turvaserveri omanikuga ja selle tulemusena vääralt seadistatud turvaserver võib põhjustada andmetele volitamata juurdepääsu või põhjuseta takistada volitatud kasutajate juurdepääsu andmeteenustele.

2.3 Vead turvaserveri liidestamisel andmeteenusega

Turvaserveri ja andmeteenuse liidestamisel tehtud vead võivad põhjustada andmelekkeid ning volitamata juurdepääsu andmeteenustele.

3 Meetmed

3.1 Elutsükkel

Kavandamine

APP.EE.1.M1 X-tee andmeteenuse kasutamise või andmise kavandamine

Evitus

APP.EE.1.M2 X-tee liitumisleping X-tee keskusega

APP.EE.1.M3 Usaldusteenuste lepingud

APP.EE.1.M15 Turvaserveri tarbimise kokkulepe

Käitus

APP.EE.1.M4 E-templi sertifikaatide haldus

APP.EE.1.M5 X-tee andmeteenuse avaldamine turvaserveri abil

APP.EE.1.M6 X-tee andmeteenuse tarbimine turvaserveri vahendusel

APP.EE.1.M7 X-tee andmeteenuste kokkulepped

APP.EE.1.M8 X-tee andmeteenuse turvaline liidestamine

APP.EE.1.M9 X-tee andmeteenuse arendamine ning testimine

APP.EE.1.M10 X-tee turvaserveri sõnumilogi arhiveerimine

APP.EE.1.M14 X-tee andmeteenuste dokumentatsiooni regulaarne ülevaatus

APP.EE.1.M16 Turvaserveri kasutamine tarbijana

APP.EE.1.M17 X-tee andmeteenuse logimine ja seire

Kõrvaldamine

APP.EE.1.M11 X-tee andmeteenuse andmise lõpetamine

APP.EE.1.M12 X-tee andmeteenuse tarbimise lõpetamine

APP.EE.1.M13 Turvaserveri tarbimise turvaline lõpetamine

Lisanduvad kõrgmeetmed

APP.EE.1.M18 X-tee andmeteenuse kõrgkäideldavus

APP.EE.1.M19 Organisatsiooni e-templi privaatvõtme turvaline kasutamine

APP.EE.1.M20 Kvalifitseeritud e-templite kasutamine

3.2 Põhimeetmed

APP.EE.1.M1 X-tee andmeteenuse kasutamise või andmise kavandamine [andmekaitse spetsialist, IT-talitus]

a. On läbi viidud X-tee andmeteenuse vajaduse ning nõuete analüüs, milles käsitletakse vähemalt järgmist:
   - äriprotsessis või -teenuse andmevahetusvajaduste tuvastamine;
   - andmevahetuse kooseisus olevate andmete edastamise/vastuvõtmise/töötlemise õiguslikud alused;
   - isikuandmete (eelkõige isikuandmete eriliikide) olemasolu ning selliste andmete töötlemise reeglid;
   - andmete puhverdamise lubatavus ja ajalised piirid;
   - käideldavusnõuete (sh teenuse kasutamise mahud ja kasutusmustrid) määratlemine.

b. Lähtuvalt läbiviidud analüüsist ning organisatsiooni võimekusest on valitud X-tee kasutusmudel: kas turvaserveri teenuse sisseost või turvaserveri omamine (vt *SYS.EE.1 X-tee turvaserver*).

c. Lähtuvalt andmeteenust kasutatava äriprotsessi nõuetest ning koostöös turvaserveri omanikuga määratakse turvaserveri teenuse sisu ja turvaserveri suutvusnäitajad:
   - andmevahetuse tõestusväärtuse tase, sh kvalifitseeritud e-templite (vt eIDAS) kasutamise vajadus;
   - ajatembelduse täpsus (sagedus) ning lubatud viivitus (maksimaalne ajavahemik mil sõnumid on ajatembeldamata);
   - sõnumilogi detailsuse nõuded (täielikud sõnumilogid, ainult päiste logimine või logimata);
   - sõnumilogi säilitustähtajad ning sõnumilogi juurdepääsu reeglid.

APP.EE.1.M2 X-tee liitumisleping X-tee keskusega [organisatsiooni juhtkond]

a. X-tee keskusega on sõlmitud X-tee liitumisleping.

b. X-tee keskuse iseteeninduses on registreeritud volitatud administratiivsed ja tehnilised kontaktisikud. Volitatud isikute muutumisel uuendatakse kontaktandmeid viivitamatult.

c. Teavituste saamise e-posti aadress on suunatud eraldiseisvale aadressile /meiligruppi, mille saajaid on rohkem kui üks inimene.

APP.EE.1.M3 Usaldusteenuste lepingud [organisatsiooni juhtkond]

a. Organisatsioon on sõlminud usaldusteenuste lepingud.

b. Eksisteerib kord lepingute ülevaatuseks. Vajadusel lepingud uuendatakse.

c. Organisatsiooni volitatud administratiivsed ja tehnilised kontaktisikud on usaldusteenuste (ajatempliteenus, sertifitseerimiskeskus, OCSP) osutaja juures registreeritud. Volitatud isikute muutumisel uuendatakse kontaktandmeid viivitamatult.

d. Teavituste saamise e-posti aadress on suunatud eraldiseisvale aadressile/meiligruppi, mille saajaid on rohkem kui üks inimene.

APP.EE.1.M4 E-templi sertifikaatide haldus [IT-talitus]

a. Koostöös turvaserveri omanikuga tagatakse e-templi sertifikaatide (ingl *signing certificate*) õigeaegne uuendamine.

b. Kasutuselt eemaldatud e-templi sertifikaatide tühistamise taotlus esitatakse usaldusteenuse pakkujale viivitamatult.

APP.EE.1.M5 X-tee andmeteenuse avaldamine turvaserveri abil

a. On määratud X-tee andmeteenuse ja otspunktide tehnilised parameetrid (WSDL aadressid, REST, andmeteenuse aadress(id), alamsüsteemi nimi jms).

b. On kokku lepitud X-tee andmeteenuse nõutav tõestusväärtus (st kasutatava e-templi ja ajatembelduse tasemed).

c. On kokku lepitud pääsuloendi uuendamise ja kontrollimise kord.

d. Igal IT-süsteemil või selle loogilisel osal on andmeteenuste andmiseks eraldiseisev X-tee alamsüsteem.

e. X-tee andmeteenuse tarbimine ilma volitatud turvaserveri vahenduseta on blokeeritud.

f. Turvaserveri omanikku teavitatakse:
   - muutustest andmeteenuse tarbijate nimekirjas (pääsuloendi uuendamiseks);
   - andmeteenuse kasutuskoormuste olulistest/oodatavatest muutustest;
   - andmeteenuse hooldustöödest ja nende kestvusest.

g. Andmeteenuse andjat teavitatakse:
   - muutustest turvaserveri tehnilistes andmetes (aadress, sertifikaadid),
   - turvaserveri hooldustöödest ja nende kestvustest;
   - turvaserveri omanikule teatavaks saanud asjaoludest, mis puudutavad andmeteenuste andjat.

h. Kasutuselt kõrvaldatud teenuste seadistused (sh otspunktide sertifikaadid) eemaldatakse turvaserveri konfiguratsioonist viivitamatult.

APP.EE.1.M6 X-tee andmeteenuse tarbimine turvaserveri vahendusel

a. On kokku lepitud X-tee andmeteenuse nõutav tõestusväärtus (st kasutatava e-templi ja ajatembelduse tasemed).

b. Turvaserveri teenust tarbitakse ainult turvaserveri omanikuga kokkulepitud viisil ning aadressidelt.

c. Igal IT-süsteemil või selle loogilisel osal on andmeteenuste tarbimiseks eraldiseisev X-tee alamsüsteem. Alamsüsteemi kirjeldus ja tehnilised parameetrid on dokumenteeritud.

d. X-tee sõnumites kasutatakse unikaalseid sõnumi identifikaatoreid.

e. X-tee sõnumitesse lisatakse autenditud kasutaja unikaalne tunnus või selle tagasiseostatav pseudonüüm (kui see on teenusekirjelduses nõutud).
f. X-tee turvaserveri teenuse tarbimine ilma volitatud infosüsteemi vahenduseta on blokeeritud.
g. Turvaserveri omanikku teavitatakse muutustest infosüsteemi liidestuses turvaserveriga ning andmeteenuse kasutuskoormuste olulistest/oodatavatest muutustest.
h. Turvaserveri tarbijat teavitatakse:
    - muutustest turvaserveri tehnilistes andmetes (aadress, sertifikaadid);
    - turvaserveri hooldustöödest ja nende kestvustest;
    - turvaserveri omanikule teatavaks saanud asjaoludest, mis puudutavad turvaserveri tarbijat.
i. Kasutuselt kõrvaldatud teenuste seadistused (sh otspunktide sertifikaadid) eemaldatakse turvaserveri konfiguratsioonist viivitamatult.

APP.EE.1.M7 X-tee andmeteenuste kokkulepped

a. Andmeteenuse andmine/tarbimine baseerub kahepoolsel kokkuleppel, milles muuhulgas kirjeldatakse:
    - andmeteenuse olemus;
    - õiguslikud alused (sh teenuse abil vahendatud andmete kasutamise õiguslikud alused, lubatud eesmärgid, andmete säilitamise ja kasutuselt kõrvaldamise üksikasjad);
    - administratiivsed ja tehnilised kontaktandmed ning nende uuendamise kord;
    - käideldavusnõuded;
    - andmeteenuse andmise ja tarbimise X-tee identifikaatorid;
    - andmeteenuse osutamise ja/või tarbimise turvaserverite tunnused või võrguaadressid (vajadusel);
    - vastastikune turvalise halduse tõendamise viis (nt E-ITS auditiraporti vastavate osade jagamine, muu sertifikaat või audit, vahetu kontroll) ning regulaarsus.
b. Andmeteenuse tarbijat teavitatakse:
    - muutustest andmeteenuse olemuses;
    - andmeteenuse hooldustöödest ja nende kestvusest.
c. Andmeteenuse andjat teavitatakse:
    - andmeteenuse kasutuskoormuste olulistest/oodatavatest muutustest;
    - andmeteenuse kasutamise lõpetamisest.

APP.EE.1.M8 X-tee andmeteenuse turvaline liidestamine

a. Turvaserveri ja andmeteenuse vahel on rakendatud vastastikku autenditud TLS ühendus, mille turvaserveri ja infosüsteemi TLS sertifikaate verifitseeritakse.
b. Iga andmeteenuse andja / -tarbija kasutab unikaalset TLS võtit. Võtme taas- ning mitmikkasutamine on keelatud.
c. Autentimata ja/või krüpteerimata protokollide kasutamisel rakendatakse täiendavaid konfidentsiaalsust ja terviklust tagavaid turvameetmeid.
d. Andmeteenuse kasutamine on võimalik ainult volitatud turvaserveri vahendusel.

APP.EE.1.M9 X-tee andmeteenuse arendamine ning testimine

a. Turvaserveri ja andmevahetuse liidestuse arendus- ning testimistööd teostatakse arendus- või testkeskkonnas.

b. Arendus- ja testkeskkondades ei tohi kasutada käidukeskkonna (ingl *production environment, operational environment*) andmeid ega teenuseid.

c. Arendus- ja testkeskkondade turvaserveri ja andmeteenuste turvameetmed takistavad nende keskkondade väärkasutamist ja ründeobjektiks saamist.

APP.EE.1.M10 X-tee turvaserveri sõnumilogi arhiveerimine

a. Turvaserveri omanikuga on kokkulepe mis sisaldab:
   - sõnumilogi arhiveerimist turvaserveri omaniku infrastruktuuris;
   - või sõnumilogi transporti ning arhiveerimist turvaserveri tarbija infrastruktuuris.

b. On määratud sõnumilogi säilitamistähtajad ning logidele juurdepääsu kord.

APP.EE.1.M11 X-tee andmeteenuse andmise lõpetamine

a. Enne X-tee andmeteenuse lõpetamist teavitatakse X-tee andmeteenuse tarbijaid ning turvaserveri omanikku.

b. Veendutakse, et turvaserveri omanik on eemaldanud vastava andmeteenusega seotud konfiguratsioonielemendid (teenuse kirjeldus, pääsuloendid, X-tee alamsüsteem jms).

c. X-tee andmeteenuse lõpetamisel tagatakse sõnumilogide säilitamine vastavalt äriprotsessi nõuetele.

APP.EE.1.M12 X-tee andmeteenuse tarbimise lõpetamine

a. Enne X-tee andmeteenuse lõpetamist teavitatakse X-tee andmeteenuse andjat, et ta eemaldaks juurdepääsu õiguse.

b. X-tee andmeteenuse lõpetamisel tagatakse sõnumilogide säilitamine vastavalt äriprotsessi nõuetele.

c. Turvaserveri ja infosüsteemi vaheliseks suhtluseks kasutatud TLS võtmed hävitatakse ning välistatakse nende taaskasutus.

APP.EE.1.M13 Turvaserveri tarbimise turvaline lõpetamine

a. Enne turvaserveri tarbimise lõpetamist teavitatakse sellest turvaserveri omanikku.

b. Tagatakse kõikide (sh veel arhiveerimata) sõnumilogide säilitamine.

c. Tühistatakse turvaserveris kasutusel olnud sertifikaadid.

d. Turvaserveri omaniku abiga taotletakse X-tee eksemplarist kasutamata konfiguratsioonielementide (kasutuseta jäävad alamsüsteemid, organisatsioonid jms) eemaldamist.

e. Veendutakse, et turvaserveri omanik on eemaldanud turvaserveri tarbimise konfiguratsioonielemendid ning võtmed.

3.3 Standardmeetmed

APP.EE.1.M14 X-tee andmeteenuste dokumentatsiooni regulaarne ülevaatus

a. Regulaarselt kontrollitakse X-tee andmeteenuste:
   - vajaduse olemasolu;

- õiguslikke aluste kehtivust;
- pääsuloendi ajakohasust;
- andmeteenuse kasutamise kokkuleppes toodud tingimustele vastavust;
- avaldatud (sh X-tee iseteenindusportaalis) dokumentatsiooni ja kirjelduste ajakohasust.

APP.EE.1.M15 Turvaserveri tarbimise kokkulepe

a. Turvaserveri teenuse tarbimiseks on sõlmitakse turvaserveri omaniku ja turvaserveri tarbija vaheline kokkulepe. Kokkulepe põhineb turvaserveri teenuse standardtingimustel kuid võib sisaldada täiendavaid tingimusi.

b. Kokkulepe sisaldab vähemalt järgmist:
   - volitatud kontaktisikud ja vastavad kontaktandmed;
   - andmete ülevaatuse ja uuendamise kord;
   - kokkulepitud suhtlusteed, teenussoovide volituskontrollid ning reageerimisajad;
   - turvaserveri omaniku volitamine organisatsiooni e-templi võtmete hoidmiseks ning aktiveerimiseks;
   - vajadusel turvaserveri omaniku volitamine suhtluseks usaldusteenuse andjaga (e-templi sertifikaatide taotlemiseks ning vajadusel tühistamiseks);
   - vastastikune kohustus turvaserveri teenusega seotud andmeid (sh teenuse andmed, sõnumilogid) töödelda vastavalt andmete kaitsetarbele (konfidentsiaalsus, terviklikus, käideldavus);
   - sõnumilogide ning teenuspäringute logide juurdepääsu, säilitamise ja kliendile üleandmise kord.
   - teenusetasemelepe teenuste mahu, iseloomu, käideldavusnõuete kohta.
   - teenusetarbija(te) volitatud otspunktide (IP-aadressid, teenusekirjeldused) turvanõuded ja nõuete ülevaatamise kord.

APP.EE.1.M16 Turvaserveri kasutamine tarbijana

a. Turvaserveri omanikule antud volitatud isikute kontaktandmed on korrektsed, muutuse korral uuendatakse andmeid viivitamatult.

b. Teavituste saamise e-posti aadress on suunatud eraldiseisvale aadressile /meiligruppi, mille saajaid on rohkem kui üks inimene.

c. Turvaserveri omaniku teavitustele reageeritakse vastavalt teate prioriteetsusele.

d. Kasutamata sertifikaadid tühistatakse viivitamatult.

APP.EE.1.M17 X-tee andmeteenuse logimine ja seire [IT-talitus]

a. Andmeteenuse andmiseks või tarbimiseks kasutatava infosüsteemi logisid logisid töödeldakse ja säilitatakse vastavalt organisatsiooni poliitikatele.

b. Andmeteenuse andmiseks või tarbimiseks kasutatava operatsioonisüsteemi tööd, ressursikasutust ning sõnumivahetuse metaandmeid seiratakse vastavalt organisatsiooni eesmärkidele.

3.4 Kõrgmeetmed

APP.EE.1.M18 X-tee andmeteenuse kõrgkäideldavus (A)

a. X-tee andmeteenuse tõrkekindluse tagamiseks ja/või jõudluse parandamiseks käitatakse teenuseid mitmes eksemplaris, liikluse suunamiseks kasutatakse koormusjaoturit.

b. Andmeteenuse eksemplaride sünkroonsus tagatakse tehniliste või protseduuriliste meetmetega.

APP.EE.1.M19 Organisatsiooni e-templi privaatvõtme turvaline kasutamine (C)

a. Koostöös turvaserveri omanikuga tagatakse, et X-teel kasutatava e-templi privaatvõtme loomisel, kasutamisel ja hoidmisel kasutatakse kvalifitseeritud e-templi loomise vahendit (HSM).

APP.EE.1.M20 Kvalifitseeritud e-templite kasutamine (C-I)

a. Andmevahetuse tõendusväärtuse parandamiseks nõuab andmeteenuse andja andmeteenuse tarbijatelt kvalifitseeritud e-templi kasutamist.

b. Andmeteenuse andja kasutab päringuvastustes kvalifitseeritud e-templit.

4 Lisateave

4.1 Kasutatud lühendid ja mõisted

Usaldusteenuse osutaja

Sertifitseerimiskeskuse (ingl *Certificate Authority*, CA), kehtivuskinnituse (ingl *Online Certificate Status Protocol*, OCSP) ja/või ajatempliteenuse (ingl *Time Stamping Authority*, TSA) osutaja, Eestis SK ID Solutions ja Riigi Infosüsteemi Amet (RIA)

X-tee

Eestis töötav X-tee eksemplar/eksemplarid. Peamiselt käidukeskkonna (ingl *production environment, operational environment*) tähenduses.

X-Road

Tarkvara, mis realiseerib X-tee turvaserveri / keskserveri funktsioone.

X-tee keskus

X-tee eksemplari haldaja, kes vastutab X-tee haldamise ja arendamise eest (Eestis Riigi Infosüsteemi Amet (RIA)) .

Turvaserver

X-tee turvaserver (ingl *X-Road Security Server*).

Turvaserveri omanik

Organisatsioon või vastutav struktuuriüksus, kes võimaldab infosüsteemidel kasutada turvaserverit X-teel suhtlemiseks (ka turvaserveri teenuse andja).

Turvaserveri tarbija

Organisatsioon või vastutav struktuuriüksus, kes omab infosüsteemi mis kasutab turvaserveri teenust. Üldnimetus X-tee andmeteenuse andja ja andmeteenuse tarbija kohta (ka turvaserveri teenuse tarbija).

X-tee andmeteenuse andja

X-teega liidestatud infosüsteem või vastava äriprotsessi omanik andmeteenuse andja rollis (ootab andmeteenuse tarbijalt päring-sõnumit ning koostab vastus-sõnumi).

X-tee andmeteenuse tarbija

X-teega liidestatud infosüsteem või vastava äriprotsessi omanik andmeteenuse tarbija rollis (koostab ja edastab päring-sõnumi ning ootab andmeteenuse andjalt vastus-sõnumit).

4.2 Publikatsioonid

SYS: IT-SÜSTEEMID

SYS.1: Server

SYS.1.1 Server üldiselt

1 Kirjeldus

1.1 Eesmärk

Esitada serverites töödeldavate andmete ning nendega seotud serveriteenuste kaitse meetmed.

Moodulit kasutatakse serverisüsteemide puhul sõltumata serveri operatsioonisüsteemist. Mooduli meetmed on kasutatavad nii eraldiseisva füüsilise serveri kui virtuaalserveri puhul.

Serveriteenuste all mõistetakse siin moodulis muuhulgas nii taustal toimuvaid põhiteenuseid kohtvõrgu toimimiseks kui kasutajale mõeldud teenuseid, mis võimaldavad näiteks vahetada e-kirju ja kasutada grupiprinterit.

1.2 Vastutus

Mooduli „Server üldiselt“ meetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Tehnikatalitus.

1.3 Piirangud

Mooduli meetmeid rakendatakse kõikidele serveritele. Kui serveriteenuse või IT-süsteemi jaoks on välja töötatud eraldiseisev E-ITS moodul, lähtutakse esmalt spetsiifilisest moodulist ja alles seejärel käesolevast moodulist. Kui serveriteenuse jaoks eraldiseisvat moodulit pole, kohandatakse serveriteenusele käesoleva mooduli meetmeid ning viiakse läbi täiendav sihtobjektikohane riskianalüüs.

Serveri turvalist haldust käsitletakse moodulites OPS.1.1.2 *IT-haldus*, OPS.1.1.3 *Paiga- ja muudatusehaldus.* Serveri turvaline paigutamist võrku käsitletakse moodulis NET.1.1 *Võrgu arhitektuur ja lahendus*.

Täiendavalt rakendatakse serverile meetmeid moodulitest ORP.4 *Identiteedi ja õiguste haldus*, DER.4 *Avariihaldus* ja OPS.1.1.4 *Kaitse kahjurprogrammide eest*.

2 Ohud

2.1 Serveri kasutuselevõtu puudulik kavandamine

Server on keerukas IT-süsteem, millel reeglina on palju funktsioone ja konfigureerimisvalikuid. Serveri tüüpkonfiguratsioon ei pruugi olla piisavalt turvaline. Kui serveri konfiguratsiooni enne serveri kasutuselevõttu ei muudeta, on serveri kasutamise ajal turvalisust juurde lisada palju keerulisem ning tihtipeale jäetakse see tegemata. Puudulikult konfigureeritud server jätab ründajale palju võimalusi eduka ründe sooritamiseks.

2.2 Serveri puudulik haldus

Serveritarkvara täiustatakse pidevalt ning tootja lisab juurde täiendavat funktsionaalsust. Serveri seadistused vajavad seetõttu pidevat ülevaatust ja muutmist. Kui IT-talitus sellega järjepidevalt ei tegele, võib serveri turvalisus väheneda. Vigu võib tekkida ka konfigureerimisel tehtud inimlike eksimuste tulemusel. Administreerimisvead võivad tekitada tõrkeid serveri funktsioneerimises, muuhulgas ka mõjutada süsteemi turvalisust.

Kui servereid on mitmeid ja ei kasutata ühtset dokumenteeritud konfiguratsiooni, muutub konfiguratsioon serverites ajapikku erinevaks. Mida rohkem tekib sarnaste funktsioonidega süsteemide turvasätetes erinevusi, seda keerukam on tagada turbeprotsessi terviklust ja järjepidevust.

2.3 Haldusõiguste lubamatu omandamine või kuritarvitamine

Kui haldur kasutab haldusõigustega kontot (eeliskontot) igapäevasteks tegevusteks, on suur oht, et ründajal õnnestub see eeliskonto (ingl *privileged account*) kaaperdada. Eeliskontodele on määratud tavaliselt väga suured õigused, mistõttu võib sellise konto kuritarvitamisel olla suur mõju. Näiteks domeenihalduri konto üle võtmisega on võimalik tekitada väga suurt kahju. Konto kasutamiseks vajaliku parooli võib ründaja hankida ka paroole ära arvamata või jõurünnet (ingl *brute-force attack*) kasutamata, kui neil õnnestub ligi pääseda parooliräsile (ingl *password hash*).

2.4 Andmekadu

Kesksetesse serveritesse talletatud andmed peavad olema vajadusel kättesaadavad. Andmete kaotusel võib sõltuvalt andmete kriitilisusest ja varukoopiate olemasolust olla organisatsiooni äriprotsessidele märkimisväärne ning pikaajaline mõju. Andmete kaotus võib peale andmete taastamiseks tehtavate kulutuste põhjustada ka muud kahju, näiteks klientide ja partnerite kaotust, seaduserikkumisest tulenevaid õiguslikke tagajärgi ja mainekahju. Rasked tagajärjed võivad kaasneda ka arhiveeritud andmete kaotamisega. Sellest tulenev otsene ja kaudne kahju võib ohtu seada isegi organisatsiooni püsimajäämise.

2.5 Teenusetõkestusründed

Teenusetõkestusründega e. ummistusründega (ingl *denial-of-service-attack*) üritab ründaja süsteemi või võrguühendust üle koormates takistada serveriteenuste kasutamist. Enamasti on IT-süsteemid üksteisest sõltuvad ja ühe serveri ressursinappus võib mõjutada ka teiste serverite toimimist. Kui teenusetõkestusründe vastu ei ole kavandatud mõju leevendavaid meetmeid, võivad serveri ressursid ja teenused muutuda täiesti kättesaamatuks.

2.6 Tarbetud operatsioonisüsteemi komponendid ja rakendused

Serveri operatsioonisüsteem sisaldab palju vaikerakendusi ja teenuseid, millest kõiki ei ole vajalik kasutada. Samuti on võimalik, et tarkvara installimisega lisatakse tarkvarakomponente, mida reaalselt vaja ei lähe. Sageli puudub halduritel ülevaade, millised mittevajalikud rakendused serverit tarbetult koormavad.

Tarbetud rakendused ja teenused võivad sisaldada turvanõrkusi. Kui paigaldatud rakendused ja teenused ei ole teada, siis puudub ülevaade ka nende ajakohastamise vajadusest. Sellistest turvanõrkustest võib saada ründajale sisenemispunkt (ingl *entry-point*) tervele sisevõrgule.

2.7 Serveri ülekoormus

Serveri ülekoormuse tõttu võib tekkida käideldavushäire, sest arvukad päringud koormavad süsteemi korraga liiga palju ja serveriteenus ei ole seetõttu ajutiselt kasutatav. Andmed võivad minna kaotsi, sest serveri kasutada olev mälumaht on ületatud ja andmebaasiserver ei suuda toimingut määratud aja jooksul teostada. Kui server ei vasta enam organisatsiooni vajadustele, võib keeruka IT-keskkonna puhul ühe serveri ülekoormus põhjustada ka teiste serverite tõrkeid.

3 Meetmed

3.1 Elutsükkel

Kavandamine

SYS.1.1.M11 Serveri turvajuhendi kehtestamine

SYS.1.1.M12 Serveri kasutuselevõtu kava

SYS.1.1.M15 Katkestusteta ja stabiilne toide

Hankimine

SYS.1.1.M13 Serveri hankimine

Evitus

SYS.1.1.M1 Serverile juurdepääsu piiramine

SYS.1.1.M2 Kasutajate autentimine

SYS.1.1.M5 Haldusliideste kaitse

SYS.1.1.M6 Tarbetute teenuste desaktiveerimine

SYS.1.1.M16 Serveri turvaline installimine ja aluskonfiguratsioon

Käitus

SYS.1.1.M9 Kahjurvaratõrje rakenduste kasutamine serveril

SYS.1.1.M10 Serveri logimine

SYS.1.1.M19 Lokaalsed paketifiltrid

SYS.1.1.M21 Serveri käidudokumentatsiooni koostamine

SYS.1.1.M23 Serverisüsteemi seire

SYS.1.1.M24 Regulaarne turbe testimine

SYS.1.1.M34 Kõvaketta krüpteerimine

SYS.1.1.M35 Serveri käidudokumentatsiooni haldus

SYS.1.1.M36 Serveri buutimise turve

SYS.1.1.M37 Turvakriitiliste rakenduste ja operatsioonisüsteemi komponentide kapseldamine

SYS.1.1.M39 Serveri turvaseadete keskne haldus

Kõrvaldamine

SYS.1.1.M25 Serveri kasutuselt kõrvaldamise kord

Avariivalmendus

SYS.1.1.M22 Integreerimine avariivalmendusega

Lisanduvad kõrgmeetmed

SYS.1.1.M27 Hostipõhine sissetungituvastus

SYS.1.1.M28 Liiasus

SYS.1.1.M30 Üks teenus serveri kohta

SYS.1.1.M31 Rakenduste käitamise tõkestamine

SYS.1.1.M33 Juursertifikaadi aktiivne haldus

SYS.1.1.M38 Serveri süsteemifailide tugevdatud kaitse

3.2 Põhimeetmed

SYS.1.1.M1 Serverile juurdepääsu piiramine [tehnikatalitus]

a. Serveri füüsilisele asukohale on juurdepääs ainult pääsuõigustega isikutel.
b. Serverid on paigutatud arvutikeskusse, lukustatud serveriruumi või lukustatud seadmekappi (vt INF.5 *Tehnilise taristu ruum või kapp*).
c. Virtualiseeritud serveri konfiguratsioonile ja ressurssidele on juurdepääs ainult selleks volitatud isikutel.
d. Serverit ei kasutata tööjaamana ega selliste tööülesannete täitmiseks, mida saab teha klientarvutis. Eelkõige tuleb serveris vältida veebibrauseri ja veebirakenduste kasutamist.
e. Tööjaamana kasutamiseks mõeldud arvutit ei kasutata serverina.

SYS.1.1.M2 Kasutajate autentimine

a. Serverisüsteemi autentimiseks kasutatakse võimalusel keskseid autentimisprotseduure.
b. Kasutaja autendib serverisse ainult isikustatud kasutajakontoga.
c. Kasutajate autentimine vastab serveri kaitsetarbele. Suure kaitsetarbe puhul kasutatakse mitmikautentimist.
d. Serveri haldusõigused on vajadusepõhiselt piiratud. Tavatööks kasutavad haldurid piiratud õigustega kasutajakontot.

SYS.1.1.M5 Haldusliideste kaitse

a. Serveri välisseadmeid ja andmekandjaid kasutatakse ainult serveri hoolduseks.
b. Serveri buutimine (ingl *booting*) CD/DVD-seadmelt ja irdmäluseadmetelt on BIOS-is desaktiveeritud.
c. Kõik tarbetud liidesed serveris on desaktiveeritud.

SYS.1.1.M6 Tarbetute teenuste desaktiveerimine

a. Kõik tarbetud teenused (eriti võrguteenused) ja tarbetu funktsionaalsus on serveris desaktiveeritud või desinstallitud.

b. Kõik tarbetud serverikomponentide püsivara (ingl *firmware*) funktsioonid on desaktiveeritud.

c. Kasutajale ja rakendusele serveris antav salvestusruum on piiratud kettakvoodiga (ingl *disc quota*).

d. Serveri tarkvara, teenuste ja kontode konfiguratsioon on dokumenteeritud.

SYS.1.1.M9 Kahjurvaratõrje rakenduste kasutamine serveril

a. Serveri kahjurvaratõrje rakenduse vajalikkuse ja otstarbekuse otsustamisel on lähtutud serveri operatsioonisüsteemist, serveriteenustest ja serveri turvamehhanismidest.

b. Serveris kasutatav kahjurvaratõrje rakendus suudab lisaks reaalajas ja nõudmisel skaneerimisele otsida kahjurvara ka pakitud andmetest.

SYS.1.1.M10 Serveri logimine

a. On kehtestatud ja dokumenteeritud, milliseid sündmusi serveris logitakse ning kes ja millistel tingimustel võib logiandmeid vaadata.

b. On otsustatud, kas logiandmeid hoitakse serveris või kasutatakse keskset logiserverit.

c. Logitakse kõik turbe jaoks olulised sündmused, sh vähemalt:

- süsteemi käivitamised ja buutimised (ingl *booting*);
- operatsioonisüsteemi ja rakendustesse sisselogimised ja sisselogimiskatsed;
- õiguste ületamise katsed;
- pääsuloendite või tulemüürireeglite rikkumiskatsed;
- kasutajate, kasutajarühmade ja õiguste loomine või muutmine;
- turvalisust puudutavad tõrketeated (nt elektrikatkestused, riistvaratõrked, mahupiirangute ületamine);
- turvamehhanismide hoiatusteated (näiteks kahjurvaratõrje rakenduse teated).

3.3 Standardmeetmed

SYS.1.1.M11 Serveri turvajuhendi kehtestamine

a. Organisatsiooni üldisest turvapoliitikast lähtuvalt on dokumenteeritud ja kehtestatud serveri turvajuhend. Turvajuhend arvestab serverite erinevat kaitsetarvet.

b. Kõik serveri hankimise, halduse ja käitusega seotud töötajad järgivad serveri turvajuhendit.

c. Serveri turvajuhend käsitleb vähemalt järgmist:

- füüsilise juurdepääsu reguleerimine;
- virtualiseerimine (vt SYS.1.5 *Virtualiseerimissüsteem*);
- halduse ja auditeerimise korraldus;
- installimine ja aluskonfiguratsioon;
- failide krüpteerimine;
- dokumenteerimine;
- turvalise käituse nõuded;
- paroolinõuded;

- side- ja võrguteenuste turve;
- logimine;

d. Juhendis esitatu täitmist kontrollitakse regulaarselt, kontrollide tulemused dokumenteeritakse.

SYS.1.1.M12 Serveri kasutuselevõtu kava

a. Serveri kasutuselevõtu kavandamisel on arvestatud järgmist:
   - riistvaraplatvorm, operatsioonisüsteem ja rakendustarkvara;
   - riistvara parameetrite sobivus (sooritusvõime, mälumaht, läbilaskevõime jne);
   - ruumivajadus ja konstruktsioonitüüp;
   - serveri energiatarve ja soojuseraldus;
   - sideliideste tüüp ja arv;
   - halduse korraldus (vt SYS.1.1.M5 *Haldusliideste kaitse*);
   - kasutajate pääsuõigused;
   - logimine (vt SYS.1.1.M10 *Logimine*);
   - seire;
   - serveri IT-komponentide ajakohastamine;
   - integratsioon olemasolevate võrguhalduse, andmevarunduse ja infoturbe (nt kahjurvaratõrje tarkvara, sissetungituvastuse süsteem) lahendustega.

b. Serveri kasutuselevõtu kavandamisel tehtud otsused on dokumenteeritud.

SYS.1.1.M13 Serveri hankimine

a. Serveri hankimiseks on koostatud nõuete spetsifikatsioon ja määratud kriteeriumid toodete omavaheliseks võrdluseks:
   - füüsilised parameetrid (mõõtmed, sobivus serverikappi);
   - funktsionaalsusnõuded (vajalikud riistvaraliidesed, ühilduvus);
   - töökindlus ja administraatorisõbralikkus (usaldusväärne teave sõltumatust allikast);
   - haldus (tootja tugi ja hooldusleping);
   - kogukulu (soetus- ja püsikulud).

b. Infoturbe seisukohast on püstitatud järgmised nõuded:
   - piisav käideldavus ja andmeterviklus;
   - turvalised protokollid andmehalduseks;
   - ühilduvus õiguste halduse ja organisatsiooniülese turbekontseptsiooniga.

SYS.1.1.M15 Katkestusteta ja stabiilne toide [tehnikatalitus]

a. Kõik serverid on ühendatud piisava võimsuse ja aku kestvusega puhvertoiteallikaga (UPS).

b. Puhvertoiteallikate haldus on vastavuses meetmega INF.2.M3 *Puhvertoiteallikas (UPS).*

SYS.1.1.M16 Serveri turvaline installimine ja aluskonfiguratsioon

a. Serveri süsteemi- ja rakendustarkvara hangitakse ainult autentsetest ja usaldusväärsetest allikatest.

b. Serveri installimine ja seadistamine viiakse läbi tootmiskeskkonnast (ingl *production environment*) eraldatud paigalduskeskkonnas.

c. Serveri seadistamisel lähtutakse tootja soovitustest ja soovituslikust konfiguratsioonist, eeldusel, et see on piisavalt turvaline ning ei ole vastuolus organisatsiooni vajaduste ja nõuetega.

d. Serveri aluskonfiguratsioon on dokumenteeritud, isegi juhul kui kasutatakse tootjapoolseid vaikeseadistusi.

e. Serveri aluskonfiguratsioon vastab turvajuhendi nõuetele. Turvaseadeid kontrollitakse enne serveri käikuandmist ja pärast iga serveris tehtavat muudatust.

f. Installitakse ainult serveri otstarbe täitmiseks vajalikud teenused.

g. Kui serveri tööks on vajalik internetiühendus, ühendatakse server Internetiga pärast installimise ja konfigureerimise lõpetamist.

SYS.1.1.M19 Lokaalsed paketifiltrid

a. Suure kaitsetarbega serverid on kaitstud lokaalse (operatsioonisüsteemi tasemel) paketifiltriga (ingl *packet filter*).

b. Serveri võrku lisamisel on paketifilter aktiveeritud aluskonfiguratsioonis (kõik ühenduskatsed lükatakse tagasi).

c. Serveri lokaalne paketifilter aktsepteerib andmesideseansse ainult määratud suhtluspartneritega. Mittevajalikud protokollid, pordid ja liidesed on blokeeritud.

d. Protokolli ICMP teateid filtreeritakse valikuliselt, sest ICMP täielik blokeerimine võib kaasa tuua raskesti diagnoositavaid võrguhäireid.

e. Paketifiltri konfiguratsiooni kontrollitakse regulaarselt ja vajadusel korrigeeritakse.

SYS.1.1.M21 Serveri käidudokumentatsiooni koostamine

a. Serveri käitusega seotud toimingud, sooritajad ja toimingu tulemid on arusaadavalt dokumenteeritud serveri käidudokumentatsioonis (ingl *operational documentation*).

b. Kõik konfiguratsioonimuudatused on dokumentatsiooni alusel jälgitavad.

c. Kõik turvalisust puudutavad toimingud on dokumenteeritud.

d. Kõik serveri käitusega seotud toimingud, mida on võimalik dokumenteerida automaatselt, on logitud automaatselt.

SYS.1.1.M22 Integreerimine avariivalmendusega

a. Organisatsiooni talitluspidevuse (ingl *business continuity*) kontseptsioon hõlmab ka serverite varundust ja taastet. (vt DER.4 *Avariihaldus*)

b. Serverite jaoks välja töötatud serverite andmevarunduse kava.

c. Talitluspidevust mõjutavate serveriteenuste taasteks ja taaskäivituseks on dokumenteeritud ja kehtestatud taastekava (ingl *disaster recovery plan*).

d. Taastekava sätestab taasteks vajalike paroolide ja krüptovõtmete turvalise kasutamise ja hoiustamise korra.

e. Taastekava rakendamist harjutatakse regulaarselt.

SYS.1.1.M23 Serverisüsteemi seire

a. Serverisüsteemide olekut, servereid ning neis käitatavaid teenuseid jälgitakse pideva seire vahenditega.

b. Ettenähtud piirnäitajate ületamisest ja tõrgete tekkimisest teavitatakse koheselt serveri haldureid.

SYS.1.1.M24 Regulaarne turbe testimine

a. Võrgurünnete tuvastamiseks ja ärahoidmiseks testitakse välisliideseid omavate serverite turvalisust vähemalt kord kuus.

b. Sisevõrgu serverite vastavust turvapoliitikale kontrollitakse regulaarselt.

c. Turbe testimise käigus kontrollitakse vähemalt järgmist:
   - paroolipoliitika järgimist;
   - pikaajaliselt passiivseid kasutajakontosid;
   - õiguste vastavust kehtestatud süsteemile;
   - süsteemiprogrammide konfiguratsiooni;
   - võrguteenuseid ja nende konfiguratsiooni;
   - automaatseire toimimist.

d. Võimalusel kasutatakse serveri turvakontrollide läbiviimiseks automatiseeritud vahendeid (testitööriistu ja -skripte).

e. Kontrolli tulemused dokumenteeritakse ja lahknevusi käsitletakse esimesel võimalusel.

SYS.1.1.M25 Serveri kasutuselt kõrvaldamise kord

a. Serveri (füüsilise serveri või virtuaalserveri) kasutajaid informeeritakse serveri kõrvaldamisest aegsasti.

b. Serveri kõrvaldamiseks on koostatud toimingute kontroll-loend, mis käsitleb vähemalt andmete varundamist, teenuste üleviimist ja andmete turvalise kustutamisega seotud aspekte.

c. Enne serveri kõrvaldamist on koostatud ülevaade serveril olevatest andmetest ja plaanitud uutest asukohtadest.

d. Enne serveri kasutuselt kõrvaldamist varundatakse olulised andmed.

e. On tagatud, et serveri antavad teenused võtab vajadusel üle teine server. Kõrge käideldavusega serveri migreerimist testitakse eelnevalt testkeskkonnas.

f. Serveri kasutuselt kõrvaldamisel jälgitakse, et andmekandjatele ei jääks alles tundlikke andmeid.

SYS.1.1.M34 Kõvaketta krüpteerimine

a. Serveri andmekandjad (nt kõvakettad) on krüpteeritud usaldusväärsete vahenditega.

b. Virtuaalmasinaid sisaldavad andmekandjad (andmemassiivid või kõvakettad) on krüpteeritud.

c. Krüptovõtmed ja -paroolid on piisavalt tugevad ja kaitstud. Krüptovõtme kaitsmiseks kasutatatakse TPM-ile (*Trusted Platform Module*) lisaks ka muid meetmeid.

d. Kettakrüpto taasteparool on talletatud turvalises asukohas (nt paroolihoidlas).

SYS.1.1.M35 Serveri käidudokumentatsiooni haldus

a. Serveri käidudokumentatsioon on koostatud iga tüüpserveri kohta. Dokumentatsioon sisaldab infoturbe vajadusi ning õigusaktidest tulenevaid nõudeid.

b. Serveri käidudokumentatsioon on kaitstud volitamata juurdepääsu eest. Avariiolukorras on volitatud isikutele tagatud juurdepääs käidudokumentatsioonile.

c. Serveri käidudokumentatsiooni uuendatakse regulaarselt.

SYS.1.1.M36 Serveri buutimise turve

a. Serveri buutimise seadeid saavad muuta ainult haldajad. Juurdepääs püsivara konfigureerimisliidesele on kaitstud vähemalt parooliga.

b. Kasutatakse serveri operatsioonisüsteeme, mis toetavad UEFI SB-d (*Secure Boot*).

c. UEFI *Secureboot* on aktiveeritud. Buutimisel (ingl *booting*) on eellaadur (ingl *bootloader*) ja operatsioonisüsteemi tuum (ingl *kernel*) signeeritud *SecureBoot* tervikluskontrolli võimaldava võtmega.

d. Tarbetud võtmed on serverist eemaldatud.

SYS.1.1.M37 Turvakriitiliste rakenduste ja operatsioonisüsteemi komponentide kapseldamine

a. Rakenduste ja operatsioonisüsteemi turvakriitilised andmed (nt autentimis- ja sertifikaadiandmed) on teiste rakenduste ja operatsioonisüsteemi komponentide juurdepääsu eest kapseldatud (ingl *encapsulation*) või isoleeritud omaette täitmiskeskonda (ingl *execution environment).*

b. Rakendusi, mis töötlevad ebaturvalistest allikatest pärit andmeid (nt veebibrauserid), käitatakse operatsioonisüsteemist lahutatud täitmiskeskkonnas.

SYS.1.1.M39 Serveri turvaseadete keskne haldus

a. Serveri konfiguratsioon talletatakse keskses haldussüsteemis (vt OPS. 1.1.7 *Süsteemihaldus*).

b. Serveri turvaseaded vastavad kehtestatud turvapoliitikatele ja -juhenditele. Erandid dokumenteeritakse koos põhjendusega.

3.4 Kõrgmeetmed

SYS.1.1.M27 Hostipõhine sissetungituvastus (I-A)

a. Anomaaliate ja rünnete tuvastamiseks on kasutusel hostipõhised sissetungituvastuse (ingl *host-based intrusion detection system*, HIDS) ja/või sissetungitõrje (ingl *host-based intrusion prevention system*, HIPS) süsteemid. Kui SIEM (ingl *security information and event management,* SIEM) lahenduses on olemas piisav logiinfo, võib hostipõhiste sissetungituvastussüsteemide asemel kasutada SIEM lahendust.

b. Anomaaliate avastamiseks kontrollitakse regulaarselt (nt igal ööl):

- serverisüsteemi konfiguratsiooni terviklust;
- muudatusi failisüsteemis;
- põhimälus töödeldavate protsesside lubatavust.

c. Kasutatavad sissetungituvastuse/sissetungitõrje mehhanismid on sobivalt konfigureeritud ja põhjalikult testitud.

d. Anomaaliatest teavitamiseks ja anomaaliate käsitlemiseks on kehtestatud kord.
e. Süsteemifailide ja konfiguratsiooniseadete muudatuste tuvastamiseks (nt Windowsi registri failis) kasutatakse täiendavalt serveri operatsioonisüsteemi omi vahendeid.

SYS.1.1.M28 Liiasus (A)

a. Serverisüsteemi kõrgkäideldavus tagatakse liiasuse (ingl *redundancy*) lisamisega.
b. Väliste tarnijate ja teenuseandjatega sõlmitud serverisüsteemide hooldusleping arvestavad kõrgendatud käideldavusnõudeid.
c. Serverisüsteemide liiasus tagatakse ühena järgmistest võimalustest:
   - varuserver külmvaru (ingl *cold standby*);
   - käsitsi ümberlülitamine ehk kuumvaru (ingl *hot standby*);
   - koormust tasakaalustav klaster (ingl *load balancing cluster*);
   - avarii-ümberlülitust võimaldav klaster (ingl *failover cluster*).
d. Liiasust tagava arhitektuuri loomisel arvestatakse selle kuluefektiivsust.
e. Väga suure käideldavustarbe puhul kasutatakse eri füüsilistes asukohtades asuvate serveritega avarii-ümberlülitust võimaldavat klastrit.

SYS.1.1.M30 Üks teenus serveri kohta (C-I-A)

a. Üldreeglina annab iga füüsiline või virtuaalne server kasutada ainult ühe serveriteenuse.
b. Erandjuhtude põhjendus on dokumenteeritud.
c. Virtualiseerimisserveris ei käitata muid teenuseid peale virtualiseerimistarkvara ja sellega vahetult seotud teenuste (virtualiseerimise haldusteenus jne).

SYS.1.1.M31 Rakenduste käitamise tõkestamine (C-I)

a. Serveril on võimalik käitada ainult lubatud programme ja skripte. Lubatud programmide nimekiri on võimalikult piiratud.
b. Lubatud programmide nimekiri põhineb sertifikaadi kontrollil, räside (ingl *hash*) võrdlemisel ja/või lubatud kataloogiteedel.

SYS.1.1.M33 Juursertifikaadi aktiivne haldus (C-I)

a. Serveri tööks vajalike juursertifikaatide loend on dokumenteeritud.
b. Serverisse on paigaldatud ainult need juursertifikaadid, mis on serveri tööks vajalikud ja eelnevalt dokumenteeritud.
c. Juursertifikaatide haldamisel arvestatakse tarkvaratoote allika juhiseid. Juursertifikaatide sobivust kontrollitakse regulaarselt.

SYS.1.1.M38 Serveri süsteemifailide tugevdatud kaitse (I)

a. Tervikluse tagamiseks on juurdepääs serveri süsteemifailidele ainult lugemispääsu (ingl *read-only access*) režiimis.

4 Lisateave

Lühend	Publikatsioon

[NIST]	NIST Special Publication 800-123 „Guide to General Server Security“

SYS.1.2: Windows Server

SYS.1.2.2 Windows Server 2012

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed serveri operatsioonisüsteemide Windows Server 2012 ja Windows Server 2012 R2 turvaliseks rakendamiseks ja serverisüsteemis töödeldavate andmete ning protsesside kaitsmiseks.

1.2 Vastutus

Mooduli „Windows Server 2012“ meetmete täitmise eest vastutab IT-talitus.

1.3 Piirangud

Moodul täiendab moodulit SYS.1.1 *Server üldiselt* Windows Serveri 2012 kohaste erisuste ja täpsustustega. Moodulis esitatud meetmed ei arvesta serverite täpset kasutusotstarvet.

Kui mõeldakse mõlemat versiooni, siis nimetatakse seda Windows Server 2012. Versiooni R2 erinevustele juhitakse tähelepanu eraldi. Mõlema operatsioonisüsteemi tootjapoolse pikendatud toe lõpp (toote ealõpp) on 10. oktoobril 2023.

Moodulis eeldatakse serveri integreerimist *Active Directory*’ga, mille turvalisust käsitletakse moodulis APP.2.2 *Active Directory*.

Microsoft Server 2012-ga seotud serverirolle käsitletakse teistes moodulites (nt APP.3.3 *Failiserver ,*APP.3.2 *Veebiserver,* APP.5.2 *Microsoft Exchange ja Outlook,* SYS.1.5 *Virtualiseerimissüsteem*).

2 Ohud

2.1 Windows Server 2012 rakendamise puudulik kavandamine

Windows Server 2012 on keeruline operatsioonisüsteem, millel on palju funktsioone ja konfigureerimisvalikuid. Iga lisanduva funktsiooniga suureneb nõrkuste ja konfigureerimisvigade tõenäosus. Kuigi Windowsi tänapäevastel versioonide vaikeseaded on muutunud turvalisemaks, sisaldab tüüpkonfiguratsioon endiselt palju turvanõrkusi. Kui Windows Server 2012 aluskonfiguratsiooni ei muudeta turvalisemaks juba enne serveri kasutuselevõttu, on serveri kasutamise ajal turvalisust juurde lisada palju keerulisem ning tihtipeale jäetakse see tegemata. Puudulikult konfigureeritud Windows Server 2012 jätab ründajale palju võimalusi eduka ründe sooritamiseks.

2.2 Pilvteenuste läbimõtlemata kasutamine

Windows Server 2012 kasutab pilvteenuseid (nt *Microsoft Azure Online Backup*) ka ilma spetsiaalse eritarkvarata. Pilvteenused võivad küll anda eeliseid (näiteks käideldavuses), kuid

läbimõtlemata kasutamisel kujutab see endast siiski ohtu konfidentsiaalsusele ja suurendada sõltuvust teenuseandjatest. Andmed võivad pilvteenustest sattuda kuritegelike kavatsustega isikute kätte.

2.3 Windowsi serveri puudulik haldus

Windows Serveri eelnevate versioonidega võrreldes on Windows Server 2012 saanud juurde palju uusi turbefunktsioone. Kui haldurid ei ole saanud Windows Server 2012 turvalise rakendamise väljaõpet, võivad tekkida konfigureerimisvead. Vigu võib tekkida ka konfigureerimisel tehtud inimlike eksimuste tulemusel. Administreerimisvead võivad tekitada tõrkeid serveri funktsioneerimises, muuhulgas ka mõjutada süsteemi turvalisust.

Kui servereid on mitmeid ja ei kasutata ühtset dokumenteeritud konfiguratsiooni, muutub konfiguratsioon serverites ajapikku erinevaks. Mida rohkem tekib sarnaste funktsioonidega süsteemide turvasätetes erinevusi, seda keerukam on tagada turbeprotsessi terviklust ja järjepidevust.

2.4 Rühmapoliitika puudulik rakendamine

Rühmapoliitika (ingl *group policy*) on kasulik ja tõhus abivahend Windows Server 2012 paljude (turva)aspektide konfigureerimisel. Kui domeenis on palju erineva otstarbega servereid ja tööjaamu, võib kergesti juhtuda, et rühmapoliitikaga määratud reeglid osutavad vastukäivateks või ühildumatuteks. See võib põhjustada töötõrkeid, halvimal juhul ka serveri või klientide turvanõrkusi.

2.5 Kaitset vajava teabe või protsessi tervikluse kadumine

Kui Windows Server 2012 tervikluse kaitse funktsioonid pole konfigureerimisvea tõttu või kasutajamugavuse eesmärgil rakendatud, võivad pahatahtlikud töötajad või välised ründajad serveris olevaid andmeid võltsida ning seejärel ka manipuleerimise jäljed kõrvaldada. Kaugjuurdepääsu saamiseks võidakse kasutada vastavat kahjurvara.

2.6 Haldusõiguste lubamatu omandamine või kuritarvitamine

Kui haldur kasutab administraatoriõigustega kontot (eeliskontot) igapäevasteks tegevusteks, on suur oht, et ründajal õnnestub see eeliskonto (ingl *privileged account*) kaaperdada. Eeliskontodele on määratud tavaliselt väga suured õigused, mistõttu võib sellise konto kuritarvitamisel olla suur mõju. Domeenihalduri konto üle võtmisega on võimalik tekitada väga suurt kahju. Konto kasutamiseks vajaliku parooli võib ründaja hankida ka paroole ära arvamata või jõurünnet (ingl *brute-force attack*) kasutamata, kui neil õnnestub ligi pääseda parooliräsile (ingl *password hash*).

2.7 Sissemurdmine kaugjuurdepääsu kaudu

Ebaturvaliste protokollide kasutamisel (kaitsmata RDP) või autentimismeetodi nõrkuste tõttu (nõrgad paroolid) on võimalik saada ründajal serverisse kaugjuurdepääs, mille kaudu on võimalik rünnata serverit ja serveriga seotud teisi süsteeme.

3 Meetmed

3.1 Elutsükkel

Kavandamine

SYS.1.2.2.M1 Windows Server 2012 kasutuselevõtu kava

Evitus

SYS.1.2.2.M2 Windows Server 2012 turvaline installimine

SYS.1.2.2.M4 Windows Server 2012 turvaline konfiguratsioon

SYS.1.2.2.M8 Süsteemi tervikluse kaitse

Käitus

SYS.1.2.2.M3 Windows Server 2012 turvaline haldus

SYS.1.2.2.M5 Kahjurvara tõrje

SYS.1.2.2.M6 Windows Server 2012 turvaline õiguste haldus ja turvaline autentimine

Lisanduvad kõrgmeetmed

SYS.1.2.2.M11 Sissetungituvastus

SYS.1.2.2.M12 Liiasus ja kõrgkäideldavuse vahendid

SYS.1.2.2.M14 Krüpteeritud serveri ja virtuaalmasina turvaline sulgemine

3.2 Põhimeetmed

SYS.1.2.2.M1 Windows Server 2012 kasutuselevõtu kava

a. Serveri operatsioonisüsteemide (sh Windows Server 2012) rakendamiseks on koostatud kasutuselevõtu kava.

b. Windows Server 2012 kasutuselevõtu kava määrab:
   - rakendamise otstarbe;
   - riistvaranõuded;
   - integreerimise *Active Directory*'ga;
   - varundamise korralduse.

c. On otsustatud, kas Windows Server 2012 operatsioonisüsteemiga integreeritud pilvteenused peab enne Windows Server 2012 kasutuselevõttu blokeerima.

SYS.1.2.2.M2 Windows Server 2012 turvaline installimine

a. Installitakse ainult vajalikud serveriga seotud rollid ning rollidega seotud funktsioonid ja täiendid.

b. Piiratud vajaduste puhul installitakse minimaalvariant Server Core. Muude funktsioonide lisamiseks on olemas kirjalik põhjendus.

c. Kohe pärast operatsioonisüsteemi laadimist installikandjalt paigaldatakse ajakohased Windows Server 2012 uuendid ja turbepaigad.

d. Pilvekontode vajaduse puudumisel kasutajate Microsofti pilvekontod blokeeritakse.

SYS.1.2.2.M3 Windows Server 2012 turvaline haldus

a. Lokaalse halduskonto (ingl *administrator account*) parool on kordumatu ja turvaline.

b. Serverisüsteemi haldurid on kursis serveri turbe aspektidega ning on läbinud Windows Server 2012 või R2 koolituse.

c. Süsteemihaldurite koolitus hõlmab järgmisi teemasid:
   - ressurssidele juurdepääsu reguleerimine ja kontroll;

- *Active Directory* sertifikaaditeenuste haldus;
- serveri protsesside ja soorituse analüüs ja haldus;
- kasutajakontode haldus;
- krüptograafiavahendite haldus;
- failide üleviimine ja kustutus;
- serveri poliitikate analüüs ja haldus;
- süsteemide turvalisuse diagnostika, kavandamine ja tagamine.

d. Serveris olevaid brausereid surfamiseks (eriti Internetis) ei kasutata.

3.3 Standardmeetmed

SYS.1.2.2.M4 Windows Server 2012 turvaline konfiguratsioon

a. Iga server täidab üldjuhul vaid üht funktsiooni või serverirolli. Rollid on sobivalt jaotatud eri serverite vahel.

b. Enne käidukeskkonda lisamist on server põhjalikult tugevdatud (ingl *hardening*). Selleks kasutatakse süsteemispetsiifilisi turvaparameetrite seadistusmalle.

c. Internet Explorerit kasutatakse serveris ainult sätetega ESC (ingl *Enhanced Security Configuration, ESC*) ja EPM (ingl *Enhanced Protected Mode*, EPM).

SYS.1.2.2.M5 Kahjurvara tõrje

a. Kahjurvaratõrje rakendus on serverisse paigaldatud enne esimese võrguühenduse loomist. Kuni kavandatud kahjurvaratõrje lahenduse rakendamiseni on serveris aktiveeritud Windows Defender.

b. Erandina võib kahjurvaratõrje programm puududa autonoomsetest Windows Server 2012 serveritest, millel puudub võrguühendus ja kus ei kasutata irdkandjaid.

c. Serveri töökettaid skaneeritakse kahjurvara leidmiseks regulaarselt.

d. Kahjurvara avastamisest teavitab kahjurvaratõrje rakendus määratud isikuid automaatselt.

SYS.1.2.2.M6 Windows Server 2012 turvaline õiguste haldus ja turvaline autentimine

a. Windows Server 2012 R2 kõik kasutajad kuuluvad turvarühma „*Protected Users*“ (PU).

b. Windows Server 2012 teenusekontod kuuluvad hallatud teenusekontode rühma „*Managed Service Accounts*“ (MSA). Teenuse- ja arvutikontod ei kuulu rühma „*Protected Users*“.

c. Lokaalse turvakeskuse LSA (*Local Security Authority*, LSA) PPL-kaitse on aktiveeritud.

d. Ressursside pääsureeglite dünaamiliseks halduseks kasutatakse DAC-d (*Dynamic Access Control*, DAC).

e. Windows Server 2012 haldustöödeks kasutatakse piiratud õigustega tööjaama.

SYS.1.2.2.M8 Süsteemi tervikluse kaitse

a. Rakenduste kasutuse reguleerimiseks on aktiveeritud *AppLocker*, mis on konfigureeritud võimalikult piiravate reeglitega. *AppLocker'*i toe puudumisel kasutatakse SRP-d (*Software Restriction Policies*, SRP).

b. Rakenduste kasutuse reguleerimine on jõustatud rühmapoliitikaobjektide (*Group Policy Object*, GPO) kaudu.

3.4 Kõrgmeetmed

SYS.1.2.2.M11 Sissetungituvastus (C-I-A)

a. Operatsioonisüsteemi Windows Server 2012 instantsi turvasündmusi kogutakse ja analüüsitakse keskselt.

b. Windows Server 2012 operatsioonisüsteemiga serverite puhul logitakse ja analüüsitakse vähemalt:
   - turvalogide kustutused;
   - haldurite ja muude oluliste kasutajarühmade muudatused;
   - serveri lokaalsete kasutajate lisamine ja eemaldamine;
   - uute teenuste lisamine.

c. Krüpteeritud sektsioonid lukustatakse pärast kindlaksmääratud arvu dekrüpteerimiskatseid.

SYS.1.2.2.M12 Liiasus ja kõrgkäideldavuse vahendid (A)

a. Sõltuvalt kaitsetarbest on rakendatud järgmisi operatsioonisüsteemi poolt toetatud kõrgkäideldavuse meetmeid:
   - DFS (*Distributed File System*, DFS);
   - ReFS (*Resilient File system*, ReFS);
   - avarii-ümberlülitust võimaldava klastri (ingl *failover cluster*) kasutamine;
   - koormuse tasakaalustamine (ingl *load balancing*);
   - võrgukaartide rühmad (*NIC-Teaming*, LBFO).

b. Kaugasukohtades on aktiveeritud lisafunktsionaalsus *BranchCache*.

SYS.1.2.2.M14 Krüpteeritud serveri ja virtuaalmasina turvaline sulgemine (C-I)

a. Füüsilised või virtuaalserverid, mida hetkel ei kasutata, on suletud. Serveri puhkeolek (ingl *hibernate mode*) ei pruugi tagada piisava kaitse.

b. Serveri käivitamiseks (ning andmete dekrüpteerimiseks) on vajalik halduri paroolisisestus, toiming registreeritakse turvalogis.

SYS.1.2.3 Windows Server

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed Microsoft Windows 10 koodil põhinevate serveri operatsioonisüsteemide Windows Server 2016, Windows Server 2019 ja Windows Server 2022 (edaspidi Windows Server) turvaliseks rakendamiseks ja serverisüsteemis töödeldavate andmete ning protsesside kaitsmiseks.

1.2 Vastutus

Mooduli „Windows Server“ meetmete täitmise eest vastutab IT-talitus.

1.3 Piirangud

Käesolev moodul täiendab moodulit SYS.1.1 *Server üldiselt* Windows Server 2016, Windows Server 2019 ja Windows Server 2022 kohaste erisuste ja täpsustustega.

Moodulis esitatud meetmed ei arvesta serverite täpset kasutusotstarvet. Sõltuvalt serveri rollist käsitletakse vajalikke meetmeid teistes moodulites (nt APP.3.2 *Veebiserver*, APP.3.3 *Failiserver,* SYS.1.5 *Virtualiseerimissüsteem*).

Moodulis eeldatakse serveri integreerimist *Active Directory*'ga, mille turvalisust käsitletakse moodulis APP.2.2 *Active Directory*.

Serveri operatsioonisüsteemiga integreeritud pilvteenuste osas (nt liidestus Microsoft Azure'i pilveplatvormiga) rakendatakse moodulit OPS.2.2 *Pilvteenuste kasutamine*.

2 Ohud

2.1 Pilvteenuste läbimõtlemata kasutamine

Windows Server kasutab pilvteenuseid (nt *Microsoft Azure Online Backup* või BitLockeri taastevõtmete salvestamine) ka ilma spetsiaalse eritarkvarata. Pilvteenused võivad küll anda eeliseid (näiteks käideldavuses), kuid läbimõtlemata kasutamisel kujutab see endast siiski ohtu konfidentsiaalsusele ja suurendada sõltuvust teenuseandjatest. Andmed võivad pilvteenustest sattuda kuritegelike kavatsustega isikute kätte.

2.2 Sissemurdmine kaugjuurdepääsu kaudu

Ebaturvaliste protokollide kasutamisel (nt kaitsmata RDP või WinRM) või autentimismeetodi nõrkuste tõttu (nõrgad paroolid) on ründajal võimalik saada serverisse kaugjuurdepääs, mille kaudu rünnata serverit ja serveriga seotud süsteeme.

2.3 Telemeetriaandmete kontrollimatu levitamine

Vaikeseadistuses väljastab Windows Server Microsoftile nn diagnostikaandmeid. Tootjal on võimalik lisaks saada andmeid operatsioonisüsteemi integreeritud telemeetriateenusest, saades nii juurdepääsu veaolukorras salvestatud mälutõmmistele (ingl *crash dump*) ja serveri logiandmetele. Potentsiaalselt tundlik teave võib sattuda volitamata isikute valdusesse.

2.4 IT-kriminalistika nõrgestamine VSM (Virtual Secure Mode) kasutamisel

VSM kasutamisel piiratakse kasutatavaid IT-kriminalistika (ingl *computer forensics*) meetodeid. IT-intsidendi toimumisel pole võimalik analüüsida protsesse ja mälutõmmiseid, mis on kaitstud Secure Kernel või Isolated user Mode (IUM) vahenditega.

3 Meetmed

3.1 Elutsükkel

Kavandamine

SYS.1.2.3.M1 Windows Serveri kasutuselevõtu kavandamine

Evitus

SYS.1.2.3.M2 Windows Serveri turvaline installimine

Käitus

SYS.1.2.3.M3 Telemeetria- ja diagnostikaandmete levitamise piiramine

SYS.1.2.3.M4 Turvanõrkuste ärakasutamise tõkestamine

SYS.1.2.3.M5 Turvaline õiguste haldus Windows Serveris

SYS.1.2.3.M6 Turvaline RDP kaugjuurdepääs

Lisanduvad kõrgmeetmed

SYS.1.2.3.M7 Windows PowerShelli turvaline kasutamine

SYS.1.2.3.M8 VSM (Virtual Secure Mode) kasutamine

3.2 Põhimeetmed

SYS.1.2.3.M1 Windows Serveri kasutuselevõtu kavandamine

a. Kasutusele võetav Windows Serveri väljalase on valitud põhjendatud ja dokumenteeritud valikukriteeriumite alusel.

b. On määratletud, kuidas uus server integreeritakse *Active Directory'*ga.

c. Iga operatsioonisüsteemiga integreeritud pilvteenuse puhul on otsustatud, kas see blokeeritakse enne kasutuselevõttu või mitte. või kuidas toimub pilvteenuse kasutuselevõtuks seadistamine.

d. Kui ei ole nõutav teisiti, on Microsofti kontode lisamine Windows Serveris blokeeritud.

SYS.1.2.3.M2 Windows Serveri turvaline installimine

a. Kui olemasolevast funktsionaalsusest piisab, installitakse minimaalvariant Server Core. Muude funktsioonide lisamiseks on olemas kirjalik põhjendus.

SYS.1.2.3.M3 Telemeetria- ja diagnostikaandmete levitamise piiramine

a. Microsoftile edastavate diagnostika- ja kasutusandmete piiramiseks on Windows Serveri telemeetria tase (parameeter *AllowTelemetry*) seadistatud valikväärtusele 0 (*Security*).

b. Kui serveri telemeetriaseadistusi ei ole võimalik piirata, takistatakse andmete tootjale edastamist muude meetmetega, nt andmeliikluse piiramisega võrgutasemel.

3.3 Standardmeetmed

SYS.1.2.3.M4 Turvanõrkuste ärakasutamise tõkestamine

a. Windows Serverile ja serveriteenustele on rakendatud meetmed teadaolevate turvanõrkuste ärakasutamise tõkestamiseks (vt ptk 4 Kasulik teave).

SYS.1.2.3.M5 Turvaline õiguste haldus Windows Serveris

a. Windows Serveri kõik kasutajad kuuluvad turvarühma „*Protected Users*“ (PU).

b. Windows Serveri teenusekontod kuuluvad hallatud teenusekontode rühma „*Managed Service Accounts*“ (MSA). Teenuse- ja arvutikontod ei kuulu rühma „*Protected Users*“.

SYS.1.2.3.M6 Turvaline RDP kaugjuurdepääs

a. Kaugjuurdepääsu kavandamisel on arvestatud lokaalse tulemüüri seadistusi.

b. RDP (Remote Desktop Protocol) kasutajate (sh vajalikud teenusekontod) rühma kuuluvad ainult volitatud kasutajad.

c. Kaugjuurdepääsu mandaatide (ingl *credential*) kaitseks ühenduse loomisel on kaalutud operatsioonisüsteemisiseste mehhanismide (nt *Remote Credential Guard* või *RestrictedAdmin*) kasutuselevõttu.

d. Kõrgendatud turvanõuetega võrgutaristus on RDP sihtsüsteem juurdepääsetav ainult RDP lüüsi (ingl *RDP Gateway*) vahendusel.

e. RDP kasutamisel järgitakse, et allpool loetletud mugavusfunktsioonid on kooskõlas sihtsüsteemi turvanõuetega:

- lõikepuhvri (ingl *clipboard*) kasutamine;
- irdandmekandjate ja võrguketaste kättesaadavaks tegemine;
- sisemise failisalvestusruumi ja serveri muude ressursside (nt kiipkaardilugeja) kasutamine;

f. Kaugjuurdepääsu loomisel kasutatavad krüptoprotokollid ja -algoritmid on kooskõlas organisatsiooni krüptokontseptsiooniga.

g. Kui kaugjuurdepääsu kasutamist antud ajavahemikus pole plaanitud, on kaugjuurdepääsu võimalus täielikult välja lülitatud.

3.4 Kõrgmeetmed

SYS.1.2.3.M7 Windows PowerShelli turvaline kasutamine (C-I-A)

a. PowerShell'is käivitatud käskude täitmine logitakse keskselt, tekkinud logisid analüüsitakse.

b. Signeerimata skriptide käivitamise takistamiseks piiratakse PowerShelli skriptide täitmist käsuga *Set-ExecutionPolicy AllSigned.*

c. Windows PowerShell'i vanemate versioonide kasutamine on blokeeritud.

d. Powershell'is kasutatavad käsud on piiratud seadega „Constrained Language Mode".

e. Windows Serveri PowerShelli kasutajate halduseks kasutatakse tööriista Just Enough Administration (JEA).

SYS.1.2.3.M8 VSM (Virtual Secure Mode) kasutamine (C-A)

a. Serveris töödeldavate andmete kaitseks on serveris aktiveeritud VSM.

b. On arvestatud asjaoluga, et VSM kasutamine piirab IT-kriminalistika läbiviimist.

4 Lisateave

Lühend	**Publikatsioon**
[MS1]	Microsoft, Windows Server Security documentation https://docs.microsoft.com/en-us/windows-server/security/security-and-assurance
[MS2]	Microsoft, Microsoft Security Compliance Toolkit 1.0 https://docs.microsoft.com/en-us/windows/security/threat-protection/security-compliance-toolkit-10

SYS.1.3 Linuxi ja Unixi server

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed Linuxi (nt *Debian, Red Hat Enterprise Linux/CentOS, SUSE Linux Enterprise/openSUSE*) või Unixi (nt *OpenBSD, Solaris,* AIX) operatsioonisüsteeme kasutavate serverite ja neis töödeldavate andmete käideldavuse, tervikluse ja konfidentsiaalsuse tagamiseks.

Meetmed kirjeldavad operatsioonisüsteemi konfigureerimist ja käitust, sõltumata serveri spetsiifilisest kasutusotstarbest. Moodul täpsustab ja täiendab Linuxi või Unixi süsteemide erisusi aspektides, mis on käsitletud moodulis SYS.1.1 *Server üldiselt*.

1.2 Vastutus

Linuxi ja Unixi serveri meetmete täitmise eest vastutab IT-talitus.

1.3 Piirangud

Moodulis ei käsitleta erinevate serveriga seotud rollide erinõudeid (nt veebiserver on kirjeldatud moodulis APP.3.2 *Veebiserver* ja rühmatarkvara moodulis APP.5.3 *E-posti server ja klient üldiselt*).

Virtualiseeritud serverite turvameetmeid käsitletakse moodulis SYS.1.5 *Virtualiseerimissüsteem*.

2 Ohud

2.1 Süsteemi- ja kasutajateabe luure

Unixis on mitmeid programme, mis võimaldavad pärida andmeid, mida IT-süsteem kasutajate kohta salvestab. Sellised andmed on kasutajate tegevusprofiilid, teave sisselogitud kasutajate kohta, samuti tehniline teave operatsioonisüsteemi installi ja konfigureerimise kohta.

Lihtsa programmiga, mis analüüsib käsu „*who“* andmeid mingi ajavahemiku jooksul, on võimalik koostada kasutaja kasutusprofiil, kindlaks teha süsteemihaldurite äraolekuajad ja kasutada hiljem neid aegu lubamatuteks toiminguteks. Samuti on võimalik kindlaks teha, millistel tööjaamadel on serverisse eelispääsuõigus. Sarnased andmete kuritarvitamise võimalusega programmid on ka *finger* ja *ruser*.

2.2 Skriptikeskkonna ärakasutamine

Unixi operatsioonisüsteemides kasutatakse halduri tegevuste lihtsustamiseks ja inimlike vigade vältimiseks skriptikeeles kirjutatud ja käsurealt aktiveeritavaid skripte. Ründaja võib skripte oma eesmärkide saavutamiseks manipuleerida ja ära kasutada.

2.3 Teekide dünaamiline laadimine

Muutuja „LD_PRELOAD“ abil laaditakse osutatud dünaamiline teek (*dynamically linked shared object library*) enne muid tüüpteeke, mida rakenduses vajatakse. See võimaldab tüüpteekide konkreetseid funktsioone enda omadega üle kirjutada. Ründaja võib näiteks

operatsioonisüsteemi manipuleerida nii, et teatud rakenduste käivitamisel aktiveeritakse kahjurprogramm.

2.4 Valideerimata allikatest pärit tarkvara

Unixi-laadsetes operatsioonisüsteemides laevad kasutajad valmisrakenduste installimise asemel paketid ise alla ja programm kompileeritakse lokaalselt. Tarkvarapaketid laaditakse sageli alla valideerimata allikatest. Kui ei kasutata tootja usaldusväärset paketivaramut, esineb oht, et tahtmatult laaditakse alla ja installitakse vale või ühildumatu tarkvarapakett või kahjurfunktsioone sisaldav tarkvara.

3 Meetmed

3.1 Elutsükkel

Evitus

SYS.1.3.M2 Korrektne identifikaatorite määramine

SYS.1.3.M3 Irdmäluseadmete automaatse failisüsteemiga sidumise vältimine

SYS.1.3.M4 Rakenduste kaitsmine

Käitus

SYS.1.3.M5 Tarkvarapakettide turvaline installimine

SYS.1.3.M6 Kasutajate ja rühmade haldus

SYS.1.3.M8 SSH-ga krüpteeritud andmevahetus

SYS.1.3.M10 Volitamata õiguste laiendamise takistamine

Lisanduvad kõrgmeetmed

SYS.1.3.M14 Süsteemi- ja kasutajateabe luure takistamine

SYS.1.3.M16 Volitamata õiguste laiendamise täiendav takistamine

SYS.1.3.M17 Tuuma lisaturve

3.2 Põhimeetmed

SYS.1.3.M2 Korrektne identifikaatorite määramine

a. Ükski kasutajanimi, kasutajaidentifikaator (ingl *User Identifier*, UID) ega rühmaidentifikaator (ingl *Group Identifier*, GID) ei kordu. Identifikaatorite korraldus kehtib üle kõigi organisatsiooni serverite.

b. Iga kasutaja kuulub vähemalt ühte rühma.

c. Kõik failis "*/etc/passwd*" esinevad rühmaidentifikaatorid on defineeritud failis "/*etc/group*".

d. Iga rühm sisaldab ainult vajalikke kasutajaid.

e. Kasutaja- ja rühmanimede ning kasutaja- ja rühmaidentifikaatorite määramise süsteem on ühtne üle kõigi organisatsiooni serverite.

SYS.1.3.M3 Irdmäluseadmete automaatse failisüsteemiga sidumise vältimine

a. Irdmäluseadmeid ja irdkandjaid (nt mälupulki või CD/DVD-plaate) ei saa külgeühendamisel automaatselt failisüsteemiga siduda (ingl *mount*).

SYS.1.3.M4 Rakenduste kaitsmine

a. Rakenduse nõrkuste ärakasutamise keerukamaks muutmiseks kasutavad rakendused tuumas (ingl *kernel*) aktiveeritud mehhanisme ASLR ja DEP/NX.

b. Tuuma ja tüüpteekide turvafunktsioonid on aktiveeritud.

SYS.1.3.M5 Tarkvarapakettide turvaline installimine

a. Enne installimist kontrollitakse installitavate tarkvarapakettide terviklust ja autentsust.

b. Tarkvara kompileerimisel lähtekoodist toimub selle lahtipakkimine, konfigureerimine ja kompileerimine priviligeerimata kontoõigustes.

c. Tarkvara lähtekoodist kompileerimisel dokumenteeritakse kõik tehtud valikud selliselt, et kompileerimist oleks võimalik samade parameetritega korrata.

d. Tarkvara ei installita serveri juurfailisüsteemi.

e. Kõik installimissammud on dokumenteeritud nii, et konfiguratsiooni saaks vajadusel kiiresti taastada.

3.3 Standardmeetmed

SYS.1.3.M6 Kasutajate ja rühmade haldus

a. Kasutajate ja rühmade halduseks kasutatakse sobivaid haldusinstrumente.

b. Konfiguratsioonifaile „*/etc/passwd*“, „*/etc/shadow*“, „*/etc/group*” ja „*/etc/sudoers*” ei redigeerita tüüpse tekstiredaktoriga.

SYS.1.3.M8 SSH-ga krüpteeritud andmevahetus

a. Andmevahetus on krüpteeritud SSH (*Secure Shell*) protokolliga.

b. Kõik ebaturvalised andmevahetusprotokollid on desaktiveeritud.

c. Autentimiseks eelistatakse kasutaja parooli asemel kasutaja sertifikaati.

SYS.1.3.M10 Volitamata õiguste laiendamise takistamine

a. Teenuseid ja rakendusi kaitstakse tuuma turvamooduliga (näiteks AppArmor või SELinux).

b. Arvesse on võetud ka *chroot*-keskkonnad ning LXC- või Docker-konteinerid.

c. Kõik õiguste tüüpprofiilid ja -reeglid on aktiveeritud.

3.4 Kõrgmeetmed

SYS.1.3.M14 Süsteemi- ja kasutajateabe luure takistamine (C)

a. Teabe väljastus operatsioonisüsteemi kohta ning juurdepääs logi- ja konfiguratsioonifailidele on rangelt vajaduspõhised.

b. Käsu parameetritena (käsurealt või skriptifailist) ei esitata tundlikke andmeid. Sellised parameetrid sisestatakse halduri poolt interaktiivselt.

SYS.1.3.M16 Volitamata õiguste laiendamise täiendav takistamine (C-I)

a. Süsteemikutsed on vajaduspõhiselt piiratud.

b. Tüüpprofiile ja -reegleid (sh *AppArmor* või *SELinux*) kontrollitakse turvapoliitika põhiselt.

c. Vajadusel olemasolevaid reegleid kohandatakse või luuakse uusi reegleid või profiile.

SYS.1.3.M17 Tuuma lisaturve (C-I)

a. Operatsioonisüsteemi tuuma (ingl *kernel*) on tugevdatud (nt grsecurity, PaX) ning täiendatud rollipõhise pääsu reguleerimisega, failisüsteemi turbe ja muude turvamehhanismidega.

SYS.1.5 Virtualiseerimissüsteem

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed virtualiseerimiskeskkonna ja virtuaalserverite (edaspidi mõlemad koos nimetatud ka kui virtualiseerimissüsteem) turbe tagamiseks.

Virtualiseerimistaristu koosneb virtualiseerimisserveritest (ingl *host*), millel siis otse riistvaraliselt või hosti operatsioonisüsteemi vahendusel on realiseeritud virtualiseerimiskeskkond. Virtualiseerimiskeskkonna hüperviisor (ingl *hypervisor*) võimaldab luua külalissüsteeme (ingl *guest*), virtuaalservereid, millel omakorda paiknevad kasutajatele juurdepääsetavad IT-süsteemid.

1.2 Vastutus

Virtualiseerimissüsteemi moodulis esitatud turvameetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Arhitekt.

1.3 Piirangud

Lisaks käesolevale etalonturbe moodulile rakendatakse virtuaalserverite puhul operatsioonisüsteemi põhiseid serveri- või kliendimooduleid ning mooduleid SYS.1.1 *Server üldiselt* ja SYS.2.1 *Klientarvuti üldiselt*.

Selles moodulis käsitletakse serveripõhist virtualiseerimist. Moodul ei käsitle virtualiseerimise osalist kasutamist (nt rakenduste virtualiseerimine terminaliserveritega, konteinerid, Java virtuaalmasin).

Virtualiseerimiskeskkonnaga on liidestatud enamasti ka salvestusvõrgud (NAS või SAN). Salvestilahenduste turve esitatakse moodulis SYS.1.8 *Salvestilahendused*.

Virtualiseerimisest tulenevad täiendavad nõuded ka võrgu ülesehitusele, mida käsitletakse moodulis NET.1.1 *Võrgu arhitektuur ja lahendus*.

2 Ohud

2.1 Vead virtualiseerimise kavandamisel

Virtualiseerimissüsteemi tehnilise ja korraldusliku kavandamise puudumine võib põhjustada vigu virtualiseerimiskeskkonna seadistamisel. Pärast virtuaalserverite kasutuselevõttu käidukeskkonnas on paigaldamise ajal tehtud vigu keeruline parandada.

Kui vastutusalad on selgelt määratlemata (näiteks rakenduste, operatsioonisüsteemide ja võrgukomponentide eest vastutus), siis võivad olulised kooskõlastused või toimingud jääda tegemata. Samuti võidakse kasutajatele anda liiga laialdased pääsuõigused.

2.2 Virtualiseerimise konfigureerimisvead

Virtuaalsed ressursid nagu protsessorid, RAM, võrguühendused ja mälu konfigureeritakse virtualiseerimiskeskkonnas hüperviisori (ingl *hypervisor*) kaudu ning need ei sõltu enam täielikult riistvarast. Vead virtuaalserveri ressursside määramisel võivad hiljem põhjustada vigu serveris seadistatud külalissüsteemide (ingl *guest*) töös. Kui tehakse viga virtuaalserverite segmentimisel, nt kui suure kaitsetarbega virtuaalne IT-süsteem paigutatakse samasse segmenti klientidega või välisesse demilitaartsooni, võivad sealt andmed lekkida.

2.3 Ressursside piisamatus virtuaalse IT-süsteemi tarbeks

Virtualiseerimisüsteemi toimimiseks vajab virtuaalserver mäluruumi ja ohtralt salvestusruumi kas siis lokaalses virtualiseerimisserveris endas või sellega ühendatud salvestivõrgus. Kui selleks vajalikke mälu- ja kettamahte ei kavandata kohe alguses piisava varuga, siis tähendab see peagi ohtu virtuaalsete IT-süsteemide käideldavusele ja neis töödeldavate andmete terviklusele. Eriti oluline on arvestada piisava ruumiga hetktõmmiste (ingl *snapshot*) tegemiseks. Ressursinappus võib avalduda ka ebapiisava läbilaskevõimega võrguühenduse puhul. Virtualiseerimisserveri puudulikud ressursid häirivad ka virtuaalmasinate omavahelist koostööd.

2.4 Hetktõmmisega seonduv andmeleke või ressursipuudus

Hetktõmmiseid kasutatakse muuhulgas virtuaalserverite varundamiseks. Kui hetktõmmis hiljem vajadusel aktiveeritakse (taastatakse), siis lähevad kõik tõmmise tegemise järel IT-süsteemis tehtud muudatused kaotsi. Kui hetktõmmis on liiga vana, siis muutub server haavatavaks, sest korra juba paigatud turvanõrkused avalduvad nüüd uuesti. Hetktõmmise tegemise ajal pooleli olevad seansid ja transaktsioonid võivad virtuaalserveri hetketõmmiselt taastamise järgselt tekitada konflikti teiste serveritega.

Ründajal on võimalik hetktõmmiseid kuritarvitada virtuaalse IT-süsteemi andmetele lubamatu juurdepääsu saamiseks. Töö käigus tehtud hetktõmmis sisaldab ka põhimälu sisu, mida on väljaspool algset IT-taristut loodud virtualiseerimiskeskkonnas võimalik analüüsimiseks taastada.

Kui hetktõmmised muutuvad väga suureks, võib vajalik kettamaht serveris jääda liiga väikeseks.

2.5 Virtualiseerimissüsteemi haldusserveri tõrge

Virtualiseerimissüsteemi funktsioone juhitakse ja hallatakse haldusserveri kaudu. Haldusserveri tõrge tähendab seda, et virtualiseerimissüsteemi ei saa enam juhtida, serverite konfiguratsiooni muuta ja virtuaalserverite tõrgetele adekvaatselt reageerida.

2.6 Valideerimata rakenduste väärkasutamine

Sageli on virtualiseeritud keskkonna haldusvahendite kasutajatele antud suuremad pääsuõigused kui tema halduses olevate virtuaalmasinate haldamiseks vajalik. See tekitab ohu, et pääsuõigusi kuritarvitatakse teenusetõkestusrünnete läbiviimiseks või virtualiseerimisserveri ülevõtmiseks.

2.7 Virtualiseerimisserveri turvarike

Virtualiseerimisserveri hüperviisor kontrollib ja juhib virtualiseerimissüsteemis loodud virtuaalservereid ja jaotab neile protsessori- ja salvestiressursse. Edukas rünne selle

komponendi vastu võib viia kõikide guest-serverite ja nendel olevate virtuaalsete IT-süsteemide lubamatu modifitseerimise või kaotamiseni.

3 Meetmed

3.1 Elutsükkel

Kavandamine

SYS.1.5.M8 Virtualiseerimissüsteemi kavandamine

SYS.1.5.M9 Virtualiseerimissüsteemi võrguarhitektuuri kavandamine

SYS.1.5.M10 Virtualiseerimissüsteemi halduse eeskiri

SYS.1.5.M14 Virtualiseerimistaristu ühtsed konfiguratsiooninõuded

Soetamine

SYS.1.5.M13 Virtualiseerimissüsteemi jaoks sobiv riistvara

Evitus

SYS.1.5.M4 Virtualiseerimistaristu turvaline võrgukonfiguratsioon

SYS.1.5.M5 Virtualiseerimiskeskkonna haldusliideste turve

SYS.1.5.M12 Virtualiseerimistaristu halduse õigused ja rollid

SYS.1.5.M16 Virtuaalmasinate isoleerimine

Käitus

SYS.1.5.M2 Virtualiseerimissüsteemi turvaline rakendamine

SYS.1.5.M3 Virtualiseerimiskeskkonna turvaline konfiguratsioon

SYS.1.5.M6 Virtualiseerimissüsteemi logimine

SYS.1.5.M7 Aja sünkroonimine virtualiseerimissüsteemis

SYS.1.5.M11 Virtualiseerimissüsteemi haldusvõrk

SYS.1.5.M15 Erineva kaitsetarbega külalissüsteemide lahusus

SYS.1.5.M17 Virtualiseerimisserveri konfiguratsiooni kontrollimine ja seire

SYS.1.5.M19 Virtualiseerimissüsteemi regulaarsed läbivaatused

Lisanduvad kõrgmeetmed

SYS.1.5.M20 Kõrgkäideldav arhitektuur

SYS.1.5.M21 Külalissüsteemide turvaline konfigureerimine

SYS.1.5.M22 Virtualiseerimisserveri tugevdamine

SYS.1.5.M23 Virtuaalserveri õiguste piiramine

SYS.1.5.M24 Virtuaalserveri hetktõmmise desaktiveerimine

SYS.1.5.M25 Virtuaalserveri konsoolpääsu minimaalne kasutamine

SYS.1.5.M26 Avaliku võtme taristu kasutamine

SYS.1.5.M27 Sertifitseeritud virtualiseerimistarkvara

SYS.1.5.M28 Virtuaalsete IT-süsteemide krüpteerimine

3.2 Põhimeetmed

SYS.1.5.M2 Virtualiseerimissüsteemi turvaline rakendamine

a. Kõik virtualiseerimissüsteemi haldurid teavad, kuidas virtualiseerimine mõjutab käitatavaid IT-süsteeme ja rakendusi.

b. Virtualiseerimissüsteemi haldurite pääsuõigused on vajadusepõhiselt piiratud.

c. Enne virtualiseerimissüsteemi rakendamist on kontrollitud, kas:

- virtualiseerimistaristu host-serveril on virtualiseerimissüsteemi jaoks piisavad andmesideühendused;
- virtualiseerimiskeskkonnas käitatavate rakenduste eraldamise ja kapseldamise nõuded on täidetud;
- virtualiseerimissüsteem vastab käideldavuse ja andmeedastusjõudluse nõuetele.

d. Pidevalt seiratakse virtualiseerimissüsteemi sooritusvõimet.

SYS.1.5.M3 Virtualiseerimiskeskkonna turvaline konfiguratsioon

a. Virtualiseerimisserverile e. hostsüsteemile (ingl *host*) juurdepääs külalissüsteemidest (ingl *guest*) on piiratud. Külalissüsteemidest puudub juurdepääsu hosti komponentidele ja liidestele. Vajadusel võib hostsüsteemi haldaja erandina anda ajutise külalispääsu õiguse.

b. Virtuaalsete külalissüsteemide ja nendes asuvate IT-süsteemide konfiguratsioon ja turve vastab organisatsiooni turvapoliitikale.

SYS.1.5.M4 Virtualiseerimistaristu turvaline võrgukonfiguratsioon

a. Virtuaalserverite andmeside läbib virtualiseerimissüsteemi võrguühenduste turvamehhanisme (nt tulemüürid) ja seiresüsteeme.

b. Mitme võrguliidesega külalissüsteemist ei saa luua lubamatuid võrguühendusi.

c. Virtuaalsete ja riistvaraliste IT-süsteemide andmesideliidesed vastavad organisatsiooni turvapoliitikale.

SYS.1.5.M5 Virtualiseerimiskeskkonna haldusliideste turve

a. Halduspääs haldussüsteemi ja hostsüsteemidesse on piiratud.

b. Haldusliidestele puudub juurdepääs ebausaldatavatest võrkudest.

c. Virtualiseerimisserveri ja haldussüsteemi seireks ja haldusjuurdepääsuks kasutatakse turvalisi protokolle. Ebaturvaliste protokollide puhul kasutatakse halduseks eraldi haldusvõrku.

SYS.1.5.M6 Virtualiseerimissüsteemi logimine

a. Pidevalt logitakse virtualiseerimissüsteemi olekut, koormust ja võrguühendusi.

b. Kui virtuaalserveri ressursid hakkavad ammenduma, suurendatakse kasutada antud ressursse või paigutatakse virtuaalserver ümber ja täiendatakse virtualiseerimisserveri riistvara.

c. Virtuaalserverite logiandmeid analüüsitakse regulaarselt.

SYS.1.5.M7 Aja sünkroonimine virtualiseerimissüsteemis

a. Kõigi kasutusel IT-süsteemide süsteemiajad on alati sünkroonsed.

3.3 Standardmeetmed

SYS.1.5.M8 Virtualiseerimissüsteemi kavandamine [arhitekt]

a. Virtualiseerimissüsteemi arhitektuur on kavandatud detailselt.

b. Virtualiseerimissüsteemi kavandamisel on arvestatud IT-süsteemide, rakenduste, võrkude (sh salvestusvõrkude) kohta kehtivaid poliitikaid ja eeskirju.

c. Kui virtualiseerimisserveril (ingl *host*) on rohkem kui üks külalissüsteem (ingl *guest*), on nende turve kooskõlas.

d. Haldustegevustega on kaetud kõik virtualiseerimissüsteemi komponendid. Haldusrühmade ülesanded on määratletud ega kattu.

SYS.1.5.M9 Virtualiseerimissüsteemi võrguarhitektuuri kavandamine [arhitekt]

a. Virtualiseerimissüsteemi võrguarhitektuur on kavandatud detailselt.

b. On määratletud loodavad võrgusegmendid (nt haldusvõrk, salvestusvõrk) ning protsessid, kuidas võrgusegmente eraldatakse ja turvatakse.

c. Haldusvõrk on töövõrgust eraldatud (vt moodulit SYS.1.5.M11 *Virtualiseerimissüsteemi haldusvõrk*). Vajadusel on loodud eraldatud võrgusegment ka teatud virtualiseerimisfunktsioonide (nt sidus (ingl *on-line*) migreerimise) tarbeks.

d. Võrguarhitektuur tagab virtualiseeritud IT-süsteemide nõutava käideldavuse.

SYS.1.5.M10 Virtualiseerimissüsteemi halduse eeskiri

a. On kehtestatud ja dokumenteeritud protseduurid virtuaalserverite ja virtualiseeritud IT-süsteemide kasutuselevõtuks, arvestuseks, käitamiseks ja kasutuselt kõrvaldamiseks.

b. Virtualiseerimissüsteemi halduse eeskirja ajakohastatakse regulaarselt.

c. Testimis- ja arenduskeskkondi ei käitata samas virtualiseerimisserveris koos käidukeskkonna IT-süsteemidega.

SYS.1.5.M11 Virtualiseerimissüsteemi haldusvõrk

a. Virtualiseerimissüsteemi hallatakse eraldi haldusvõrgu kaudu.

b. Autentimiseks, tervikluse tagamiseks ja krüpteerimiseks kasutatavate haldusprotokollide turvamehhanismid on aktiveeritud.

c. Kõik ebaturvalised haldusprotokollid on desaktiveeritud (vt NET.1.2 *Võrguhaldus*).

SYS.1.5.M12 Virtualiseerimistaristu halduse õigused ja rollid

a. On kehtestatud virtualiseerimisserveri halduseks vajalikud õigused ja rollid (vt SYS.1.5.M8 *Virtualiseerimissüsteemi kavandamine*).

b. Keskne identiteedi ja õiguste halduse protsess hõlmab ka virtualiseerimissüsteemi komponente.

c. Virtuaalserverite haldurid ja virtualiseerimisserveri ning hüperviisori administraatorid on erinevad isikud ja neil on erinevad pääsuõigused.

d. Halduskeskkond võimaldab virtuaalmasinaid rühmitada, et kehtestada haldurite rollijaotusega sobiv hierarhiline struktuur.

SYS.1.5.M13 Virtualiseerimissüsteemi jaoks sobiv riistvara

a. Kasutatav riistvara vastab rakendatud virtualiseerimislahendusele.

b. Kavandatud kasutamisperioodiks on riistvarale tagatud tootetugi.

SYS.1.5.M14 Virtualiseerimistaristu ühtsed konfiguratsiooninõuded

a. Virtualiseerimistaristu (sh külalissüsteemide) jaoks on määratud ühtne tüüpkonfiguratsioon.

b. Külalissüsteemide seadistamisel järgitakse tüüpkonfiguratsiooni.

c. Konfiguratsioonireegleid kontrollitakse regulaarselt ja vajadusel korrigeeritakse.

SYS.1.5.M15 Erineva kaitsetarbega külalissüsteemide lahusus

a. Kui samas virtualiseerimisserveris (ingl *host*) käitatakse erineva kaitsetarbega virtuaalseid külalissüsteeme (ingl *guest*), siis on virtuaalsed külalissüsteemid üksteisest eraldatud ja kapseldatud.

b. Erineva kaitsetarbega külalissüsteemide võrguühendused on virtualiseerimissüsteemis piisavalt turvaliselt eraldatud.

SYS.1.5.M16 Virtuaalmasinate isoleerimine

a. Virtuaalmasinate vaheline andmete ülekandmine andmete lähtemasinast kopeerimise (ingl *copy*) ja sihtmasinas kleepimise (ingl *paste*) kaudu on desaktiveeritud.

SYS.1.5.M17 Virtualiseerimisserveri konfiguratsiooni kontrollimine ja seire

a. Virtualiseerimisserveri pideva seire käigus kontrollitakse muuhulgas, kas:
   - virtualiseerimisserveri ressursid on piisavad;
   - virtualiseerimisserveri ühiskasutatavates ressurssides ei ole tekkinud konflikte;
   - konfiguratsioonifailides ei ole tehtud lubamatuid muudatusi;
   - virtuaalvõrgud on seostatud õigete virtuaalsete IT-süsteemidega.

b. Virtualiseerimisserveri konfiguratsioonimuudatused testitakse enne muudatuse rakendamist.

SYS.1.5.M19 Virtualiseerimissüsteemi regulaarsed läbivaatused

a. Regulaarsete läbivaatuste käigus kontrollitakse, kas virtualiseerimissüsteemi seisund vastab kavandatule.

b. Kontrollitakse regulaarselt, kas virtuaalsete komponentide konfiguratsioon vastab ettenähtud tüüpkonfiguratsioonile.

c. Läbivaatuste tulemused dokumenteeritakse ja tuvastatud lahknevused kõrvaldatakse esimesel võimalusel.

3.4 Kõrgmeetmed

SYS.1.5.M20 Kõrgkäideldav arhitektuur [arhitekt] (A)

a. Virtualiseerimistaristu on kavandatud kõrgkäideldavana.

b. Rohkemate virtualiseerimisserverite kasutamisel on virtualiseerimisserverid koondatud klastritesse (ingl *cluster*).

SYS.1.5.M21 Külalissüsteemide turvaline konfigureerimine (I-A)

a. Külalissüsteemidele (ingl *guest*) ressursside eraldamisel ei reserveerita ressursse summaarselt rohkem kui on füüsilisi ressursse.

b. Ressursside kattuvust võimaldav funktsionaalsus on desaktiveeritud.

SYS.1.5.M22 Virtualiseerimisserveri tugevdamine (C-I)

a. Virtualiseerimisserverit ja hüperviisorit on tugevdatud (ingl *hardening*).

b. Virtuaalsete IT-süsteemide kapselduseks ning üksteisest ja virtualiseerimisserverist eraldamiseks kasutatakse MAC-i (ingl *mandatory access control*, MAC).

SYS.1.5.M23 Virtuaalserveri õiguste piiramine (C-I)

a. Kõik liidesed ja sidekanalid, mis võimaldavad virtuaalserverist hostsüsteemi andmeid lugeda ja pärida, on kõrvaldatud või desaktiveeritud.

b. Virtualiseerimisserveri ressurssidele pääseb juurde ainult server ise.

c. Virtuaalserverid ei saa ühiskasutada virtualiseerimisserveri põhimälu sektsioone.

SYS.1.5.M24 Virtuaalserverite hetktõmmiste desaktiveerimine (C-I-A)

a. Virtuaalserverite administreerimiskonsoolis on hetktõmmise funktsioon desaktiveeritud.

SYS.1.5.M25 Virtuaalserveri konsoolpääsu minimaalne kasutamine (A)

a. Juurdepääs virtualiseerimissüsteemi emuleeritud konsoolidele on piiratud miinimumini.

b. Võimalusel hallatakse virtuaalserverit võrgu kaudu.

SYS.1.5.M26 Avaliku võtme taristu kasutamine [arhitekt] (C-I-A)

a. Virtualiseerimissüsteemi komponentide vahelise side krüpteerimisel kasutatakse võtmesertifikaate avaliku võtme taristust (ingl *public key infrastructure*, PKI).

SYS.1.5.M27 Sertifitseeritud virtualiseerimistarkvara (C-I-A)

a. Virtualiseerimistarkvara on ISO/IEC 15408 kohaselt sertifitseeritud, soovituslik tase on EAL 4 või kõrgem.

SYS.1.5.M28 Virtualiseeritud IT-süsteemide krüpteerimine (C)

a. Kõik virtualiseeritud IT-süsteemid on krüpteeritud.

4 Lisateave

Lühend	Publikatsioon
[NIST]	NIST Special Publication 800-125 „Guide to Security for Full Virtualization Technologie“

SYS.1.6 Konteinerdus

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed konteinerites (eng *container*) asuvate või konteineritega töödeldavate andmete kaitseks.

Erinevalt virtualiseerimisest võimaldab konteinerdus (ingl *containerization*) kapseldada rakendusi operatsioonisüsteemisisese ressursiga, ilma täiendavaid iseseisva operatsioonisüsteemiga virtuaalmasinaid (ingl *virtual machine*) kasutamata.

1.2 Vastutus

Konteinerduse turvameetmete rakendamise eest vastutab IT-talitus.

Lisavastutajad

Lisavastutajad puuduvad.

1.3 Piirangud

Moodul käsitleb nii konteinerite loomise ja haldamise tarkvara ja IT-teenuseid kui ka konteineris olevaid rakendusi ja teenuseid. Moodulis esitatakse konteinerduse üldised meetmed, eristamata konkreetseid tooteid. Toote valimisel järgitakse moodulit APP.6 *Tarkvara üldiselt*.

Moodul täiendab „SYS.1.1 *Server üldiselt*“ ning „SYS.1.3 *Linuxi ja Unixi server*“ meetmeid konteinerduse spetsiifikaga. Samuti laiendab antud moodul moodulites „CON.8 *Tarkvaraarendus*“ ja „OPS.1.1 *IT-põhitööd*“ esitatud turvameetmeid.

Konteinerites asuvad rakendused suhtlevad omavahel tavaliselt hostil (ingl *host*) realiseeritud virtuaalse võrgu kaudu. Seetõttu tuleb täiendavalt arvestada moodulites „NET.1 *Võrgu arhitektuur ja lahendus*“ ja „NET.3 *Võrgukomponendid“* esitatud meetmetega.

Juhul kui host ise on virtuaalne, rakendatakse meetmeid moodulist SYS.1.5 *Virtualiseerimissüsteem*.

Kui konteineritega seotud hostsüsteem või taristukomponendid ei kuulu täielikult organisatsioonile, vaid on osaliselt kolmandate poolte kasutuses või kolmandatelt pooltelt pilvteenusena sisse ostetud, rakendatakse lisaks meetmeid moodulitest OPS.2.3 *Väljasttellimine*, OPS.2.2 *Pilvteenuste kasutamine* ja OPS.3.1 *Teenuseandja infoturve*.

Moodulis ei käsitleta tegevusi seoses konteineri tõmmiste (ingl *image*) loomise ja haldusega.

Konteinerite orkestreerimist Kubernetese abil käsitletakse moodulis APP.4.4 *Kubernetes.*

2 Ohud

2.1 Konteineritõmmiste turvanõrkused või kahjurvara

Konteinerite loomisel kasutatakse omaloodud konteinerite kõrval sageli Internetist hangitud valmiskujul konteineritõmmiseid (ingl container image). Üha enam tarnitakse ka tarkvara eelnevalt loodud konteineritõmmiste kujul. IT-talitusel on võimalik tõmmiseid kohandada, lisades, muutes või eemaldades tarkvara või konfiguratsioone.

Kui algne konteineritõmmis sisaldab kahjurvara, levib see edasi organisatsiooni IT-süsteemi. Organisatsiooni IT-talitus ei ole võimalikest turvanõrkustest või kahjurvara (nt

krüptorahakaeve rakendus) olemasolust teadlik, sest konteineritõmmis loodi IT-talituse otsese osavõtuta. On raske kindlaks teha, milliseid tarkvarapakette on tõmmises kasutatud ja kas tarkvara sisaldab kõiki turvauuendeid. Kui ühe tõmmise alusel luuakse palju konteinereid, on potentsiaalne kahju veelgi suurem.

2.2 Turvamata hooldusjuurdepääsud

Hostsüsteemil asuvate konteineriteenuste haldamiseks vajalik hooldusjuurdepääs on enamasti realiseeritud võrguühenduse kaudu. Sageli on autentimis- ja krüptomehhanismid turvaliseks andmevahetuseks olemas, kuid neid pole vaikeseadistuses ega hilisema konfigureerimise käigus aktiveeritud.

Saades volitamata juurdepääsu hostsüsteemi võrguühendusele ning kasutades ära turvamata haldusjuurdepääsu, saab ründaja edastada hosti ohustavaid süsteemikäske. Raskemal juhul võib haldusjuurdepääsu pahatahtlik kasutamine kaasa tuua kõigi hostil asuvate konteinerite kaotuse.

2.3 Hostisisene ressursikonflikt

Üks konteiner võib hosti ressursid üle koormata ja seega ohustada hosti teiste konteinerite käideldavust. Halvimal juhul muutub kättesaamatuks terve hostsüsteem.

2.4 Andmevahetus volitamata IT-süsteemidega

Konteinerid on võimelised suhtlema üksteisega, oma hostiga ja teiste hostsüsteemidega. Kui andmevahetust pole piiratud, võib ründaja seda võimalust teiste konteinerite või hostide ründamiseks ära kasutada.

Eksisteerib oht, et konteinerile saadakse volitamata juurdepääs väljastpoolt hostsüsteemi. Väljastpoolt algatatud rünne ainult sisekasutuseks mõeldud IT-teenuste vastu võib kaasa tuua raskeid tagajärgi. Sageli on siseste IT-teenuste kaitsele pööratud vähe tähelepanu.

2.5 Konteineri eraldatuse rike

Kui ründaja suudab konteineris käivitada oma koodi, võib ta katkestada konteineri isoleerituse teistest konteineritest või hostist. Rünne, mille eesmärk on saada juurdepääs teistele konteineritele, hostsüsteemile või infrastruktuurile, võib toimuda näiteks protsessorite, operatsioonisüsteemi tuuma või lokaalsete teenuste (nt DNS või SSH) turvanõrkuste tõttu.

Kui ründaja saab kontrolli hostsüsteemi üle, ohustab ta kõigis selles hostis asuvate konteinerite turvalisust.

2.6 Konteinerite väärast haldusest tingitud andmekadu

Kui haldustööde käigus lülitatakse konteiner välja, ilma et konteineris töötav tarkvara saaks oma jooksva tööülesande lõpetada (nt lõpetada poolelioleva kirjutusprotsessi), võib sellise ootamatu seiskamise tulemusel tekkida andmekadu. Andmekadu võib olla laialdasem kui seda on parasjagu konteineri seiskamise hetkel töödeldavad andmed.

2.7 Konteineri pääsuandmete leke

Konteineri või konteineritõmmise loomisel on konteineris oleva tarkvara installimiseks ja konfigureerimiseks vaja vastavate eelisõigustega kasutajakontosid. Kõrgema taseme volitusi on vaja ka konteineris asuvate andmebaaside seadistamiseks. Konteineritõmmiste loomise automatiseerimisel võivad skriptides kasutatud kasutajakontod, paroolid või muu juurdepääsuks vajalik teave sattuda volitamata isikute kätte. Oht on suurem kui versioonihaldus ei ole piisavalt turvaline või kui samu konteineritõmmiseid kasutatakse erinevates süsteemides.

2.8 Konteinertõmmiste kontrollimatu levitamine

Konteinerid erinevad tavameetodil installitud ja seadistatud IT-süsteemidest, mille puhul on IT-talitusel olemas täielik kontroll installitud rakendustest, komponentidest ja teenustest. Kolmandate poolte hallatud konteinerite puhul IT-talitusel selline kontroll puudub. Tavaliselt pakub IT-talitus ainult platvormi, kuhu arendajad saavad oma konteinerid või konteinerdatud rakendused tõsta. Seetõttu eksisteerib oht, et konteinerid sisaldavad teadmata turvanõrkusi.

3 Meetmed

3.1 Elutsükkel

Kavandamine

SYS.1.6.M1 Konteinerduse kavandamine

SYS.1.6.M2 Konteinerduse halduse kavandamine

SYS.1.6.M3 Konteinerdatud IT-süsteemide turvaline käitamine

SYS.1.6.M9 Rakenduste sobivuse hindamine

SYS.1.6.M10 Konteinerite kasutamise eeskiri

Evitus

SYS.1.6.M4 Konteineritõmmiste turvaline evitus

SYS.1.6.M5 Konteinerite haldusvõrgu eraldamine

SYS.1.6.M11 Rakenduste eraldamine konteinerites

SYS.1.6.M12 Konteineritõmmiste turvaline levitamine

SYS.1.6.M13 Konteineritõmmiste kasutuseks kinnitamine

Käitus

SYS.1.6.M6 Turvaliste konteineritõmmiste kasutamine

SYS.1.6.M7 Konteineri logiandmete säilitamine

SYS.1.6.M8 Konteineri pääsuandmete turvaline haldus

SYS.1.6.M14 Konteineritõmmiste ajakohastamine

SYS.1.6.M15 Konteineri ressursipiirangute määratlemine

SYS.1.6.M16 Konteinerite kaughoolduse turve

SYS.1.6.M17 Konteineri käitamiseks minimaalselt vajalike õiguste määratlemime

SYS.1.6.M18 Konteinerdatud rakenduste õiguste piiramine

SYS.1.6.M19 Andmesalvestitele juurdepääsu reguleerimine

SYS.1.6.M20 Konteineri konfiguratsiooniandmete turve

Lisanduvad kõrgmeetmed

SYS.1.6.M21 Konteirduse laiendatud turvaeeskiri

SYS.1.6.M22 Konteineritõmmise kasutamine asitõendina

SYS.1.6.M23 Konteinerite muutumatuse tagamine

SYS.1.6.M24 Hostipõhine ründetuvastus

SYS.1.6.M25 Konteinerdatud rakenduste kõrgkäideldavus

SYS.1.6.M26 Konteinerite täiendav isoleerimine ja kapseldamine

3.2 Põhimeetmed

SYS.1.6.M1 Konteinerduse kavandamine

a. Enne konteinerduse kasutuselevõttu on määratud eesmärgid, mida konteinerdusega tahetakse saavutada (nt skaleeritavus, käideldavus, CI/CD välearendus (ingl *agile development*), turvalisus läbi rakenduste eraldatuse).

b. Kavandamisel on kaardistatud konteinerduse turvariskid ning nende mõjud organisatsiooni äriprotsessidele.

c. Kavandamisel on arvestatud tegevuskulusid, mis tekivad konteinerite kasutuselevõtu ja käigushoiuga.

d. Konteinerduse eesmärgid, riski- ja kuluhinnangud on dokumenteeritud.

SYS.1.6.M2 Konteinerduse halduse kavandamine

d. Konteinerite haldusprotsessid hõlmavad konteinerduse kogu elutsüklit alates konteinerite kasutuselevõtust kuni kasutuselt kõrvaldamiseni (ingl d*ecommisioning*).

e. Konteinerite haldus sisaldab konteinerduse turvalisuse tagamist ja regulaarset turvauuendite paigaldamist.

SYS.1.6.M3 Konteinerdatud IT-süsteemide turvaline käitamine

a. Enne konteinerite kasutuselevõttu on analüüsitud, kuidas konteinerdus mõjutab kasutatavaid IT-süsteeme ja rakendusi, eelkõige rakenduste käitust ja haldamist.

b. On analüüsitud, kas konteinerite IT-süsteemide, virtuaalsete võrkude ning opereeritavate rakenduste isoleerimine ja kapseldamine on kooskõlas rakenduste kaitsetarbega.

c. On kontrollitud, kas hosti operatsioonisüsteemi turvamehhanismid tagavad konteinerite piisava turvalisuse.

d. Virtuaalvõrgu turvalisuse tõstmiseks on hostile rakendatud meetmed mooduligruppidest „NET.1 *Võrgud ja side*“ ning NET.3 *Võrgukomponendid*.

e. Konteinerites asuvate IT-süsteemide käideldavus on vastavuses eelnevalt püstitatud käideldavuse ja andmeedastusvõimekuse nõuetega.

f. Konteinerite käitamisel seiratakse süsteemi toimivust ning viiakse läbi perioodilisi seisundikontrolle (ingl *health check*).

SYS.1.6.M4 Konteineritõmmiste turvaline evitus

a. Konteineritõmmiste loomise ja rakendamise protsess on piisava detailsusega kavandatud ja dokumenteeritud.

SYS.1.6.M5 Konteinerite haldusvõrgu eraldamine

a. Piisava turvataseme tagamiseks on hostsüsteemi haldusvõrk, konteinerite haldusvõrk ja konteinerdatud rakendustele juurdepääsuks kasutatavad võrgud üksteisest asjakohaselt eraldatud.

b. Hostsüsteemi kaughaldust tehakse ainult spetsialiseeritud haldusvõrgu kaudu.

c. Konteinerite käitamiseks mittevajalikud andmesideühendused on blokeeritud.

SYS.1.6.M6 Turvaliste konteineritõmmiste kasutamine

a. Kõik kasutatavad konteineritõmmised pärinevad usaldusväärsetest allikatest. Konteineritõmmise looja on üheselt tuvastatav.

b. Enne konteineritõmmise kasutuselevõttu veendutakse, et selle looja on kontrollinud konteineri sisu turvanõrkuste osas, on teadaolevad turvanõrkused parandanud ja vastava dokumentatsiooni oma klientidele edastanud.

c. Kasutatavad konteineritõmmised versioonitakse. Kasutatakse võimalikult viimast konteineritõmmise versiooni.

d. Kui on saadaval on uuema versiooninumbriga konteineritõmmis, planeeritakse selle kasutuselevõtt vastavalt kehtestatud muudatuste halduse protsessile.

SYS.1.6.M7 Konteineri logiandmete säilitamine

a. Konteineri logiandmed salvestatakse ja säilitatakse väljaspool konteinerit (vähemalt hostsüsteemi tasemel).

SYS.1.6.M8 Konteineri pääsuandmete turvaline haldus

a. Mandaatide (ingl *credentials*) ja juurdepääsuandmete salvestamisel ja haldamisel on juurdepääs mandaatidele ainult volitatud isikutel ja konteineritel.

b. Juurdepääsuandmed on salvestatud ainult spetsiaalsetesse, turvatud asukohtadesse. Konteineritõmmises juurdepääsuandmeid ei hoita.

c. Konteineriteenuste haldustarkvara olemasolul kasutatakse haldustarkvarasse integreeritud mandaatide halduse mehhanisme.

d. Turvaliselt on talletatud vähemalt järgmised mandaadid:
   - kõik kontoparoolid;
   - rakenduste teenuste API krüptovõtmed;
   - sümmeetrilise krüpteerimise võtmed;
   - avaliku võtme taristu (ingl *public key infrastructure*, PKI) privaatvõtmed.

3.3 Standardmeetmed

SYS.1.6.M9 Rakenduste sobivuse hindamine

a. Konteineris kasutatav rakenduste ja teenuste sobivust konteineris kasutamiseks on eelnevalt testitud.

b. Rakenduste sobivuse hindamisel on arvestatud konteineri ootamatust katkestusest tulenevate võimalike tagajärgedega.

c. Rakenduste konteineris käitamise sobivuse kontrollid (vt SYS.1.6.M3 *Konteinerdatud IT-süsteemide turvaline käitamine*) on dokumenteeritud.

SYS.1.6.M10 Konteinerite kasutamise eeskiri

a. On loodud ja rakendatud eeskiri, mis määrab konteinerite käitamise reeglid.

b. Konteinerite kasutamise eeskiri sisaldab ka nõudeid konteineritõmmiste turvaliseks loomiseks ja rakendamiseks.

SYS.1.6.M11 Rakenduste eraldamine konteinerites

a. Iga konteiner kannab samaaegselt ainult üht IT-teenust.

SYS.1.6.M12 Konteineritõmmiste turvaline levitamine

a. On koostatud ja kinnitatud kriteeriumid, mille alusel on võimalik hinnata konteineritõmmiste usaldusväärsust ja konteineritõmmis kasutuseks kinnitada.

b. Konteineritõmmised on varustatud metaandmetega tõmmise koostaja, otstarbe ja ajaloo kohta.

c. Konteineritõmmised on kaitstud volitamata muutmise eest (nt digiallkirja abil).

SYS.1.6.M13 Konteineritõmmiste kasutuseks kinnitamine

a. Sarnaselt tarkvaratoodetega testitakse konteineritõmmised enne käituskeskkonda (ingl *operational environment*) paigaldamist.

b. Konteineritõmmiste kasutuseks kinnitamine toimub vastavalt kehtestatud korrale (vt OPS.1.1.6 *Tarkvara testimine ja kasutuselevõtt*).

SYS.1.6.M14 Konteineritõmmiste ajakohastamine

a. Konteineritõmmiste uuendite paigaldamine toimub kinnitatud muudatusehalduse protsessi kohaselt (OPS.1.1.3 *Paiga- ja muudatusehaldus*).

b. On määratud, millal ja kuidas konteineritõmmiste, konteineritest käitatava tarkvara või teenuste uuendeid paigaldatakse ja kasutusele võetakse.

c. Pikaajaliselt kasutuses olnud konteinerite puhul otsustakse, kas otstarbekas oleks uuendada kasutatava konteineri sisu või tuleks konteiner taasluua.

SYS.1.6.M15 Konteineri ressursipiirangute määratlemine

a. Iga konteineri jaoks on määratud ja reserveeritud toimimiseks vajalikud hostsüsteemi ressursid (nt CPU, muutmälu maht, võrgu läbilaskevõime).

b. On olemas tegevuskava juhuks, kui ressurssidele määratud piirväärtused ületatakse.

SYS.1.6.M16 Konteinerite kaughoolduse turve

a. Kõiki konteineritest hostide suunas ja vastupidi tehtavaid haldustegevusi käsitletakse kaughooldusena (vt OPS.1.2.5 *Kaughooldus*).

b. Hosti kaughooldust ei tehta samal hostil asuvast konteinerist.

c. Rakendusi käitavas konteineris on kaughooldusjuurdepääsud teistesse IT-süsteemidesse piiratud.

d. Konteineri kaughooldust tehakse ainult konteineri käituskeskkonna (ingl *container runtime*) kaudu.

SYS.1.6.M17 Konteineri käitamiseks minimaalselt vajalike õiguste määratlemime

a. Konteineri käituskeskkonda (ingl *container runtime*) ja selles loodud konteinereid käitatakse selleks otstarbeks loodud lihtkasutaja õigustega kontoga (ingl *non-privileged account*), millel puuduvad eeliskonto õigused konteinerirakendustes või hostsüsteemi operatsioonisüsteemis.

b. On kasutusele võetud täiendavad meetmed konteineri käituskeskkonna kapseldamiseks (ingl *encapsulation*), nt protsessoripõhise virtualiseerimise (ingl *CPU virtualization extension*) abil.

c. Kui erandkorras on vajalik konteinerit käitava konto õigustes käivitada hostsüsteemi tegumeid (ingl *task*), on konto kasutajaõigused hostsüsteemis piiratud minimaalselt vajalike õigustega. Kõik sellised erandid on dokumenteeritud.

SYS.1.6.M18 Konteinerdatud rakenduste õiguste piiramine

a. Konteinerisisestel süsteemikontodel ei ole õigusi hostsüsteemis. Erandite korral toimub konto haldus hostsüsteemis, kontole antakse juurdepääs ainult vajalikele andmetele ja IT-süsteemidele.

SYS.1.6.M19 Andmesalvestitele juurdepääsu reguleerimine

a. Konteineritele on antud juurdepääs ainult tööks vajalikele andmesalvestitele ja jagatud kataloogidele. Juurdepääs on antud ainult määral, mis on antud tööülesannete täitmiseks vajalik.

b. Kui konteineri käituskeskkonnas on seadistatud andmesalvestuseks konteineri lokaalne salvestusruum, on juurdepääs salvestusruumile lubatud ainult konteinerisisestel kontodel.

c. Kui kasutatakse võrgupõhiseid salvestisüsteeme (SAN või NAS), antakse vajalikud juurdepääsuõigused konteinerile salvestisüsteemist.

SYS.1.6.M20 Konteineri konfiguratsiooniandmete turve

a. Konteineri konfiguratsiooniandmed on versioonitud.

b. Kõik konfiguratsioonimuudatused on selgesõnaliselt dokumenteeritud.

3.4 Kõrgmeetmed

SYS.1.6.M21 Konteirduse laiendatud turvaeeskiri (C-I-A)

a. On koostatud täpsed eeskirjad konteinerite pääsuõiguste halduseks.

b. Detailsed pääsuõigused jõustatakse vastavalt eeldefineeritud reeglitele MAC (Mandatory Access Control) või sellega samaväärse mehhanismi abil.

c. Pääsueeskiri sätestab juurdepääsu andmise vähemalt järgmisele:
   - sisenevad ja väljuvad võrguühendused;
   - juurdepääsuõigused failisüsteemile;
   - operatsioonisüsteemi tuuma (ingl *kernel*) päringud (*syscalls*).

d. Konteineri käivitamisel käituskeskkonnast (ingl *container runtime*) on hosti operatsioonisüsteemi tuum võimeline blokeerima pääsureeglitega keelatud konteineri tegevused (nt lokaalse paketifiltri seadistuste muutmine või õiguste tühistamine) või sellest teavitama.

SYS.1.6.M22 Konteineritõmmise kasutamine asitõendina (C-I)

a. Et võimaldada konteinerite hetketõmmiste kasutamist asitõendina võimalikul uurimisel, on konteineritõmmiste loomisel järgitud määratud reegleid (vt DER.2.2 *IT-kriminalistika võimaldamine*).

SYS.1.6.M23 Konteinerite muutumatuse tagamine (I)

a. Konteineri failisüsteemi muutmine konteineri käitamise ajal on blokeeritud.

b. Failisüsteem on maunditud (ingl *mount*) konteineriga ilma kirjutusõiguseta (ingl *write permisssion*).

SYS.1.6.M24 Hostipõhine ründetuvastus (C-I-A)

a. Konteinerid ja neis kasutatavad rakendused ning teenused on allutatud pidevale seirele.

b. Kõrvalekalded konteinerite tavapärasest toimimisest registreeritakse. Kõrvalekalletest teavitatakse määratud isikuid. Sündmusi käsitletakse vastavalt kesksele turvasündmuste halduse protsessile.

c. Seiratakse vähemalt järgmisi tegevusi ja protsesse:
   - võrguühendused ja andmevahetus;
   - konteineris algatatud protsessid;
   - failisüsteemi poole pöördumised;
   - operatsioonisüsteemi tuuma (ingl *kernel*) päringud (*syscalls*).

SYS.1.6.M25 Konteinerdatud rakenduste kõrgkäideldavus (A)

a. Konteinerdatud rakenduse kõrkäideldavuse nõude puhul tehakse valik, mis tasemel käideldavust tõstetakse (nt liiasuse tagamine hostide tasemel (hostide dubleerimine)).

SYS.1.6.M26 Konteinerite täiendav isoleerimine ja kapseldamine (C-I)

a. Konteinerite isoleerimise ja kapseldamise rangemate nõuete kehtestamisel kaalutakse järgmiste meetmete rakendamist:
   - konteinerite määramine fikseeritud hostidele;
   - üksikute konteinerite ja/või hostide käitamine hüperviisoritega (ingl *hypervisor*);
   - konkreetse konteineri sidumine konkreetse hostiga.

4 Lisateave

Lühend	**Publikatsioon**
[NIST]	NIST Special Publication 800-190 “Application Container Security Guide”, https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-190.pdf
[CIS]	CIS Benchmark Docker, https://www.cisecurity.org/benchmark/docker/
[OCI]	Open Container Initiative, https://www.opencontainers.org/
[CNCF]	Cloud Native Computing Fountation, https://www.cncf.io/
[SANS]	SANS Checklist for Audit of Docker Containers, https://www.sans.org/reading-room/whitepapers/auditing/checklist-audit-docker-containers-37437
[DOCKER]	Docker Security Guide, https://docs.docker.com/engine/security/

SYS.1.8 Salvestilahendused

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed salvestilahenduse (ingl *storage solution*) kavandamiseks, rakendamiseks, turvaliseks käituseks ja kasutuselt kõrvaldamiseks.

Selle mooduli tüüpilised sihtobjektid on salvestisüsteemid - võrgusalvestid (ingl *network attached storage*, NAS) ja salvestusvõrgud (ingl *storage area network*, SAN). Salvestisüsteemides talletatakse andmed salvestites (ingl *storage device*).

1.2 Vastutus

Salvestilahenduste meetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Tehnikatalitus, infoturbejuht.

1.3 Piirangud

Põhinõuded salvestilahenduste kasutamiseks failiserverina on esitatud moodulites SYS.1.1 *Server üldiselt* ja APP.3.3 *Failiserver*. Andmete pikaajalist säilitamist salvestisüseemis käsitletakse moodulites OPS.1.2.2 *Arhiveerimine* ja CON.3 *Andmevarunduse kontseptsioon*.

Salvestilahenduste turvalist paigutamist organisatsiooni sisevõrku käsitletakse moodulis NET.1.1 *Võrgu arhitektuur ja lahendus*.

Salvestilahenduste kasutajate haldust käsitletakse moodulis ORP.4 *Identiteedi ja õiguste haldus*.

Kui salvestilahendus on võetud teenusena väliselt teenuseandjalt, siis rakendatakse täiendavalt meetmeid moodulist OPS.2.3 *Väljasttellimine*.

2 Ohud

2.1 Salvestikomponentide ebaturvaline vaikeseadistus

Salvestikomponentide lihtsa ja ühildusprobleemideta kasutusevõtu soodustamiseks tarnitakse salvestikomponendid tüüpkonfiguratsiooniga, milles võimalikult paljud funktsioonid on aktiveeritud. Seetõttu on seadmetes avatud ka lubamatud protokollid, nagu näiteks HTTP, Telnet ja SNMP (ingl S*imple Network Management Protocol*, SNMP) protokolli ebaturvalised versioonid. Ebaturvaliste tehaseseadetega salvestilahendusele on ründajal lihtsam lubamatult juurde pääseda. Selle tulemusena võib IT-süsteemide töö katkeda, kuna andmebaasid pole enam kättesaadavad. Samuti on ründajal võimalik saada juurdepääs organisatsiooni konfidentsiaalsetele andmetele.

2.2 Andmete manipuleerimine salvestisüsteemi kaudu

Puudulikult konfigureeritud salvestisüsteem võib lihtsustada ründaja juurdepääsu organisatsiooni andmetele. Kui SAN-iga ühenduses olevasse serverisse on võimalik ühenduda väljastpoolt sisevõrku (Internetist), on ründajal edu korral võimalik seda serverit kasutada hüppelauana salvestusvõrku talletatud tundlikule teabele juurdepääsuks, ilma et organisatsiooni tulemüür või sissetungituvastuse süsteem teda takistaks.

2.3 Andmepüük salvestipõhisel andmete dubleerimisel

Sageli kasutatakse andmekao vältimiseks salvestisüsteemis andmete reaalajas dubleerimist. Krüpteerimata andmete automaatsel dubleerimisel on oht, et salvestite vahelist liiklust lubamatult salvestatakse, kasutades näiteks FC-analüsaatoreid või võrgunuuskureid (ingl *network sniffer*).

2.4 WWN-identifikaatori võltsimise rünne

Fiiberoptiliste kaabliühendustega FC-salvestusvõrgu seadmete identifitseerimiseks kasutatavaid WWN (*World Wide Name*, WWN) identifikaatoreid (sarnaselt Etherneti võrguadapterite MAC-aadressidele) on võimalik manipuleerida. Hosti siiniadapteri (ingl *host bus adapter*, HBA) WWN-identifikaatorit on võimalik muuta adapteri tootja tarkvaraga. Seadme WWN identifikaatorit võltsides on suuremas süsteemis võimalik ligi pääseda võõrastele andmetele. Sellisel juhul on neil võimalik juurde pääseda teiste klientide andmetele.

2.5 Võrkude loogilise lahususe rikkumine

Organisatsiooni teabe turvalisus võib olla ohus, kui eri klientide võrgud on võrkude füüsilise eraldamise asemel eraldatud virtuaalsete salvestusvõrkude (ingl *virtual storage area network*, VSAN) abil. Kui ründajal õnnestub tungida teise kliendi võrku, võib ta saada juurdepääsu nii selle kliendi virtuaalsele salvestusvõrgule kui ka edastatavatele andmetele.

2.6 Salvestilahenduse komponendi tõrge

Komplekssed võrgupõhised salvestilahendused koosnevad paljudest komponentidest (näiteks FC-kommutaatorid, salvestikontrollerid, virtualiseerimisseadmed). Kui komponentide tasemel liiasust pole rakendatud, võib salvestilahenduse komponendi tehniline rike tekitada tõrke salvestilahenduse töös või põhjustada andmekadu.

2.7 Lubamatu füüsiline juurdepääs salvestusvõrgu kommutaatoritele

Kui organisatsioonis salvestisüsteemi kaitsmiseks rakendatud pääsukontrollid pole piisavad, võib ründaja kommutaatoritele juurde pääseda. Ründaja võib ühendada andmepüügiks võrku täiendavaid FC-kommutaatoreid, et salvestada salvestisüsteemi andmeid.

3 Meetmed

3.1 Elutsükkel

Kavandamine

SYS.1.8.M6 Salvestilahenduse turvajuhend

SYS.1.8.M7 Salvestilahenduse kavandamine

SYS.1.8.M14 Salvestusvõrgu (SAN) segmentimine

Soetamine

SYS.1.8.M8 Sobiva salvestilahenduse valimine

SYS.1.8.M9 Salvestilahenduse hooldustpartneri valimine

Evitus

SYS.1.8.M1 Salvestisüsteemi sobiv paigalduskoht

SYS.1.8.M2 Salvestilahenduse turvaline aluskonfiguratsioon

SYS.1.8.M15 Salvestilahenduse tarbijate turvaline lahusus

Käitus

SYS.1.8.M4 Haldusliideste turve

SYS.1.8.M10 Salvestilahenduse käitamise juhend

SYS.1.8.M11 Salvestilahenduse turvaline käitus

SYS.1.8.M13 Salvestilahenduse seire ja haldus

SYS.1.8.M16 Andmete turvaline kustutamine

SYS.1.8.M17 Salvestisüsteemide konfiguratsiooni dokumenteerimine

SYS.1.8.M18 Salvestisüsteemide läbivaatused ja aruandlus

Kõrvaldamine

SYS.1.8.M19 Salvestisüsteemi kasutuselt kõrvaldamine

Avariivalmendus

SYS.1.8.M20 Salvestilahenduse avariivalmendus ja -toimingud

Lisanduvad kõrgmeetmed

SYS.1.8.M21 Salvestipuuli (*storage pool*) kasutamine tarbijate lahutamiseks

SYS.1.8.M22 Kõrgkäideldav salvestusvõrk

SYS.1.8.M23 Krüpteerimine salvestilahendustes

SYS.1.8.M24 Salvestusvõrgukanga (*SAN fabric*) tervikluse tagamine

SYS.1.8.M25 Andmete mitmekordne ülekirjutamine kustutamisel

SYS.1.8.M26 Salvestusvõrgu „tugev“ tsoonimine

3.2 Põhimeetmed

SYS.1.8.M1 Salvestisüsteemi sobiv paigalduskoht [tehnikatalitus]

a. Salvestisüsteemi komponendid on paigaldatud lukustatud ruumidesse. Juurdepääs ruumidesse on ainult pääsuõigusega isikutel.

b. Ruumides on tagatud katkematu elektritoide.

c. Keskkonna temperatuur ja õhuniiskus vastab salvestisüsteemi tootja soovitatule.

SYS.1.8.M2 Salvestilahenduse turvaline aluskonfiguratsioon

a. Enne salvestilahenduse käidukeskkonda paigaldamist on paigaldatud tarkvarakomponentide uuendid ja ajakohastatud riistvarakomponentide püsivara.

b. Aluskonfiguratsioonis on kõik vaikeparoolid muudetud ja tarbetud kasutajakontod desaktiveeritud.

c. Salvestisüsteemi tarbetud liidesed on desaktiveeritud.

d. Vaikekonfiguratsiooni, aluskonfiguratsiooni ja hetkekonfiguratsiooni failid on varundatud ja kaitstud.

SYS.1.8.M4 Haldusliideste turve

a. Salvestisüsteemide halduse pääsuõigused on piiratud.

b. Haldusliidestele puudub juurdepääs ebausaldatavatest võrkudest.
c. Salvestisüsteemi kaughaldusel kasutatakse turvalisi protokolle. Ebaturvaliste protokollide puhul toimub salvestisüsteemi haldus muudest võrkudest eraldatud haldusvõrgu kaudu.

3.3 Standardmeetmed

SYS.1.8.M6 Salvestilahenduse turvajuhend [infoturbejuht]

a. Organisatsiooni üldise turvapoliitika alusel on koostatud salvestilahenduste turvajuhend, mis sisaldab nõudeid salvestilahenduse turvaliseks kavandamiseks, rakendamiseks, halduseks, käituseks ja kõrvaldamiseks.
b. Turvajuhendit on töötajatele tutvustatud. Kõik salvestisüsteemi haldurid järgivad turvajuhendit.
c. Salvestilahenduse turvajuhendi muudatused kooskõlastatakse infoturbejuhiga ja dokumenteeritakse.
d. Turvajuhendi rakendamist kontrollitakse regulaarselt. Kontrolli tulemused dokumenteeritakse.

SYS.1.8.M7 Salvestilahenduse kavandamine

a. Salvestilahenduse kavandamise etapis on läbi viidud salvestilahenduse vajaduste, jõudluse ja mahu analüüs.
b. Nõuete spetsifikatsiooni alusel on koostatud salvestilahenduse rakendamise kava, mis määratleb:
    - sobiva riistvaraspetsifikatsiooni;
    - valmistaja ja tarnija valimise kriteeriumid;
    - hangitava lahenduse arhitektuuri (tsentraliseeritud või hajutatud);
    - võrguühenduste kava;
    - vajaliku infrastruktuuri;
    - integratsiooni olemasolevate protsessidega.

SYS.1.8.M8 Sobiva salvestilahenduse valimine

a. Erinevate salvestisüsteemide tehnilist spetsifikatsiooni ja sobivust organisatsiooni nõuetega on analüüsitud ja kontrollitud piisava detailsusega.
b. Salvestilahenduse valikukriteeriumid on üheselt arusaadavalt dokumenteeritud.
c. Hankeotsuse tegijatele on erinevate salvestisüsteemide võimalusi ja piiranguid tutvustatud.
d. Salvestilahenduse valimise otsus koos valikukriteeriumitele vastavuse põhjendusega on dokumenteeritud.

SYS.1.8.M9 Salvestilahenduse hoolduspartneri valimine

a. Salvestilahenduse hoolduspartner on valitud lähtuvalt salvestilahenduse nõuetest.
b. Hoolduspartneriga sõlmitud teenusetasemelepe (*service level agreement*, SLA) sisaldab salvestilahenduse garantiitingimuste, hoolduse ja remondiga seonduvaid aspekte.
c. Teenusetasemelepe on üheselt arusaadav ja selle täitmist on võimalik mõõdetavalt hinnata.

SYS.1.8.M10 Salvestilahenduse käitamise juhend

a. On koostatud salvestilahenduse käitamise juhend, mis esitab käitamise protsessid, nõuded ja konfiguratsiooni.

b. Salvestilahenduse käitamise juhendit ajakohastatakse regulaarselt.

SYS.1.8.M11 Salvestilahenduse turvaline käitus

a. Salvestilahenduse käitamisel jälgitakse pidevalt rakenduste käideldavust, süsteemide koormusnäitajaid ja sündmuseteateid.

b. Muudatuste tegemisel salvestilahenduses on määratud kindlad hooldusajad.

c. Salvestilahenduse püsivara, operatsioonisüsteemi või võrgukomponentide uuendeid installitakse üksnes eelnevalt kokku lepitud hooldusaegadel.

SYS.1.8.M13 Salvestilahenduse seire ja haldus

a. Salvestilahenduse ja ta komponente seire ja haldus toimuvad keskselt.

b. Seireandmete alusel on võimalik järeldada, kas salvestilahenduse käitamine toimub vastavalt juhendile.

c. Kui salvestilahendust haldab väline teenuseandja, on teenusetasemeleppes määratud ja dokumenteeritud seireobjektid, seire korraldus, oluliste süsteemiteadete filtreerimine ja osapoolte teavitamise kord.

SYS.1.8.M14 Salvestusvõrgu (SAN) segmentimine

a. Salvestusvõrgu (ingl *storage area network*, SAN) ressursside jaotus serveritele on dokumenteeritud.

b. SAN-i ressursijaotus ja tegelik ressursikulu on haldusvahenditega selgelt jälgitavad.

c. Salvestilahenduse võrk on segmenditud turva- ja haldusnõuete põhjal.

d. Kehtiv tsoonimiskonfiguratsioon on dokumenteeritud. Dokumentatsioon on kättesaadav ka avarii korral.

SYS.1.8.M15 Salvestilahenduse tarbijate turvaline lahusus

a. Organisatsiooni nõuded salvestilahenduse simultaanteenindusvõimele (ingl *multi-tenancy*) on määratud ja dokumenteeritud.

b. Salvestilahendus vastab dokumenteeritud lahususenõuetele.

c. Plokksalvestuse puhul on tarbijad üksteisest eraldatud (nt loogilise üksuse numbri e. LUN (ingl *logical unit number*, LUN) maskimisega).

d. Failiteenuseid erinevatele tarbijatele antakse eraldatud virtuaalsete failiserveritega. Iga klientüksuse jaoks on määratud oma failiteenus.

e. IP või iSCSI kasutamisel on tarbijad üksteisest lahutatud võrgu segmentimise abil.

f. FC (infl F*ibre Channel*, FC) kasutamisel on eraldatus tagatud virtuaalsete salvestusvõrkudega (*virtual storage area network*, VSAN) ja WWN-ide alusel tehtud „pehme“ tsoonimisega (ingl *soft zoning*).

SYS.1.8.M16 Andmete turvaline kustutamine

a. Turvalise kustutamise kord on määratud salvestilahenduse käitamise juhendiga (vt SYS.1.8.M10 *Salvestilahenduse käitamise juhend*). Sealhulgas sätestab juhend, mis andmeid ja millise protseduuriga kustutatakse.

b. Simultaanivõimega salvestusvõrkudes kustutatakse viimaks ka tarbijale kinnistatud LUN.

SYS.1.8.M17 Salvestisüsteemi konfiguratsiooni dokumenteerimine

a. Salvestisüsteemide konfiguratsioon (sh spetsiifilised süsteemikonfiguratsioonid) on dokumenteeritud.
b. Konfiguratsioonidokumentatsioon on kaitstud lubamatu juurdepääsu eest.
c. Konfiguratsioonidokumentatsioon on alati ajakohane (eriti pääsuõiguste andmise osas).
d. Salvestisüsteemi konfiguratsioonidokumentatsioon on kättesaadav ka avariiolukorras.

SYS.1.8.M18 Salvestisüsteemide läbivaatused ja aruandlus [infoturbejuht]

a. On kehtestatud kord salvestisüsteemide regulaarseks läbivaatuseks ja seda järgitakse.
b. On kehtestatud salvestisüsteemide läbivaatuste sagedus ja detailsusaste.
c. On määratud, milline on läbivaatuse aruande sisu ja kuidas käsitletakse kõrvalekaldeid nõuetest.

SYS.1.8.M19 Salvestisüsteemi kasutuselt kõrvaldamine

a. Enne salvestisüsteemi kõrvaldamist migreeritakse kõik salvestisüsteemis olevad andmed muudesse salvestisüsteemidesse.
b. Migreerimiseks on olemas dokumenteeritud ja testitud siirdeprotseduur.
c. Salvestisüsteemist kustutatakse turvaliselt kõik kasutaja- ja konfiguratsiooniandmed.
d. Salvestilahenduse dokumentatsioonist kustutatakse kõik viited kõrvaldatud salvestisüsteemile.

SYS.1.8.M20 Salvestilahenduse avariivalmendus ja -toimingud

a. On koostatud salvestilahenduse avariikava, mis annab täpsed juhised avariiolukorras tegutsemiseks.
b. Avariikava sisaldab ka tehnilisi juhiseid salvestilahenduse tõrkeanalüüsiks ja tõrkekõrvalduseks.
c. Avariikava harjutamiseks korraldatakse regulaarselt õppusi ja taastetestimisi.
d. Pärast õppusi ja testimisi kustutatakse turvaliselt kõik õppuse või testimise käigus loodud andmed.

3.4 Kõrgmeetmed

SYS.1.8.M21 Salvestipuuli (s*torage pool)* kasutamine tarbijate lahutamiseks (C-I)

a. Eri tarbijatele jagatakse salvestusruum erinevatest salvestipuulidest (ingl *storage pool*).
b. Üks salvestuskandja kuulub ainult ühe salvestipuuli koosseisu.
c. Sellisest salvestipuulist genereeritud iga LUN (Logical Unit Number, LUN) on määratud ainult ühe tarbija kasutusse.

SYS.1.8.M22 Kõrgkäideldav salvestusvõrk (A)

a. On kasutusele võetud kõrgkäideldav salvestusvõrk (SAN), mille dubleerimismehhanismid ja lahenduse konfiguratsioon vastavad organisatsiooni salvestilahenduse käideldavusnõuetele.
b. Lahenduse testimiseks on olemas eraldi süsteem.

SYS.1.8.M23 Krüpteerimine salvestilahendustes (C-I)

a. Kõik salvestilahenduses talletatavad andmed on krüpteeritud.

b. Vajadusel on andmed krüpteeritud ka edastusel, sealhulgas dubleerimisel ja varundamisel.

SYS.1.8.M24 Salvestusvõrgukanga (*SAN fabric*) tervikluse tagamine (I)

a. Salvestusvõrgukanga (ingl *SAN fabric*) moodustavate võrguseadmete kogumi tervikluse tagamiseks kasutatakse tugevdatud turvaparameetritega protokolle.

b. Andmevahetusseansi alustamiseks kasutatakse järgmiseid protokolle:

- *Diffie Hellman Challenge Handshake Authentication Protocol* (DH-CHAP);
- *Fiber Channel Authentication Protocol* (FCAP);
- *Fiber Channel Password Authentication Protocol* (FCPAP).

SYS.1.8.M25 Andmete mitmekordne ülekirjutamine kustutamisel (C)

a. Salvestusvõrgukeskkondades kustutatakse andmed loogilise üksuse numbri e. LUN-i (ingl *logical unit number*, LUN) juurde kinnistatud salvestiosade mitmekordse spetsiaalse andmemustriga ülekirjutamise abil.

SYS.1.8.M26 Salvestusvõrgu „tugev“ tsoonimine (C-I-A)

a. Salvestusvõrgu segmentimisel kasutatakse kommutaatorite portide eraldamisel põhinevat „tugevat“ tsoonimist (ingl *hard zoning*).

4 Lisateave

Lühend	Publikatsioon
[ISO]	ISO/IEC 27040:2015 „Information technology – Security techniques – Storage security“

SYS.1.9 Terminaliserver

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed terminaliserveri (ingl *terminal server*) kaudu käideldavate andmete kaitseks, sh terminaliserveri kavandamiseks, rakendamiseks, turvaliseks käituseks ja kasutuselt kõrvaldamiseks.

Terminaliserveri klientarvuti (edaspidi klient) võib olla nn paks klient (ingl *fat client*) või õhuke klient (ingl *thin client*). Paksud kliendid on varustatud täisväärtusliku operatsioonisüsteemiga. Seevastu õhukesed kliendid on kavandatud ainult terminaliserveriga ühenduse loomiseks ja selles olevate rakenduste käitamiseks.

Terminaliserveris käitatakse rakendusi, mida on otsustatud (nt tehnilistel või korralduslikel põhjustel) otse kliendist mitte käivitada. Kliendile edastatakse graafilise kasutajaliidese kuva ning hiire ja klaviatuuri sisend spetsiifiliste terminaliserveri protokollide (nt RDP, PCoIP) või VNC vahendusel.

Terminaliserveri operatsioonisüsteemis saavad töötada mitmed kasutajad korraga, kes võivad käitada ühtesama või erinevaid rakendusi.

1.2 Vastutus

Terminaliserveri meetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Arhitekt.

1.3 Piirangud

Moodulis esitatud meetmed rakenduvad nii terminaliserverile kui ka terminaliserveri klientidele.

Üldised nõuded terminaliserverile ja kliendile on esitatud moodulites SYS.1.1 *Server üldiselt*, SYS.2.1 *Klientarvuti üldiselt* ja erinevaid operatsioonisüsteeme käsitlevates moodulites.

Terminaliserveri tarkvarale rakenduvad meetmed moodulist APP.6 *Tarkvara üldiselt*. Terminaliserveri võrgulahenduse turvet käsitletakse moodulis NET.1.1 *Võrgu arhitektuur ja lahendus*.

Käesolev moodul ei käsitle kaughalduse läbiviimist ega kaughaldustööriistade kasutamist. Neid teemasid käsitletakse moodulis OPS.1.2.5 *Kaughooldus*.

2 Ohud

2.1 Ebakvaliteetne andmeedastus

Terminaliserveri kasutamisel peab terminaliserveri vastus kliendi päringule olema selgelt arusaadav ja jõudma klientideni ilma märgatava viivituseta. Ülemäärane hilistus võib põhjustada tõrkeid teenuse toimimises, nt väljenduda selles, et hiire- või tekstikursori liikumist ja piltide vahetumist ekraanil on raske jälgida. On võimalik teha sisestusvigu, terminaliserverit saab kasutada ainult piiratud ulatuses.

Viivitusi võib põhjustada sidekanali või võrgukomponentide ülemäärane latentsusaeg. Samuti võib täiendavat hilistumist tekitada ebapiisavalt dimensioonitud turvakomponent, nt VPN-lüüs.

Terminaliserver võib päringule vastata viivitusega ka juhul, kui ta on ülekoormatud. Ülekoormus võib olla tingitud hulgast samaaegsetest kliendipäringutest või ebapiisavast terminaliserveri jõudlusest.

2.2 Terminaliserveri juurdepääsematus

Rakendused käivitatakse terminaliserveris, kliendile saadetakse ainult ekraaniväljund. Kui terminaliserver pole tõrke tõttu kättesaadav, nt kui seanss kliendi ja terminaliserveri vahel on katkenud, kaob kontroll käitatava rakenduse üle. Kasutaja ei pääse terminaliserveris käivitatud rakendusi juhtima, isegi kui need on terminaliserveris hetkel aktiivsed.

Kui rakendusel puudub alternatiivne kasutajaliides, võib IT-süsteemi töö täielikult katkeda. Terminaliserveri rike võib mõjutada korraga suurt hulka kliente.

2.3 Rünne terminaliserverile

Terminaliserveris käivitatud klientrakendused kasutavad tavaliselt teistes serverites asuvaid teenuseid ja andmeid. Seetõttu on terminaliserverisse juurdepääsu saanud ründajal lihtne edasi liikuda teistesse serveritesse, kasutades terminaliserverit teiste IT-süsteemide vastu kavandatud rünnete lähtepunktina. Eriti ohtlik on rünne juhul, kui terminaliserverist on juurdepääs erinevates võrgusegmentides paiknevatele rakendustele.

2.4 Puudulik seansihaldus

Terminaliserveris käitatavad rakendused jagavad operatsioonisüsteemi piires erinevate rakenduste ja klientidega sama ressurssi, nt tuuma (ingl *kernel*), teeke ning riistvarakomponente (nt CPU või RAM). Konfiguratsioonivigade või tarkvaras esinevate nõrkuste tõttu on võimalik, et erinevad rakenduste instantsid saavad üksteisega suhelda. Näiteks saab ründaja turvanõrkuste olemasolul kasutada kahjurkoodi, mis otsib muutmälust (RAM) kasutajate sisestatud paroole.

Kui terminaliserveri seansi kasutajal on ülemäärased pääsuõigused, võib ta läbi rakenduse saada juurdepääsu ka failisüsteemile ja läbi failihaldusdialoogi vaadata, muuta või salvestada faile aladelt, millele juurdepääsuks puudub kasutajal vajadus.

Teine võimalik rünne on nn RDP seansi kaaperdusrünne (ingl *hijack attack*). Kui kasutajad jäävad pärast terminaliserveri seansside lõppu sisse logituks, võib ründaja vastavate õiguste olemasolul RDP seansi üle võtta ning jätkata seanssi eelmise kasutaja õigustes.

2.5 Andmesideprotokolli nõrkuste ärakasutamine

Reeglina kasutatakse terminaliserverite andmesideprotokollides terminaliserveri klientide tõsikindlat autentimist ja krüpteeritud andmevahetust. Terminaliserveri protokolli turvanõrkuste esinemisel (või kui olulised turvafunktsioonid on konfiguratsioonivea tõttu blokeeritud) on võimalik klientide ja terminaliserveri vahelist suhtlust pealt kuulata. Ründaja võib saada volitamata juurdepääsu klientide autentimisandmetele, kasutaja lõikepuhvri sisule või edastatavatele failidele.

2.6 Ühiskasutatavad kasutajakontod

Terminaliserveris käitatava rakenduse pidevaks seireks (nt välise hoolduspartneri poolt) võib tekkida soov luua ühiskasutatav kasutajakonto. See võib minna vastuollu organisatsiooni sise-eeskirjade, turvapoliitika või terminaliserveri tarkvara litsentsitingimustega.

Ühiskasutatav konto tõttu ei ole võimalik seostada terminaliserveris tehtavaid toiminguid konkreetsete isikuga. Sellel võivad olla ka õiguslikud tagajärjed, nt juhul kui läbi terminaliserveri töödeldakse isikuandmeid.

2.7 Vead pääsuõiguste piiramisel

Terminaliserveri olemusest tingituna võib terminaliserver samaaegselt toimida nii serverina kui ka klientarvutina, kust käivitatakse teistes serverites töötavaid rakendusi. See võib põhjustada pääsuõiguste määramisel vigu, mis väljenduvad kas liigsete pääsuõiguste andmises või õiguste liigses piiramises.

Reeglina tuleb kasutajale anda võimalikult vähesed juurdepääsuõigused. Selline käitumine võib tekitada olukorra, kus kasutaja saab rakendust kasutada ebaefektiivselt ja ainult väga piiratud ulatuses. Näiteks võivad kasutajad lokaalsele kõvakettale kirjutamise blokeerimise tagajärjel hakata salvestama andmeid pilvteenustesse.

2.8 Terminaliserverile sobimatute rakenduste kasutamine

Kõik rakendused ei pruugi terminaliserveris kasutamiseks sobida. Näiteks võib tekkida probleeme keerulist ekraanigraafikat kasutatavate rakenduste või 3D-rakendustega. Terminaliserveri emuleeritud graafikamoodul ei pruugi toetada riistvaralise graafikaprotsessori (GPU) funktsioone.

Terminaliserver, selle klienditarkvara või andmevahetusprotokoll ei pruugi kliendiga ühendatud eriotstarbelistest välisseadmetest andmeid vastu võtta. Ilma piisava testimiseta ilmnevad need puudused alles töö käigus. See kahandab oluliselt terminaliserveri kasutuselevõtust plaanitud lisandväärtust.

3 Meetmed

3.1 Elutsükkel

Kavandamine

SYS.1.9.M1 Terminaliserveri turvanõuete kehtestamine

SYS.1.9.M2 Terminaliserveri kasutuselevõtu kavandamine

SYS.1.9.M5 Klientide ja klienttarkvara plaanimine

SYS.1.9.M6 Terminaliserveri võrgulahenduse kavandamine

Soetamine

SYS.1.9.M8 Terminaliserveri turvaline määramine võrgusegmenti

SYS.1.9.M9 Terminaliserveri kasutajate teadlikkuse tõstmine

Evitus

SYS.1.9.M3 Rollide ja volituste haldus terminaliserveris

SYS.1.9.M4 Terminaliserveri turvaline konfiguratsioon

SYS.1.9.M9 Terminaliserveri kasutajate teadlikkuse tõstmine

Käitus

SYS.1.9.M7 Terminaliserveri juurdepääsu turve

SYS.1.9.M8 Terminaliserveri turvaline määramine võrgusegmenti

SYS.1.9.M10 Keskne terminaliserveri identiteedi- ja volituste haldus

SYS.1.9.M11 Terminaliserveri turvalised kasutajaprofiilid

SYS.1.9.M12 Jõudeolekus seansside automaatne lõpetamine

SYS.1.9.M13 Terminaliserveri toimingute logimine

SYS.1.9.M14 Terminaliserveri seire

SYS.1.9.M15 Terminaliserveri tugevdamine (ingl hardening)

SYS.1.9.M16 Andmetihenduse optimeerimine

Lisanduvad kõrgmeetmed

SYS.1.9.M17 Andmeedastuse täiendav krüpteerimine

SYS.1.9.M18 Ainult õhukeste klientide kasutamine

SYS.1.9.M19 Terminaliserveri laiendatud seire

SYS.1.9.M20 Terminaliserverite jaotus kasutuseesmärgi või kasutajagrupi põhiselt

SYS.1.9.M21 Terminaliserverite kõrgkäideldavuse tagamine

SYS.1.9.M22 Andmete edastamise blokeerimine

3.2 Põhimeetmed

SYS.1.9.M1 Terminaliserveri turvanõuete kehtestamine

a. Organisatsioon on dokumenteerinud ja kehtestanud terminaliserveri turvanõuded. Turvanõuded käsitlevad vähemalt järgnevaid teemasid:
   - terminaliserveritesse installitav tarkvara;
   - rakendused, mis on lubatud läbi terminaliserveri kasutada;
   - turvanõuded klientidele või klienditarkvara kasutavatele klientarvutitele, sh füüsilise turbe nõuded;
   - võrguturve, sh lubatavad andmesideprotokollid ning nõuded kliendi võrgule;
   - klientide ja terminaliserverite vahelised krüpteerimismehhanismid ja autentimismeetodid;
   - failide ja muude andmete edastamine terminaliserveri protokolli kaudu lisaks ekraaniväljundile;
   - lisaks tavapäraste sisend- ja väljundseadmetele kliendiga täiendavalt ühendatavad välisseadmed.

SYS.1.9.M2 Terminaliserveri kasutuselevõtu kavandamine

a. On dokumenteeritud terminaliserveris käitatavatele rakendustele esitatavad funktsionaalsed nõuded.

b. Terminaliserveri rakendused on kooskõlas terminaliserveri turvanõuetega.

c. Terminaliserveri rakenduste toimimist on eelnevalt testitud.

d. On koostatud prognoos terminaliserveri kasutajate koguhulga ning samaaegsete kasutajate eeldatava arvu kohta terminaliserveri eeldatava elukaare ulatuses.

e. Tulenevalt eeldatavast kasutajate arvust ning terminaliserveris käitatavatele rakendustele esitatud nõuetest on määratud terminaliserveri minimaalsed jõudlusparameetrid (nt protsessori ja põhimälu osas).

f. Terminaliserveri riistvara, tarkvara ja käitatavate rakenduste valikul arvestatakse kokkulepitud teenusetaset ja samaaegsete terminaliserveri kasutajate eeldatavat hulka.

g. Terminaliserveri rakenduste litsentsiskeemid lubavad rakenduste kasutamist terminaliserverites.

SYS.1.9.M3 Rollide ja volituste haldus terminaliserveris

a. Ühiskasutatavaid kontosid võib terminaliserverites kasutada ainult juhul kui sellega ei rikuta sise-eeskirju või tarkvara litsentsitingimusi. Ühiskasutava konto kasutuselevõtuks on vajalik kirjalik ja põhjendatud otsus.

b. Terminaliserveris kasutatavatele rakendustele antud pääsuõigused vastavad eelnevalt määratletud terminaliserveri kasutajate rollidele ja volitustele.

c. Terminaliserveri seansside vaheline andmeside on lubatud ainult rakenduse funktsionaalsuse jaoks vajalikul määral.
d. Kõigi järgnevate õiguste vajalikkust on hoolikalt kaalutud:
    - rakenduste käitamine eeliskasutaja õigustes;
    - juurdepääs operatsioonisüsteemi spetsiifilistele funktsioonidele;
    - juurdepääs terminaliserveri failisüsteemile;
    - juurdepääs klientarvuti liidestele ja failisüsteemile;
    - juurdepääs terminaliserveri rakenduste käitamist võimaldavatele tugiteenustele;
    - failiedastus klientarvuti ja terminaliserveri vahel (nt kliendi juures printimiseks);
    - klientarvuti välisseadmete ühendamine.

SYS.1.9.M4 Terminaliserveri turvaline konfiguratsioon

a. Terminaliserveritele on kehtestatud ja dokumenteeritud rakenduste turva- ja funktsionaalsusnõuetest lähtuvad tüüpkonfiguratsioonid.
b. Terminaliserveri kasutuselevõtul on arvestatud riist- ja tarkvaratootjate soovitusi terminaliserveri turvaliseks konfigureerimiseks.
c. Terminaliserveri tüüpkonfiguratsioonis on arvestatud vähemalt järgmist:
    - rollid ja volitused;
    - krüpteerimine ja selle ulatus;
    - terminaliserveri andmevahetusprotokollid ja nende autentimisfunktsioonid;
    - terminaliserveri seansside vaheline andmevahetus;
    - andmevahetus terminaliserveri rakenduste ja terminaliserverist väljapoole jäävate rakenduste vahel;
    - andmevahetus terminaliserveri ja teiste serverite vahel.
d. Konfiguratsioonide asjakohasust ja nende korrektset rakendamist kontrollitakse regulaarselt.

SYS.1.9.M5 Klientide ja klienttarkvara plaanimine

a. On määratud, milline klienttarkvara on terminaliserverile juurdepääsuks lubatud ja kas sama tarkvara on võimalik kasutada teistes terminaliserverites.
b. On määratud, millistele tingimustele peavad kliendid vastama, et terminaliserveriga ühenduda. Arvestatakse vähemalt järgmist:
    - õhukeste klientide (ingl *thin client*) või paksude klientide (ingl *fat client*) kasutamine;
    - nõuded kliendi riistvarale;
    - kliendil kasutatavad operatsioonisüsteemid.

SYS.1.9.M6 Terminaliserveri võrgulahenduse kavandamine [arhitekt]

a. On kehtestatud nõuded andmesidevõrkudele, mille kaudu klient terminaliserveriga ühendub. Nõuetena on määratletud vähemalt järgnev:
    - eeldatav samaaegsete terminaliserveri seansside arv;
    - võrgu suutvus (ingl *network capacity*),

- suurim lubatav paketikadu (ingl *packet loss*);
- suurim lubatav pakettide edastushilistuse kõikumine (ingl *jitter*);
- suurim lubatav latentsusaeg (ingl *latency*).

SYS.1.9.M7 Terminaliserveri juurdepääsu turve

a. Terminaliserverisse on võimalik juurde pääseda ainult selleks otstarbeks lubatud võrkudest.

b. Andmesidekanalid on kaitstud krüpteeritud andmesideprotokolliga. Kui terminaliserveri protokollid ei võimalda piisaval turvatasemel krüpteerimist, kaitstakse andmesidekanaleid täiendavate võrguturbemeetmetega.

c. Kui kliendid ja terminaliserver suhtlevad ebapiisava usaldusväärsusega võrkude (nt avalike sidevõrkude) kaudu, on ühenduse loomisel nõutav nii klientide kui ka terminaliserveri vastastikune autentimine.

SYS.1.9.M8 Terminaliserveri turvaline määramine võrgusegmenti

a. Terminaliserver on paigutatud kas muudest eraldatud võrgusegmenti või terminaliserveri kliente sisaldavasse võrgusegmenti.

b. Terminaliserver on kättesaadav ainult määratud võrgusegmentidest.

c. Terminaliserveri abil ei ole võimalik mööda hiilida organisatsioonis kehtestatud võrkude eraldamise reeglitest.

SYS.1.9.M9 Terminaliserveri kasutajate teadlikkuse tõstmine

a. Kõiki terminaliserverite kasutajaid on terminaliserverite turvalise kasutamise osas koolitatud.

b. Terminaliserveri kasutajaid on koolitatud vähemalt järgmises osas:
   - terminaliserveri põhifunktsioonid;
   - sidekvaliteedi mõju terminaliserveri kasutatavusele;
   - andmete võimalikud ja lubatavad salvestuskohad;
   - andmevahetus kliendi ja terminaliserveri vahel (nt lõikepuhvri abil);
   - ressursitarbimise mõju teistele samaaegsetele kasutajatele;
   - rollid ja volitused terminaliserverile juurdepääsuks;
   - kasutajate autentimine terminaliserveri rakendustes;
   - seansi pikim lubatud kestus ja väljalogimise kord (sh kasutajate automaatne väljalogimine).

3.3 Standardmeetmed

SYS.1.9.M10 Keskne terminaliserveri identiteedi- ja volituste haldus

a. Terminaliserveri pääsuõiguste määratlemine ja andmine toimub läbi keskse haldussüsteemi.

SYS.1.9.M11 Terminaliserveri turvalised kasutajaprofiilid

a. Terminaliserveri kasutaja ei saa muuta kasutajakohaseid seadistusi (kasutajaprofiile) määral, mis võiks ohustada terminaliserveri turvalisust või piirata terminaliserveri kasutamist.

b. Kasutajaprofiili parameetrid on antud terminaliserveri kasutamiseks sobivad. Kui kasutatakse mitmeid terminaliservereid, talletatakse kasutajaprofiile keskses asukohas.

SYS.1.9.M12 Jõudeolekus seansside automaatne lõpetamine

a. Terminaliserveri jõudeolekus (e passiivsed) seansid lõpetatakse eelnevalt määratud aja möödudes automaatselt. Ajavahemik, mille möödudes jõudeolekus seanss lõpetatakse, määratakse sõltuvalt kasutajarühmast.

b. Seansi automaatsest lõpetamisest teavitatakse sellest mõjutatud isikuid.

c. Seansi lõpetamisel logitakse kasutaja terminaliserveri operatsioonisüsteemist automaatselt välja. Erandi moodustavad olukorrad, kus aktiivne seanss operatsioonisüsteemis on vajalik rakenduste jätkuvaks käitamiseks.

SYS.1.9.M13 Terminaliserveri toimingute logimine

a. Terminaliserverite puhul on määratud, millised sündmused edastatakse kesksesse logitaristusse (vt OPS.1.1.5 *Logimine).*

b. Terminaliserveritest logitakse vähemalt järgmised sündmused:

- kliendi välisseadme ühendamine terminaliserveri protokolliga;
- eelisõigustega kasutaja toimingud terminaliserveris;
- terminaliserveri teenuseid mõjutavad konfiguratsioonimuudatused.

SYS.1.9.M14 Terminaliserveri seire

a. Terminaliserver on hõlmatud kesksesse seiresse.

b. Seiratakse vähemalt järgmisi parameetreid:

- terminaliserveri ressursikasutus;
- terminaliserveri võrguliideste koormatus;
- võrgu läbilaskevõime (ingl *bandwidth*) ja terminaliserveri võrgukasutus;
- võrguühenduste latentsus, võttes arvesse kehtestatud nõudeid (vt. SYS.1.9.M6 *Terminaliserveri võrgulahenduse kavandamine*).

c. Seire tulemuste hindamiseks on terminaliserveri käideldavus- ja sooritusparameetrite läviväärtused eelnevalt määratletud. Läviväärtuste asjakohasust kontrollitakse regulaarselt.

SYS.1.9.M15 Terminaliserveri tugevdamine (ingl *hardening*)

a. Terminaliserveri mittevajalikud rakendused ja tarbetud operatsioonisüsteemi komponendid on eemaldatud. Kui mittevajalike komponentide eemaldamine pole võimalik, blokeeritakse nende käitamine.

b. Terminaliserveri seansi käigus on välisseadmete kasutamine on piiratud, lubatud on ainult vajalikud välisseadmed.

SYS.1.9.M16 Andmetihenduse optimeerimine

a. Andmete terminalserveri ja kliendi vahel ülekandmisel kasutatakse andmete tihendamiseks optimaalset taset. Seejuures on arvestatud nõudeid graafiliste elementide täpsuse, värvitruuduse ja ekraani kaadrisageduse osas.

3.4 Kõrgmeetmed

SYS.1.9.M17 Andmeedastuse täiendav krüpteerimine (C-I)

a. Kogu andmevahetus kliendi ja terminaliserveri vahel toimub läbi turvaliselt krüpteeritud andmevahetuskanalite.

SYS.1.9.M18 Ainult õhukeste klientide kasutamine (I-A)

a. Terminaliserveri klientidena kasutatakse ainult tootja poolt terminaliserveriga ühildavaks tunnistatud füüsilisi terminale, nn õhukesi kliente (ingl *thin client*).

SYS.1.9.M19 Terminaliserveri laiendatud seire (C-I-A)

a. Terminaliserveri logimise (vt SYS.1.9.M13 *Terminaliserveri toimingute logimine*) toimimist seiratakse pidevalt.

b. Terminaliserveri turvasündmuste logimine on liidestatud olemasoleva turvateabe ja -sündmuste halduse (ingl *security information and event management*, SIEM) süsteemiga.

c. Turvanõrkuste avastamiseks testitakse terminaliserverit regulaarselt.

SYS.1.9.M20 Terminaliserverite jaotus kasutuseesmärgi või kasutajagrupi põhiselt (C-I-A)

a. Organisatsiooni terminaliserverid on kasutuseesmärgi või kasutajagrupi põhiselt jaotatud mitmeteks, kitsast tööülesannet täitvateks terminaliserveriteks.

b. Konkreetse ülesande täitmiseks kohandatud terminaliserver on juurdepääsetav ainult volitatud kasutajatele.

SYS.1.9.M21 Terminaliserverite kõrgkäideldavuse tagamine (A)

a. Terminaliserveri olulised riistvarakomponendid ja kasutatavad võrguühendused on dubleeritud.

b. Organisatsioonis on olemas asendusseadmed terminaliserveri ning klientide asendamiseks.

SYS.1.9.M22 Andmete edastamise blokeerimine (I-A)

a. Terminaliserveri rakenduses kasutatavate andmete edastamine kliendile on blokeeritud.

b. Andmeedastus lõikepuhvri (ingl *clipboard*) kaudu on blokeeritud.

SYS.2: Klientarvutid

SYS.2.1 Klientarvuti üldiselt

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed klientarvutis töödeldavate andmete kaitseks (olenemata klientarvuti tüübist või selles kasutatavast operatsioonisüsteemist) ning suurendada teadlikkust selle seadmeklassi spetsiifilistest ohtudest.

„Klientarvuti üldiselt“ moodul käsitleb mistahes operatsioonisüsteemiga klientarvutit, mis on seotud konkreetse kasutajaga. Klientarvutis on üldjuhul üks administraatori- ja vähemalt üks kasutajakonto. Klientarvuti on enamasti osa „klient-server“ tüüpi IT-lahendusest.

1.2 Vastutus

„Klientarvuti üldiselt“ meetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Kasutaja, tehnikatalitus.

1.3 Piirangud

Klientarvuti levinud operatsioonisüsteemide kaitseks tuleb lisaks rakendada mooduligrupis SYS.2 *Klientarvutid* olevaid operatsioonisüsteemipõhised meetmed. Mobiilseadmete (nt nutitelefonid või tahvelarvutid) turbe meetmed on esitatud mooduligrupis SYS.3 *Mobiilseadmed*.

Klientarvuti andmevahetusliideseid (nt USB, Bluetooth, kohtvõrk või raadiokohtvõrk) käsitletakse asjakohastes moodulites (nt NET.2.2 *Raadiokohtvõrgu kasutamine).* Irdandmekandjate kasutamist käsitletakse moodulis SYS.4.5 *Irdandmekandjad.*

Klientarvuti kaitset kahjurvara eest käsitletakse moodulis OPS.1.1.4 *Kaitse kahjurprogrammide eest*. Klientarvuti logimise meetmed esitatakse moodulis OPS.1.1.5 *Logimine.*

2 Ohud

2.1 Kahjurprogrammid

Kahjurprogrammid aktiveeritakse enamasti varjatult ja ilma kasutaja nõusolekuta. Olenevalt teostusest tagavad kahjurprogrammid ründajale klientarvutis ulatuslikud andmevahetus- ja haldusvõimalused. Muuhulgas võimaldavad kahjurprogrammid juurdepääsu kasutaja paroolidele ja IT-süsteemidele, desaktiveerida kaitsetarkvara ja luurata kasutajaandmeid.

Klientarvutid on kahjurvara suhtes väga haavatavad. Kui kasutajad külastavad nakatunud veebisaite, avavad kahjuliku sisuga e-kirju või kopeerivad kahjurvara andmekandjate kaudu klientarvutisse, levib kahjurvara klientarvutist organisatsiooni arvutivõrku. Niiviisi on võimalik ründajal mööda pääseda keskselt rakendatud turvamehhanismidest, näiteks meiliserveri viirusetõrjest.

2.2 Andmekadu keskse andmetalletuse puudumise tõttu

Paljud kasutajad hoiavad oma faile arvuti lokaalsetes kataloogides, mitte keskses failiserveris. Riistvaratõrke korral võivad andmed kergesti kaotsi minna. Vaid lokaalses arvutis eksisteerinud andmete kaotsiminek võib põhjustada peale tööseisaku ka klientide ja partnerite usalduse kaotust.

Kui olulisi andmeid talletatakse üksnes lokaalselt, puudub teistel kasutajatel andmetele juurdepääs (nt puhkuse või haiguse korral asendamiseks). Kui klientarvutit kontrollib ründaja, võib ta organisatsiooni jaoks olulised andmed kustutada või andmeid manipuleerida.

Kui kesksesse andmehoidlasse salvestatud andmetest tehakse kohalikke koopiaid, mida töödeldakse klientarvutis, võib tekkida probleem andmeterviklusega. Pole kindel, kus asuvad õiged andmed.

2.3 Väärkasutusest tingitud riistvaratõrked

Kasutajad võivad oma arvutit tahtlikult või hooletusest kahjustada (arvuti laualt maha tõmmata, klaviatuuri peale vedelikke valada jne). Sageli tekib kahjustusest riistvararike, mille tõttu ei saa klientarvutit ajutiselt kasutada. Kui vigastada saab ka kõvaketas, ei pruugi enne riistvaratõrget klientarvutis talletatud andmed olla taastatavad. Kui riistvaratõrge juhtub töötaja reisil oleku ajal, on võimalik normaalset tööd jätkata alles pärast naasmist.

2.4 Infotehnoloogia lubamatu kasutamine

Arvutile juurdepääsu kaitsmine üksnes kasutajanime ja parooli abil ei kaitse, kui parooli on võimalik hõlpsalt ära arvata või teada saada üle õla piilumise (ingl *shoulder surfing*) abil.

Kui arvuti juurest lahkudes ei aktiveeri kasutaja ekraanilukku, on võimalik arvutit lubamatult kasutada isegi lühiajalise äraoleku korral.

2.5 Tarbetute rakenduste ja operatsioonisüsteemi komponentide installimine

Operatsioonisüsteemi installimisel on enamasti võimalik valida, millised operatsioonisüsteemi lisamoodulid installitakse. Praktikas tehakse enamasti operatsioonisüsteemi tüüpinstall, mis laeb klientarvutisse lisaks vajalikele ka palju tarbetuid komponente. Mida rohkem rakendusi on arvutisse installitud, seda suurem on varjatud nõrkuste esinemise tõenäosus. Kui tarkvaral on liiga vähe kasutajaid, siis tootja ei saa turvavigade kohta piisavalt tagasisidet ja need jäävad kõrvaldamata. Kui rakendusel tootjapoolset tuge enam pole, siis võib eeldada, et aja jooksul kogunenud turvanõrkused on tegelikult parandamata ja et selline rakendus on ebaturvaline.

2.6 Pealtkuulamine arvutimikrofoni ja -kaameraga

Paljud klientarvutid on varustatud arvutimikrofoni ja kaameraga. Neid aktiveerida võivad ka kõik vastavat pääsuõigust omavad rakendused (nt personaalsed digitaalsed assistendid). Võrgustatud süsteemide puhul on võimalik arvutimikrofoni ja kaamerat juhtida ka kaugelt. Ründaja võib klientarvuti mikrofoni ja kaamerat kasutada vestluste pealtkuulamiseks või nõupidamiste märkamatuks salvestamiseks.

2.7 Seadmete ja süsteemide puudulik haldus

Klientarvuti operatsioonisüsteemi või rakenduste konfigureerimisvead vähendavad klientarvuti turvalisust. Konfigureerimisviga võib mõjutada klientarvuti funktsioneerimist. Lisaks tekib oht, et konfigureerimisvea tulemusel võib juurdepääsu arvutile saada selleks volitamata isik.

Ka seadmete, IT-süsteemide ja rakenduste lubamatu või mittenõuetekohane kasutamine võib turvalisust vähendada, eriti siis kui kasutaja ignoreerib turvameetmeid (nt kui kasutatakse liiga lihtsaid paroole).

3 Meetmed

3.1 Elutsükkel

Kavandamine

SYS.2.1.M9 Klientarvuti turvalise kasutamise juhend

SYS.2.1.M10 Klientarvutite kasutuselevõtu kava

Soetamine

SYS.2.1.M11 Klientarvuti hankimise kord

Evitus

SYS.2.1.M8 Buutimise turve
SYS.2.1.M13 Piiratud juurdepääs täitmiskeskkonda
SYS.2.1.M15 Klientarvuti turvaline install ja seadistus
SYS.2.1.M16 Tarbetute komponentide ja kontode desaktiveerimine
SYS.2.1.M21 Arvutimikrofoni ja -kaamera kasutamise kord
SYS.2.1.M23 Klient-server-teenuste eelistamine
SYS.2.1.M24 Väliste andmekandjate kasutamise piiramine
SYS.2.1.M26 Rakenduste turvaline käitus
SYS.2.1.M30 Klientarvuti etaloninstall
SYS.2.1.M43 Klientarvuti lokaalsed turvaseaded
SYS.2.1.M44 Keskne klientarvutite turvaseadete haldus

Käitus

SYS.2.1.M1 Kasutajate turvaline autentimine
SYS.2.1.M3 Uuendite automaatpaigaldus
SYS.2.1.M6 Kahjurvaratõrje tarkvara
SYS.2.1.M18 Krüptoprotokollide kasutamine andmesides
SYS.2.1.M20 Haldusprotseduuride turve
SYS.2.1.M29 Klientarvutite seire
SYS.2.1.M34 Turvakriitiliste rakenduste kapseldamine
SYS.2.1.M42 Pilve- ja võrgufunktsioonide kasutamine

Kõrvaldamine

SYS.2.1.M27 Klientarvuti kõrvaldamise kord

Lisanduvad kõrgmeetmed

SYS.2.1.M28 Klientarvuti sisu krüpteerimine
SYS.2.1.M31 Lokaalne paketifilter
SYS.2.1.M32 Lisameetmed rünnete tõrjeks
SYS.2.1.M33 Rakenduste käitamise tõkestamine
SYS.2.1.M35 Juursertifikaatide aktiivne haldus
SYS.2.1.M36 Funktsiooni *SecureBoot* ja mooduli TPM rakendamine
SYS.2.1.M37 Mitmikautentimise kasutamine
SYS.2.1.M38 Integreerimine avariivalmendusega
SYS.2.1.M39 Katkematu ja stabiilne toide
SYS.2.1.M40 Hooldusdokumentatsioon
SYS.2.1.M41 Klientarvuti kõvaketta salvestusruumi piiramine

SYS.2.1.M45 Klientarvuti laiendatud logimine

3.2 Põhimeetmed

SYS.2.1.M1 Kasutajate turvaline autentimine [kasutaja]

a. Klientarvutit on võimalik kasutada ainult end nõuetekohaselt autentinud kasutajal.

b. Mistahes tegevuse puhul klientarvutis on võimalik tuvastada tegevuse sooritaja.

c. Autentimisandmeid (nt parooli) muuta saab üksnes selleks volitatud kasutaja.

d. Kasutaja eemaloleku ajaks lukustab kasutaja arvuti juurest lahkudes ekraani. Ekraanilukk käivitub kasutaja poolt käsitsi aktiveerituna või automaatselt pärast ettemääratud ajavahemikku. Ajavahemiku pikkus sõltub arvutikasutaja tööspetsiifikast. Ekraaniluku avamine on võimalik vaid kasutaja autentimisega.

e. Pikema eemaloleku puhul logib kasutaja end klientarvutist välja või sulgeb arvuti.

SYS.2.1.M3 Uuendite automaatpaigaldus

a. Klientarvuti operatsioonisüsteemis ja tüüptarkvaras on aktiveeritud uuendite (ingl *update*) automaatpaigaldus. Erandiks on need IT-süsteemid, kus uuendeid tuleb paigaldada käsitsi.

b. Automaatselt kontrollitakse uuendite saadaolekut vähemalt kord päevas.

c. Tootja avalikust uuendusserverist uuendite laadimisel kontrollitakse uuendusserveri autentsust ja uuenduspakettide terviklust.

d. Uuendite halduseks kasutatakse organisatsioonisisest uuendusserverit (nt *Windows Server Update Services*, WSUS).

e. Mobiilsed seadmed võivad uuendeid saada nii organisatsiooni uuendusserverist kui tootja avalikust uuendusserverist.

f. Vajadusel on võimalik klientarvutis taastada uuendamise eelne tarkvaraseis.

SYS.2.1.M6 Kahjurvaratõrje tarkvara

a. Klientarvutid on varustatud aktiveeritud kahjurvaratõrje tarkvaraga.

b. Erandjuhud, kui kahjurvaratõrje rakendust klientarvutisse ei paigaldata, on põhjendatud ja dokumenteeritud.

c. Kahjurvaratõrje rakendus kontrollib faile nende avamisel. Edastatavaid ja vastuvõetavaid faile kontrollitakse automaatselt kohe enne väljasaatmist ja kohe pärast vastuvõtmist.

d. Kasutaja ei saa klientarvuti kahjurvaratõrje rakendust desaktiveerida ega muuta selle konfiguratsiooni.

e. Kahjurprogrammiga nakatunud klientarvuti eemaldatakse võrgust.

SYS.2.1.M8 Buutimise turve

a. Klientarvuti alglaadimine (buutimine) on manipulatsioonide eest kaitstud.

b. On määratud, millistelt andmekandjatelt on buutimine lubatud. Klientarvutit buutida sisemistelt optilistelt draividelt ja välistelt salvestuskandjatelt on lubatud ainult klientarvutite halduritele.

c. Automaatkäivitus välistelt andmekandjatelt on desaktiveeritud.

d. Buutimise seadeid põhivaras saavad muuta ainult haldajad. Juurdepääs püsivara konfigureerimisliidesele on kaitstud vähemalt parooliga.

e. Püsivaras on kõik tarbetud funktsioonid desaktiveeritud.

f. UEFI püsivaraga klientarvutites on aktiveeritud valik *SecureBoot*.

SYS.2.1.M9 Klientarvuti turvalise kasutamise juhend

a. Organisatsiooni üldise turvapoliitika alusel on kehtestatud klientarvutite kaitsetarbele vastav klientarvuti turvalise kasutamise juhend.

b. Klientarvuti turvalise kasutamise juhendis on turvalisus (funktsioonide ja õiguste piiramine) ja kasutusmugavus tasakaalus.

c. Klientarvuti turvapoliitikaga on määratud vähemalt alljärgnev:
   - kasutajate õigused ja kohustused arvuti igapäevasel kasutamisel;
   - haldurite õigused ja piirangud;
   - installimise kord ja aluskonfiguratsioon;
   - pääsu reguleerimine ja autentimine;
   - andmevarundus;
   - võrguühendused ja võrguteenused;
   - logimine.

d. Klientarvuti turvalise kasutamise juhendit järgivad kõik klientarvutite hankimise, halduse ja kasutamisega seotud töötajad.

e. Juhendi järgimist kontrollitakse regulaarselt. Kontrolli tulemused dokumenteeritakse.

SYS.2.1.M42 Pilve- ja võrgufunktsioonide kasutamine

a. Klientarvutis on aktiveeritud ainult vajalikud pilve- ja võrgufunktsioonid. Tarbetud pilvepõhised funktsioonid on desaktiveeritud või blokeeritud.

b. Klientarvutites lubatavad pilve- ja võrgufunktsioonid on dokumenteeritud.

c. Klientarvuti tüüpseadistus on vastavuses organisatsiooni infoturbe- ja andmekaitsenõuetega.

3.3 Standardmeetmed

SYS.2.1.M10 Klientarvutite kasutuselevõtu kava

a. Klientarvutite profileerimiseks, turvaliseks rakendamiseks ja käituseks on koostatud klientarvutite kasutuselevõtu kava.

b. Kasutuselevõtu kavas on arvestatud alljärgnevaid aspekte:
   - klientarvuti eesmärk ja ülesanded;
   - nõuded riistvarale (protsessor, põhimälu, kettamaht, võrguliidesed jne);
   - seosed ja ühilduvus olemasolevate süsteemide ja andmetega;
   - operatsioonisüsteem ja failisüsteem;
   - kaitsetarve ja turvamehhanismid;
   - käideldavusnõuded;
   - haldus ja hooldus.

c. Vajadusel on koostatud rohkem kui üks arvutiprofiil (nt üldine bürooarvuti, sülearvuti, halduri arvuti).

d. Kavandamisfaasis tehtud otsused on dokumenteeritud.

SYS.2.1.M11 Klientarvuti hankimise kord

a. Hankimisel arvestatakse klientarvuti kasutuselevõtu kavas kirjeldatud arvutiprofiile.

b. Reeglina hangitakse võimalikult palju klientarvuteid samalt tootjalt ja sarnase riistvaraplatvormiga.

c. Klientarvuti riistvara ja operatsioonisüsteemi tootjad ja hoolduspartnerid tagavad varuosade ja turvauuendite toe kogu plaanitud klientarvuti kasutusaja vältel.

d. Hangitavad klientarvutid on turvalise keskhalduse tarbeks varustatud konfigureeritava püsivaraliidese (UEFI) ja integreeritud TPM (Trusted Platform Module) kiibiga.

SYS.2.1.M13 Piiratud juurdepääs täitmiskeskkonda

a. Operatsioonisüsteemis tavakasutajale mittenähtav täitmiskeskkond (salvestuspiirkonnad, püsivara alad, ingl *executable space*), on tavakasutajale juurdepääsematu.

b. Täitmiskeskkondades programmikoodi käivitamine on võimalik ainult vastava haldusõiguse olemasolul.

c. BIOS-i või UEFI püsivara seaded on lubamatute muudatuste eest parooliga kaitstud.

SYS.2.1.M15 Klientarvuti turvaline install ja seadistus

a. Enne installi on koostatud ammendav nimekiri operatsioonisüsteemi komponentidest, rakendustest ja utiliitidest, mis klientarvutisse paigaldatakse.

b. Installida tohivad ainult selleks volitatud haldurid või lepinguga määratud välised teenuseandjad.

c. Klientarvutite seadistamiseks on koostatud ja dokumenteeritud turvaline aluskonfiguratsioon. Aluskonfiguratsioon sisaldab vähemalt järgmisi aspekte:

- haldusõigustega kontod;
- süsteemikataloogid- ja failid;
- kasutajakontod ja -kataloogid;
- võrkupääs;
- lokaalsed turvafunktsioonid (nt paketifilter);
- seirefunktsioonid (sh kasutusinfo tootjale edastamise („Phone Home“) funktsioonid).

d. Installimise ja konfigureerimise protseduur on dokumenteeritud selliselt, et pädev kolmas isik saaks dokumentatsioonist juhindudes installimise ja konfigureerimisega iseseisvalt hakkama.

e. Installimise ja konfigureerimise dokumentatsioon on kaitstud lubamatute muudatuste eest ning on kättesaadav ka avariiolukorras.

SYS.2.1.M16 Tarbetute komponentide ja kontode desaktiveerimine

a. On olemas ajakohastatud ülevaade, millised operatsioonisüsteemi komponendid ning rakendused on klientarvutites paigaldatud ja aktiveeritud.

b. Tarbetud moodulid, programmid, teenused, kasutajakontod ja liidesed on desaktiveeritud või desinstallitud.

c. Tarbetud käigukeskkonnad (ingl *runtime environment*), interpretaatorid ja kompilaatorid on desinstallitud.

d. Tarbetute komponentide desaktiveerimise otsused on dokumenteeritud.

SYS.2.1.M18 Krüptoprotokollide kasutamine andmesides

a. Klientarvuti sideseanside kaitsmiseks kasutatakse seal kus võimalik krüpteerimist.
b. Klientarvutites kasutatavad krüptoalgoritmid ja võtmepikkused on ajakohased (nt TLS v1.3) ja vastavad moodulile CON.1 *Krüptokontseptsioon*.
c. Uued sertifikaadid aktiveeritakse alles pärast sertifikaadi autentsuse ja tervikluse kontrolli.
d. Rakendusprogrammid (nt brauserid ja meilikliendid) valideerivad asjassepuutuvaid sertifikaate.

SYS.2.1.M20 Haldusprotseduuride turve

a. Klientarvuti tavapäraste haldustööde jaoks on koostatud haldusjuhis, mis hõlmab vähemalt järgmist:
   - kasutajate loomine ja desaktiveerimine;
   - rakenduste installimine ja desinstallimine;
   - turvauuendite ja turbepaikade paigaldamine;
   - uute rakenduste paigaldamine;
   - regulaarne tervikluse kontroll.
b. On rakendatud klientarvutite haldusviisile (lokaalselt, kaugjuurdepääsuga või kesksete haldusvahenditega) sobivad turvameetmed.
c. Kaughalduse andmesideks kasutatakse turvalisi protokolle.

SYS.2.1.M21 Arvutimikrofoni ja -kaamera kasutamise kord

a. Klientarvuti mikrofoni ja kaamera kasutamiseks on kehtestatud kord.
b. Klientarvuti mikrofoni ja kaamerat ei kasutata ilma kasutaja nõusolekuta.
c. Kui mikrofoni ja kaamera kasutamine pole lubatud, on kaamera füüsiliselt välja lülitatud või kinni kaetud ning mikrofon desaktiveeritud.
d. Konfidentsiaalse nõupidamise ajal on ruumis arvutite mikrofonid ja kaamerad välja lülitatud.

SYS.2.1.M23 Klient-server teenuste eelistamine

a. Andmevahetuseks kohtvõrgu piires kasutatakse võimalusel klient-server arhitektuuril põhinevaid teenuseid ja rakendusi.
b. Kui klientarvutite otsesuhtlus (ingl *peer-to-peer communication*) osutub siiski vajalikuks (nt VoIP sideteenuse puhul), siis on lubatavad erandid määratletud.
c. Klientarvutite vaheline otsesuhtlus on võimalik ainult kohtvõrgus.

SYS.2.1.M24 Väliste andmekandjate kasutamise piiramine

a. Klientarvutiga tohib ühendada ainult lubatud andmekandjaid. Näiteks võib andmete lugemis- ja kirjutusõigus olla lubatud üksnes kindlate krüptovõtmetega krüpteeritud mobiilsetele andmekandjatele (vt CON.9 *Teabevahetus*).
b. Võimalusel kasutatakse klientarvuteid, millel draivide (nt CD/DVD kirjutaja, mälukaardiluger) ja välisliideste vähendamisega on piiratud lokaalsed andmevahetusvõimalused.

c. Klientarvutite BIOS-is või UEFI-s on välistelt andmekandjatelt buutimine blokeeritud.

d. Andmekandja sisu automaatkäivitus või -esitus on blokeeritud.

SYS.2.1.M26 Rakenduste turvaline käitus

a. Rakenduste nõrkuste ärakasutamise takistamiseks on operatsioonisüsteemis aktiveeritud ja rakendustes kasutusel ASLR (*Address Space Layout Randomization*, ASLR), DEP (*Data Execution Prevention*, DEP) ja NX (*No-Execute*, NX) turvamehhanismid.

b. Operatsioonisüsteemi tuuma (ing *kernel*) ja teekide (ingl *library*) turvafunktsioonid on aktiveeritud.

SYS.2.1.M27 Klientarvuti kõrvaldamise kord

a. Enne klientarvuti kasutuselt kõrvaldamist on olulised andmed varundatud ja kõrvaldamisele määratud klientarvutist andmed kustutatud.

b. On olemas ajakohane dokumenteeritud ülevaade IT-süsteemides talletatud andmetest ja andmete asukohtadest.

c. Klientarvuti kõrvaldamiseks koostatakse alati kontroll-loend, mis määrab,

- millised andmed tuleb enne arvuti kõrvaldamist varundada või arhiveerida ja kuidas;
- millised kõrvaldatava arvutiga seotud õigused, viited ja kirjed tuleb kõrvaldada;
- millised jääkandmed ja varundatud andmed tuleb kustutada ja kuidas.

SYS.2.1.M29 Klientarvutite seire

a. Klientarvuti logid talletatakse kesksesse logiserverisse. Klientarvutid on lülitatud kesksesse seiresüsteemi.

b. Klientarvutite olekut ja töövõimet jälgitakse pidevalt.

c. Klientarvutite tõrgetest ja määratud piirnäitajate ületamisest teavitatakse haldureid.

SYS.2.1.M30 Klientarvuti etaloninstall

a. Klientarvutite jaoks on loodud etaloninstall, mida kasutatakse klientarvutite installimise ja taasinstallimise lihtsustamiseks ja automatiseerimiseks. Installimise käigus kloonitakse sobivalt eelkonfigureeritud etaloninstall klientarvutisse.

b. Etaloninstall sisaldab kõiki konfiguratsioonimuudatusi, uuendeid ja turvapaiku.

c. Etaloninstalli on enne selle klientarvutisse paigaldamist põhjalikult testitud (sh arvuti kasutajate poolt).

d. Testimiseks on koostatud tüüpstsenaariumid, testitulemused dokumenteeritakse.

SYS.2.1.M34 Turvakriitiliste rakenduste kapseldamine

a. Rakenduste turvakriitilised andmed (nt autentimis- ja sertifikaadiandmed) on teiste rakenduste ja operatsioonisüsteemi komponentide juurdepääsu eest kapseldatud (ingl *encapsulation*) või isoleeritud omaette täitmiskeskonda (ingl *execution environment).*

b. Rakendusi, mis töötlevad ebaturvalistest allikatest pärit andmeid (nt veebibrauserid), käitatakse operatsioonisüsteemist lahutatud täitmiskeskkonnas.

SYS.2.1.M43 Klientarvuti lokaalsed turvaseaded

a. Klientarvuti turvaseadeid on enne rakendamist põhjalikult testitud ja kontrollitud.

b. Lokaalsed turvaseaded on konfigureeritud lähtudes klientarvutis talletatud andmete kaitsetarbest.

c. Lokaalsed turvaseaded on vastavuses üldise turvapoliitika ja teiste organisatsioonis rakendavate turvanõuetega. Lahknevused turvapoliitikast on põhjendatud ja dokumenteeritud.

d. Tarbetud rakendused ja mittevajalikud operatsioonisüsteemi komponendid on desaktiveeritud.

SYS.2.1.M44 Keskne klientarvutite turvaseadete haldus

a. Klientarvutite turvaseadeid hallatakse keskselt ning vastavuses organisatsiooni poolt kehtestatud kordadega.

b. Lokaalselt hallatud konfigureerimisparameetrid on põhjendatud ja infoturbejuhiga kooskõlastatud.

3.4 Kõrgmeetmed

SYS.2.1.M28 Klientarvuti sisu krüpteerimine (C)

a. Klientarvutis talletatakse konfidentsiaalsed andmed ainult krüpteeritud kujul. Soovituslik on krüpteerida terve kõvaketas.

b. Krüpteerimise konfiguratsioon ning krüpteerimise ja dekrüpteerimise protsessid on dokumenteeritud.

c. Krüpteeritud andmetele on juurdepääs üksnes pääsuõigusega isikutel.

d. Krüpteeritud failide, kataloogide ja andmekandjate varundamise järgselt pole andmed avatekstina loetavad.

e. Krüptovõti ei ole klientarvutis avateksti kujul salvestatud.

f. Kasutaja teavad, kuidas tegutseda autentimisvahendi (nt parool, PIN-kood, identsustõend) paljastumise korral.

SYS.2.1.M31 Lokaalne paketifilter (C-I-A)

a. Peale keskse turvalüüsi (ingl *security gateway*) on klientarvutites aktiveeritud lokaalsed paketifiltrid (ingl *packet filter*).

b. Lokaalne paketifilter töötab valge nimekirja (ingl *whitelisting*) alusel.

c. Pärast lokaalse paketifiltri aktiveerimist või reeglimuudatuste tegemist kontrollitakse teenuste ja portide olekut.

SYS.2.1.M32 Lisameetmed rünnete tõrjeks (C-I-A)

a. Kui olemasolevates operatsioonisüsteemides või turvatoodetes puudub piisav funktsionaalsus, kasutatakse täiendavaid turvatooteid vähemalt järgneva funktsionaalsuse tugevdamiseks:
   - halduri ja kasutaja rollide lahutamine;
   - õiguste haldus;
   - autentimine;
   - logimine ja seire.

b. Kui tehnilised meetmed pole piisavad, rakendatakse täiendavaid korralduslikke meetmeid (nt automaatse ekraaniluku puudumisel on kasutaja kohustatud seda aktiveerima käsitsi).

SYS.2.1.M33 Rakenduste käitamise tõkestamine (C-I)

a. Klientarvutis võimalik käitada ainult lubatud programme ja skripte. Lubatud programmide nimekiri on võimalikult piiratud.

b. Lubatud programmide nimekiri põhineb sertifikaadi kontrollil, räside (ingl *hash*) võrdlemisel ja/või lubatud kataloogiteedel.

SYS.2.1.M35 Juursertifikaatide aktiivne haldus (C-I)

a. Klientarvuti ettevalmistamisel dokumenteeritakse klientarvuti tööks vajalikud juursertifikaadid.

b. Kontrollitakse regulaarselt, ega klientarvutisse pole lisandunud muid juursertifikaate ning otsustatakse, kas kasutatavad juursertifikaadid vastavad endiselt organisatsiooni nõuetele.

c. Juursertifikaatide kontrollimisel arvestatakse kõikide sertifikaadihoidlatega (nt UEFI sertifikaadihoidla, veebibrauserite sertifikaadihoidlad).

SYS.2.1.M36 Funktsiooni *SecureBoot* ja mooduli TPM rakendamine (C-I)

a. UEFI-t kasutavates süsteemides on eellaadur (ingl *boot loader*), tuum (ingl *kernel*) ja kõik vajalikud püsivarakomponendid signeeritud turvalise võtmega.

b. Tarbetud võtmed on eemaldatud.

c. Kui moodulit TPM (*Trusted Platform Module*, TPM) ei kasutata, on see desaktiveeritud.

SYS.2.1.M37 Mitmikautentimise kasutamine (C)

a. Suurema kaitsetarbe korral kasutatakse klientarvutisse sisselogimiseks mitmikautentimist (ingl *multifactor authentication*).

SYS.2.1.M38 Integreerimine avariivalmendusega (A)

a. Klientarvuti avariivalmendus on integreeritud organisatsiooni üldise avariihaldusega (vt DER.4. *Avariihaldus*).

b. Klientarvutite andmevarundus on osa organisatsiooni üldisest andmevarunduse kontseptsioonist (vt CON.3 *Andmevarunduse kontseptsioon*).

c. Klientarvuti taasteprioriteet on määratud klientarvutit kasutava äriprotsessi prioriteedi põhjal.

d. On koostatud klientarvuti avariikava, milles on määratud järgnev:
   - varuosade olemasolu või nende saamine hooldelepingute raames;
   - taastekäivitustrigerid ja taastamise prioriteedid;
   - paroolide ja krüptovõtmete asukohad;
   - taasteplaan (süsteemi järkjärgulise taastamise protseduuri);
   - süsteemi konfiguratsiooni dokumentatsioon;
   - taasteks vajalik lisatarkvara ja -riistvara.

e. Taastamise võimaldamiseks on komplekteeritud ja turvaliselt hoiustatud varuarvuti töökorras riistvara, tarkvara ja andmestikuga.

f. Varuarvutit on pärast süsteemi muudatusi uuendatud ja testitud.

SYS.2.1.M39 Katkematu ja stabiilne toide [tehnikatalitus] (A)

a. Suurema käideldavustarbe korral võetakse klientarvuti toide läbi puhvertoiteallika (UPS-i), mis tagab klientarvuti elektrivarustuse vähemalt rakenduste nõuetekohaseks sulgemiseks vajamineva aja jooksul.
b. Puhvertoiteallika koormatust ja toitetoe kestvuse piisavust kontrollitakse regulaarselt ning täiendavalt toite tarbijate lisandumisel.
c. Klientarvutid ja puhvertoiteallikad on kaitstud liigpinge ja pingehäiringute eest.

SYS.2.1.M40 Hooldusdokumentatsioon (A)

a. Klientarvuti hooldustööd on selgelt dokumenteeritud. Dokumentatsioon sisaldab, kes ja millal töid teostas ning mis oli hooldustöö sisu.
b. Kõik konfiguratsiooni muudatused ja turvalisust puudutavad toimingud (nt kõvaketta vahetus) on dokumenteeritud.
c. Kui hooldustöid on võimalik automaatselt logida, siis dokumenteeritakse need automaatselt.
d. Hooldusdokumentatsioon on kaitstud lubamatu juurdepääsu eest.

SYS.2.1.M41 Klientarvuti kõvaketta salvestusruumi piiramine (A)

a. Salvestusruumi peatse täitumise eest hoiatavad mehhanismid on aktiveeritud.
b. Vajadusel on salvestusruumile seatud piirangud (ingl *disk quota*).

SYS.2.1.M45 Klientarvuti laiendatud logimine (C-I-A)

a. Klientarvutis logitakse ka infoturbega otseselt mitteseonduvad kasutajategevused.

SYS.2.2: Windows kliendid

SYS.2.2.3 Windows 10 ja Windows 11

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed operatsioonisüsteeme Windows 10 ja Windows 11 kasutavates klientarvutites (klientides) olevate andmete kaitseks. Neid operatsioonisüsteeme iseloomustab suurem integreeritus Microsofti serveritaristu ja pilvteenustega.

1.2 Vastutus

Windows 10 ja Windows 11 klientarvutitele esitatud turvameetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Kasutaja.

1.3 Piirangud

Selle mooduli Windows 10 ja Windows 11 spetsiifilised meetmed täiendavad moodulis „SYS.2.1 *Klientarvuti üldiselt“* esitatud meetmeid.

Windowsi klientidele kohalduvad lisaks rakendusekohaste moodulite meetmeid, näiteks „APP.1.1 *Kontoritarkvara“* või APP.1.2 *Veebibrauser*. Windowsi domeeni ühendatud klientide puhul rakendatakse meetmeid moodulist APP.2.2 *Active Directory*.

2 Ohud

2.1 Windowsile suunatud kahjurprogrammid

Tänu Windowsi operatsioonisüsteemide laialdasele levikule eksisteerib ka palju Windows 10 või Windows 11 kasutajate vastu suunatud kahjurprogramme. Windows operatsioonisüsteemi põlvkondade vaheline tagasiühilduvus suurendab lubamatu juurdepääsu ohtu veelgi. Kahjurprogrammid võivad ründajale anda ulatuslikke võimalusi klientarvuti kaugjuhtimiseks, paroolide paljastamiseks ja andmete luureks. Suure kahju võib kaasa tuua andmekadu või andmete võltsimine. Ka ründe tagajärjel tekkinud mainekahju võib olla märkimisväärne.

2.2 Integreeritud pilvefunktsioonid

Windows 10 ja Windows 11 sisaldavad arvukalt funktsioone, mis võimaldavad Microsofti pilvteenuste abil andmeid arhiveerida ja sünkroonida. Pole välistatud, et pilvteenuseid kasutatakse organisatsiooni jaoks oluliste andmete või isikuandmete töötlemiseks ja talletamiseks välisriigis asuvas serveris.

Kui kasutaja logib oma Microsofti kontoga sisse uude seadmesse, siis määratakse tema kasutatavad Microsofti pilvteenused seadmes automaatselt. Nii tekib oht, et organisatsiooni andmed sünkroonitakse töötajate isiklikesse seadmetesse.

Samuti pakub Windows vaikeseadena võimalust varundada BitLockeri taastevõti Microsofti konto kaudu pilve. Nii võivad kaitset vajavale teabele juurdepääsu saada volitamata isikud.

2.3 Tarkvara ühilduvusprobleemid

Kuigi Microsoft tagab üldiselt Windowsi varasemates versioonides töötava tarkvara ühilduvuse operatsioonisüsteemi uuemate versioonidega, võib Windows 10 ja Windows 11 puhul esineda ühilduvusprobleeme. Seetõttu vana tarkvara enam klientarvutis kasutada ei saa või on see võimalik ainult piiratud ulatuses. Ühildusprobleeme võivad põhjustada uued turvafunktsioonid, nagu kasutajakonto kontroll või operatsioonisüsteemi 64-bitise versioonis tuuma kaitse funktsioon (*Kernel Patch Guard*). Vanemate seadmete puhul võivad tekkida probleemid signeeritud draiveritega (ingl *driver*), mida ei pruugi vanade riistvarakomponentide jaoks enam saadaval olla.

2.4 Windows telemeetriafunktsioonide väärkasutus

Windows 10 ja Windows 11 saadavad Microsoftile diagnostikaandmeid. Lisaks võib Microsoft integreeritud telemeetriateenuse abil kliendile ka ise päringuid saata. Windowsi vaikeseadistuse korral on lubatud telemeetriatase, mis näiteks võimaldab juurdepääsu klientarvuti registrile ja teatud diagnostikavahendite rakendamist. Sellega kaasneb oht, et diagnostika- või telemeetriaandmetes sisalduvad tundlikud andmed satuvad volitamata isikute kätte.

2.5 Raskendatud intsidendikäsitlus VSM (Virtual Secure Mode) kasutamisel

Kui Windows Enterprise versioonides kasutatakse andmete kaitsmiseks ja juurdepääsu tõkestamiseks VSM (Virtual Secure Mode) virtualiseerimislahendust, halvenevad võimalused arvutiprotsesside analüüsiks. VSM ja IUM (Isolated User Mode) abil kapseldatud protsesside andmetest ei saa IT-kriminalistika (ingl *computer forensics*) eesmärgil teha hilisemaks analüüsiks mälutõmmiseid (ingl *memory dump*), mistõttu on IT-intsidendi käsitlemine raskendatud.

3 Meetmed

3.1 Elutsükkel

Kavandamine

SYS.2.2.3.M1 Microsofti pilvteenuste rakendamise kava

Soetamine

SYS.2.2.3.M2 Sobiva Windowsi versiooni valimine

Evitus

SYS.2.2.3.M4 Telemeetria andmekaitseseaded

SYS.2.2.3.M5 Windows klientarvuti kahjurvara tõrje

SYS.2.2.3.M9 Keskne autentimine

SYS.2.2.3.M12 Faili- ja kataloogiõiguste haldus

SYS.2.2.3.M13 Funktsiooni *SmartScreen* desaktiveerimine

SYS.2.2.3.M14 Digitaalse assistendi *Cortana* desaktiveerimine

SYS.2.2.3.M15 Windowsi sünkroonimismehhanismide desaktiveerimine

SYS.2.2.3.M16 *Microsoft Store* turvaline kasutus

SYS.2.2.3.M17 Automaatse sisselogimise keeld

SYS.2.2.3.M18 *Remote Assistance* kaugtoe turvaline rakendamine

SYS.2.2.3.M19 Kaughaldusvahendi RDP turvaline rakendamine

SYS.2.2.3.M20 UAC kasutamine eeliskontodega

Käitus

SYS.2.2.3.M6 Võrgukontode integreerimine

Lisanduvad kõrgmeetmed

SYS.2.2.3.M21 Krüpteeringuga failisüsteemi EFS kasutamine

SYS.2.2.3.M22 *Windows PowerShell*'i kasutamine

SYS.2.2.3.M23 Sisselogimisteabe lisaturve

SYS.2.2.3.M24 Viimase pöördumise ajatembelduse aktiveerimine

SYS.2.2.3.M25 Komponendi CUET kaugjuurdepääsufunktsioonide turvaline rakendamine

SYS.2.2.3.M26 VSM (Virtual Secure Mode) kasutamine

3.2 Põhimeetmed

SYS.2.2.3.M1 Microsofti pilvteenuste rakendamise kava

a. Windows klientarvutite hankimisel on otsustatud, milliseid Microsofti pilvteenuseid ja millises ulatuses on lubatud kasutada.

SYS.2.2.3.M2 Sobiva Windowsi versiooni valimine

a. Klientarvutitele Windowsi versiooni valikul on arvestatud IT strateegiat, klientarvutite hulka, klientarvutite kasutusotstarvet ja kaitsetarvet.

b. Hankekava alusel valitakse organisatsioonile sobiv tarkvara litsentsimudel ja uute versioonide kasutuselevõtu korraldus, nt SAC (Semi-Annual Channel*)* või LTSC (Long-Term Servicing Channel).

SYS.2.2.3.M4 Telemeetria andmekaitseseaded

a. Telemeetriateenuste andmete edastamine operatsioonisüsteemi tootjale on seadistuses piiratud. Windows 10 või Windows 11 Enterprise versiooni kasutamisel on telemeetria tase seadistatud valikväärtusele 0 (*Security*).

b. Kui klientarvuti telemeetriaseadistusi ei ole võimalik piirata, on andmete edastamine operatsioonisüsteemi tootjale blokeeritud võrgutaseme meetmetega (nt tulemüürireeglitega).

SYS.2.2.3.M5 Windows klientarvuti kahjurvara tõrje

a. Kui IT-süsteemi kaitsmiseks kahjurvaraga nakatumise eest ei ole kasutusele võetud samaväärseid või rangemaid meetmeid, on Windows klientarvutis aktiveeritud Microsofti kahjurvaratõrje (nt *Windows Defender*) komponendid.

SYS.2.2.3.M12 Faili- ja kataloogiõiguste haldus

a. Juurdepääs lokaalsetele ja kohtvõrgus asuvatele failidele ja kaustadele on antud vajadusepõhiselt ning lähtuvalt identiteedi ja õiguste halduse põhimõtetest (vt ORP.4 *Identiteedi ja õiguste haldus*).

b. Windows klientarvuti halduril on piisavad õigused haldustööde läbiviimiseks.

c. Kasutajale on antud kirjutusõigused ainult konkreetselt määratud failisüsteemi piirkonnas. Kasutajatel ei ole kirjutusõigust operatsioonisüsteemi ja rakenduste kaustades.

3.3 Standardmeetmed

SYS.2.2.3.M6 Võrgukontode integreerimine [kasutaja]

a. Kasutaja autentimine domeeni ja võimalusel ka rakendustesse toimub kataloogiteenuse abil.

b. Klientarvutisse lokaalse kontoga sisselogimise õigus on ainult halduritel.

c. Klientarvutisse sisselogimiseks ei kasutata veebipõhiseid identiteedihalduslahendusi (nt Google või Microsofti kontot).

SYS.2.2.3.M9 Keskne autentimine

a. Kerkseks autentimiseks kasutatakse Kerberost. Kui seda ei tehta, siis alternatiivina võib kasutada autentimisprotokolli NTLMv2.

b. Vanemate protokollide kasutamine (LAN-Manager ja NTLMv1) on organisatsiooni igapäevases töökeskkonnas keelatud Windowsi rühmapoliitikaga.

c. Kasutatavad krüptomehhanismid vastavad kaitsetarbele ning on dokumenteeritud.

d. Kõik lahknevused kesksest autentimisest on põhjendatud ja kooskõlastatud infoturbejuhiga.

SYS.2.2.3.M13 Funktsiooni *SmartScreen* desaktiveerimine

a. Microsoft Defenderi funktsioon *SmartScreen,* mis kontrollib Internetist alla laaditud faile ja veebisisu võimaliku kahjurtarkvara suhtes, kuid võib teatud tingimustel edastada Microsoftile isikuandmeid, on desaktiveeritud.

SYS.2.2.3.M14 Digitaalse assistendi *Cortana* desaktiveerimine [kasutaja]

a. Digitaalne assistent *Cortana* on desaktiveeritud.

SYS.2.2.3.M15 Windowsi sünkroonimismehhanismide desaktiveerimine

a. Kasutajaandmete sünkroonimine Microsofti pilvteenustega on desaktiveeritud.

b. WLAN-paroolide ühiskasutus on desaktiveeritud.

SYS.2.2.3.M16 *Microsoft Store* turvaline kasutus

a. *Microsoft Store* kasutamise vastavust organisatsiooni andmekaitse- ja turvanõuetele on hinnatud.

b. Kui *Microsoft Store* pole rakenduste klientarvutisse installimiseks vajalik, on *Microsoft Store* desaktiveeritud.

SYS.2.2.3.M17 Automaatse sisselogimise keeld

a. Paroolide, sertifikaatide ja muu teabe salvestamine veebilehtedele ja IT-süsteemidesse automaatseks sisselogimiseks on keelatud.

SYS.2.2.3.M18 *Remote Assistance* kaugtoe turvaline rakendamine

a. Lokaalse tulemüüri konfiguratsioon võimaldab kasutada kaugtoevahendit *Remote Assistance*.

b. Kaugtoe andmist on võimalik algatada ainult pärast selgelt väljendatud kutset. Kui kutse salvestatakse faili, siis kaitstakse see parooliga.

c. Sisseloginud kasutaja annab kaugtoeseansi loomisele selgesõnalise nõusoleku.

d. Kaugtoe tellimusele on seatud sobiva pikkusega kehtivusaeg.

e. Kui *Remote Assistance* teenus pole vajalik, siis on see klientarvutites desaktiveeritud.

SYS.2.2.3.M19 Kaughaldusvahendi RDP turvaline rakendamine [kasutaja]

a. Lokaalse tulemüüri konfiguratsioon võimaldab kasutada RDP-d (Remote Desktop Protocol, RDP).

b. RDP kaugpöörduse õigused on ainult selleks määratud kasutajarühmal.

c. Suurema kaitsetarbe puhul on pääs sihtsüsteemi võimalik ainult RDP lüüsi kaudu.

d. RDP kasutuselevõtu kavandamisel on otsustatud, kas järgmised mugavusfunktsioonid on lubatud ja kooskõlas sihtsüsteemi kaitsetarbega:

   - lõikepuhvri (ingl *clipboard*) kasutamine;
   - printerite integreerimine;

- irdandmekandjate ja võrguketaste integreerimine;
- failihoidlate kasutamine.

e. Kui RDP kasutamist ei ole ette nähtud, siis on see klientarvutites täielikult desaktiveeritud.

f. Kasutatavad krüptoprotokollid ja -algoritmid vastavad organisatsiooni nõuetele (vt CON.1 *Krüptokontseptsioon*).

SYS.2.2.3.M20 UAC kasutamine eeliskontodega

a. UAC (User Account Control, UAC) konfiguratsioonis on eeliskontode (ingl *privileged account*) turvatase ja kasutatavus tasakaalus.

b. UAC konfiguratsioon on dokumenteeritud.

c. UAC dokumentatsioonis esitatakse kõik haldusõigusega kontod. Õiguste põhjendatust kontrollitakse regulaarselt.

3.4 Kõrgmeetmed

SYS.2.2.3.M21 Krüpteeringuga failisüsteemi EFS kasutamine (C-I)

a. Kuna EFS'i (Encrypting File System) turvalisus sõltub kasutajakonto paroolist, kaitstakse kasutajakontot tugeva parooliga.

b. Taasteagent (Data Recovery Agent) on spetsialiseeritud konto, taasteagendina ei kasutata halduskontot.

c. Taasteagendi privaatvõtit hoitakse turvaliselt süsteemist eemal välisel andmekandjal. Kõigist privaatvõtmetest on olemas varukoopia.

d. EFS-i kasutamisel koos lokaalse kasutajakontoga on lokaalne paroolihoidla *Syskey* abil krüpteeritud. Alternatiivina võib kasutada *Windows Defender Credential Guard'*i.

e. Kasutajaid on koolitatud EFS-i turvaliselt kasutama.

SYS.2.2.3.M22 Windows PowerShelli kasutamine (C-I-A)

a. *PowerShell*'i ja WPS-faile tohivad käivitada ainult süsteemihaldurid.

b. *PowerShell*'is käivitatud käsud logitakse keskselt.

c. Signeerimata skriptide käivitamise takistamiseks piiratakse *PowerShell*'i skriptide käivitamist käsuga *Set-ExecutionPolicy AllSigned*.

SYS.2.2.3.M23 Sisselogimisteabe lisaturve (C-I)

a. UEFI-põhistes süsteemides on rakendatud *SecureBoot* meetodit.

b. Süsteemi käivitamisel kontrollitakse LSA (Local Security Authority,LSA) mandaadihoidla oleku kaitstust (vt SYS.2.2.3.M11 *Sisselogimisteabe turve*).

c. Kui klientsüsteemide kaughooldust tehakse RDP abil ja domeeni funktsionaaltase on 2012 R2 või kõrgem, siis on RDP töörežiimiks seatud *restrictedAdmin*.

SYS.2.2.3.M24 Viimase pöördumise ajatembelduse aktiveerimine (A)

a. Failisüsteemis (NTFS-is) on aktiveeritud viimase pöördumise („Last Access") ajatempel.

b. Pidevat ajatembeldust kasutatakse siis, kui see ei avalda olulist mõju süsteemi jõudlusele.

SYS.2.2.3.M25 Komponendi CUET kaugjuurdepääsufunktsioonide turvaline rakendamine (C-I)

a. Kaugpöördused Windows 10 komponendiga CUET (Connected User Experience and Telemetry, CUET) logitakse.

b. Kuna CUET abil võib operatsioonisüsteemi tootja pärida klientarvuti andmeid, siis vajadusel CUET blokeeritakse.

SYS.2.2.3.M26 VSM (Virtual Secure Mode) kasutamine (C-A)

a. On arvestatud asjaoluga, et VSM kasutamine piirab IT-kriminalistika läbiviimist.

SYS.2.3 Linuxi ja Unixi klient

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed Linuxi ja Unixi operatsioonisüsteemi kasutavate klientarvutite (klientide) andmete kaitseks.

Linuxi distributiive ja Unixi derivaate on erinevaid, kuid klientide konfigureerimine ja käitamine on sarnased, seetõttu kasutatakse selles moodulis Linuxi ja Unixi kohta ühist terminit „Unixi klient“. Unixil põhinevad klientarvutid on tavaliselt võrgustatud ja kasutavad klient-server tüüpi IT-lahendusi.

1.2 Vastutus

Unixi kliendi turvameetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Kasutaja.

1.3 Piirangud

Moodul konkretiseerib ja täiendab moodulis „SYS.2.1 „*Klientarvuti üldiselt*“ esitatud meetmeid Unixi süsteemide kohta käivate spetsiifiliste juhistega. Klientarvutis käitatava tarkvara (nt meilikliendid või kontoritarkvara) turbe meetmed on esitatud mooduligrupi „APP.1 *Klientrakendused“* asjakohastes moodulites.

Moodulis eeldatakse, et lisaks klientarvuti halduseks ette nähtud halduskontole on klientarvutis püsivalt aktiivne ainult üks kasutajakonto.

2 Ohud

2.1 Valideerimata allikatest pärit tarkvara

Unixi-laadsete IT-süsteemide valmisrakenduste installimise asemel laaditakse paketid ise alla ja programm kompileeritakse kohapeal. Tarkvarapaketid laaditakse sageli alla valideerimata allikatest. Kui ei kasutata tootja usaldusväärset paketivaramut, esineb oht, et tahtmatult laaditakse alla ja installitakse vale või ühildumatu tarkvarapakett või kahjurfunktsioone sisaldav tarkvara.

2.2 Skriptikeskkonna ärakasutamine

Unixi operatsioonisüsteemides kasutatakse halduri tegevuste lihtsustamiseks ja inimlike vigade vältimiseks skriptikeeles kirjutatud ja käsurealt aktiveeritavaid skripte. Ründaja võib skripte oma eesmärkide saavutamiseks ulatuslikult manipuleerida ja ära kasutada.

2.3 Ühisteekide dünaamiline laadimine

Käsk „LD_PRELOAD“ laadib valitud dünaamilise teegi (*dynamically linked shared object library*) enne muid tüüpteeke, mida rakenduses vajatakse. See võimaldab tüüpteekide konkreetseid funktsioone ignoreerida. Ründaja võib manipuleerida süsteemi nii, et teatud rakenduste käivitamisel aktiveeritakse kahjurprogramm.

2.4 Konfigureerimisvead

Unixi operatsioonisüsteemide standardinstalli käigus installitakse arvukalt eraldi seadistatavaid rakendusi. Kuna paljud rakendused on konfigureeritud üksteisest sõltumatult, võivad konfigureerimisvalikud üksteisega vastuollu minna ja tekitada konflikte mida üksiku rakenduse seadetest otseselt näha ei ole. Samuti võivad rakendused sisaldada lisafunktsioone, mida klientarvuti kasutaja tegelikult ei soovi, või vastupidi, olulised turvafunktsioonid on jäänud aktiveerimata.

3 Meetmed

3.1 Elutsükkel

Soetamine

SYS.2.3.M2 Sobiva distributiivi valimine

Evitus

SYS.2.3.M5 Tarkvarapakettide turvaline install

SYS.2.3.M6 Irdseadmete automaatse failisüsteemiga sidumise keeld

SYS.2.3.M7 Faili- ja kataloogiõiguste piiramine

SYS.2.3.M8 Rakenduste pääsuõiguste piiramine

SYS.2.3.M11 Kõvaketta liigtäituvuse vältimine

Käitus

SYS.2.3.M1 Haldurite ja kasutajate autentimine

SYS.2.3.M4 Operatsioonisüsteemi tuuma uuendamine

SYS.2.3.M9 Paroolide turvaline kasutamine käsureal

SYS.2.3.M12 Linuxiga spetsiaalseadmete turvaline kasutamine

Lisanduvad kõrgmeetmed

SYS.2.3.M14 Lubamatute välisseadmete vältimine

SYS.2.3.M15 Soovimatute failide käivitamise lisakaitse

SYS.2.3.M17 Nõrkuste ärakasutuse lisatõrje

SYS.2.3.M18 Tuuma lisaturve

SYS.2.3.M19 Kõvaketta või failide krüpteerimine

SYS.2.3.M20 Kriitiliste *SysRq*-funktsioonide piiramine

3.2 Põhimeetmed

SYS.2.3.M1 Haldurite ja kasutajate autentimine [kasutaja]

a. Haldurid ei logi igapäevaseks tööks ennast klientarvutisse juurkasutajana (ingl *root*, *superuser*).

b. Haldusülesannete jaoks kasutatakse käsku *sudo* või sobivat alternatiivi.

c. Mitu kasutajat ei saa olla samaaegselt lokaalselt ühte klientarvutisse sisse logitud.

SYS.2.3.M2 Sobiva distributiivi valimine

a. Sobiv Unixi derivaat (ingl *derivative*) või Linuxi distributiiv (ingl *distribution*) on valitud kasutusotstarbe ja turvanõuete alusel.

b. Kasutamiseks on valitud operatsioonisüsteem, mille väljaandja tagab tootetoe (nt riistvarakomponentide draiverite näol) plaanitud kasutusaja jooksul.

c. Enimkasutatavad rakendused on distributiivi osa ja neid ei laeta valideerimata allikatest. Distributiivile lisaks paigaldatud rakendusprogrammidele on tagatud tootja tugi.

d. Tööalaseks kasutamiseks ei valita distrubitiive, millele antakse välja väga tihti väikeuuendusi. Samuti ei kasutata enda kompileeritud distributiive.

SYS.2.3.M4 Operatsioonisüsteemi tuuma uuendamine

a. Enne klientarvutite operatsioonisüsteemi tuuma (ingl *kernel*) uuendamist testitakse, kas uuend ühildub olemasoleva süsteemiga ega põhjusta vigu.

b. Pärast tuuma uuendamist tehakse kohe klientarvuti taaskäivitus. Süsteemide puhul, kus see pole võimalik, kasutatakse tuuma dünaamilist paikamist (*Linux Kernel Live Patching*).

SYS.2.3.M5 Tarkvarapakettide turvaline install

a. Tarkvara lähtekoodist kompileerimisel on tarkvara lubatud lahti pakkida, konfigureerida ja kompileerida ainult kasutaja lihtõigustega konto alt.

b. Tarkvara kompileerimisel lähtekoodist dokumenteeritakse kõik kasutatud parameetrid. Dokumentatsiooni kasutades on võimalik tarkvara kompileerimist korrata.

c. Tarkvara ei installita serveri juurfailisüsteemi.

d. Soovituslikult installitakse tarkvarapakette paketihalduri abil ja mitte ükshaaval käsurealt.

3.3 Standardmeetmed

SYS.2.3.M6 Irdseadmete automaatse failisüsteemiga sidumise keeld [kasutaja]

a. Irdseadmeid (ingl *removable device*) ei seota failisüsteemiga (ingl *mount*) automaatselt.

b. Irdseadmete failisüsteemiga sidumine on konfigureeritud nii, et faile ei saa käivitada (valik *noexec*).

SYS.2.3.M7 Faili- ja kataloogiõiguste piiramine

a. Teenused ja rakendused saavad luua, muuta ja kustutada ainult neile määratud faile.

b. Kataloogidele, kus kõigil kasutajail on kirjutusõigus (nt */tmp*), on määratud omandibitt (ingl *sticky bit*).

SYS.2.3.M8 Rakenduste pääsuõiguste piiramine

a. Rakenduse juurdepääs failidele, seadmetele ja võrkudele on piiratud konkreetse distributiivi tuuma turvamooduliga (nt *App-Armor* või *SELinux*).

b. Rakenduste pääsuõigused on vaikeseades blokeeritud, õigusi lisatakse lähtudes ärivajadusest.

c. Õigusi piiratakse turvamooduli sundrežiimi (ingl *enforcing mode*) või vastava alternatiivi abil.

SYS.2.3.M9 Paroolide turvaline kasutamine käsureal [kasutaja]

a. Paroole ja muud tundlikku teavet ei edastata programmidele käsureaparameetritena.

SYS.2.3.M11 Kõvaketta liigtäituvuse vältimine

a. Kasutajatele ja teenustele on seatud kvoodid (ingl *quota*). Teatud kettamahu täitumise tasemest alates jäetakse kirjutusõigus ainult juurkasutajale.

b. Operatsioonisüsteemi tuuma ja andmeid hoitakse üldreeglina erinevates kettasektsioonides (ingl *disk partition*).

SYS.2.3.M12 Linuxiga spetsiaalseadmete turvaline kasutamine

a. Linuxi operatsioonisüsteemi kasutavate spetsiaalseadmete (ingl *appliance*) turvatase on samaväärne standardsete Linuxi klientarvutitega.

b. Spetsiaalseadmetele kehtivad turvanõuded on dokumenteeritud.

c. Vajadusel nõutakse seadme valmistajalt turbe vastavuse tõendamist.

3.4 Kõrgmeetmed

SYS.2.3.M14 Lubamatute välisseadmete vältimine (C-I-A)

a. Klientarvuti välisseadet (ingl *peripheral*) saab kasutada ainult juhul kui antud välisseade on dokumenteeritult kasutamiseks lubatud.

b. Välisseadme toimimiseks vajalikud tuuma (ingl *kernel*) moodulid laaditakse ja aktiveeritakse ainult siis, kui seadmel on kasutusluba.

SYS.2.3.M15 Soovimatute failide käivitamise lisakaitse (C-I)

a. Sektsioonid ja kataloogid, kuhu kasutajatel on kirjutusõigus, on failisüsteemiga seotud (ingl *mount*) nii, et faile ei saa käivitada (sidumisparameeter *noexec*).

SYS.2.3.M17 Nõrkuste ärakasutuse lisatõrje (C-I)

a. Ohustatud teenuste ja rakenduste süsteemikutsete (ingl *system call*) kasutus on piiratud sobiva määrani (nt *seccomp* abil).

b. *App-Armor'i*, *SELinux*'i ja alternatiivsete turvamoodulite tüüpprofiilid ja -reeglid on kohandatud organisatsiooni turvapoliitika kohaselt.

c. Vajadusel on loodud uusi reegleid või profiile.

SYS.2.3.M18 Tuuma lisaturve (C-I)

a. Tuuma tugevdamiseks on rakendatud sobivaid laiendeid (nt *grsecurity*, *PaX*), mis takistavad kahjurvara levimist ja operatsioonisüsteemi nõrkuste ärakasutamist.

SYS.2.3.M19 Kõvaketta või failide krüpteerimine (C-I)

a. Klientarvuti kõvakettad või sellele salvestatud failid on krüpteeritud. Vastavaid krüptovõtmeid hoitakse väljaspool IT-süsteemi.

b. Ketaste ja failide krüpteerimiseks kasutatakse AEAD (Authenticated Encryption with Associated Data, AEAD) krüptoprotseduuri või selle alternatiivina rakendust *dm-crypt* koos rakendusega *dm-verity*.

SYS.2.3.M20 Kriitiliste *SysRq*-funktsioonide piiramine (C-I-A)

a. On määratud, mis SysRq-funktsioone kasutajad klahvikombinatsiooni abil tuumas käivitada saavad.

b. Klahvikombinatsiooniga ei saa käivitada potentsiaalselt ohtlikke käske.

SYS.2.4 *macOS*-i klient

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed macOS operatsioonisüsteemi kasutavate klientarvutites talletatud andmete kaitseks.

macOS on Apple arvutites kasutatav operatsioonisüsteem. Selles moodulis keskendutakse selliste macOS-i kasutavate Mac arvutite turbele, mida käitatakse autonoomse süsteemina või klient-server tüüpi võrgu kliendina.

1.2 Vastutus

macOS-i kliendi turvameetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Kasutaja.

1.3 Piirangud

Moodulis ei käsitleta macOS-i võimalikku kasutamist serveri operatsioonisüsteemina.

Moodul konkretiseerib ja täiendab moodulis „SYS.2.1 „Klientarvuti üldiselt“ esitatud meetmeid macOS’i kohta käivate spetsiifiliste juhistega.

Klientarvutis käitatava tarkvara (nt meilikliendid või kontoritarkvara) turbe meetmed on esitatud mooduligrupi „APP.1 Klientrakendused“ asjakohastes moodulites.

Kuna mõlemad Apple'i operatsioonisüsteemid (macOS Mac arvutitele ja iOS iPhone’ile ning iPadile) on omavahel tihedalt seotud, siis ka keskse Mac arvutite halduse turvaaspekte käsitletakse moodulites SYS.3.2.2 *Mobiilseadmete haldus (MDM)* ja SYS.3.2.3 *Organisatsiooni iOS.*

2 Ohud

2.1 Kontrollimatu juurdepääs väljaspool organisatsiooni hoitavatele andmetele

macOS võimaldab mitmeid teenuseid (nt iCloud andmete salvestamiseks ja sünkroonimiseks), mida käitatakse Apple'i keskserverites. Kuna kõik andmed ei ole enam

täielikult organisatsiooni kontrolli all, on võimalik serveritele juurde pääseda kõrvalistel isikutel, kes võivad seal talletatud või edastatud andmeid näha ning neid oma eesmärkidel kuritarvitada.

2.2 Apple ID konto kuritarvitamine

macOS-i funktsioonide kasutamiseks on pääsuandmete hulgas nõutav Apple ID olemasolu. Apple ID abil antakse keskselt juurdepääs erinevatele Apple'i teenustele, nagu iCloud, iMessage, iTunes ja App Store. Kui volitamata isikul on Apple ID juurdepääs, võib ta neid teenuseid võltsitud identiteediga kasutada ning pääseda näiteks juurde iCloudis olevale teabele.

2.3 Ründed raadioliidestele

Mac arvutil on raadiokohtvõrgu ja Bluetoothi liidesed, mida paljud teenused kasutavad ja mis on arvutis tavaliselt aktiveeritud. Näiteks on võimalik raadiokohtvõrgu funktsiooni abil Apple'i seadmete vahel otse faile vahetada (AirDrop). AirPlay abil on võimalik video- ja audiostriimi saata ühilduvatesse taasesitusseadmetesse. Ründaja võib raadioliideseid kuritarvitada Mac arvuti, iPhone'i, iPadi jm seadmete vahel edastatava konfidentsiaalse teabe püüdmiseks.

2.4 Ründed elvaatefunktsiooni sisaldavatele rakendustele

Mõned macOS-i integreeritud rakendused (Finder, brauser Safari, macOS-i meiliprogramm) toetavad teatud failivormingute eelvaate funktsiooni, mis avab failid ja e-kirja manused automaatselt. Ründaja võib peita kahjurkoodi e-kirja manusesse lisatud dokumenti või pildifaili. Sellisel juhul eelvaatefunktsioon käivitab faili avades tõenäoliselt kahjurkoodi, mis võib lõppeda tundlike andmete lekke, andmete kustutamise või arvuti ülevõtmisega ründaja poolt.

2.5 Ebaturvalised protokollid macOS-is või macOS-rakendustes

Keskserverite või teiste seadmetega suhtlemiseks toetavad macOS ja selle rakendused erinevaid, osaliselt Apple'i enda protokolle, nt AFP (*Apple Filing Protocol,* AFP). Kui andmesideprotokollidel ei ole piisavaid turvamehhanisme või need on ebaturvaliselt konfigureeritud, siis on võimalik nende protokollide kaudu edastatavaid andmeid lubamatult lugeda, võltsida või muul viisil kuritarvitada.

3 Meetmed

3.1 Elutsükkel

Kavandamine

SYS.2.4.M1 macOS-i turvalise rakendamise kava

Soetamine

SYS.2.4.M6 Ajakohane riistvara

Evitus

SYS.2.4.M2 macOS-i turvafunktsioonide kasutamine

SYS.2.4.M3 Kasutajakontode haldus

SYS.2.4.M4 Kõvaketta krüpteerimine

SYS.2.4.M5 Turvalisust ohustavate funktsioonide desaktiveerimine

SYS.2.4.M7 Apple ID mitmikautentimine

SYS.2.4.M9 Täiendava turvatarkvara kasutamine

SYS.2.4.M10 macOS-i personaalse tulemüüri kasutamine

Käitus

SYS.2.4.M8 iCloudi keeld tundlike andmete hoiustamisel

Kõrvaldamine

SYS.2.4.M11 Seadme turvaline kõrvaldamine

Lisanduvad kõrgmeetmed

SYS.2.4.M12 Püsivaraparool ja buutimiskaitse

3.2 Põhimeetmed

SYS.2.4.M1 macOS-i turvalise rakendamise kava

a. macOS-i klientide kasutuselevõtuks on koostatud kava.

b. macOS-i rakendamise kava sisaldab vähemalt järgmist:
   - macOS-i ja rakenduste regulaarne ajakohastamine;
   - macOS-i kliendi logimine;
   - klientarvuti andmete varundus;
   - kahjurvara tõrje macOS-is.

c. On analüüsitud macOS-i ühilduvust kasutusel olevate rakenduste, seadmete, protokollide ja litsentsilepingutega ning platvormivahetusega kaasnevat vajadust rakenduste väljavahetamiseks.

d. macOS-i kliendi kasutamiseks võrgus on analüüsitud täiendavate võrguprotokollide kasutamise vajadust.

SYS.2.4.M2 macOS-i turvafunktsioonide kasutamine

a. macOS-i integreeritud turvamehhanismid SIP (System Integrity Protection, SIP), Xprotect ja Gatekeeper on aktiveeritud.

b. Gatekeeper võimaldab käivitada ainult AppStore'st hangitud ja signeeritud rakendusi, välja arvatud juhul kui organisatsioonis kasutab signeerimata erirakendusi.

c. Uue rakenduse installimisel kontrollitakse selle signatuuri vastavust, vajadusel tehakse kahjurvarakontroll.

SYS.2.4.M3 Kasutajakontode haldus [kasutaja]

a. macOS-i esmase konfigureerimise käigus loodud halduskontot kasutatakse ainult haldustegevusteks.

b. macOS-i kliendi tavakasutuse jaoks on loodud tavakasutajakonto. Kui MacOS-ga arvutit kasutab mitu kasutajat, on igale kasutajale loodud personaalne konto.

c. Süsteemi sisselogimine on võimalik üksnes kasutajanime ja parooliga, automaatne sisselogimine (valik „*Automatic login*“) on desaktiveeritud.

d. Pärast pikemat kasutamispausi logitakse kasutaja automaatselt välja (turva-ja privaatsusseade „*Log out after... minutes of inactivity*“ on aktiveeritud).

e. Külaliskonto on desaktiveeritud.
f. Süsteemiseadetes on valik „*Allow guests to connect to shared folders*“ desaktiveeritud.
g. Ekraaniluku kasutamine on aktiveeritud. Ekraaniluku lukustusest vabastamisel küsitakse kasutaja parooli.
h. MacOS kliendi turva- ja privaatsusseadetes on aktiveeritud valik *“Require an administrator password to access system-wide preferences*“ .

3.3 Standardmeetmed

SYS.2.4.M4 Kõvaketta krüpteerimine

a. Mac arvuti (eriti mobiilse MacBook arvuti) kõvaketas on krüpteeritud.
b. macOS-i integreeritud krüpteerimisfunktsiooni *FileVault* kasutamisel:
   - ei säilitata võtmeinfot Apple'i veebikeskkonnas;
   - hoitakse *FileVault* taastevõti (ingl *recovery key*) turvalises kohas.
c. *FileVault*i taastevõti on halduritele vajadusel kättesaadav.
d. Mac arvutist tehtud kettatõmmised on krüpteeritud.

SYS.2.4.M5 Turvalisust ohustavate funktsioonide desaktiveerimine

a. macOS-i asukohateenused on desaktiveeritud.
b. Safaris alla laetud faile ei avata automaatselt.
c. Andmekandja sisu automaatkäivitus või -esitus on blokeeritud.
d. Viimati kasutatud rakenduste, dokumentide ja võrguühenduste loendit on lühendatud.
e. Mac arvuti prügikasti tühjendamisel kasutatakse valikut „*Secure EmptyTrash*“.

SYS.2.4.M6 Ajakohane riistvara

a. Uute Mac arvutite hankimisel valitakse ajakohased tootemudelid.
b. Olemasolevatel Mac arvutitel on jätkuvalt Apple’i turvauuendite tugi.
c. Apple’i tootetoe lõppemisel kõrvaldatakse mõjutatud Mac tootemudelid kasutuselt.
d. Kui on võimalik, kasutatakse alati macOS-i uusimat versiooni.

SYS.2.4.M7 Apple ID mitmikautentimine [kasutaja]

a. Apple ID konto kasutamiseks on aktiveeritud mitmikautentimine.
b. Mitmikautentimiseks kasutatakse kahte sõltumatut komponenti (nt parool ja telefoni saadetud kood).

SYS.2.4.M8 iCloudi keeld tundlike andmete hoiustamisel [kasutaja]

a. Tundlike andmete sünkroonimine erinevate seadmete vahel läbi iCloudi teenuse on keelatud.
b. Tundlikke andmeid on lubatud sünkroonida ainult organisatsiooni siseteenuste vahel.
c. Tundlikke andmeid ei salvestata iCloudi.
d. Dokumentide ja e-kirjade mustandite automaatne salvestamine iCloudi on blokeeritud.
e. Funktsioon *Handoff* andmete ülekandmiseks teise seadmesse on desaktiveeritud.

SYS.2.4.M9 Täiendava turvatarkvara kasutamine

a. Vajadusel (nt kui Maci arvuteid kasutatakse võrgus koos Windowsi arvutitega), kasutatakse lisaks macOS-i integreeritud Xprotectile täiendavalt muude tootjate kahjurvaratõrje lahendusi või muid turbeprogramme.

SYS.2.4.M10 macOS-i personaalse tulemüüri kasutamine

a. macOS-i integreeritud personaalne tulemüür on aktiveeritud ja see on sobival viisil konfigureeritud.

b. Rakenduste tulemüür (*Application Firewall*) on aktiveeritud ja sobivalt konfigureeritud.

c. Peitrežiim (ingl *camouflage mode*) on desaktiveeritud.

d. Peale igat operatsioonisüsteemi ajakohastamist kontrollitakse tulemüüri konfiguratsiooni.

SYS.2.4.M11 Seadme turvaline kõrvaldamine

a. Enne seadme kõrvaldamist on andmed andmekandjatelt turvaliselt kustutatud. Selleks võib kasutada macOS-i installimeedial olevat kettautiliiti.

b. Mac arvuti kõrvaldamisel lähtestatakse ka süsteemiseadeid sisaldav säilmälu (NVRAM).

3.4 Kõrgmeetmed

SYS.2.4.M12 Püsivaraparool ja buutimiskaitse (C-I-A)

a. Mac arvuti buutimine väliselt andmekandjalt on keelatud ja seadete muutmise kaitseks on aktiveeritud püsivaraparool. Vanematel Mac arvutitel tuleb püsivara parool aktiveerida käsurežiimis.

b. T2-turvakiibiga Mac arvutites seadistatakse püsivara parool *Startup Security Utility* abil, milles aktiveeritakse valik „Täielik turvalisus“ („Full Security“).

SYS.3: Mobiilseadmed

SYS.3.1 Sülearvutid

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed sülearvutite turvaliseks kasutamiseks organisatsioonis ja suurendada teadlikkust selle seadmeklassi spetsiifilistest ohtudest.

Sülearvuteid kasutatakse kõigi levinud operatsioonisüsteemidega (Microsoft Windows, Apple macOS või Linuxi distributiivid). Sülearvutid on levinud enamikes organisatsioonides ning asendavad sageli klassikalist lauaarvutit.

1.2 Vastutus

Sülearvutite meetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Kasutaja, hankeosakond, infoturbejuht.

1.3 Piirangud

Moodulit SYS.3.1 *Sülearvutid* kasutatakse kõigi mobiilselt või statsionaarselt kasutatavate sülearvutite puhul. Kõigile klientarvutitele sobivad turvameetmed on esitatud moodulis SYS.2.1 *Klientarvuti üldiselt*.

Sülearvuti eri operatsioonisüsteemide turvameetmeid kirjeldatakse moodulites SYS.2.2.3 *Windows 10 klient*, SYS 2.3 *Linuxi ja Unixi klient* või SYS.2.4 *macOS-i klient*.

Sülearvuti võrguühendusi käsitletakse moodulites „NET.2.2 *Raadiokohtvõrgu kasutamine"* ja NET.3.3 *Virtuaalne privaatvõrk (VPN)*.

Sülearvuti andmete varundamist kirjeldatakse moodulis CON3. *Andmevarunduse kontseptsioon*.

2 Ohud

2.1 Muutuvast kasutuskeskkonnast tingitud ohud

Sülearvuteid võivad kahjustada keskkonnamõjud, näiteks liiga kõrge või liiga madal temperatuur, samuti tolm või niiskus. Mobiilseadmed võivad saada füüsilisi kahjustusi transpordil või pideva kaasaskandmise tagajärjel. Sülearvuteid ühendatakse sageli, eriti reisil olles, tundmatute IT-süsteemide või võrkudega. Sellega kaasneb alati kahjurvaraga nakatumise ja andmevargusega seotud oht.

2.2 Sülearvuti kaotamine või vargus

Sülearvutite kasutamisega väljaspool organisatsiooni kaasneb sülearvuti kaotamise või varguse oht. Seadmeid transporditakse autos või ühissõidukis, jäetakse töö vaheaegadeks võõrasse bürooruumi või valveta hotellituppa. Sülearvuti kaotamise või vargusega seonduvatele arvuti asenduskuludele lisanduvad kulutused sülearvuti uuesti seadistamisele ja andmete taastamisele.

Sülearvuti puhul on oht andmed kaotada palju suurem kui statsionaarselt sisevõrku ühendatud lauaarvuti puhul. Kui andmed on varundamata, lähevad need sülearvuti varguse korral kaotsi. Samuti võivad kõrvalised isikud pääseda ligi sülearvutis olevatele tundlikele andmetele. Enamasti on andmelekkest tekkiv kahju märkimisväärselt suurem kui seadme asenduskulu.

2.3 Sülearvuti kasutajate vahetumine

Kui töötajad vajavad mobiilseid IT-süsteeme ainult erandjuhtudel, nagu näiteks töölähetuses olles, siis on sageli otstarbekas omada paljude kasutajate jaoks üht sülearvutit. Sülearvuti üleandmisel järgmisele töötajale kaasneb oht, et edasi antakse ka seadmes endiselt leiduvad kaitset vajavad andmed. Peale selle on võimalik, et sülearvuti on kahjurvaraga nakatunud. On raske kindlaks teha, kes ja millal sülearvutit kasutas või kes seda hetkel kasutab. Sülearvuti sisaldab paljude kasutajate jääkandmeid, mis võivad sisalda paroole ja tundlikku teavet.

3 Meetmed

3.1 Elutsükkel

Kavandamine

SYS.3.1.M1 Sülearvutite mobiilse kasutamise kord

SYS.3.1.M6 Sülearvuti kasutamise eeskiri

Soetamine

SYS.3.1.M15 Sülearvuti valimise kord

Evitus

SYS.3.1.M3 Personaalne tulemüür

SYS.3.1.M8 Turvaline ühendamine andmesidevõrguga

SYS.3.1.M13 Sülearvuti sisu krüpteerimine

Käitus

SYS.3.1.M7 Sülearvutite väljastuse ja tagastuse kord

SYS.3.1.M9 Turvaline kaugjuurdepääs

SYS.3.1.M10 Andmete sünkroonimine

SYS.3.1.M11 Toite tagamine

SYS.3.1.M12 Sülearvuti kaotusest teatamine

SYS.3.1.M14 Sülearvuti füüsiline turve

Avariivalmendus

SYS.3.1.M5 Sülearvuti andmevarundus

Lisanduvad kõrgmeetmed

SYS.3.1.M16 Keskne sülearvutite haldus

SYS.3.1.M17 Sülearvutite turvaline ladustamine

SYS.3.1.M18 Varguskaitsevahendite kasutamine

3.2 Põhimeetmed

SYS.3.1.M1 Sülearvutite mobiilse kasutamise kord

a. Organisatsioonis on kehtestatud sülearvutite mobiilse kasutamise kord, mis määrab:
b. Sülearvutite mobiilse kasutamise kord määrab:
   - milliseid sülearvuteid on lubatud väljaspool organisatsiooni kasutada;
   - kes tohib neid kaasas kanda;
   - milliseid turvameetmeid tuleb rakendada;
   - milline on kasutaja vastutus.
c. Sülearvuti turvameetmed vastavad selles käideldavate andmete kaitsetarbele.
d. Kasutajatele on sülearvuti mobiilse kasutamise korda tutvustatud.

SYS.3.1.M3 Personaalne tulemüür

a. Kui sülearvutit kasutatakse väljaspool organisatsiooni sisevõrku, on sülearvutis aktiveeritud personaalne tulemüür (ingl *personal firewall*).
b. Personaalne tulemüür võib olla kas operatsioonisüsteemiga kaasatulev komponent või osa kolmanda tootja turbelahendusest, mitme tulemüüri üheaegne rakendamine on keelatud.
c. Personaalset tulemüüri haldavad üksnes selleks volitatud haldurid.

d. Tulemüüri filtreerimisreeglid on määratud võimalikult kitsendavalt. Lubatud sissetulevad ühendused piirduvad kaughoolduse, süsteemi uuendamise ja seire jaoks nõutud ühendustega.
e. Personaalne tulemüür on konfigureeritud toimima ilma kasutajatele kuvatavate keerukate hoiatusteadeteta.
f. Kui personaalne tulemüür toetab logimist, siis turvasündmused logitakse.

SYS.3.1.M5 Sülearvuti andmevarundus [kasutaja]

a. Faile, mida talletatakse lokaalselt, kuid mitte serveris, varundatakse regulaarselt.
b. Vajadusel varundatakse sülearvutite andmed ajutiste võrguühenduste (nt VPN) käigus. Kui võrguühendus puudub, varundatakse sülearvuti andmed krüpteeritult välisele andmekandjale.

SYS.3.1.M9 Turvaline kaugjuurdepääs

a. Pääs sülearvutist sisevõrku toimub krüpteeritult, virtuaalse privaatvõrgu (VPN) kaudu (vt NET.3.3 *Virtuaalne privaatvõrk*).
b. Pärast VPN-ühenduse kasutamise lõppu kustutatakse autentimisandmed ja ajutised andmed.

3.3 Standardmeetmed

SYS.3.1.M6 Sülearvuti kasutamise eeskiri [infoturbejuht]

a. Organisatsioonis on koostatud ja kehtestatud sülearvuti kasutamise eeskiri.
b. Sülearvuti kasutamise eeskiri määrab:
   - kuidas sülearvuteid hallatakse, väljastatakse ja tagastatakse;
   - milliseid andmeid ja millistel tingimustel ei tohi sülearvutis hoida;
   - millised andmed peavad alati olema krüpteeritud;
   - kuidas on sülearvutist võimalik kasutada organisatsiooni serveriressursse;
   - kas sülearvutit tohib kasutada isiklikuks otstarbeks;
   - kuidas vältida sülearvuti kaotust või vargust;
   - kuidas kasutada paroole ja PIN-koode;
   - kas ja kuidas on lubatud avalikus kohas töötamine (vt INF.9 *Mobiiltöökoht*);
   - kus ja millal ei tohi sülearvuteid kasutada.
c. Kasutajad on teadlikud sülearvuti kasutamisega kaasnevatest ohtudest ning on kohustatud sülearvuti kasutamise eeskirja järgima.

SYS.3.1.M7 Sülearvutite väljastuse ja tagastuse kord [kasutaja]

a. Võimalusel kasutab sülearvutit ainult üks töötaja. Kui sülearvuteid kasutavad vaheldumisi erinevad isikud, siis on määratud, kuidas toimub sülearvuti kasutajalt kasutajale üleandmine.
b. Sülearvuti kasutaja vahetumisel kustutatakse sülearvutist turvaliselt kõik tundlikud andmed, kaasaarvatud jääkandmed.
c. Sülearvuti tagastatakse komplektselt ja terviklikult.

d. Kasutusel olnud sülearvuti uuele kasutajale andmisel taastatakse etaloninstalli abil sülearvuti algne seis. Kui pärast kasutaja vahetumist arvutit uuesti ei lähtestata, kontrollitakse, kas sülearvutis või sellega seotud andmekandjatel ei leidu kahjurvara.

SYS.3.1.M8 Turvaline ühendamine andmesidevõrguga

a. Andmeside kasutamisel on alati aktiveeritud personaalne tulemüür (vt SYS.3.1.M3 *Personaalne tulemüür*).

b. Organisatsiooni sisevõrku sisselogimine on võimalik ainult selleks lubatud sülearvutitel (nt sertifikaadipõhise seadmete autentimise abil).

c. Mittevajalikud liidesed ja protokollid on sülearvutitel desaktiveeritud.

SYS.3.1.M10 Andmete sünkroonimine

a. Sülearvutis on olemas sünkroonimisvahendid ja on koostatud protseduur andmete sünkroonimiseks sülearvutite ja organisatsiooni IT-süsteemide vahel.

b. Sünkroonimisvahendid ja sünkroonimise seadistus on kaitstud lubamatu juurdepääsu eest.

c. Sünkroonimisvahend võimaldab sünkroonimisprotsesse logida ja võimalikke sünkroonimiskonflikte lahendada.

d. Kasutajad on teadlikud, kuidas kontrollida sünkroonimise logisid.

SYS.3.1.M11 Toite tagamine [kasutaja]

a. Andmekao vältimiseks salvestab kasutaja akutoitel töötades andmeid piisavalt sageli.

b. Aku kasutusea pikendamiseks laetakse sülearvutit tootja heakskiidetud laadijaga ja kasutusjuhendis näidatud viisil.

c. Sülearvuti pikemaajalisel mobiilsel kasutamisel on alati kaasas ka laadija.

d. Kui sülearvutite tarbeks on olemas varuakud, siis transporditakse ja hoitakse neid ainult vastavates ümbristes ja sobilikes keskkonnatingimustes.

SYS.3.1.M12 Sülearvuti kaotusest teatamine [kasutaja]

a. Organisatsioonis on kehtestatud kord sülearvuti kaotamisest, vargusest või rikkest teavitamiseks.

b. Sülearvuti kaotamisest, vargusest või rikkest teatab kasutaja viivitamatult.

c. Võimalusel tuleb pärast sülearvuti kaotamist rakendada ka meetmed, mis võimaldavad seadet lukustada, kustutada või lokaliseerida (vt SYS.3.2.2 *Mobiilseadmete haldus (MDM)).*

d. Pärast sülearvuti kaotust muudetakse kõigis eeldatavasti mõjutatud IT-süsteemides kasutaja pääsuandmed.

e. Kaotatud sülearvuti tagasisaamisel kontrollitakse, kas seda ei ole manipuleeritud. Reeglina installitakse selline sülearvuti täielikult uuesti.

SYS.3.1.M13 Sülearvuti sisu krüpteerimine

a. Sülearvutisse integreeritud andmekandjad (kõvaketas, SSD) on krüpteeritud.

b. Kõvaketta krüpteerimiseks kasutatakse reeglina operatsioonisüsteemiga integreeritud krüptovahendeid.

SYS.3.1.M14 Sülearvuti füüsiline turve [kasutaja]

a. Organisatsiooni ruumides kaitstakse sülearvutit nii tööajal kui väljaspool tööaega varguse ja lubamatu kasutamise eest.

b. Reeglina ei jäeta sülearvutit ilma järelevalveta. Väljaspool organisatsiooni hoiab kasutaja sülearvutit varguse eest kaitstud ja lukustatud asukohas (vt INF.8 *Kodutöökoht*).

c. Võõrastes ruumides võtab töötaja sülearvuti endaga kaasa ka siis, kui lahkub ruumist vaid korraks. Kui seda teha ei saa, suletakse ja lukustatakse seade.

d. Sülearvutit transporditakse spetsiaalsete taskute ja polsterdusega arvutikotis.

e. Sülearvuti jätmisel mootorsõidukisse ei tohi sülearvuti olla väljastpoolt sõidukit nähtav.

f. Sülearvutit kaitstakse kahjulike keskkonnatingimuste (nt liigniiskus, äärmuslikud temperatuurid) eest.

SYS.3.1.M15 Sülearvuti valimise kord [hankeosakond]

a. Enne sülearvutite hankimist on sülearvutite kasutusotstarbe põhjal koostatud nõuded riist- ja tarkvarakomponentidele.

b. Sülearvutite valimisel on võetud arvesse vähemalt alljärgnevat:
   - tootetoe olemasolu ja hooldatavus;
   - töökindlus;
   - kasutatavus (kasutajasõbralikkus ning installimise, konfigureerimise hõlpsus);
   - mõõtmed, mass ja aku vastupidavusaeg;
   - ühilduvus olemasolevate süsteemidega;
   - võrguliidesed ja ühendusvõimalused;
   - turvamehhanismid ja nende lisamise võimalused;
   - täiendav riistvara (nt arvutidokid ja monitorid);
   - riistvara ja tarkvara soetusmaksumus ja täiendavad kulud.

c. Hankimisotsus põhineb vajaduste analüüsi tulemustel ning on kooskõlastatud haldurite ja IT-toe eest vastutajatega.

3.4 Kõrgmeetmed

SYS.3.1.M16 Keskne sülearvutite haldus (C-I)

a. On kehtestatud keskse sülearvutite halduse protseduur (vt SYS.3.2.2 *Mobiilseadmete haldus (MDM)*).

b. Kesksed haldusvahendid toetavad kõiki organisatsiooni sülearvutites kasutusel olevaid operatsioonisüsteeme.

SYS.3.1.M17 Sülearvutite turvaline ladustamine (A)

a. Organisatsiooni sülearvuteid, mida hetkel ei kasutata, hoitakse turvaliselt.

b. Hoiuruumile on rakendatud meetmed moodulist INF.5 *Tehnilise taristu ruum või kapp*.

SYS.3.1.M18 Varguskaitsevahendite kasutamine (C-I-A)

a. Sülearvuti kasutajatele on antud sülearvuti valveta jätmisel kasutamiseks varguskaitsevahendid.

b. Mehaanilised varguskaitsevahendid (nt trosslukud, turvakorpused) on varustatud tõhusa lukustussüsteemiga.
c. Uute sülearvutite hankimisel arvestatakse, et sülearvuti korpus oleks trosslukuga kinnitatav.

SYS.3.2: Nutitelefon ja tahvelarvuti

SYS.3.2.1 Nutitelefon ja tahvelarvuti üldiselt

1 Kirjeldus

1.1 Eesmärk

Tutvustada nutitelefonide ja tahvelarvutitega seotud tüüpilisi ohte ning esitada meetmed nende ohtude vältimiseks ja kõrvaldamiseks.

Tahvelarvuti erineb nutitelefonist eelkõige suurema puutetundliku ekraani ja piiratud helistamisvõimaluste poolest. Ohud ja meetmed on mõlema seadmetüübi puhul sarnased.

1.2 Vastutus

Nutitelefon ja tahvelarvuti üldiselt meetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Kasutaja, infoturbejuht.

1.3 Piirangud

Nutitelefonide ja tahvelarvutite konkreetsete operatsioonisüsteemide kaitset käsitletakse vastavate süsteemide moodulites SYS.3.2.3 *Organisatsiooni iOS* ja SYS.3.2.4 *Android*. Mobiilseadmete haldusega seonduvaid meetmeid kirjeldatakse moodulites SYS.3.2.2 *Mobiilseadmete haldus (MDM)* ja SYS.3.3 *Mobiiltelefon*.

Nutitelefonide ja tahvelarvutite klientrakenduste kaitset käsitletakse moodulites APP.1.4 *Mobiilrakendused (äpid)* ja APP.1.2 *Veebibrauser*.

Meetmed kahjurvara eest kaitsmiseks on esitatud moodulis OPS.1.1.4 *Kaitse kahjurprogrammide eest*.

2 Ohud

2.1 Ajakohastamata operatsioonisüsteem

Mobiilsetes seadmetes kasutavatele operatsioonisüsteemidele ilmuvad regulaarselt uued versioonid ja uuendid. Tavaliselt pakub tootja uusi versioone ja uuendeid ainult uusima põlvkonna seadmetele. Vanemad ja madalama hinnaklassi nutitelefonid ja tahvelarvutid tarkvarauuendusi enam ei saa. Nende operatsioonisüsteemides esineb teadaolevaid nõrkusi, mida ei saa enam regulaarsete turvapaikadega kõrvaldada ja ründajad saavad neid nõrkusi eriti lihtsalt ära kasutada.

2.2 Tarkvaranõrkused mobiilirakendustes (äppides)

Nutitelefoni või tahvelarvutiga kaasa pandud ja seadmesse eelpaigaldatud rakendused võivad sisaldada turvanõrkusi. Neid nõrkusi on võimalik ära kasutada seadme ründamiseks võrguühenduse kaudu. Ka paljusid kasutaja enda poolt seadmesse laetud äppe aja möödudes enam ei hooldata ega uuendata. Siis võivad nad samuti sisaldada nõrkusi, mida ei saa kõrvaldada isegi operatsioonisüsteemi uuendamisega.

2.3 Nutitelefoni või tahvelarvuti manipuleerimine

Ründaja võib nutitelefonile või tahvelarvutile juurde pääsedes seadmes olevaid andmeid sihipäraselt manipuleerida. Ta võib näiteks muuta seadme konfiguratsiooni, käivitada täiendavaid teenuseid või märkamatult installida kahjurvara. Manipuleeritud süsteemis on võimalik näiteks sideseansse salvestada (ehk tekitada andmeleke) või luua oma vajaduste kohaselt seadmele uusi juurdepääsuvõimalusi (nt lubada seadme kontrollimiseks juurdepääs Internetist).

2.4 Nutitelefonide ja tahvelarvutite kahjurprogrammid

Nii nagu kõigil internetiühendusega seadmetel, on ka nutitelefonide ja tahvelarvutite puhul kahjurvaraga nakatumise oht eriti suur. Eriti viimasel ajal on palju ründeid suunatud just nimelt mobiilsete seadmete vastu, sest endiselt on kasutuses on palju seadmeid, kuivõrd aegunud ja uuendamata tarkvaraga seadmeid on kasutuses palju. Samuti pole nutiseadmete jaoks loodud viiruse- ja kahjurvaratõrje rakendused nii efektiivsed kui arvutite operatsioonisüsteemidele mõeldud turvarakendused. Kui kasutaja on hankinud äppe ebausaldusväärsetest allikatest või kui nõrkuste jaoks ei ole uuendeid saadaval, siis on nakatumise oht eriti suur. Kahjurvaraga seadmes saavad ründajad lugeda, muuta ja kustutada andmeid või mobiilseadme kaudu juurde pääseda organisatsiooni IT-ressurssidele.

2.5 Veebipõhised ründed mobiilibrauseritele

Mobiilibrauserid ei ole nii võimekad ja turvalised kui seda on analoogilised arvutitele mõeldud veebibrauserid. Samuti võivad veebisisu kuvada peale tunnustatud tootjate välja antud veebibrauserite (Chrome, Safari, Edge jne) ka muud mobiiliäpid. See muudab nutitelefonid ja tahvelarvutid haavatavaks erinevat tüüpi veebipõhiste rünnete vastu (nt õngitsemisründed või vaatenakkused (ingl *drive-by attack*)).

2.6 Tervise- või asukohaandmete kuritarvitamine

Nutitelefonide ja tahvelarvutite äpid võivad sisaldada spetsiaalseid funktsioone ja lisarakendusi, et hallata seadmekasutaja tervise-, treeningu- ja asukohaandmeid. Tundlikud isikuandmed, eriti kui neid on kogutud pika aja jooksul, on ründaja jaoks atraktiivne sihtmärk.

Nii võib näiteks seadme või seotud pilvteenuste vastu suunatud ründe abil tuvastada töötaja asukoha. Lisaks eraelu puutumatuse riivele võib see põhjustada edasisi ründeid. Näiteks võib varas sisse murda nende töötajate kodudesse, kes viibivad mobiilseadme asukohaandmete järgi reisil.

2.7 Lukustatud ekraanil näidatavate andmete kuritarvitamine

Paljudel mobiilseademete operatsioonisüsteemidel on funktsioon, mis võimaldab ka lukustatud ekraanilt vaadata aktiveeritud vidinate (ingl *widget*) poolt kuvatavaid teateid, SMS teavitusi ja e-kirjade päiseid. Sel viisil võib kasutaja konfidentsiaalne teave volitamata isikutele nähtavaks saada ning seda teavet on võimalik ära kasutada. Ka mõned suhtlusprogrammid võimaldavad juurdepääsu isikute kontaktandmetele isegi lukustatud olekus.

2.8 Töötelefoni või tahvelarvuti kasutamine isiklikuks otstarbeks

Tavaliselt võimaldatakse organisatsioonile kuuluvaid nutitelefone ja tahvelarvuteid kasutada ka isiklikuks tarbeks. See tekitab organisatsiooni vaatest mitmeid turvaprobleeme. Näiteks võib kasutaja installida kahjurfunktsioone sisaldavaid rakendusi või külastada veebisaiti, mis nakatab seadme kahjurvaraga. Samuti võib ründaja kasutaja isiklikuks tarbeks paigaldatud rakenduste (nt sotsiaalmeedia äpi või kiirsõnumirakenduse) kaudu juurde pääseda organisatsiooni kontaktidele (nt aadressiraamatule).

2.9 Isikliku seadme kasutamisest (BYOD) tulenevad ohud

Kui isiklikke nutitelefone või tahvelarvuteid kasutatakse tööülesannete täitmiseks, siis kaasneb sellega mitmeid ohte. Kui keskse mobiilseadmete halduse kaudu ilmneb vajadus tööga seotud andmed kustutada, võib see mõjutada ka kasutaja isiklikke andmeid. IT eest vastutavad isikud ei saa kontrollida iga isikliku seadme vastavust organisatsiooni turvanõuetele. Nii kasutatakse ebasobivaid ja turvanõrkustega seadmeid. Kasutajad vastutavad ise oma seadmete hooldamise ja parandamise eest. Nutitelefoni remonti saatmisel võib seadme parandaja pääseda juurde organisatsiooni andmetele. Lisaks võib tekkida probleem sobivate tarkvaralitsentside puudumisega (nt ainult isiklikuks tarbeks lubatud äppide kasutamisel tööülesannete täitmiseks).

2.10 Tarkvara nõrkuste kasutamine volitamata juurdepääsuks

Paljude tootjate seadmete operatsioonisüsteemid (eriti vanemad Androidi versioonid) sisaldavad nõrkusi, mis võimaldavad tootja rakendatud turvameetmeid eirata. Ründajal on võimalik saada seadme kaitstud süsteemiprotsessidele ja seadme mälupiirkondadele volitamata juurdepääs, nn juurkasutaja juurdepääs (ingl *root access*). Juurkasutaja õigustes on ründajal võimalik seadet ja selles olevaid andmeid manipuleerida, installida lubamatuid äppe ning kahjurvara seadme või organisatsiooni sisevõrgu ründamiseks. Nõrkuste ärakasutamine on igaühel võimalik avalikus käibes leiduvate vahendite ning juhendite abil.

3 Meetmed

3.1 Elutsükkel

Kavandamine

SYS.3.2.1.M1 Nutitelefonide ja tahvelarvutite turvanõuete kehtestamine

SYS.3.2.1.M2 Pilvteenuste kasutamise kord

Evitus

SYS.3.2.1.M3 Mobiilseadme turvaline aluskonfiguratsioon

SYS.3.2.1.M8 Mobiilirakenduste installimise kord

SYS.3.2.1.M9 Lisafunktsionaalsuse piiramine

SYS.3.2.1.M10 Mobiilseadmete kasutamise eeskiri

SYS.3.2.1.M11 Nutitelefoni ja tahvelarvuti mälu krüpteerimine

SYS.3.2.1.M12 Anonüümsete seadmenimede kasutamine

SYS.3.2.1.M13 Ekraanijagamise ja meedia ühiskasutuse kord

SYS.3.2.1.M16 Tarbetute sideliideste desaktiveerimine

SYS.3.2.1.M19 Virtuaalassistentide kasutamise piiramine

SYS.3.2.1.M31 Mobiilmaksete käsitlemise kord

Käitus

SYS.3.2.1.M4 Lubamatu kasutuse tõkestamine

SYS.3.2.1.M5 Operatsioonisüsteemi ja rakenduste ajakohastamine

SYS.3.2.1.M6 Privaatsussätete ja rakenduste juurdepääsude haldamine

SYS.3.2.1.M7 Turvasündmusele reageerimise kord

SYS.3.2.1.M18 Biomeetriline autentimine

SYS.3.2.1.M22 VPN-i kasutamine ühenduseks sisevõrguga

SYS.3.2.1.M28 Veebilehtede filtreerimine

SYS.3.2.1.M32 Keskse mobiilseadmete halduse (MDM) kasutamine

SYS.3.2.1.M33 Kahjurvaratõrje rakenduse kasutamine

SYS.3.2.1.M34 Turvaline DNS-serveri seadistus

Lisanduvad kõrgmeetmed

SYS.3.2.1.M25 Täitmiskeskkondade lahusus

SYS.3.2.1.M26 PIM kasutamine

SYS.3.2.1.M27 Kõrgturvaline mobiilseade

SYS.3.2.1.M29 Organisatsioonipõhine pääsupunkt (APN)

SYS.3.2.1.M30 Äppide installimise valge nimekiri

SYS.3.2.1.M35 Mobiilseadmete tulemüür

3.2 Põhimeetmed

SYS.3.2.1.M1 Nutitelefonide ja tahvelarvutite turvanõuete kehtestamine [infoturbejuht]

a. Organisatsioonis on kehtestatud nutitelefonide ja tahvelarvutite turvalise kasutamise kord.

b. On määratud, milliseid organisatsiooni andmeid sisaldavaid teenuseid (nt e-posti teenus) mobiilseadmetes kasutada tohib.

SYS.3.2.1.M2 Pilvteenuste kasutamise kord

a. On kehtestatud nutitelefonide ja tahvelarvutite turvalise pilvekasutuse kord, millega määratakse, millised pilvteenused on kasutamiseks lubatud ja kuidas töötajate pilvkasutust kontrollitakse.

b. Lubatud ja keelatud (sh isiklikuks kasutuseks lubatud ja keelatud) pilvteenused on kasutajatele teatavaks tehtud.

c. Kasutajaid koolitatakse pilvteenuseid turvaliselt kasutama.

SYS.3.2.1.M3 Mobiilseadme turvaline aluskonfiguratsioon

a. Mobiilseadmed on enne kasutajale väljastamist konfigureeritud lähtudes andmete kaitsetarbest.

b. On koostatud ja dokumenteeritud turvamehhanisme toetav nutitelefonide ja tahvelarvutite aluskonfiguratsioon.

c. Tarbetud funktsioonid ja andmesideliidesed on mobiilseadmetes desaktiveeritud.

d. Mobiilseadmete keskhalduseks vajalikud kliendikomponendid on lisatud aluskonfiguratsiooni.

SYS.3.2.1.M4 Lubamatu kasutuse tõkestamine [kasutaja]

a. Nutitelefonid ja tahvelarvutid on kaitstud piisavalt keeruka pääsukoodiga.

b. Ekraaniluku (ingl *screen lock*) kasutamine mobiilseadmetes on kohustuslik. Ekraanilukk aktiveerub piisavalt lühikese aja jooksul (sõltuvalt kaitsetarbest 15 s – 1 min).

c. Mobiilseadme parooli või PIN-koodi muutmisel ei saa valida paroole, mida oli viimati kasutatud.

SYS.3.2.1.M5 Operatsioonisüsteemi ja rakenduste ajakohastamine

a. Mobiilseadme tootja tagab seadme plaanitud kasutusaja jooksul regulaarse operatsioonisüsteemi uuendite (ingl *update*) saamise.

b. Vanemad seadmed, mille operatsioonisüsteemi turbepaiku (ingl *security patch*) enam ei väljastata, kõrvaldatakse kasutuselt ja asendatakse seadmetega, millel on tootja tarkvaratugi.

c. Organisatsiooni nutitelefonides ja tahvelarvutites ei kasutata rakendusi (äppe), millel tootja tugi on lõpetatud.

SYS.3.2.1.M6 Privaatsussätete ja rakenduste juurdepääsude haldamine

a. Rakenduste juurdepääs andmetele ja andmevahetusliidestele on rangelt vajaduspõhine. Rakenduse juurdepääsud kinnitab mobiilseadme kasutaja.

b. Privaatsussätted on konfigureeritud maksimaalselt kitsendavaiks.

c. Juurdepääs kaamerale, mikrofonile, kasutaja asukoha- ja terviseandmetele vastab andmekaitsenõuetele. Vajadusel juurdepääs piiratakse või vastav funktsioon desaktiveeritakse.

d. Mobiilirakenduste juurdepääsuõiguste ülevaatust viiakse läbi vastavalt vajadusele.

SYS.3.2.1.M7 Turvasündmusele reageerimise kord [kasutaja]

a. Kasutaja teavitab organisatsiooni kõigist nutitelefoni või tahvelarvutiga seotud turvasündmustest esimesel võimalusel.

b. Turvasündmustest teavitamine toimub läbi määratud teavituskanalite.

c. Seadme kaotuse puhul või tarkvara lubamatute muudatuste avastamisel rakendavad vastutavad töötajad viivitamatult meetmeid andmetele juurdepääsu tõkestamiseks.

SYS.3.2.1.M8 Mobiilirakenduste installimise kord

a. Organisatsioon on määranud, kas ja milliseid äppe on kasutajal lubatud mobiilseadmesse installida.

b. Äppide hankimiseks on määratud lubatavad allikad ja allikate valiku kriteeriumid.

c. Mobiilirakenduste installimine mujalt kui selleks määratud ja lubatud allikaist on keelatud ja võimalusel blokeeritud.

3.3 Standardmeetmed

SYS.3.2.1.M9 Lisafunktsionaalsuse piiramine

a. Nutitelefonide või tahvelarvutite täiendava funktsionaalsuse (nt uute äppide) kasutuselevõttu kaalutakse hoolikalt. Otsese vajaduse puudumisel lisafunktsionaalsusest loobutakse.

b. Täiendava funktsionaalsuse lisamine ei tekita juurdepääsu tundlikele andmetele, väljaarvatud siis kui see on möödapääsmatult vajalik.

c. Lisafunktsionaalsus ei muuda aluskonfiguratsioonis määratud turvaseadeid (vt SYS.3.2.1.M3 *Mobiilseadme turvaline aluskonfiguratsioon*).

SYS.3.2.1.M10 Mobiilseadmete kasutamise eeskiri [kasutaja, infoturbejuht]

a. On koostatud eeskiri mobiilseadmete turvaliseks kasutamiseks.

b. Mobiilseadmete kasutamise eeskiri sisaldab vähemalt järgmist:
   - mobiilseadmete turvalise kasutamise nõuded;
   - mobiilseadmete turvaline hoidmine ajal, kui neid ei kasutata;
   - mobiilseadmete hooldus;
   - juhised mobiilseadme kaotuse või rikke puhul tegutsemiseks.

c. Nutitelefonist ja tahvelarvutist on keelatud eemaldada sinna paigutatud haldustarkvara ja muuta mobiilseadme turvaseadeid.

d. Eeskiri sätestab nutitelefoni ja tahvelarvuti juurimise (ingl *root*) keelu.

SYS.3.2.1.M11 Nutitelefoni ja tahvelarvuti mälu krüpteerimine

a. Nutitelefoni ja tahvelarvuti püsimälu (ingl *read-only memory*, ROM) on krüpteeritud.

b. Tundlikud andmed täiendavatel salvestuskandjatel (nt SD-kaardil) on krüpteeritud.

SYS.3.2.1.M12 Anonüümsete seadmenimede kasutamine

a. Nutitelefonis või tahvelarvutis määratud seadmenimi ei sisaldada viidet organisatsioonile ega kasutajale.

SYS.3.2.1.M13 Ekraanijagamise ja meedia ühiskasutuse kord

a. Ekraanijagamine (ingl *screen sharing*) ning heli ja video ühiskasutus nutitelefonis või tahvelarvutis on korralduslikult või tehniliselt reguleeritud.

b. Kasutajatele on ekraanijagamise ja meedia ühiskasutuse korda tutvustatud.

SYS.3.2.1.M16 Tarbetute sideliideste desaktiveerimine [kasutaja]

a. Sideliidesed on aktiveeritud ainult vajadusel ja ainult sobivas keskkonnas.

b. Kui on kasutusel keskne mobiilseadmete halduse süsteem, hallatakse liideseid selle kaudu.

SYS.3.2.1.M18 Biomeetriline autentimine

a. Biomeetrilise autentimist (nt sõrmejäljeanduri abil) kasutatakse vaid juhul, kui see tagab paroolikaitsega võrreldes vähemalt samaväärse või kõrgema turvalisuse.

b. Biomeetrilise autentimise kaheldava tugevuse puhul biomeetrilist autentimist ei kasutata.

c. Kasutajad on teadlikud, kuidas ründaja võiks üritada biomeetrilisi tunnuseid identiteedivarguse eesmärgil võltsida.

SYS.3.2.1.M19 Virtuaalassistentide kasutamise piiramine

a. Kõnetuvastusega virtuaalassistente (ingl *voice assistant*), nt *Siri* ja *Google Assistant*, kasutatakse ainult tungival vajadusel. Reeglina on see funktsionaalsus seadmes desaktiveeritud.

b. Virtuaalassistendi kasutamine on keelatud, kui seade on lukustatud olekus.

SYS.3.2.1.M22 VPN-i kasutamine ühenduseks sisevõrguga

a. Mobiilseadmete ühendamine sisevõrguga väljastpoolt on võimalik ainult virtuaalse privaatvõrgu (VPN) kaudu.

b. VPN kasutamiseks on loodud sobivad protseduurid. Paroolide asemel kasutatakse sertifikaatidel tuginevat autentimist.

SYS.3.2.1.M28 Veebilehtede filtreerimine

a. Kui organisatsioonis on kasutusel maineteenus (ingl *reputation service*) või vastav proksi (ingl *proxy server*), on see määratud globaalseks HTTP-proksiks kõigis kasutatavates brauserites.

b. Kui proksi on sisevõrgus, on mobiilseade sellega VPN kaudu püsivalt või äpipõhiselt ühendatud.

c. Kui mobiilseadmetes veebilehti proksipõhiselt ei filtreerita, kasutatakse mobiilseadme veebibrauseris mustfiltreerimist (ingl *blacklisting*) või sõltumatu tootja sisufiltritel põhinevat filtreerimist.

SYS.3.2.1.M31 Mobiilmaksete käsitlemise kord

a. Organisatsioonis on kehtestatud kord, mis reguleerib nutitelefonidest ja tahvelarvutitest tehtavaid mobiilmakseid ja nende hüvitamist.

SYS.3.2.1.M32 Keskse mobiilseadmete halduse (MDM) kasutamine

a. Nutitelefonid ja tahvelarvutid on hallatud keskse mobiilseadmete halduse (ingl *mobile device management*, MDM) lahendusega (vt SYS.3.2.2 *Mobiilseadmete haldus (MDM)*).

SYS.3.2.1.M33 Kahjurvaratõrje rakenduse kasutamine

a. Kõikidesse nutitelefonidesse ja tahvelarvutitesse on installitud kahjurvaratõrje rakendus (äpp).

b. Võimalusel on kahjurvara äpp paigaldatud läbi keskse mobiilseadmete halduse lahenduse ning äpi staatus ja häireteated on keskselt hallatavad.

SYS.3.2.1.M34 Turvaline DNS-serveri seadistus

a. Nutitelefoni või tahvelarvuti tootja DNS-server on asendatud organisatsiooni või organisatsiooni teenuseandja DNS-serveriga.

b. Kui teenuseandja võimaldab kasutada DNS-teenust üle HTTPS-i (ingl *DNS over HTTPS,* DoH), on see funktsionaalsus seadmetes aktiveeritud.

3.4 Kõrgmeetmed

SYS.3.2.1.M25 Täitmiskeskkondade lahusus (C-I)

a. Kui töötajad võivad organisatsiooni antud tööseadmeid kasutada ka isiklikuks tarbeks, siis on selleks loodud seadmes eraldi täitmiskeskkond.

b. Võimalusel kasutatakse lahutatud täitmiskeskkondi ainult selleks sertifitseeritud seadmetes (nt Common Criteria alusel).

c. Tööga seotud andmed asuvad eranditult tööotstarbelises täitmiskeskkonnas.

d. Pärast määratud arvu järjestikuseid ebaõnnestunud mobiilseadme avamiskatseid kustutatakse mobiilseadmest tööotstarbelise täitmiskeskkonna andmed.

SYS.3.2.1.M26 PIM kasutamine (C-I-A)

a. Mobiilseadmetes olev isikuteave on kapseldatud PIM (Personal Information Manager, PIM) vahendiga.

b. Isikuteave on kaitstud eraldi autentimise ning operatsioonisüsteemist sõltumatu krüpteerimisega.

SYS.3.2.1.M27 Kõrgturvaline mobiilseade (C-I-A)

a. Organisatsioon kasutab ainult mobiilseadmeid, mis on infotöötluseks lubatud (teabekaitseklassifikatsiooni kohaselt sertifitseeritud või vastavad kehtestatud nõuetele).

SYS.3.2.1.M29 Organisatsioonipõhine pääsupunkt (APN) (C-I-A)

a. Lubatud mobiilseadmete määratlemiseks organisatsioonipõhise pääsupunktiga (ingl *Access Point Name*, APN) on mobiilside teenuseandjaga kokku lepitud tugev, kuni 64-kohaline autentimisparool.

b. Kõik seadmed, mis kasutavad seda APN-i, saavad mobiilside teenuseandjalt organisatsiooniga kooskõlastatud IP-aadressi.

c. Autentimiseks kasutatakse protokolli CHAP (ingl *challenge-handshake authentication protocol*, CHAP).

SYS.3.2.1.M30 Äppide installimise valge nimekiri (C-I-A)

a. Nutitelefoni või tahvelarvuti kasutajal on lubatud installida ainult valges nimekirjas olevaid, kinnitatud ja kontrollitud rakendusi.

b. Mobiilseadmete keskhalduse vahend välistab muude rakenduste installimise või kõrvaldab lubamatud rakendused viivitamatult.

SYS.3.2.1.M35 Mobiilseadmete tulemüür (C-I-A)

a. Nutitelefonides ja tahvelarvutites on paigaldatud ja aktiveeritud lokaalne tulemüür.

4 Lisateave

Lühend	Publikatsioon
[NIST]	NIST Special Publication 800-124 „Guidelines for Managing the Security of Mobile Devices in the Enterprise“

SYS.3.2.2 Mobiilseadmete haldus (MDM)

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed mobiilseadmete halduse (ingl *mobile device management*, MDM) turvaliseks kavandamiseks, evitamiseks ja rakendamiseks.

Mobiilseadmed selle mooduli tähenduses on nutitelefonid ja tahvelarvutid, milles on kasutusel mobiilseadmetele kohandatud operatsioonisüsteemid Android ja iOS.

1.2 Vastutus

Mobiilseadmete halduse meetmete täitmise eest vastutab IT-talitus.

1.3 Piirangud

Moodul täiendab „SYS.3.2.1 *Nutitelefon ja tahvelarvuti üldiselt“* meetmeid mobiilseadmete keskse halduse kontekstis. Nutitelefonide ja tahvelarvutite turbe meetmeid kirjeldatakse lisaks konkreetsete operatsioonisüsteemide moodulites „SYS.3.2.3 *Organisatsiooni iOS“* ja „SYS.3.2.4 *Android“*.

Mobiilseadmete haldamisel järgitakse meetmeid moodulitest OPS.1.1.2 *IT-haldus* ning ORP.4 *Identiteedi ja õiguste haldus*.

Moodul ei käsitle isiklike mobiilseadmete kasutamist tööeesmärkidel (*Bring Your Own Device*, BYOD).

2 Ohud

2.1 Puudulik sünkroonimine

Mobiilseadmete keskse halduse toimimiseks on vajalik haldustarkvara ja mobiilseadme vaheline regulaarne andmevahetus. Kui mobiilseadet pole mobiilseadmete haldustarkvaraga pikka aega sünkroonitud, puudub ülevaade nutiseadme hetkeseisust. Samuti pole võimalik seadmesse keskselt installida uusi rakendusi või muuta reegleid (seadistusi) mille on määranud mobiilseadmete haldurid.

Kui haldustarkvara ei suuda ühenduda kaotatud mobiilseadmega, siis pole võimalik sealt andmeid kaugkustutada. Ründaja võib blokeerida nutiseadme andmesideühendused ja üritada seadmest andmeid kopeerida.

2.2 Vead mobiilseadmete halduses

Mobiilseadmete keskse haldustarkvara seadistamine on keerukas, konfigureerimise tegelik tulemus võib sõltuda erinevates kohtades tehtud seadistuste koosmõjust. Mobiilseadmete haldustarkvara konfigureerimisel tehtud vigu on keeruline tuvastada. Halduses tehtud vead võivad põhjustada mobiilseadmetele mitmesuguseid ohte, mõjutades otseselt või kaudselt andmete ja rakenduste turvalisust.

2.3 Puudulik pääsuõiguste haldus

Mobiilseadmete halduses (ingl *mobile device management*, MDM) on oluline täpselt määrata, kes milliseid seadeid tohib muuta ja kes millistele andmetele juurde pääseb. Kui töötaja

rollile on omistatud liiga suured õigused, võib töötaja saada juurdepääsu andmetele või muuta lubamatult seadme seadistusi. Liigsete õiguste puhul õnnestub töötajal installida mobiilirakendusi, mis ei ole organisatsioonis lubatud (nt kasutada lubamatuid pilvtalletuse teenuseid). Puuduliku õiguste halduse tulemusena võivad tundlikud andmed lekkida. Samuti tekib andmekaitsenõuete rikkumise oht.

2.4 Asukohainfo lubamatu jälgimine mobiilseadmete halduse kaudu

Enamik mobiilseadmete haldusvahendeid näitab, kus konkreetne seade antud hetkel asub. See on erinevatel põhjustel vajalik, nt olenevalt asukohast on võimalik andmeid või rakendusi lubada või blokeerida (nn geotarastus). Paraku tekivad niimoodi ka seadme ja sellega seotud kasutaja üksikasjalikud liikumisprofiilid. Kui neid andmeid kogutakse kasutajat sellest ettenähtud viisil informeerimata, rikutakse seadusandlusest tulenevaid andmekaitsenõudeid. Samuti on oht, et töötajate asukohaprofiilile pääseb juurde ründaja, kes võib seda infot ära kasutada nt väljapressimiseks või varguse toimepanemiseks. Ka organisatsioon võib asukohainfot kuritarvitada töötajate lubamatuks kontrollimiseks.

3 Meetmed

3.1 Elutsükkel

Kavandamine

SYS.3.2.2.M1 Mobiilseadmete halduse põhimõtted

Soetamine

SYS.3.2.2.M3 MDM tarkvara valimine

Evitus

SYS.3.2.2.M2 Mobiilseadmete aktsepteeritud mudelid

SYS.3.2.2.M5 MDM kliendi installimine

SYS.3.2.2.M12 MDM-i turve

SYS.3.2.2.M22 Mobiilseadmete kasutuselt kõrvaldamine

Käitus

SYS.3.2.2.M4 Mobiilseadmete integreerimine MDM tarkvaraga

SYS.3.2.2.M6 Logimine ja seadme oleku seire

SYS.3.2.2.M20 Mobiilseadmete halduse regulaarne läbivaatus

SYS.3.2.2.M7 Mobiilirakenduste (äppide) installimine

SYS.3.2.2.M21 Sertifikaatide haldus

Lisanduvad kõrgmeetmed

SYS.3.2.2.M14 Äppide hindamine välise maineteenuse abil

SYS.3.2.2.M17 Mobiilseadmete kasutamise seire

SYS.3.2.2.M19 Geotarastuse kasutamine

SYS.3.2.2.M23 Vastavusnõuete jõustamine

3.2 Põhimeetmed

SYS.3.2.2.M1 Mobiilseadmete halduse põhimõtted

a. Lähtuvalt töödeldava teabe kaitsetarbest on välja töötatud põhimõtted organisatsioonis kasutatavate mobiilseadmete integreerimiseks organisatsiooni IT-taristuga.

b. Mobiilseadmete halduse (ingl *mobile device management*, MDM) põhimõtted sisaldavad vähemalt järgmist:
   - kas mobiilseadmete haldust tehakse ise, tellitakse väljast või kasutatakse pilvteenust;
   - millised on nõuded haldusteenuse sisule;
   - millised on soovitud reageerimisajad;
   - mis seadustele, poliitikatele ja eeskirjadele mobiilseadmete haldus vastab;
   - milliseid mobiilseadmeid ja operatsioonisüsteeme mobiilseadmete haldus toetab;
   - kas mobiilseadmete halduse lahendus toetab üksteisest sõltumatult hallatavaid seadmegruppe;
   - kas MDM-ga liidestatakse ka dokumendihalduse ja andmetalletuse süsteemid (nt pilvteenused);
   - kas mobiilseadmete haldusesse on kaasatud ka organisatsioonivälised (isiklikud) mobiilseadmeid;
   - milline on mobiilseadmete kasutusmudel (töötajate isiklikud seadmed, organisatsiooni omandis olevad isikustatud seadmed või ühiskasutatavad seadmed).

c. Mobiilseadmete halduse põhimõtted on dokumenteeritud ning kooskõlastatud infoturbejuhiga.

SYS.3.2.2.M2 Mobiilseadmete aktsepteeritud mudelid

a. Enne mobiilseadmete hankimist on määratud, millised seadmeid ja operatsioonisüsteeme võib organisatsioonis kasutada.

b. Kõik hangitud mobiilseadmed ja nende operatsioonisüsteemid vastavad mobiilseadmete halduse põhimõtetele ja organisatsiooni kehtestatud turvanõuetele.

c. MDM tarkvara on konfigureeritud nii, et juurdepääs organisatsiooni teabele on võimalik üksnes sobivaks tunnistatud seadmetest.

SYS.3.2.2.M3 MDM tarkvara valimine

a. Mobiilseadmete halduse (MDM) tarkvara vastab mobiilseadete halduse põhimõtetele.

b. MDM tarkvara võimaldab rakendada tehnilisi ja korralduslikke turvameetmeid.

c. MDM tarkvara toetab kõiki organisatsioonis kasutatavaid mobiilseadmeid.

SYS.3.2.2.M4 Mobiilseadmete integreerimine MDM tarkvaraga

a. Kõik organisatsiooni mobiilseadmed integreeritakse MDM tarkvaraga.

b. MDM tarkvara võimaldab mobiilseadmeid keskselt konfigureerida ning konfiguratsioone keskselt hallata.

c. Enne eelnevalt kasutusele võetud mobiilseadme MDM tarkvaraga integreerimist ja konfigureerimist lähtestatakse mobiilseade tehaseseadetele.

d. Ilma keskselt paigaldatud seadistuseta mobiilseade organisatsiooni siseressurssidele juurde ei pääse.

SYS.3.2.2.M5 MDM kliendi installimine

a. Mobiilseadmete tarbeks on koostatud ja dokumenteeritud sobivad aluskonfiguratsioonid.

b. MDM klient on paigaldatud mobiilseadmesse enne seadme kasutajatele üleandmist. Erandjuhtudel on kasutaja kohustatud MDM kliendi installima ise.

SYS.3.2.2.M20 Mobiilseadmete halduse regulaarne läbivaatus

a. Mobiilseadmete turvasätteid kontrollitakse regulaarselt.

b. Mobiilseadmete operatsioonisüsteemide uute versioonide ilmumisel kontrollitakse, kas MDM operatsioonisüsteemi uuendusi toetab ning kas aluskonfiguratsiooni profiilid ja turvasätted on endiselt tõhusad ja piisavad.

c. Vajadusel muudetakse mobiilseadmete aluskonfiguratsiooni või kohandatakse turvasätteid.

d. Kasutajatele ja halduritele antud õiguste põhjendatust kontrollitakse regulaarselt.

3.3 Standardmeetmed

SYS.3.2.2.M6 Logimine ja seadme oleku seire

a. Mobiilseadmete halduse (MDM) süsteem logib kõik turvasündmused ja konfiguratsiooni muutused kogu mobiilseadme elutsükli vältel.

b. Mobiilseadme turvasündmuste ja konfiguratsiooni muutuste logid on keskselt juurdepääsetavad.

c. Vajadusel on halduril võimalik välja selgitada hallatavate mobiilseadmete hetkeseis.

SYS.3.2.2.M7 Mobiilirakenduste (äppide) installimine

a. Äppe hallatakse MDM kaudu. Pärast äpi kasutuseks lubamist publitseeritakse äpp sisemises äpikataloogis.

b. Mobiilseadmete halduse süsteem käivitab mobiilirakenduste installimise, desinstallimise ja värskendamise kohe pärast mobiilseadmega ühenduse loomist.

c. MDM kaudu installitud äppe ei saa kasutaja desinstallida.

SYS.3.2.2.M12 MDM-i turve

a. Mobiilseadmete halduse turve vastab käideldavate andmete kaitsetarbele.

b. Haldusarvuti operatsioonisüsteem on tugevdatud (ingl *hardening*) ja arvutile on paigaldatud kõik turvauuendid.

SYS.3.2.2.M21 Sertifikaatide haldus

a. Teenuste sertifikaate installitakse, uuendatakse ja desinstallitakse mobiilseadmetes keskselt.

b. MDM süsteem takistab kasutajal ebausaldusväärsete ja kontrollimata (juur)sertifikaatide installimist.

c. MDM süsteem toetab sertifikaatide kehtivuskontrolli mehhanisme.

SYS.3.2.2.M22 Mobiilseadmete kasutuselt kõrvaldamine

a. Mobiilseadmete halduse süsteem võimaldab mobiilseadmes olevate andmete kaugkustutust.

b. Mobiilseadme kõrvaldamise ja registrist kustutamise protsess tagab, et mobiilseadmesse või integreeritud irdandmekandjale ei jääks kaitset vajavaid andmeid.

3.4 Kõrgmeetmed

SYS.3.2.2.M14 Äppide hindamine välise maineteenuse abil (C-I)

a. Kui kasutajatel lubatakse seadmesse ise äppe valida ja installida, tuginetakse otsustamisel välisele maineteenusele (ingl *reputation service*) ja selle kehtestatud eranditele.

b. MDM süsteem piirab äppide installimist, kasutades selleks maineteenusest saadud teavet.

SYS.3.2.2.M17 Mobiilseadmete kasutamise seire (I)

a. Mobiilseadmete seire võimaldab tuvastada seadmete lahtimurdmist (ingl *jailbreaking, rooting*).

b. Mobiilseadmete seirel järgitakse isikuandmete kaitse alaseid regulatsioone.

SYS.3.2.2.M19 Geotarastuse kasutamine (C-I)

a. Geotarastusega (ingl *geofencing*) on tagatud, et tundlikke andmeid sisaldavaid seadmeid ei saa kasutada kindlaksmääratud geograafilisest piirkonnast väljaspool.

b. Lubatavast geograafilisest piirkonnast väljumisel hoiatatakse kasutajat ja haldurit ning pärast määratud ooteaega kustutatakse tundlikud andmed.

c. Geotarastuse piirkonnad on määratud õigusaktide, organisatsiooni nõuete ning kaitsetarbe analüüsi alusel.

SYS.3.2.2.M23 Vastavusnõuete jõustamine (C-I)

a. MDM süsteem tuvastab organisatsiooni nõuete rikkumise ja operatsioonisüsteemi manipuleerimise katsed ning blokeerib seadme automaatselt.

b. Rikkumis- või manipuleerimiskahtluse korral saadab MDM süsteem hoiatuse organisatsiooni vastutavatele halduritele ja infoturbejuhile.

c. MDM süsteem on võimeline kustutama seadmest kas ainult tundlikud või kõik seadmes olevad andmed.

SYS.3.2.3 Organisatsiooni iOS

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed, mida tuleb järgida ja täita kõigi tööülesannete täitmiseks kasutatavate nutitelefonide ja tahvelarvutite puhul, mis töötavad Apple'i operatsioonisüsteemidel iOS ja iPadOS (edaspidi nimetatud iOS-seadmed).

1.2 Vastutus

„Organisatsiooni iOS" meetmete rakendamise eest vastutab IT-talitus.

1.3 Piirangud

Mooduli rakendamine eeldab, et hallatavad iOS-seadmed on integreeritud mobiilseadmete halduse taristusse. Vastavad meetmed on esitatud moodulis SYS.3.2.2 *Mobiilseadmete haldus (MDM)*.

Nutitelefonide ja tahvelarvutitega töötamise üldised ja ühised meetmed, olenemata seadmes kasutatavast operatsioonisüsteemist, on esitatud moodulis „SYS.3.2.1 *Nutitelefon ja tahvelarvuti üldiselt“* ning neid tuleb rakendada ka iOS-põhiste seadmete kasutamisel.

2 Ohud

2.1 iOS seadme lahtimurdmine (jailbreaking)

iOS varasemates versioonides on turvanõrkused, mis võimaldavad Apple'i kehtestatud turvaraamistikust mööduda ning pääseda juurde süsteemiprotsessidele ja kaitstud mälupiirkondadele. Kasutaja võib seda ise soovida teha alternatiivsetest rakendusepoodidest äppide laadimiseks või Apple'i mittesoovitavate laienduste lisamiseks. Sama meetodit kasutavad ründajad kahjurprogrammi installimiseks või iOS seadmes muude kahjulike manipulatsioonide tegemiseks.

2.2 Apple ID konto kuritarvitamine

Apple ID volitustõendi alusel antakse juurdepääs kõigile Apple'i pakutavatele teenustele (nt iCloud, iMessage, FaceTime, App Store, iTunes). Apple ID volitamata kasutamisel on võimalik ründajal kõigile Apple’i teenustele valeidentiteediga juurde pääseda. Samuti võib ründaja häirida Apple ID põhiste teenuste käideldavust, jälgida seadme asukohta, lähtestada tehaseseadeid ning pääseda juurde iCloudis olevatele andmetele. Kui seadmes on aktiveeritud iCloudBackup, on ründajal võimalik kõik kasutaja failid oma iOS-seadmesse kloonida.

2.3 Eelpaigaldatud rakenduste laialdased õigused

iOS-iga koos on Apple’i seadmesse eelpaigaldatud mitmeid operatsioonisüsteemiga tihedalt integreeritud rakendusi (nt Mail ja Safari). Neid rakendusi käitatakse kohati suuremate õigustega kui App Store'ist allalaaditavaid rakendusi. See suurendab rakenduse vastu suunatud ründe õnnestumisel tekitatavat kahju.

2.4 Biomeetrilise autentimise kuritarvitamine

Operatsioonisüsteem iOS sisaldab biomeetrilise autentimise võimalusi, kasutades kas sõrmejälge („Touch ID“) või näotuvastust („Face ID“). „Touch ID“ ja „Face ID“ võimaldavad seadme lihtsustatud avamist või ilma lisakontrollideta rakenduste poest ostude sooritamist. Samuti on võimalik teatud juhtudel asendada Apple ID autentimisel vajaminevat pääsukoodi (ingl *passcode*). Biomeetrilisi turvafunktsioone on sageli võimalik ära petta, kasutades kunstliku sõrme tekitamist sõrmejälje digitaalse puhastamise abil.

2.5 Lukustatud ekraanil näidatavate andmete kuritarvitamine

Operatsioonisüsteemil iOS on funktsioon, mis võimaldab ka lukustatud ekraanilt vaadata aktiveeritud vidinaid (ingl *widget*) ja automaatteavitusi (ingl *push message*). Sel viisil võib kasutaja konfidentsiaalne teave volitamata isikutele nähtavaks saada ning seda saab ära kasutada. Ka digitaalse assistendi Siri kaudu on telefoni funktsioonidele ja kontaktandmetele võimalik juurde pääseda isegi lukustatud olekus.

2.6 Lubamatu juurdepääs väljaspool organisatsiooni hoitavatele andmetele

Mitmete iOS-i spetsiaalfunktsioonide jaoks on vaja kasutada Apple´i käitatavat taristut. Kui kasutatakse funktsioone „iCloud Keychain“, iMessage, FaceTime, Siri, Continuity, „Spotlight Suggestions“ , automaatteavitusi, iCloudi varukoopiate loomist või ühiste dokumentidega töötamise funktsioone, siis sünkroonitakse erinevate seadmete või kasutajate andmed alati Apple'i kesktaristu kaudu. Seetõttu on oht, et Apple'i serverites hoitavatele andmetele juurdepääsu omavad isikud või organisatsioonid võivad kasutada talletatud andmeid kuritegelikel eesmärkidel.

3 Meetmed

3.1 Elutsükkel

Kavandamine

SYS.3.2.3.M1 iOS-põhiste seadmete rakendamise põhimõtted

SYS.3.2.3.M2 Pilvteenuste rakendamise kava

Evitus

SYS.3.2.3.M7 Konfiguratsiooniprofiilide turve

SYS.3.2.3.M13 iOS teenuste ja rakenduste piiramine

SYS.3.2.3.M14 iCloudi kasutamise turve

SYS.3.2.3.M15 „Continuity“ funktsioonide kitsendamine

SYS.3.2.3.M17 Apple ID-ga seotud seadmete hulga piiramine

SYS.3.2.3.M18 Safari turvaline konfiguratsioon

Käitus

SYS.3.2.3.M10 Biomeetriline autentimine

SYS.3.2.3.M12 Apple ID anonüümimine

Lisanduvad kõrgmeetmed

SYS.3.2.3.M21 Rakenduste lisamise ja kinnitamise kord

SYS.3.2.3.M23 Konfiguratsiooniprofiili automaatne kustutamine

SYS.3.2.3.M25 Teenuse AirPrint turvaline kasutamine

SYS.3.2.3.M26 IT-süsteemidega lubamatu ühendamise vältimine

3.2 Põhimeetmed

SYS.3.2.3.M1 iOS-põhiste seadmete rakendamise põhimõtted

a. On välja töötatud ja dokumenteeritud iOS-põhiste seadmete rakendamise põhimõtted, milles on käsitletud:
   - iOS-põhiste seadmete valimise kriteeriumid;
   - iOS-põhiste seadmete haldus ja konfigureerimine;
   - valideerimata rakenduste kasutamine;

- varundusstrateegia.

b. iOS-põhiseid seadmeid hallatakse ja konfigureeritakse mobiilseadmete halduse (MDM) kaudu.

c. iOS-põhise seadme lahtimurdmine (ingl *jailbreaking*) on korralduslikult keelatud ja MDM-ga tehniliselt piiratud.

SYS.3.2.3.M2 Pilvteenuste rakendamise kava

a. Enne iOS-põhiste seadmete kasutuselevõttu on otsustatud pilvteenuste kasutamise võimalikkus ja ulatus.

b. Pilvteenuste rakendamise kavas on kaalutud iCloudi teenuse kasutuse piiramist.

c. Kuna ka Apple ID registreerimine vajab iCloudi teenust, siis võimalusel kasutatakse seadme registreerimiseks Apple Business Manageri (endine Device Enrollment Program, DEP).

SYS.3.2.3.M7 Konfiguratsiooniprofiilide turve

a. On rakendatud korralduslikke ja tehnilisi meetmeid konfiguratsiooniprofiilide lubamatu kustutamise vältimiseks.

b. iOS seadmete kasutajad on teadlikud meetmete vajadusest ja otstarbest.

3.3 Standardmeetmed

SYS.3.2.3.M10 Biomeetriline autentimine

a. „Touch ID“ või „Face ID“ kasutamine on lubatud siis, kui on arvestatud sellega kaasnevaid riske ja kasutajad on määranud seadmele pikema ja keerukama pääsukoodi (ingl *passcode*).

b. Kasutajatele on koostatud biomeetrilise autentimise juhend.

c. Kasutajaid on teavitatud, et „Touch ID“ või „Face ID“ autentimine ei ole täiesti võltsimiskindel.

SYS.3.2.3.M12 Apple ID anonüümimine

a. Apple ID-d nõudvate teenuste puhul kasutatakse isikule viitava Apple ID asemel isikuga mitte seonduvat (nn anonüümset) Apple ID stringi.

b. Võimalusel kasutatakse iOS seadmete ettevalmistamiseks ja keskseks rakenduste installimiseks teenust Apple Business Manager.

SYS.3.2.3.M13 iOS teenuste ja rakenduste piiramine

a. Kõik tarbetud või keelatud teenused ja rakendused on seadme konfigureerimisvalikutes (sh süsteemiseadistuse menüüs „Screen Time“) desaktiveeritud.

b. Aktiveeritud teenused ja rakendused vastavad seadme kasutusotstarbele ja andmete kaitsetarbele.

SYS.3.2.3.M14 iCloudi kasutamise turve

a. Enne iCloudi kasutamist tööülesannete täitmiseks on hinnatud, kas Apple'i teenusetingimused on kooskõlas organisatsiooni infoturbe- ja andmekaitsenõuetega.

b. Kui iCloudi taristu on lubatud, siis autentimisel kasutatakse mitmikautentimist.

SYS.3.2.3.M15 „Continuity“ funktsioonide kitsendamine

a. On hinnatud „Continuity“ funktsioonide (nt „Handoff“, „SMS forwarding“, „Call forwarding“) vajalikkust ja vastavust organisatsiooni nõuetele.

b. Hindamistulemustele tuginedes on „Continuity“ funktsioone tehniliselt või korralduslikult piiratud.

SYS.3.2.3.M17 Apple ID-ga seotud seadmete hulga piiramine

a. Apple ID konfiguratsiooniprofiilis on kontoga ühendatud unikaalsete seadmekoodide arv seatud võimalikult väikseks.

SYS.3.2.3.M18 Safari turvaline konfiguratsioon

a. Safari konfiguratsioon vastab brauseritele kehtestatud üldistele nõuetele ja seal on rakendatud samu piiranguid kui arvutite brauserites.

SYS.3.2.3.M21 Rakenduste lisamise ja kinnitamise kord

a. Rakenduse kasutuselevõtuks läbib äpp organisatsioonisisese tarkvara kinnitusprotseduuri ning App Store'i mobiilirakenduste (äppide) valideerimise.

b. Kõik kasutamiseks kinnitatud mobiilirakendused avaldatakse MDM-i äpikataloogis. Äppide kasutuselevõtuks on MDM-ga integreeritud Apple Business Manager.

c. App Store´i rakenduste makseid ei kinnitata biomeetriliste meetoditega.

3.4 Kõrgmeetmed

SYS.3.2.3.M23 Konfiguratsiooniprofiili automaatne kustutamine (C-I)

a. Kui iOS seade ei ole määratud ajavahemiku jooksul kordagi sisevõrguga ühenduses olnud, kustutatakse konfiguratsiooniprofiil automaatselt.

SYS.3.2.3.M25 Teenuse AirPrint turvaline kasutamine (C-I)

a. Lubatavad AirPrint printerid on lisatud konfiguratsiooniprofiili.

b. Selleks, et kasutajad ei saaks kasutada ebausaldusväärseid printereid, tehakse kõik ühendused printeriga organisatsiooni taristu kaudu.

SYS.3.2.3.M26 IT-süsteemidega lubamatu ühendamise vältimine (C-I)

a. Muude IT-süsteemidega on võimalik iOS-seadmeid ühendada ainult mobiilseadmete halduse süsteemi (MDM) kaudu.

SYS.3.2.4 Android

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed, mida tuleb järgida ja täita kõigi tööülesannete täitmiseks kasutatavate nutitelefonide ja tahvelarvutite puhul, mis töötavad operatsioonisüsteemil Android.

1.2 Vastutus

Androidi meetmete rakendamise eest vastutab IT-talitus.

1.3 Piirangud

Nutitelefonide ja tahvelarvutitega töötamise üldised ja ühised meetmed, olenemata seadmes kasutatavast operatsioonisüsteemist, on esitatud moodulis „*SYS.3.2.1 Nutitelefon ja tahvelarvuti üldiselt*“ ning neid tuleb rakendada ka Androidil põhinevate seadmete kasutamisel.

Androidil põhinevate seadmete keskhalduse meetmed on esitatud moodulis SYS.3.2.2 *Mobiilseadmete haldus (MDM)*.

2 Ohud

2.1 Juurimine (rooting) Androidiga seadmes

Paljude tootjate seadmed, seda eriti vanemate Androidi versioonide puhul, sisaldavad nõrkusi, mis võimaldavad tootja rakendatud turvameetmeid eirata ja anda teatud mobiilirakendustele juurkasutaja juurdepääs (ingl *root access*). Juurimine on igaühel võimalik avalikult kättesaadavate vahendite ning juhendite abil.

Juurkasutaja õigused annavad juurdepääsu operatsioonisüsteemi ja muude rakenduste kaitstud andmetele. Juurkasutaja õigustes kahjurprogrammiga on võimalik seadet ja selles olevaid andmeid manipuleerida. Samuti on võimalik installida kahjurvara seadme või organisatsiooni sisevõrgu ründamiseks.

2.2 Androidiga seadmete kahjurvara

Laia leviku ja avatud arhitektuuri tõttu on Android operatsioonisüsteemiga seadmed kahjurvara jaoks levinud sihtmärk. Androidiga seadmesse on võimalik laadida äppe lisaks Google Play rakendustepoele ka alternatiivsetest allikatest. Samuti võib installifaili kopeerida otse seadmes lokaalseks käivitamiseks. Seetõttu on ka kahjurprogrammide levitamine lihtsam. Ründaja võib näiteks nakatada kahjurvaraga mõne populaarse tasulise äpi ja teha selle kõigile tasuta allalaadimiseks kättesaadavaks.

2.3 Ajakohastamata operatsioonisüsteem

Paljud tootjad tarnivad nutitelefone ja tahvelarvuteid, millel on Androidi aegunud versioonid või mis ei paku operatsioonisüsteemile regulaarseid uuendeid. Androidi avatuse tõttu avastatakse operatsioonisüsteemis pidevalt uusi nõrkusi, seetõttu on Androidiga seadmed rünnete suhtes eriti ohustatud. Probleem esineb eeskätt odavamate mudelite ja vähetuntumate tootjatega. Kuid ka tuntud tootja tippmudeli omamine ei taga uuenditega varustatust kogu seadme eluea jooksul. Seetõttu jäävad tarkvaranõrkused kõrvaldamata ja ründaja võib neid hõlpsasti ära kasutada.

2.4 Google konto kuritarvitamine

Pärast Google’i kontoga (Google Account) autentimist muutuvad kasutajale kättesaadavaks paljud Google poolt pakutavad teenused (nt Google Play, Google Maps, Google Drive, Google Chrome, Gmail jne). Ka paljud teised teenuseandjad Internetis kasutavad kasutajate tuvastamiseks Google ID-d. Kui Google ID on lekkinud, võib iga võõras isik neid autentimisandmeid kuritarvitada. Samuti võib ründaja jälgida seadme asukohta, pääseda juurde seadmes talletatud andmetele, seadme sisu kaugkustutuse teel kustutada või muuta ära tegeliku kasutaja paroolid.

2.5 Eelpaigaldatud rakenduste laialdased õigused Androidis

Koos Android operatsioonisüsteemiga on seadmesse eelpaigaldatud operatsioonisüsteemiga tihedalt integreeritud rakendused (nt Play pood ja nendega seotud Play teenused, Google Chrome brauser), kuid samuti ka mitmeid valideerimata tootjate äppe, mida kasutaja seadmest eemaldada ei saa. See lisab operatsioonisüsteemi nõrkustele ka erinevate rakenduste nõrkused ning neid on võimalik rünnata. Kahjurvaraga nakatunud äpi kaudu on võimalik ründajal pääseda juurde seadmes asuvatele andmetele.

3 Meetmed

3.1 Elutsükkel

Soetamine

SYS.3.2.4.M1 Androidiga seadmete valimise kord

Evitus

SYS.3.2.4.M2 Arendaja sätete desaktiveerimine

SYS.3.2.4.M3 Mitmekasutajarežiimi ja külalisrežiimi piiramine

Käitus

SYS.3.2.4.M5 Laiendatud turbeseaded

3.2 Põhimeetmed

SYS.3.2.4.M1 Androidiga seadmete valimise kord

a. Hangitakse ainult selliseid Android operatsioonisüsteemiga seadmeid, millele tootja väljastab regulaarselt turvauuendeid kuni seadme ettenähtud kasutusaja lõpuni.
b. Androidiga seadmed tarnitakse Androidi ajakohase versiooniga või on võimalik seadmeid ajakohasele versioonile kohe uuendada.

3.3 Standardmeetmed

SYS.3.2.4.M2 Arendaja sätete desaktiveerimine

a. Kõigis Androidiga seadmetes on seadistustes arendaja valikud (ingl *developer options*) desaktiveeritud.

SYS.3.2.4.M3 Mitmekasutajarežiimi ja külalisrežiimi piiramine

a. On määratud, kas Androidi seadmes võib olla aktiveeritud mitmekasutajarežiim või külalisrežiim (ingl *guest mode*).
b. Organisatsiooni androidipõhise seadme kasutaja on üheselt tuvastatav isik.

SYS.3.2.4.M5 Laiendatud turbeseaded

a. Seadmes antakse täieliku juurdepääsuga seadmeadministraatori (ingl *Device Administrator*) õigused ainult kasutamiseks kinnitatud turvarakendustele.
b. Äpile antakse seadmes ainult sellised õigused, mis on äpi tööks nõutavad. Ainult lubatud rakendustel on juurdepääs tundlikele andmetele.
c. Laiendatud õigustega äppide registrit vaadatakse regulaarselt üle.

3.4 Kõrgmeetmed

Moodulis kõrgmeetmed puuduvad.

SYS.3.3 Mobiiltelefon

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed mobiiltelefoni (sh „nuputelefoni“) turvaliseks kasutamiseks mobiilsidevõrgu kaudu telefonside ja sõnumite edastamiseks.

1.2 Vastutus

Mobiiltelefoni meetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Kasutaja.

1.3 Piirangud

Meetmed rakenduvad kõigile mobiiltelefonidele, mida kasutatakse tööülesannete täitmiseks.

Nutitelefonide ja nendes kasutatavate operatsioonisüsteemide turvanõuded on esitatud mooduligrupis SYS.3.2 *Nutitelefon ja tahvelarvuti*. Nutitelefonidele rakendatakse kõiki meetmeid moodulist SYS.3.2.1 *Nutitelefon ja tahvelarvuti üldiselt*.

Andmesidepõhise telefonside aspekte käsitletakse moodulis NET.4.2 *Netitelefon (VOIP)*.

Kui vaadeldav mobiiltelefon kasutab virtuaalse privaatvõrgu tehnoloogiaid, siis tuleb arvesse võtta ka moodulit NET.3.3 *Virtuaalne privaatvõrk (VPN)*.

2 Ohud

2.1 Vead mobiiltelefonide hankimisel

Kui mobiiltelefonidele pole nõudeid määratud ning pole tehtud piisavalt eeltööd, võib juhtuda, et soetatud mobiiltelefonidel puudub mõni oluline funktsionaalsus. Näiteks teatud mobiilsidestandardite funktsionaalsuse realiseerimatajätmine konkreetses telefonis võib tähendada, et telefoni ei saa osades riikides kasutada. Eri riikide vahel liikuvad töötajad võivad vajada mitme SIM-kaardi funktsionaalsusega mobiiltelefoni. Ka infoturbe seisukohast ei pruugi kõikide tootjate telefonimudelid olla lubatud ega vastata organisatsiooni nõuetele.

2.2 Mobiiltelefoni kaotamine

Mobiiltelefonid on tavaliselt kerged ja väikeste mõõtmetega ning neid kantakse pidevalt kaasas. Seetõttu võivad telefonid kergesti maha ununeda, kaotsi minna või osutuda varastatuks. Seadme ostuhinnast suuremat kahju põhjustab seadmesse talletatud andmete kadu. Ründaja võib varastatud mobiiltelefoni kaudu saada juurdepääsu organisatsiooni konfidentsiaalsele teabele.

2.3 Hooletus mobiiltelefoni käsitsemisel

Töötajate tähelepanematust ja hooletust mobiiltelefoni kasutamise ajal võib pahatahtlik isik ära kasutada telefonikõne pealtkuulamiseks või sõnumi kirjutamise jälgimiseks. Nii võib lekkida organisatsiooni jaoks oluline teave. Ründaja võib niiviisi kogutud teavet kasutada suhtlusründe (ingl *social engineering*) ettevalmistamiseks.

2.4 Organisatsiooni mobiiltelefoni kasutamine isiklikuks tarbeks

Organisatsioonile kuuluvate mobiiltelefonide kasutamisel võivad tekkida hooletusvead, mille käigus aetakse segi konfidentsiaalsust nõudvad tööasjad ja personaalne kommunikatsioon. Sel moel võivad volitamata isikud saada organisatsiooni kohta konfidentsiaalset teavet. Töötelefoni kasutamine isiklikuks tarbeks (nt parkimise eest tasumiseks või tasulistele teenusnumbritele helistamiseks) võib organisatsioonile kaasa tuua täiendavaid kulusid.

2.5 Mobiiltelefoni tõrge

Mobiiltelefoni tehnilisel rikkel võib olla erinevaid põhjusi. Telefon võib hooletul käsitsemisel maha kukkuda ja teda võib kahjustada liigne niiskus. Palju probleeme on seotud telefoni akuga, näiteks kui aku on kaotanud energia salvestamise võime. Samuti on võimalik, et kasutaja unustab parooli või PIN-koodi ja seadme kasutamine pärast mitmekordset vale koodi sisestamist blokeeritakse. Kõigil nimetatud juhtudel võib telefon muutuda kasutuskõlbmatuks, kasutaja ei ole enam kättesaadav ega saa ka ise kellegagi mobiiltelefoni teel ühendust võtta.

2.6 Ühendusandmete kuritarvitamine

Mobiilside omaduste tõttu on keeruline takistada edastavate signaalide pealtkuulamist eritehnikaga. Enamikel juhtudel on võimalik üsna täpselt määrata raadioside suhtluspartnerite asukohad. Kogutud teavet on võimalik kasutada helistaja liikumisprofiili koostamiseks.

2.7 Vestluste lubamatu salvestamine

Mobiiltelefone võib väga edukalt kasutada märkamatuks vestluste salvestamiseks või ruumi jäetuna kasutada seda kui pealtkuulamisseadet. Nõupidamistel on võimalik kaasavõetud mobiiltelefonist luua ühendus pealtkuulajatega. Paljude seadmete puhul ei ole ka näha, kas salvestus on sisse lülitatud või mitte.

2.8 Vananenud mobiiltelefonide kasutamine

Turul ületab nutitelefonide pakkumine tunduvalt „nuputelefonide“ pakkumist ja viimaseid peaaegu enam ei toodeta. Piiratud pakkumise tõttu kasutatakse arvukalt vanu, korra juba kasutusest maha võetud mobiiltelefone.

Sageli on neile vananenud mobiiltelefonidele paigaldatud operatsioonisüsteemid, mida enam edasi ei arendata. Seega ei saa tarkvara nõrkusi enam uuenditega kõrvaldada.

Isegi kui kolmandad tootjad pakuvad neile telefonimudelitele varuosi, siis ei ole mingit tagatist, et nendel komponentidel oleks originaalosadega samaväärne kvaliteet. Nii näiteks on järeletehtud akud sageli väiksema vastupidavusega kui originaalakud. Enamasti ei saa neid seadmeid enam remontida ja probleemide tekkimisel ei leidu enam eksperti, kes aidata võiks.

3 Meetmed

3.1 Elutsükkel

Kavandamine

SYS.3.3.M1 Mobiiltelefonide kasutamise eeskiri

Soetamine

SYS.3.3.M7 Mobiiltelefonide hankimise kord

Evitus

SYS.3.3.M3 Kasutajate koolitamine ja teadlikkuse tõstmine

SYS.3.3.M5 Mobiiltelefonide turvamehhanismide kasutamine

SYS.3.3.M8 Tarbetute raadioliideste desaktiveerimine

SYS.3.3.M10 Turvaline andmevahetus

Käitus

SYS.3.3.M2 Mobiiltelefoni blokeerimine seadme kaotamisel

SYS.3.3.M6 Mobiiltelefoni tarkvara ajakohastamine

SYS.3.3.M12 Piisav mobiiltelefonide varu

Kõrvaldamine

SYS.3.3.M4 Mobiiltelefonide kasutuselt kõrvaldamise kord

Avariivalmendus

SYS.3.3.M11 Mobiiltelefoni avariivalmendus

Lisanduvad kõrgmeetmed

SYS.3.3.M9 Mobiiltelefonide toite tagamine

SYS.3.3.M13 Liikumise seire vältimine

SYS.3.3.M14 Telefoninumbri näitamise blokeerimine

SYS.3.3.M15 Kaitse mobiiltelefoniga pealtkuulamise eest

3.2 Põhimeetmed

SYS.3.3.M1 Mobiiltelefonide kasutamise eeskiri

a. Organisatsioonis on koostatud ja kehtestatud mobiiltelefonide kasutamise eeskiri.

b. Mobiiltelefonide kasutamise eeskirjas on määratud vähemalt alljärgnev:

- vajalikud pääsumehhanismid ja nende rakendamine;
- lubatavad teenused (sh lubatavad teenused välismaal);
- mobiiltelefoni turvaline kasutamine;
- konfidentsiaalsete andmete käitlemine;
- mobiiltelefoni kasutamine isiklikuks otstarbeks:
- mobiiltelefonide haldus ja hooldus;

- toimingud mobiiltelefoni või SIM-kaardi kaotuse või varguse puhul.

c. Mobiiltelefoni kasutaja veendub alati suhtluspartneri tegelikus identiteedis (nt katkestades sissetuleva kõne ja helistades tagasi ametlikule numbrile).

d. Sõidu ajal tohib mobiiltelefoni kasutada ainult „käed-vabad“ seadmega.

e. Konfidentsiaalse teabe edastamisel veendub töötaja, et tema vahetus läheduses ei ole inimesi, kes võiksid kõnet pealt kuulata.

f. Iga kasutaja on mobiiltelefonide kasutamise eeskirjaga tutvunud.

g. Mobiiltelefonide kasutamise eeskirja järgimist kontrollitakse regulaarselt.

h. Võimalike anomaaliate ja eksimuste tuvastamiseks kontrollitakse sideteenuste arveid telefoninumbrite haaval.

SYS.3.3.M2 Mobiiltelefoni blokeerimine seadme kaotamisel [kasutaja]

a. Mobiiltelefoni kaotamisel blokeeritakse telefoni SIM-kaart viivitamatult.

b. Vargusvastaste kaugmehhanismide olemasolul blokeeritakse mobiiltelefon või kustutatakse selle sisu viivitamatult.

c. SIM-kaardi ja mobiiltelefoni blokeerimiseks nõutav teave on halduritele koheselt kättesaadav.

SYS.3.3.M3 Kasutajate koolitamine ja teadlikkuse tõstmine

a. Mobiiltelefoni turvaline kasutamine on lisatud töötajate infoturbe koolitusprogrammi.

b. Kasutajatele on mobiiltelefonidega seotud ohte tutvustatud.

c. Kasutajad tunnevad ära petukõned ja petusõnumid ning oskavad neile reageerida.

d. Kasutajad oskavad kasutada mobiiltelefonide turvafunktsionaalsust.

e. Kasutajad oskavad oma mobiiltelefoni ja SIM-kaarti telefoni kaotamise järgselt blokeerida.

SYS.3.3.M4 Mobiiltelefonide kasutuselt kõrvaldamise kord

a. Enne mobiiltelefoni kasutuselt kõrvaldamist taastatakse mobiiltelefoni tehaseseaded (mis ühtlasi kustutab telefonist ka kasutaja andmed) ja kontrollitakse, kas kõik andmed on telefonist kustutatud.

b. Kui andmeid ei õnnestu telefonist kustutada, hävitatakse seade füüsiliselt.

c. Mobiiltelefoni kasutuselt kõrvaldamisel võetakse telefonist välja ja kustutatakse turvaliselt või hävitatakse telefonis olev mälukaart (vt CON.6 *Andmete kustutus ja hävitamine*)

d. Kui mobiiltelefone tuleb enne kõrvaldamist hoiustada (nt niikaua kuni telefone on kogunenud suurem kogus), siis kaitstakse kogutud mobiiltelefone ja mälukaarte lubamatu juurdepääsu eest.

SYS.3.3.M5 Mobiiltelefonide turvamehhanismide kasutamine [kasutaja]

a. Mobiiltelefonidesse integreeritud turvamehhanismid on konfigureeritud ja kasutusele võetud.

b. SIM-kaardi algne PIN-kood on asendatud piisavalt keerulise PIN-koodiga.

c. Käivitamisel küsib telefon PIN-koodi.

d. Mobiiltelefon on kaitstud seadmeparooli või muu turvamehhanismiga.

e. Pääsukoode (sh PUK-koodid) ja teenuste paroole hoitakse mobiiltelefonist lahus ja neid kasutatakse ainult määratud otstarbeks.

f. Mobiiltelefoni ekraanilukk rakendub mõne minutiga.

SYS.3.3.M6 Mobiiltelefoni tarkvara ajakohastamine [kasutaja]

a. Kontrollitakse regulaarselt, kas mobiiltelefonile on tarkvarauuendeid.

b. On määratud, kas kasutajad installivad uuendeid ise või tehakse seda keskselt.

c. Mobiiltelefonide uuendid laaditakse telefoni viivitamata.

3.3 Standardmeetmed

SYS.3.3.M7 Mobiiltelefonide hankimise kord

a. Enne mobiiltelefonide hankimist on koostatud nõuete spetsifikatsioon.

b. Telefone valitakse lähtuvalt nõuete spetsifikatsioonist.

c. Hankimisel arvestatakse tarnijalt saadavat kliendituge ja varuosade (nt akud, laadimisseadmed) saadavust.

SYS.3.3.M8 Tarbetute raadioliideste desaktiveerimine [kasutaja]

a. Vajaduse puudumisel või kasutamise vaheaegadel on mobiiltelefonide raadioliidesed (nt WLAN või Bluetooth) desaktiveeritud.

SYS.3.3.M10 Turvaline andmevahetus[kasutaja]

a. Andmete töötlemine mobiiltelefonis on reguleeritud mobiiltelefonide kasutamise eeskirjas (vt SYS.3.3.M1 *Mobiiltelefonide kasutamise eeskiri*).

b. On määratud, milliseid liideseid tohib andmevahetuseks kasutada ja kas andmed tuleb transportimisel krüpteerida.

c. Meilivahetusel mobiiltelefoni kaudu on meilimanuste automaatne laadimine blokeeritud.

SYS.3.3.M11 Mobiiltelefoni avariivalmendus [kasutaja]

a. Mobiiltelefonisse salvestatud andmeid (nt kontakte ja sõnumeid) varundatakse regulaarselt telefonist eemal asuvasse asukohta.

b. Olulised mobiiltelefonide pääsu- ja konfiguratsiooniandmed on dokumenteeritud

c. Enne defektse mobiiltelefoni remonti saatmist eemaldatakse sellest SIM-kaart ja mälukaart ja kui võimalik, siis kustutatakse telefonist kõik andmed ja lähtestatakse telefon tehaseseadetele.

d. Mobiiltelefone remonditakse usaldusväärses ettevõttes.

e. Mobiiltelefonide rikete puhuks on alati varuks asendustelefonid.

f. Kriitilistel ametikohtade täitjatel on lisaks mobiiltelefoniga suhtlemisele võimalik kasutada ka alternatiivset sidekanalit.

SYS.3.3.M12 Piisav mobiiltelefonide varu

a. Kui organisatsioonis on palju mobiiltelefone või telefonikasutajad vahetuvad sageli, hoitakse piisaval hulgal telefone varuks.

b. Mobiiltelefonide ja tarvikute väljastamine ja tagastamine dokumenteeritakse.

c. Enne kasutuseks väljastamist varustatakse mobiiltelefonid uuele omanikule vajalike programmide ja andmetega.
d. Mobiiltelefonide tagastamisel kustutatakse telefonist andmed ja lähtestatakse telefon tehaseseadetele.
e. Mobiiltelefoni vastuvõtja kontrollib tagastatud või üleantud seadmete komplektsust, seisundit ja konfiguratsiooni.

3.4 Kõrgmeetmed

SYS.3.3.M9 Mobiiltelefonide toite tagamine [kasutaja] (A)

a. Mobiiltelefonide toite tagamiseks hoitakse telefoni aku piisavalt laetuna.
b. Pikemaajalisel mobiiltelefoni kasutusel kantakse kaasas laadurit ja/või akupanka.
c. Aku säästmiseks välditakse äärmuslikke temperatuure ja lülitatakse välja mittevajalikud raadioliidesed.

SYS.3.3.M13 Liikumise seire vältimine [kasutaja] (C)

a. On otsustatud, kas töötajate asukohaandmete kättesaadavus omab sellist negatiivset mõju, mille vähendamiseks tuleb rakendada täiendavaid meetmeid.
b. Mobiiltelefonis ei kasutata GPS-andmeid töötlevaid valideerimata rakendusi.
c. GPS-i funktsionaalsus mobiiltelefonis desaktiveeritud, kuniks GPS kasutamiseks pole otsest vajadust.
d. Kui konkreetsete töötajate asukohateave on salastatud, vahetatakse tihti nende töötajate telefone ja SIM-kaarte.
e. Kui töötaja asukohta ei tohi saada ajutiselt tuvastada, lülitatakse mobiiltelefon välja ja eemaldatakse sellelt aku.

SYS.3.3.M14 Telefoninumbri näitamise blokeerimine [kasutaja] (C)

a. Väljuvate kõnede numbri näitamine on telefonis desaktiveeritud.
b. Varjatud telefoninumbriga SIM-kaarti kasutavast telefonist ei saadeta SMS- ja MMS-sõnumeid.
c. Mobiiltelefoni numbrit ei avaldata ega saadeta kolmandatele isikutele.

SYS.3.3.M15 Kaitse mobiiltelefoniga pealtkuulamise eest (C)

a. Mobiiltelefonide kaasavõtmine konfidentsiaalsetele nõupidamistele on keelatud.
b. Telefonikeeluga ruumide sissekäigu juures on selgelt mõistetavad keelusildid ja ettevalmistatud kohad telefonide turvalise hoiustamiseks.
c. Vajadusel kontrollitakse ruumi mobiiltelefonide detektoriga.

SYS.4: Muud süsteemid

SYS.4.1 Printer ja kontorikombain

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed printeri ja kontorikombaini turvaliseks kasutamiseks.

Tänapäevased printerid, koopiamasinad ja kontorikombainid on keerukad võrgustatud seadmed ja sageli töödeldakse neis konfidentsiaalset teavet.

Märkus: edaspidi koopiamasinaid eraldi ei mainita, aga paljusid selles moodulis toodud ohte ja meetmeid tuleb arvestada ja rakendada ka koopiamasinate puhul**.**

1.2 Vastutus

„Printer ja kontorikombain“ meetmete rakendamise eest vastutab IT-talitus.

Lisavastutajad

Infoturbejuht.

1.3 Piirangud

Moodulis esitatud meetmed kehtivad kõikide organisatsiooni võrku ühendatud printerite, kontorikombainide ja koopiamasinate kasutamisel. Seetõttu rakendatakse meetmeid mooduligrupist NET.1 *Võrgud.* Raadiokohtvõrku (WLAN) kasutavate seadmete kaitseks rakendatakse täiendavalt meetmeid moodulist NET.2.2 *Raadiokohtvõrgu kasutamine*.

Printeritesse ja kontoriseadmetesse salvestatud või väljatrükitud teabe turvalist kõrvaldamist käsitletakse moodulis CON.6 *Andmete kustutus ja hävitamine*.

Prindiserveri (IT-süsteemid, mis võimaldavad prindijärjekorra ja printimistaotluste haldamist) puhul rakendatakse serveri üldisi (vt SYS.1.1 *Server üldiselt*) ja operatsioonisüsteemikohaseid turvameetmeid. Printeri ja kontorikombaini tarkvara regulaarset ajakohastamist käsitletakse moodulis OPS.1.1.3 *Paiga- ja muudatusehaldus*.

2 Ohud

2.1 Prinditud dokumentide lubamatu nähtavalejätmine

Kasutajad jätavad prinditud dokumente sageli pikaks ajaks printerite ja kontorikombainide väljastussalve (nt et käia prinditud dokumentidel järel ainult ühe korra). Samuti võib juhtuda, et kasutaja valib kogemata vale printeri, mis asub asukohas, kuhu kasutaja dokumendile järele ei lähe.

Korruse- ja osakonnaprintereid kasutavad või neist mööduvad paljud töötajad, seetõttu võib tundliku teabega dokument sattuda volitamata isiku kätte. Ka lokaalse printeri juurde võib sattuda kõrvalisi isikuid (nt koristaja).

Sageli visatakse pikalt seisnud väljatrükid lähedalasuvasse prügikasti. Sealt võivad väljatrükid sattuda jäätmekäitlusettevõttesse ja edasi volitamata isikute kätte.

Samad ohud eksisteerivad kaugtöökohas, mis on varustatud lokaalse printeriga. Ka sealt võib tundlik teave paberdokumentide kujul lekkida.

2.2 Metaandmete nähtavus

Koos prinditööga saadetakse prindiserverisse metaandmed, mis sisaldavad tavaliselt kasutajatunnust, kuupäeva, kellaaega ja prinditöö nime. Prindiserveris on metaandmed vaadeldavad lihtteksti kujul (juhul kui neid pole anonüümitud). Teatud seadmete puhul näidatakse neid andmeid seadme juhtpaneelil ning samuti printeri või kontorikombaini veebiserveris. Nii on printimistegevusi võimalik jälgida brauseri kaudu.

Teatud printerid ja paljundusmasinad prindivad paberile nn kollatäpid (ingl *yellow dots, machine identification code, tracking dots*). Need vesimärgid on palja silmaga vaevu nähtavad, aga võivad sisaldada kuupäeva ja kellaaega ning printeri seerianumbrit. Sel viisil saab prinditud dokumendi siduda konkreetse organisatsiooni või kasutajaga ja autori tagantjärele kindlaks teha.

2.3 Salvestatud teabe ebapiisav kaitse

Printerid ja kontorikombainid on varustatud säilmäluga (ingl *non-volatile memory*) või kõvakettaga, kus andmeid kas ajutiselt või pikaajaliselt talletatakse (nt aadressiraamatud ja prinditavad dokumendid). Kui need andmed ei ole piisavalt kaitstud, on võimalik säilmälu sisule juurde pääseda. Ebaturvaliste kustutamismeetodite kasutamisel saab ründaja teatud juhtudel isegi kustutatud teabe taastada.

Andmeid saab printerisse salvestada võrguprotokollide kaudu, mistõttu on oht, et printerit kasutakse lubamatu failiserverina.

2.4 Krüpteerimata side

Prinditud ja skaneeritud andmeid edastatakse võrgus sageli krüpteerimata kujul. Nii on ründajal võimalik printerisse saadetavaid andmeid pealt kuulata, samuti lugeda prindiserverites ajutiselt salvestatud prindifaile.

Kui seadmete haldus toimub krüpteerimata liideste kaudu (nt kui printeritele on juurdepääs HTTP, SNMPv2 või Telneti kaudu), siis on ohus ka seadmete pääsuandmed ja paroolid.

2.5 Dokumentide lubamatu edastamine

Paljusid võrgustatud printereid saab konfigureerida Internetist prinditöid vastu võtma e-postiga. Samuti on võimalik skaneeritud dokumente välja saata e-kirja manusena. Nii võivad dokumendid kas teadlikult või tahtmatult sattuda volitamata vastuvõtjate kätte. See võib näiteks juhtuda, kui kasutajad sisestavad saaja aadressi vääralt. Saatja aadressi vaba sisestamist saab kuritarvitada, saates sisemistele ja välistele adressaatidele võõra nime all e-kirju.

2.6 Dokumentide lubamatu kopeerimine ja skaneerimine

Paberdokumente saab kontorikombainiga kiiresti ja kvaliteetselt kopeerida. Kontorikombaini USB- või SD-ühenduste abil on võimalik ka suures koguses paberdokumente otse ja ilma igasuguse kontrollita digitaliseerida, mälupulkadele või SD-kaartidele salvestada ja neid märkamatult endaga kaasa võtta.

Võrguliidese kaudu on võimalik juurde pääseda teiste kasutajate poolt printeri või kontorikombaini säilmälusse salvestatud digitaalsetele dokumentidele ning neid lubamatult kopeerida või välja trükkida.

2.7 Ebapiisav võrguturve

Kohtvõrgu ja Interneti vahelised tulemüürid on sageli konfigureeritud nii, et Interneti-ühendus on lubatud tervele alamvõrgule. Sageli on printerid ja kontorikombainid määratud samasse alamvõrku mis tööjaamad. Seetõttu pääseb ka võrguprinterist juurde Internetis

olevale teabele. Kui turvalüüsid ei blokeeri printeritesse sisenevat ja sealt väljuvat Interneti-liiklust, siis on võimalik printeri kaudu tundlikke andmeid võrgust välja saata. Samuti võib seade Internetist andmeid vastu võtta ja edasi jagada. Võrguprinter võib seetõttu muutuda Internetist lähtuvate rünnete sissepääsuväravaks.

2.8 Seadmete halduse ebapiisav turve

Võrgustatud printereid ja kontorikombaine saab hallata juhtpaneeli ja seadme veebiserveri kaudu. Seadmete tüüpseadetes algselt parool puudub või kasutatakse lihtsat ning teadaolevat vaikeparooli. Kui seadme pääsuparooli ei määrata või ei muudeta, on võimalik seadmetele väga lihtsalt juurde pääseda.

Paljudes organisatsioonides kasutatakse kõigi printerite ja kontorikombainide jaoks ühtseid paroole, mida muudetakse harva. Seetõttu teavad neid paljud organisatsioonisisesed ja -välised isikud ning seda võidakse seadmele lubamatu juurdepääsu saamiseks ära kasutada.

Printereid ja kontorikombaine on võimalik otse seadme juhtmenüüst tehaseseadetele lähtestada, mille käigus muudetakse ära ka turvaseaded. Nii näiteks muutub seatud parool tagasi algseks parooliks.

Printerid ja kontorikombainid toetavad paljusid võrguprotokolle, mis on algseadistuses enamasti kõik ka aktiveeritud. See annab ründajale võimaluse printeri või kontorikombaini konfiguratsiooni manipuleerida.

Suurtes organisatsioonides kasutatakse seadmete keskseks halduseks seadmehaldustarkvara. Kuid paljud organisatsioonid ei kaitse seda tarkvara piisavalt lubamatu juurdepääsu eest. Seadmehaldustarkvara kaudu printereid ja kontorikombaine manipuleerides võib ründaja tekitada märkimisväärset kahju.

3 Meetmed

3.1 Elutsükkel

Kavandamine

SYS.4.1.M1 Printerite ja kontorikombainide rakendamise kava

SYS.4.1.M4 Printerite ja kontorikombainide turvaeeskiri

Evitus

SYS.4.1.M2 Printeri ja kontorikombaini füüsilise juurdepääsu piiramine

SYS.4.1.M5 Printerite ja kontorikombainide kasutamise eeskiri

SYS.4.1.M7 Printeri ja kontorikombaini halduspääsu kitsendamine

SYS.4.1.M11 Printeri ja kontorikombaini võrguühenduse piiramine

SYS.4.1.M17 Ajutiste andmete ja metaandmete turve

SYS.4.1.M18 Printeri ja kontorikombaini turvaline konfiguratsioon

Käitus

SYS.4.1.M15 Andmete krüpteerimine printeris ja kontorikombainis

SYS.4.1.M16 Printeri ja kontorikombaini seisakuaja vähendamine

Kõrvaldamine

SYS.4.1.M22 Prinditud dokumentide kasutuselt kõrvaldamise kord

Lisanduvad kõrgmeetmed

SYS.4.1.M14 Seadme kasutaja täiendav autentimine

SYS.4.1.M20 Printeri ja kontorikombaini andmestiku täiendav turve

SYS.4.1.M21 Printeri ja kontorikombaini laiendatud turve

3.2 Põhimeetmed

SYS.4.1.M1 Printerite ja kontorikombainide rakendamise kava

a. Organisatsioon on koostanud ja dokumenteerinud printerite ja kontorikombainide rakendamise kava, mis määrab:
   - millised on printerite ja kontorikombainide vajalikud funktsioonid ja tootlus;
   - kas printerid ja kontorikombainid ostetakse või renditakse;
   - kas kasutatakse lokaalseid või võrgustatud seadmeid;
   - kellel on printerite ja kontorikombainide kasutus- ja haldusõigused;
   - milliste ohtude eest tuleb seadmeid kaitsta;
   - millised on andmeedastuse ja seadme füüsilise turbe nõuded;
   - mis on nõutavad andmeedastusprotokollid ja failivormingud;
   - kuidas on takistatud juurdepääs võõrastele dokumentidele;
   - kuidas korraldatakse printerite ja kontorikombainide hooldust ja kulumaterjalidega varustamist;
   - kuidas tagatakse printerite ja kontorikombainide käideldavus;
   - kuidas korraldatakse kasutajate ja haldajate koolitus.

b. Printeritele ja kontorikombainidele on planeeritud sobivad turvalised asukohad.

SYS.4.1.M2 Printeri ja kontorikombaini füüsilise juurdepääsu piiramine

a. Printerid ja kontorikombainid on paigutatud asukohtadesse, kus töötamine seadmega on teistele töötajatele märgatav ja kus ei käi ilma saatjata külalisi.

b. Printereid ja kontorikombaine haldavad ainult haldusõigusega isikud. Teenuseandjaga (nt hoolduseks ja remondiks) on sõlmitud kirjalikud konfidentsiaalsuskokkulepped.

c. Printerite ja kontorikombainide konfigureerimine juhtpaneeli ja veebiserveri kaudu on paroolikaitsega.

SYS.4.1.M5 Printerite ja kontorikombainide kasutamise eeskiri [infoturbejuht]

a. Infoturbejuht on printerite ja kontorikombainide kasutajatele koostanud eeskirja printerite ja kontorikombainide turvaliseks käsitsemiseks.

b. Printerite ja kontorikombainide kasutamise eeskiri sisaldab vähemalt järgmist:
   - kuidas valida printerit (nt mitmete võrgustatud printeri hulgast);
   - kuidas tuleb end seadme kasutamiseks autentida (juhul kui seda funktsiooni kasutatakse);
   - kohustus prinditud dokumendi koheseks eemaldamiseks või hävitamiseks;
   - kuidas kasutada seadme mälu;

- kuidas käituda tehniliste probleemide ja rikete korral;
- tundlike dokumentide printimise ja kopeerimise piirangud.

c. Printerite ja kontorikombainide kasutamise eeskirja on tutvustatud kõikidele kasutajatele.

d. Olulisemad juhised on vormistatud printerite ja kontorikombainide juures nähtava teabelehena.

SYS.4.1.M22 Prinditud dokumentide kasutuselt kõrvaldamise kord

a. Tarbetute tundlikku teavet sisaldavate dokumentide kõrvaldamiseks on kehtestatud kord.

b. Printeri või kontorikombaini läheduses asub paberipurusti või hävitamisele minevate paberdokumentide konteiner.

c. Ekslikult prinditud tarbetu dokument hävitatakse kohe, ekslikult skännitud dokument kustutatakse.

3.3 Standardmeetmed

SYS.4.1.M4 Printerite ja kontorikombainide turvaeeskiri [infoturbejuht]

a. Organisatsioonis on koostatud ja dokumenteeritud printerite ja kontorikombainide turvaeeskiri, mis sätestab seadmetes andmete töötlemise turvanõuded ja tingimused.

b. Printerite ja kontorikombainide turvaeeskirjas on määratud:

- seadme füüsilise ja tehnilise turbe nõuded;
- võrgustatud seadme võrguspetsiifilised turvanõuded;
- pääsuõiguste korraldus;
- käideldavuse tagamine;
- seadmete halduse nõuded;
- krüpteerimise kasutamine;
- seadmete turvaline kõrvaldamine.

SYS.4.1.M7 Printeri ja kontorikombaini halduspääsu kitsendamine

a. Printerite ja kontorikombainide halduspääs on võimaldatud ainult määratud halduritele ja hooldustehnikutele.

b. Keskse seadmehaldustarkvara kasutamisel on haldusvahendi pääsuõigused antud ainult määratud halduritele.

c. Juurdepääs seadmele on võimalik alles pärast kasutaja autentimist (nt parooli või PIN-koodi abil).

d. Kaugjuurdepääs on võimalik ainult pärast kasutaja autentimist.

e. Ühendused on krüpteeritud (nt HTTPS või SNMPv3 abil).

f. Krüpteerimata ühenduste kasutamine on blokeeritud.

g. Kõik printeri või kontorikombaini pordid, mida ei ole vaja printimiseks ja printeri halduseks, on võimalusel blokeeritud.

h. Printerite ja kontorikombainide juhtpaneeli kuva kaugseire on lubatud ainult määratud halduritele.

i. Printerite ja kontorikombainide liigsed ja tarbetud funktsioonid on desaktiveeritud.

SYS.4.1.M11 Printeri ja kontorikombaini võrguühenduse piiramine

a. Olenemata seadmete lokaalsest seadistusest on võrguprinterite ja kontorikombainide ühendus välisvõrgust blokeeritud keskses tulemüüris (ingl *firewall*).

b. Prindiserveri kasutamisel on printerite ja kontorikombainidega võimalik ühenduda ainult prindiserverist ja haldurite tööjaamadest, kust seadmeid konfigureeritakse ja seiratakse.

c. Halduse lihtsustamiseks on võrguprinterid ja kontorikombainid paigutatud eraldatud võrgusegmenti.

d. Telefonivõrku ühendatud kontorikombainid ei ole kohtvõrku ühendatud või on kohtvõrgust eraldatud täiendava tulemüüriga.

e. Kui kontorikombaini faksi- ja modemifunktsionaalsus pole vajalik, on lähedalasuvad telefoni pistikupesad telefonijaamast lahti ühendatud või kontorikombaini telefonivõrgu liides seadmest eemaldatud.

SYS.4.1.M15 Andmete krüpteerimine printeris ja kontorikombainis

a. Kui printer või kontorikombain andmete krüpteerimist võimaldab, on seadme mälus olev informatsioon krüpteeritud.

b. Prinditööd edastatakse printerile krüpteerimist võimaldavate protokollide kaudu (TLS/SSL koos IPP protokolliga). Krüpteerimist mittetoetavaid printimisprotokolle (nt Unixi LPR/LPD ja Windowsi SMB/CIFS) ei kasutata.

SYS.4.1.M16 Printeri ja kontorikombaini seisakuaja vähendamine

a. Printerite ja kontorikombainide tõrgetest ja hooldusest tingitud seisakuajad on nii lühikesed kui võimalik.

b. Printerite ja kontorikombainide kulumaterjalide varu on alati piisav.

c. Võimalusel hoitakse sageli vajaminevaid varuosi kohalikus laos ja vahetatakse varuosa ilma välist hooldustehnikut kutsumata.

d. Kriitilisemate seadmete asenduseks on alati olemas sarnase funktsionaalsusega asendusseade.

e. Hoolduslepingutega on tagatud piisavalt kiire reageerimisaeg. Varuosasid on vajadusel võimalik hankida erinevatelt tarnijatelt.

SYS.4.1.M17 Ajutiste andmete ja metaandmete turve

a. Ajutisi andmeid ja metaandmeid (näiteks prinditööde ja skaneerimisfailide andmed) salvestatakse seadmetesse nii lühikeseks ajaks kui võimalik ja need ei ole kõrvalistele isikutele nähtavad.

b. Ajutised andmed ja metaandmed kustutatakse määratud aja möödumisel automaatselt.

c. Seadme sisemine failiserver ja mälusse salvestatud objektide nimekirja väljastamise funktsioonid on desaktiveeritud.

SYS.4.1.M18 Printeri ja kontorikombaini turvaline konfiguratsioon

a. Printereid ja kontorikombaine konfigureerivad ainult selleks volitatud haldurid.

b. Mittevajalikud funktsioonid ja võrguliidesed on konfiguratsioonis desaktiveeritud.

c. Eelseadistatud paroolid on muudetud.

d. Halduse andmesides kasutatakse krüpteeritud protokolle (HTTPS, SNMPv3).

e. Ebaturvalised, krüpteerimist mitte kasutavad protokollid (SNMP, Telnet, PJL) on blokeeritud.

3.4 Kõrgmeetmed

SYS.4.1.M14 Seadme kasutaja täiendav autentimine (C-I-A)

a. Juurdepääs prinditud või kopeeritud dokumentidele on ainult pääsuõigustega isikutel.
b. Kasutatakse ainult keskselt hallatavaid printereid ja kontorikombaine.
c. Kasutajad peavad end väljatrüki printerist kättesaamiseks või skanneri kasutamiseks autentima (nt kasutaja pääsukaardiga seotud *Secure-Print* lahenduse abil).
d. Autenditud kasutaja saab kasutada ainult talle lubatud funktsioone ning näha ainult enda prinditöid.

SYS.4.1.M20 Printeri ja kontorikombaini andmestiku täiendav turve (C)

a. Prinditööde nimed prindiserveris on anonüümitud.
b. Seadme väliste salvestuskandjate liidesed on blokeeritud.
c. Seadme sisemise aadressiraamatu kasutamine on blokeeritud.
d. e-posti funktsiooniga printeritest ja kontorikombainidest saab dokumente e-posti teel saata ainult sisemistele meiliaadressidele.
e. Sissetulevad faksidokumendid ja saatmisteated on kättesaadavad ainult volitatud kasutajatele.

SYS.4.1.M21 Printeri ja kontorikombaini laiendatud turve (I-A)

a. Printerite ja kontorikombainide turvasätteid kontrollitakse regulaarselt ja vajadusel korrigeeritakse.
b. Võimalusel kasutatakse seadmete konfiguratsiooni kontrollimiseks automaatset kontrollisüsteemi.
c. Seadmete buutimismenüüst tehaseseadete lähtestamise võimalus on blokeeritud.
d. Printerites ja kontorikombainides ei kasutada püsivara ega tarkvara, millel pole konkreetse seadmetootja heakskiitu.

SYS.4.3 Sardsüsteemid (*embedded systems*)

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed sardsüsteemide (ingl *embedded systems*) turvaliseks kasutamiseks.

Sardsüsteem on spetsiaalse riist- ja tarkvaraga, määratud andmetöötlusülesannet täitev funktsionaalüksus, mis on integreeritud laiema IT-süsteemi või toote koosseisu. Sardsüsteemid täidavad juhtimise, reguleerimise ja andmetöötlusega seotud ülesandeid (nt lennuki arvutisüsteem, eriotstarbeline meditsiinitehnika või andmesidekeskuse komponent). Sardsüsteem on programmeeritav ning üldjoontes sarnane universaalse arvutiga, kuid tema tarkvara hoitakse EEPROM-is ja ROM-is. Sardsüsteemil puudub tavapärane kasutajaliides.

Sardsüsteemi sisenditeks ja väljunditeks on andmesiinid ja lokaalsed pordid. Mõnda tüüpi sardsüsteemidel on ka veebiliides sardsüsteemi konfigureerimiseks.

1.2 Vastutus

Sardsüsteemide meetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Hankeosakond, arendaja, arhitekt.

1.3 Piirangud

Moodul ei käsitle spetsiifiliste sardsüsteemides kasutatavate riist- ja tarkvaraarhitektuuride erisusi.

Tööstuslikes juhtsüsteemides kasutatavate sardsüsteemide turvaaspektid on esitatud mooduligrupis IND (Tööstuse IT).

Selle mooduli käsitlusalasse ei kuulu ka esemevõrgusüsteemide turvaaspektid. Erinevalt sardsüsteemidest ei ole nutifunktsioone omavad võrgustatud esemevõrgusüsteemid integreeritud suuremasse süsteemi või tootesse. Nende traadita ühenduse tõttu andmesidevõrkudega tuleb rakendada erinevaid turvameetmeid, mida käsitletakse moodulis SYS.4.4 *Esemevõrgu (IoT) seade üldiselt*.

2 Ohud

2.1 Puudulikud turvanõuded sardsüsteemide väljatöötamisel

Sardsüsteemide (ingl *embedded systems*) arendamisel on turvalisus sageli jäänud finantskaalutlustel funktsionaalsuse ja sooritusvõime kõrval tahaplaanile. Kui süsteemi arenduse ühel või mitmel arendusetapil turvanõuetega ei arvestata, võib tulemina saadud sardsüsteemil esineda märkimisväärsed turvanõrkusi.

2.2 Sardsüsteemi turvamata sisend- ja väljundliidesed

Sardsüsteemide liidesed on potentsiaalsed ründeobjektid. Kui liideste juurdepääsu kontrollimehhanismid on nõrgad, saab ründaja sardsüsteemi märkamatult ühendada seadmeid (nt miniatuurseid juhtseadmeid), mis toetavad spionaaži või sabotaaži. Kui mikrokontroller on sisend- ja väljundportidega ühendatud, on võimalik andmeid laadida otse mikrokontrollerisse või salvestada mikrokontrolleri väljundsignaale. Lähtestamissisendi olemasolu korral on ründajal võimalik süsteemi ajutiselt välja lülitada.

2.3 Sardsüsteemi puudulik füüsiline turve

Kui sardsüsteemid on füüsiliselt lihtsalt juurdepääsetavad, saab ründaja mehaanilise jõu, lühistamise või ülepinge abil süsteemi hävitada või süsteemi kahjustada. Samuti võib ründaja ligi pääseda sardsüsteemi elektroonilistele komponentidele, näiteks mikroskeemide väljaviikudele või kontaktidele. Kui ründaja saab sardsüsteemi andmeid manipuleerida, on ohus terve süsteemi terviklus ja käideldavus.

2.4 Sardsüsteemi riistvaratõrge või -viga

Ümbritseva keskkonna mõjud (nt elektromagnethäired, temperatuurikõikumised, ebastabiilne elektritoide) võivad põhjustada sardsüsteemide tõrkeid. Süsteemi tõrked võivad olla tingitud ka komponentide normaalsest või enneaegsest kulumisest. Tõrked võivad tugevalt häirida ka sardsüsteemiga seotud süsteemide tööd.

2.5 Sardsüsteemi tarkvarauuendite manipuleerimine

Paljud sardsüsteemid salvestavad oma tarkvara välkmällu (ingl *flash memory*) või EEPROM-i. Selliste sardsüsteemide püsivara uuendamine toimub liidese või võrguühenduse kaudu ühendatud programmeerimisvahendi abil. Sarnaselt on ka ründajal võimalik laadida manipuleeritud tarkvarauuendeid ja sellega sardsüsteemi normaalset toimimist mõjutada.

2.6 Sisseehitatud krüptosüsteemide kõrvalkanalrünne

Krüptosüsteemi või signatuuride murdmiseks on võimalik kasutada kõrvalkanalrünnet (ingl *side-channel attack*). Kõrvalkanalrünne tugineb krüptosüsteemi füüsilise ja programmilise teostuse jälgitavate omaduste analüüsil. Nii on võimalik mikroprotsessori krüptoloogilise arvutuste energiatarbimise ja signaalide ajastuse põhjal teha järeldusi tehtud toimingute ja võtmete kohta.

2.7 Sardsüsteemi manipuleerimine sideliidese kaudu

Sardsüsteemi energiakulu, mõõtmed, mälumaht, tarkvara maksimaalne koodimaht, maksumus ja muud piirangud ei võimalda arendada piisavaid turvafunktsioone (nt tugevdatud krüptograafia). Tänapäevased sardsüsteemid on levinud tehnoloogiate ja protokollide kaudu ühendatud võrku ning seetõttu potentsiaalselt haavatavad.

Ründaja võib proovida sardsüsteemi üle võtta IP-andmevahetuse, raadiokohtvõrgu, Bluetoothi või mobiilsideliideste kaudu. Süsteemi tungida saab ka lokaalsete sideliideste, näiteks USB-pordi kaudu.

2.8 Järeletehtud komponentide kasutamine

Kui sardsüsteemi tootmises või hoolduses kasutatakse originaalkomponentide asemel nende analooge, siis ei pruugi need olla sama töökindlad kui originaalkomponendid. Seetõttu võib süsteem vääralt töötada või seiskuda.

Ründajad võivad ka spetsiaalselt välja töötada seadme või komponendi, mis näeb välja täpselt nagu originaal, kuid mille funktsioonid on ründaja poolt manipuleeritud. Selliselt muudetud komponendiga saab sardsüsteemi paigaldada tagauksi või manipuleerida konkreetseid funktsioone.

3 Meetmed

3.1 Elutsükkel

Kavandamine

SYS.4.3.M1 Sardsüsteemide rakendamise kord

SYS.4.3.M5 Sardsüsteemi kaitse kahjulike keskkonnamõjude eest

SYS.4.3.M7 Sardsüsteemi funktsioonide turvaline teostus riistvaras

Soetamine

SYS.4.3.M4 Sardsüsteemi nõuete spetsifikatsioon

Evitus

SYS.4.3.M2 Sardsüsteemi mittevajalike liideste ja teenuste desaktiveerimine

SYS.4.3.M6 Sardsüsteemi programmikoodi turve

SYS.4.3.M8 Sardsüsteemi turvaline operatsioonisüsteem

Käitus

SYS.4.3.M3 Sardsüsteemi turvasündmuste logimine

SYS.4.3.M9 Krüptoprotsessorite ja kaasprotsessorite kasutamine

Kõrvaldamine

SYS.4.3.M11 Sardsüsteemi turvaline kõrvaldamine

Avariivalmendus

SYS.4.3.M10 Sardsüsteemi taaste

Lisanduvad kõrgmeetmed

SYS.4.3.M12 Usaldusväärne sardsüsteemi tarne- ja logistikaahel

SYS.4.3.M13 Sertifitseeritud operatsioonisüsteem

SYS.4.3.M14 Sardsüsteemi buutimise turve ja autentimine

SYS.4.3.M15 Sardsüsteemi mäluhalduse turve

SYS.4.3.M16 Sardsüsteemi muukimisrünnete tõrje

SYS.4.3.M17 Sardsüsteemi moodulite enesetestimine

SYS.4.3.M18 Sardsüsteemi kõrvalkanalrünnete tõrje

3.2 Põhimeetmed

SYS.4.3.M1 Sardsüsteemide rakendamise kord

a. Sardsüsteemide rakendamiseks ja probleemideta halduse tagamiseks on määratud:
   - nõuded ühilduvusele, töökeskkonnale ja taristule (vt SYS.4.3.M4 *Sardsüsteemi nõuete spetsifikatsioon*);
   - rollid, vastutajad, õigused ja kohustused;
   - teavituskanalid ja kontaktisikud tõrgete ja turvaintsidentide puhuks.
b. Kõik sardsüsteemid ja sardsüsteemide liidesed on dokumenteeritud.
c. On kehtestatud sardsüsteemide tervikluse ja töövõimelisuse testimise kord.
d. Sardsüsteemid on turvaliselt eelseadistatud. Kasutatavad konfiguratsioonid on dokumenteeritud.
e. Kõigile kasutajatele ja halduritele on tutvustatud tõrgete, talitlushäirete või turvaintsidendi kahtluse korral tegutsemise juhiseid ja teavituskanaleid.

SYS.4.3.M2 Sardsüsteemi mittevajalike liideste ja teenuste desaktiveerimine [arendaja]

a. Kasutajatel on juurdepääs ainult vajalikele füüsilistele ja loogilistele liidestele.
b. Aktiveeritud on ainult otstarbe täitmiseks vajalikud teenused ja protokollid.
c. Sardsüsteemi liidestega seotud nõrkuste tuvastamiseks kasutatakse pordiskannereid ja muid asjakohaseid võrguturbe rakendusi. Tarbetud ja ebaturvalised protokollid ja teenused (nt NetBios, Telnet, http, ftp) on desaktiveeritud.
d. Sardsüsteemi kasutava rakenduse juurdepääs sardsüsteemi liidestele on kaitstud turvalise autentimisega.

SYS.4.3.M3 Sardsüsteemi turvasündmuste logimine

a. Sardsüsteemi võimaluste piires logitakse järgnevad turvasündmused:
   - volitamata juurdepääsu katsed;
   - lubamatud juurdepääsud;
   - süsteemi tõrked;
   - eelisõigustega toimingud;
   - eelisõiguste omandamise katsed.

b. Kui elektrooniliselt logida ei saa või on logimine võimalik ainult väga piiratud määral, siis dokumenteeritakse käsitsi peetavas logiraamatus:

c. kõik sardsüsteemis tehtavad tööd koos koha, aja, täideviija ning toimingu tüübi ja põhjuse kirjeldusega;

d. kõik tõrked, ilmsed rikkumised ja muud kõrvalekalded.

e. Sardsüsteemi logidele on juurdepääs üksnes määratud isikutel.

f. Logisid ja logiraamatu sissekandeid analüüsitakse regulaarselt ja intsidendipõhiselt.

SYS.4.3.M5 Sardsüsteemi kaitse kahjulike keskkonnamõjude eest [arendaja, arhitekt]

a. Tulenevalt sardsüsteemi kasutusviisist ja -kohast kaitstakse sardsüsteemi komponente tolmu, kuumuse, niiskuse ja muude kahjulike keskkonnamõjude eest.

b. Vajalike kaitsemeetmetega on arvestatud juba sardsüsteemi taristu kavandamise järgus.

c. Sardsüsteemi enda kaitsemeetmed sõltuvad süsteemi asukohast (nt suurema süsteemi koosseisus ei pruugi olla vajalik sardsüsteemi kaitsmine kinnise ja purunemiskindla korpusega).

3.3 Standardmeetmed

SYS.4.3.M4 Sardsüsteemi nõuete spetsifikatsioon [hankeosakond]

a. Sardsüsteemi hankimiseks on koostatud nõuete spetsifikatsioon mille alusel süsteeme või komponente hinnatakse.

b. Nõuete spetsifikatsioon sisaldab vähemalt järgmisi turvanõudeid:
   - korralduslikud raamtingimused (teavitus, klienditugi, uuendid, koolitus jms);
   - tehnilised ja majanduslikud nõuded (funktsioonid, reaalajanõuded, energiatarve, kulud jms);
   - vastavus tööstusala standarditele ja tavadele (sertifikaatide olemasolu);
   - füüsiline kaitstus keskkonnaohtude ja rünnete eest;
   - nõuded riistvarale (protsessori arhitektuur, püsivaramälu liik);
   - nõuded tarkvarale (õiguste haldus, logimine, alarmid jms);
   - TPM-mooduli (ingl Trusted Platform Module, TPM) tugi;
   - arendusvahendid ja nende turvamehhanismid.

SYS.4.3.M6 Sardsüsteemi programmikoodi turve [arendaja]

a. Sardsüsteemi silumise (ingl *debugging*) funktsioon on desaktiveeritud või süsteemist täielikult eemaldatud.

b. Vigade diagnostika ja kõrvaldamise vahendite (ingl *debugger)* kasutamine kaugühenduse kaudu on blokeeritud.

c. Testsignaalide sisendliidesed, mõõtepunktid ja kiipide silumisliidesed on lubamatu kasutamise eest kaitstud.

SYS.4.3.M7 Sardsüsteemi funktsioonide turvaline teostus riistvaras [arendaja, arhitekt, hankeosakond]

a. Universaalsete, programmeeritavate protsessorite baasil loodud sardsüsteemi puhul on rakendatud täiendavaid turvameetmeid kaitseks soovimatute funktsioonide ja tagauste paigaldamise vastu.

b. Kui sardsüsteemi arendatakse kohapeal, siis selle arendus- ja käidukeskkond on kaitstud lubamatu juurdepääsu eest.

c. Komponendid ja arendusvahendid on pärit usaldusväärsetest allikatest ning on testitud.

SYS.4.3.M8 Sardsüsteemi turvaline operatsioonisüsteem [arendaja, arhitekt]

a. Sardsüsteemis kasutatav operatsioonisüsteem ja selle konfiguratsioon vastavad ettenähtud kasutusotstarbele.

b. Operatsioonisüsteemis on aktiveeritud ainult sardsüsteemi kasutusotstarbele vastavad teenused, funktsioonid ja liidesed.

c. Operatsioonisüsteem toetab TPM-mooduli kasutamist.

SYS.4.3.M10 Sardsüsteemi taaste

a. Uue tarkvaraversiooni laadimisel on võimalik ennistada eelmist versiooni.

b. Konfiguratsiooni muudatusi saab tagasi võtta ja süsteemi ennistada algolekusse.

c. Alati on varundatud süsteemi viimane töövõimeline seis.

SYS.4.3.M11 Sardsüsteemi turvaline kõrvaldamine

a. Enne sardsüsteemi kasutuselt kõrvaldamist kustutatakse süsteemist turvaliselt kõik andmed.

b. Kui sardsüsteemi talletatud andmeid ei ole võimalik kustutada, hävitatakse sardsüsteemi riistvara füüsiliselt.

c. Andmete kustutamine ja riistvara hävitamine dokumenteeritakse.

3.4 Kõrgmeetmed

SYS.4.3.M9 Krüptoprotsessorite ja kaasprotsessorite kasutamine [arendaja, arhitekt] (C-I)

a. Kui krüptograafilisteks operatsioonideks kasutatakse täiendavat mikrokontrollerit, on selle andmevahetuseks süsteemi mikrokontrolleriga rakendatud täiendavaid meetmeid.

b. Sardsüsteemis on rakendatud usaldusahel (ingl *chain of trust*) ja loodud vajalikud ankurvõtmed (ingl *trust anchor*).

SYS.4.3.M12 Usaldusväärne sardsüsteemi tarne- ja logistikaahel [hankeosakond] (C-I-A)

a. Sardsüsteemi valmistaja ning tarne- ja logistikaahelasse kuuluvate firmade kvalifikatsioon ja usaldatavus on tõendatav.

b. Süsteemi tootja on kontrollinud, et sardsüsteemid ei sisalda manipuleeritud, võltsitud ega vahetatud komponente.

c. Ladustamise, edasimüügi ja transpordi ajal on sardsüsteemid kaitstud programmeeritavate loogikamoodulite manipuleerimise ja komponentide vahetamise eest.

d. Süsteemi tarnija on kontrollinud sardsüsteemide vastavust spetsifikatsioonile.

e. Sardsüsteemides puuduvad varjatud funktsioonid. Sardsüsteemi kaudu ei saada lubamatut juurdepääsu konfidentsiaalsele teabele.

SYS.4.3.M13 Sertifitseeritud operatsioonisüsteem [arendaja, arhitekt] (C-I-A)

a. Sardsüsteemi operatsioonisüsteem on tunnustatud standardi (nt ISO 15408) kohaselt hinnatud nõuetekohasele tasemele vastavaks.

SYS.4.3.M14 Sardsüsteemi buutimise turve ja autentimine [arendaja, arhitekt] (C-I)

a. Buutimine toimub mitmeetapiliselt, iga etapi turvalisust kontrollitakse.

b. Sardsüsteemi buutimisel kontrollib eellaadur operatsioonisüsteemi terviklust ja laadib operatsioonisüsteemi ainult siis, kui süsteem on terviklik. Operatsioonisüsteem käivitub üksnes siis, kui operatsioonisüsteem on kinnitanud eellaaduri usaldusväärsust.

c. ARM-põhise sardsüsteemi puhul kasutatakse turvavahendit ARM *Secure Boot* või käivitatakse operatsioonisüsteem ühekordselt kirjutatavast mälust.

d. x86 platvormi UEFI (*Unified Extensible Firmware Interface*, UEFI) puhul kasutatakse turvavahendit *Secure Boot*.

SYS.4.3.M15 Sardsüsteemi mäluhalduse turve [arendaja, arhitekt] (C-I)

a. Sardsüsteemi põhimälu on struktureeritud selliselt, et ühe programmi viga ei mõjuta teiste programmide või kogu süsteemi stabiilsust.

b. Programmide andmepääs teiste programmide mälupiirkondadele on tõkestatud riistvaraliselt MPU (*Memory Protection Unit*, MPU) või MMU (*Memory Management Unit*, MMU) abil.

c. Riistvaralise turbe puudumisel kontrollitakse mälupöördumisi tarkvaraliselt. Kontrollimine võib toimuda pärast kompileerimist või programmi käituse ajal automaatsete kontrollidena.

SYS.4.3.M16 Sardsüsteemi muukimisrünnete tõrje (C-I)

a. Muukimisrünnete (ingl *tampering attack*) avastamiseks, registreerimiseks ja takistamiseks (*ingl tamper response)* kasutatakse sobivaid vahendeid.

b. Sardsüsteemi füüsiliseks kaitseks kasutatakse turvalisi korpuseid ning kinnitatakse sardsüsteem tugevalt metallkonstruktsiooni külge.

c. Muukimise avastamiseks kasutatakse seadmete plommimist, turvakleepse või aktiivandureid, mis reageerivad muutustele keskkonnas.

d. Muukimisintsidendile reageerimiseks on koostatud juhend.

SYS.4.3.M17 Sardsüsteemi moodulite enesetestimine (I-A)

a. Sardsüsteemi moodulitesse on integreeritud enesetestimise funktsioon (ingl *Built-In Self Test*, BIST).

b. Enesetestimisega kontrollitakse mooduli terviklust nii sisselülitamise ajal kui ka töö ajal ettenähtud ajavahemike järel.

c. Tehnilise võimekuse olemasolul testitakse ka mooduli turvafunktsioone.
d. Suurema kaitsetarbega moodulis (nt elutähtsad juhtsüsteemid) kontrollitakse integreeritud enesetestimise raames lisaks sisend- ja väljundkomponentide ning mälu terviklust.

SYS.4.3.M18 Sardsüsteemi kõrvalkanalrünnete tõrje (C)

a. Sardsüsteemi kõrvalkanalrünnete (ingl *side-channel attack*) vastu kasutatakse näiteks:
   - vahetulemite ja/või ooteaegade juhuslikustavat maskeerimist;
   - ühtse voolutarbimisprofiili tagamist krüpteerimise ja dekrüpteerimise ajal;
   - voolutarbe taustamürasse peitmine (nt kunstlike voolutarbijate abil);
   - mälu lisaelemente, mille sisu normaalse töö käigus ei muutu.

SYS.4.4 Esemevõrgu (IoT) seade üldiselt

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed esemevõrgu (ingl *Internet of Things*, IoT) seadmete turvaliseks kasutamiseks.

Esemevõrgu seadmed on nutifunktsioone omavad võrgustatud objektid või seadmed. Esemevõrgu seadmed ühendatakse enamasti raadiovõrku, seadmetel on juurdepääs Internetis olevatele andmetele ja nad on ise Internetist kättesaadavad (nt valvekaamerad, kaugjuhitavad kütteseadmed).

1.2 Vastutus

„Esemevõrgu (IoT) seade üldiselt“ meetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Hankeosakond, tehnikatalitus, infoturbejuht.

1.3 Piirangud

Moodul ei käsitle erinevate IoT seadmete riist- ja tarkvaraarhitektuuride erisusi.

Tööstuslike juhtsüsteemide seadmete turvaaspektid on esitatud mooduligrupis IND (Tööstuse IT*)*.

See moodul ei käsitle ka sardsüsteeme. Erinevalt IoT seadmetest on nutifunktsioone omavad sardsüsteemid integreeritud laiemasse süsteemi või tootesse. Sardsüsteemide turvet käsitletakse moodulis SYS.4.3 *Sardsüsteemid (embedded systems*).

Esemevõrgu seadmete jaoks vajaliku traadita andmeside meetmed esitatakse mooduligrupis NET.2 *Raadiovõrgud*.

Esemevõrgu seadmete pääsuõiguste halduse meetmeid käsitletakse moodulis ORP.4 *Identiteedi ja õiguste haldus*.

2 Ohud

2.1 Luure esemevõrgu seadme kaudu

Esemevõrgu seadmete väljatöötamisel ei arvestata tavaliselt piisavalt infoturbeaspektiga. Seetõttu on esemevõrgu seadmeid kasutajate või kasutusvaldkonna kohta teabe kogumiseks korduvalt kuritarvitatud (nt on korduvalt esinenud intsidente IP-põhiste võrgustatud valvekaameratega).

2.2 Automaathäälestuse (UPnP) kasutamine

Kohtvõrkudesse integreeritud esemevõrgu seadmed loovad sageli UPnP (*Universal Plug and Play*) kaudu internetiühenduse, et pordisuunamise (ingl *port forwarding*) abil olla ka väljastpoolt kohtvõrku nähtav ja kättesaadav. Tekitatud kanali kaudu on võimalik võrku toimetada muud kahjurvara või kasutada seda ära muude kuritahtlike tegevuste jaoks. Ründaja saab esemevõrgu seadme nõrkust ära kasutades muuta IoT seadme robotvõrgu (ingl *botnet*) osaks.

2.3 Hajus ummistusrünne (DDoS)

Kui esemevõrgu seadmetele ei paigaldata regulaarselt turvauuendeid, saab ründaja IoT seadme teadaolevaid turvanõrkusi ära kasutades liita seadme robotvõrguga. Edaspidi on ründajal seadet kuritarvitades võimalik läbi viia hajusaid ummistusründeid (ingl *Distributed Denial of Service attack, DDoS attack*), et häirida sihtmärgiks oleva organisatsiooni teenuste käideldavust.

2.4 Spionaaž esemevõrgu seadme tagaukse kaudu

On kindlaks tehtud, et osad valvekaamerate ja ruumiandurite mudelid on varustatud tagaustega, mis võimaldavad juurdepääsu kaamera piltidele ja videotele ning kopeerida neid Internetis asuvasse serverisse. See võimaldab edukalt läbi viia spionaaži, teada saada töötajate harjumusi ning teha konfidentsiaalne teave kättesaadavaks volitamata isikutele. Samuti võib kaamerapilt aidata murda kasutajate ja süsteemihaldurite paroole ning seadmete konfiguratsioone. Eriti suur on oht IoT seadmete puhul, mida kasutatakse arvutikeskustes ja serveriruumides.

3 Meetmed

3.1 Elutsükkel

Kavandamine

SYS.4.4.M6 IoT seadmete kaasamine organisatsiooni turvapoliitikasse

SYS.4.4.M7 IoT seadmete rakendamise kava

Soetamine

SYS.4.4.M1 IoT seadmete turvanõuete määramine

SYS.4.4.M8 IoT seadmete hankimise kriteeriumid

Evitus

SYS.4.4.M2 IoT seadme autentimine

SYS.4.4.M5 IoT seadme võrkupääsu piiramine

SYS.4.4.M9 IoT seadme kasutamise kord

SYS.4.4.M10 Esemevõrgu seadme turvaline install ja konfiguratsioon

SYS.4.4.M11 Andmevahetuse krüpteerimine

SYS.4.4.M13 IoT seadme tarbetute komponentide desaktiveerimine ja desinstall

SYS.4.4.M15 IoT seadme pääsuõiguste kitsendamine

Käitus

SYS.4.4.M16 Kahjurprogrammide tõrje

SYS.4.4.M17 IoT seadme andmevahetuse seire

SYS.4.4.M18 IoT seadme turvasündmuste logimine

SYS.4.4.M19 IoT seadme haldusliidese turve

Kõrvaldamine

SYS.4.4.M20 Esemevõrgu seadme korrakohane kasutuselt kõrvaldamine

Lisanduvad kõrgmeetmed

SYS.4.4.M21 Töökeskkond ja elektritoide

SYS.4.4.M22 Esemevõrgu seire

SYS.4.4.M23 Esemevõrgu seadmete audit

SYS.4.4.M24 IoT seadme veebiserveri turvaline konfiguratsioon ja kasutamine

3.2 Põhimeetmed

SYS.4.4.M1 IoT seadmete turvanõuete määramine

a. Esemevõrgu seadmete jaoks on koostatud minimaalselt vajalikud turvanõuded, millele kõik organisatsioonis kasutatavad IoT seadmed peavad vastama.

b. Kõik esemevõrgu seadmed peavad tagama vähemalt järgmist:

- seadme püsivara (ingl *firmware*) ja tarkvara on võimalik uuendada;
- tootja tagab seadme mõistliku kasutusaja jooksul seadmetele regulaarsed turvauuendid;
- seade võimaldab autentimist;
- seadme vaikeparoolid on muudetavad;
- seadmel ei ole varjatud funktsioone.

SYS.4.4.M2 IoT seadme autentimine

a. IoT seadmes on autentimine alati aktiveeritud.

b. Autentimiseks kasutatavad paroolid vastavad organisatsiooni paroolipoliitikale ning ei kattu muudes IT-süsteemides kasutavate paroolidega. Kui see on tehniliselt võimalik, kasutatakse turvalisemaid autentimismehhanisme (nt sertifikaadipõhist autentimist).

c. Enne seadme ühendamist organisatsiooni sisevõrku on muudetud IoT seadme vaikeparoolid.

SYS.4.4.M5 IoT seadme võrkupääsu piiramine

a. Esemevõrgu seadmete pääs sisevõrku on võimalikult kitsendatud. Kui esemevõrgu seadmed (nt valvekaamerad) kuuluvad mingisse laiema otstarbega süsteemi (nt hoone halduse süsteemi), vahetavad nad andmeid ainult selle süsteemiga.

b. Sisenevad ja väljuvad võrguühendused ja sihtkohad on piiratud ruuterite pääsuloenditega (ACL) ja tulemüüri reeglitega (nt valvekaamerale piisab ühendustest tootja uuendusserveri, videoandmete salvestuskoha ja haldussüsteemiga).

c. Telneti (port 23) kaudu juurdepääs on blokeeritud.

d. Marsruutimine on kitsendav, vaikemarsruudid on blokeeritud.

e. Kõigis ruuterites on automaathäälestuse funktsioon UPnP desaktiveeritud.

f. Esemevõrgu seadmed ja andurid asuvad eraldatud võrgusegmendis, mis omab ühendust ainult halduse võrgusegmendiga.

g. Kaugpöördumine esemevõrgu seadme poole toimub SSH (vaikeport 22) ja turvalise autentimisega.

h. Esemevõrgu seadmed on kaitstud lubamatu füüsilise juurdepääsu eest.

3.3 Standardmeetmed

SYS.4.4.M6 IoT seadmete kaasamine organisatsiooni turvapoliitikasse [infoturbejuht]

a. Organisatsiooni üldises turvapoliitikas on kehtestatud nõuded esemevõrgu seadmetele. Esemevõrgu seadmete turvanõuetes on arvestatud nii turvalisuse kui funktsionaalsuse aspekte.

b. Kõik esemevõrgu seadmeid hankivad ja käitavad isikud teavad turvapoliitika nõudeid.

c. Poliitika nõuete järgmist kontrollitakse regulaarselt. Kontrolli tulemused dokumenteeritakse.

SYS.4.4.M7 IoT seadmete rakendamise kava

a. IoT seadmete rakendamise kava sisaldab vähemalt järgmist:
   - esemevõrgu otstarve ja teenused;
   - kasutuskohad ja kasutusviis;
   - autentimise vajadus ja tüüp;
   - seadmete haldus;
   - võrguühendused ja võrguteenused;
   - logimine;
   - turvamehhanismid.

b. Kõik kavandamise etapis tehtud otsused dokumenteeritakse.

SYS.4.4.M8 IoT seadmete hankimise kriteeriumid [hankeosakond, infoturbejuht]

a. Esemevõrgu seadmete hankimisse on kaasatud infoturbejuht.

b. Hankimisel lähtutakse esemevõrgu seadmete rakendamise kavast (vt SYS.4.4.M7 *IoT seadmete rakendamise kava*).

c. Enne IoT-seadmete ostmist selgitatakse välja turvanõuded, millele seadmed peavad vastama ning kasutatakse neid turul saadaolevate toodete hindamiseks. Muuhulgas võrreldakse tooteid järgmiste kriteeriumite põhjal:
   - füüsiline kaitstus keskkonnaohtude ja rünnete eest;
   - tõrke- ja töökindlus;
   - vastavus ala standarditele ja tavadele;
   - süsteemiarhitektuur;
   - tarkvara ja selle turvamehhanismid (sideprotokollid, õiguste haldus, logimine, alarmid jms).

SYS.4.4.M9 IoT seadme kasutamise kord

a. Iga esemevõrgu seadme jaoks on määratud selle peakasutaja, kes tunneb hästi seadme spetsiifikat.
b. Seadme kasutuselevõtuks on olemas nõutavad keskkonnatingimused ja elektritoide.
c. Esemevõrgu seade on konfigureeritud vastavalt tööalastele vajadustele ja turvanõuetele.

SYS.4.4.M10 Esemevõrgu seadme turvaline install ja konfiguratsioon

a. Esemevõrgu seadmeid installivad ja konfigureerivad ainult volitatud isikud (esemevõrgu seadmete eest vastutavad isikud, haldurid või lepingulised teenuseandjad), kes järgivad määratud protseduure.
b. Kõik installimis- ja konfigureerimisetapid on dokumenteeritud nii, et pädev kolmas isik suudaks protseduuri dokumentatsiooni põhjal läbi viia.
c. Algkonfiguratsioonis muudetakse vähemalt järgnevat:
   - muudetakse ära vaikeparoolid;
   - seatakse kasutajate ja haldurite õigused;
   - konfigureeritakse pääs välisvõrku ja juurdepääs olulistele välisteenustele;
   - blokeeritakse andmete saatmine valmistajale või tarnijale.
d. Esemevõrgu seadmete algkonfiguratsioon on vastav kasutuseesmärgile ja turvapoliitika nõuetele.
e. Võimalusel ühendatakse esemevõrgu seadmed andmesidevõrguga alles pärast installimise ja konfigureerimise lõpuleviimist.

SYS.4.4.M11 Andmevahetuse krüpteerimine

a. Esemevõrgu seadmed vahetavad andmeid SSL/TLS või SSH-ga krüpteeritult.
b. Mitteturvalised võrguprotokollid (nt Telnet) on desaktiveeritud.
c. Kui toode krüpteerimist ei toeta, kasutatakse andmevahetuseks VPN-i.

SYS.4.4.M13 IoT seadme tarbetute komponentide desaktiveerimine ja desinstall

a. Pärast esemevõrgu seadme installi kontrollitakse, millised protokollid, rakendused ja teenused on seadmes paigaldatud ja aktiveeritud.
b. Tarbetud protokollid, teenused, kasutajakontod ja liidesed (nt Bluetooth, Zigbee, Firewire) desaktiveeritakse või desinstallitakse.

c. Kui tarbetuid võrguteenuseid ei saa desaktiveerida otse seadmes, kasutatakse teenuste blokeerimiseks tulemüüri.
d. Saadaolevate teenuste tegelikku seisu kontrollitakse portide skaneerimisega.

SYS.4.4.M15 IoT seadme pääsuõiguste kitsendamine

a. Esemevõrgu seadmetele on antud juurdepääsud ainult tööks vajaminevas minimaalses ulatuses.
b. Kui pääsuõigusi ei saa piisavalt piirata esemevõrgu seadmetes, kitsendatakse pääsuõigusi kohtvõrgu tasemel.

SYS.4.4.M16 Kahjurprogrammide tõrje

a. IT-talitus on kursis esemevõrgu seadmete kahjurvara ohtude ja riskide leevendamise meetmetega.
b. Kahjurprogrammid kõrvaldatakse viivitamatult.
c. Kui kahjurprogramm saab olla ainult põhimälus, kõrvaldatakse ta seadme alglaadimisega (see ei välista siiski seadme uuesti nakatumist).
d. Kui nakkuse põhjust ei saa kõrvaldada või uut nakatumist ei ole võimalik vältida, kõrvaldatakse nakatatud seade kasutuselt.

SYS.4.4.M17 IoT seadme andmevahetuse seire

a. Regulaarselt kontrollitakse, milliste IT-süsteemidega esemevõrgu seadmed andmeid vahetavad, mis protokolli kaudu proovisid esemevõrgu seadmed ühenduda ja kas neid ühendusi lubati või blokeeriti.
b. Vajadusel kasutatakse teabe kogumiseks logimist ja võrguliikluse statistilist analüüsi.

SYS.4.4.M18 IoT seadme turvasündmuste logimine

a. Turvasündmused logitakse automaatselt. Kui logimine pole esemevõrgu seadmete enda kaudu võimalik, kasutatakse ruuterite või teiste IT-süsteemide logimismehhanisme.
b. Sõltuvalt tehnilistest võimalustest logitakse järgnevad turvasündmused:
    - volitamata juurdepääsu katsed;
    - lubamatud juurdepääsud;
    - süsteemi tõrked;
    - eelisõigustega toimingud;
    - eelisõiguste omandamise katsed.
c. Kui elektrooniliselt logida ei saa või on see võimalik ainult väga piiratud määral, siis dokumenteeritakse käsitsi peetavas logiraamatus:
    - kõik IoT seadmetega tehtavad tööd koos koha, aja, täideviija ning toimingu tüübi ja põhjuse kirjeldusega;
    - kõik tõrked, ilmsed juurdepääsu- ja andmepääsurikkumised ja muud kõrvalekalded.
d. IoT seadme logidele on juurdepääs üksnes määratud isikutel.
e. Logisid analüüsitakse intsidendipõhiselt aga ka regulaarselt.

SYS.4.4.M19 IoT seadme haldusliidese turve

a. Esemevõrgu seadmete halduses järgitakse turvapoliitikas kinnitatud haldusmeetodeid.

b. Kaughaldusliidesele on juurdepääs selleks määratud IT-süsteemist või võrgusegmendist.
c. Esemevõrgu seadmete halduseks kasutatakse eelistatult lokaalseid haldusliideseid.

SYS.4.4.M20 Esemevõrgu seadme korrakohane kasutuselt kõrvaldamine

a. On olemas ülevaade sellest, milliseid andmeid millistes esemevõrgu seadmetes hoitakse.
b. Enne esemevõrgu seadme kasutuselt kõrvaldamist varundatakse seadme andmed ja kustutatakse tundlik teave.
c. IoT-seadmete kasutusest kõrvaldamiseks luuakse kontrollnimekiri, mis sisaldab vähemalt vajalikke andmete varundamise ja turvalise kustutamise aspekte; muuhulgas arvestatakse andmeid, mis olid salvestatud pilve või irdandmekandjale.
d. Kõrvaldatava seadmega seotud õigused, lingid ja viited eemaldatakse vastavalt vajadusele.

3.4 Kõrgmeetmed

SYS.4.4.M21 Töökeskkond ja elektritoide [tehnikatalitus] (I)

a. Enne esemevõrgu seadme paigaldamist on kontrollitud, kas antud asukohas on täidetud:
   - tootja poolt nõutud keskkonnatingimused (sobiv temperatuur, õhuniiskus, elektritoite parameetrid);
   - infoturbe nõuded (nt seotud süsteemide kaitsetarbe ja andmekaitse nõuded).
b. Esemevõrgu seadmed on kaitstud varguse, purustamise ja manipuleerimise eest. Vajadusel rakendatakse täiendavaid turvamehhanisme (nt seadme tugevdatud korpus).
c. Kui seadmel on sisemine toiteallikas, kontrollitakse selle toimimist regulaarselt. Vajadusel aku laetakse või vahetatakse.

SYS.4.4.M22 Esemevõrgu seire (A)

a. On rakendatud pidev esemevõrgu seadmete seire. Määratud piirnäitajate ületamisel teavitatakse seadme haldureid viivitamatult.
b. Kui esemevõrgu seadmete käideldavusele on seatud kõrgendatud nõuded, siis on pidevalt olemas eelseadistatud varuseade või on loodud seadmetest klaster, kus ühe seadme väljalangemine ei ohusta terve süsteemi käideldavust.

SYS.4.4.M23 Esemevõrgu seadmete audit (C-I-A)

a. Turvakriitilistes valdkondades on kõik kasutatavad esemevõrgu seadmed läbinud enne seadmete paigaldamist turvatehnilise auditi ja testimise.

SYS.4.4.M24 IoT seadme veebiserveri turvaline konfiguratsioon ja kasutamine (C-I-A)

a. Esemevõrgu seadmes oleva veebiserveri konfiguratsioon on maksimaalselt kitsendav.
b. Installitud ja aktiveeritud on ainult vajalikud komponendid ja funktsioonid.
c. Veebiserverit hallatakse võimalikult piiratud õigustega konto kaudu.
d. Veebiserverit ei käivitata eeliskontoga.
e. Juurdepääs serverile on võimalik ainult tugeva autentimise kaudu.
f. Andmevahetus on krüpteeritud.

g. Kõik turvalisuse ja tõrgetega seotud teated (tulemuslikud ja mittetulemuslikud andmepääsud, tõrketeated, vigased või mittetäielikud HTTP-päringud ja süsteemisteated) logitakse.

SYS.4.5 Irdandmekandjad

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed irdandmekandjate (ingl *removable storage device*, *removable media*) turvaliseks kasutamiseks.

Irdandmekandjaid kasutatakse andmete transportimiseks ja säilitamiseks või neile mobiilse juurdepääsu tagamiseks. Irdkandjate hulka kuuluvad muuhulgas välised kõvakettad, CD-d, DVD-d, mälukaardid, magnetlindid ja mälupulgad.

1.2 Vastutus

Irdkandjate meetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Kasutaja, vastutav spetsialist.

1.3 Piirangud

Moodul ei käsitle IT-süsteemide kaitset, millega irdandmekandjaid ühendatakse. Vastavad meetmed esitatakse moodulites „SYS.1.1 *Server üldiselt“,* „SYS.2.1 *Klientarvuti üldiselt“* ja operatsioonisüsteemi spetsiifilistes moodulites.

Meetmed mobiilsetele seadmetele, mis erinevalt irdandmekandjatest on võimelised ise andmeid töötlema (nt nutitelefonid) esitatakse moodulis SYS.3.2.1 *Nutitelefon ja tahvelarvuti üldiselt*.

Turvalise andmevahetuse korraldamist irdandmekandjate abil käsitletakse moodulis CON.9 *Teabevahetus*.

2 Ohud

2.1 Hooletus teabe käitlemisel

Irdandmekandja kasutamisel tehtud hooletusviga võib irdandmekandjaid (ingl *removable storage device, removable media*) füüsiliselt kahjustada. Kui andmetest ei ole tehtud varukoopiat, on võimalik, et neid andmeid ei ole enam võimalik taastada.

On oht, et tundlikke andmeid sisaldavat irdandmekandjat (nt DVD-d) hoitakse järelevalveta või unustatakse ebaturvalisse asukohta. Kui andmed on andmekandjal krüpteerimata, on volitamata isikutel võimalik andmetele juurde pääseda.

2.2 Puudulik eeskirjade tundmine

Kui töötajatele pole koostatud irdandmekandjate turvalise kasutamise eeskirja, siis ei saa nõuda töötajatelt ka nõuete täitmist. Kui töötaja ei ole teadlik irdandmekandjatega seotud ohtudest, võib ta teadmatusest või hooletusest põhjustada turvaintsidendi (nt kui organisatsiooni IT-süsteemidega ühendatakse kontrollimata mälupulk).

2.3 Irdandmekandjate vargus või kaotamine

Irdandmekandjate kasutamisel on andmekao risk suurem kui statsionaarsete süsteemide korral. Eriti suur oht kaasneb andmekandja varguse või kaotamisega. Irdandmekandjal arhiveeritud teave on sellistel juhtudel jäädavalt kadunud. Samuti on võimalik, et andmed varastatud või kaotatud andmekandjalt satuvad kõrvaliste isikute kätte.

2.4 Defektsed andmekandjad

Irdandmekandjad on oma kompaktsuse ja kasutavate tehnoloogiate tõttu altid kahjustustele, vigadele ja tõrgetele, mida võivad põhjustada mehaanilised mõjutused irdandmekandjate transpordil või kasutamisel.

Irdandmekandjate kahjustumist võivad soodustada andmekandja tootmisvead või halb koostekvaliteet.

2.5 Kahjustus muutuva kasutuskeskkonna tõttu

Irdandmekandjaid kasutatakse ka tingimustes, kus esinevad kahjulikud keskkonnamõjud (nt liiga kõrge või liiga madal temperatuur, tolm või niiskus) ja need võivad andmekandjat kahjustada.

Ka tundmatute IT-süsteemidega ühendamisel on oht, et irdandmekandjat kahjustab vigane lugemisseade (nt CD-luger).

2.6 Kahjurprogrammide levitamine

Irdandmekandja kasutamisel erinevates seadmetes ja töökohtades on oht, et andmekandjaga levitatakse ühest IT-süsteemist teise kahjurprogramme. Kahjurprogrammid võivad rikkuda või kustutada ka andmekandjal olevad andmed.

3 Meetmed

3.1 Elutsükkel

Kavandamine

SYS.4.5.M4 Irdandmekandjate kasutamise eeskiri

SYS.4.5.M5 Irdandmekandjate kaasavõtmise kord

Evitus

SYS.4.5.M1 Töötajate teadlikkuse tõstmine

SYS.4.5.M6 Irdandmekandjate halduse kord

Käitus

SYS.4.5.M2 Irdandmekandja kaotamisest või manipulatsioonist teatamine

SYS.4.5.M12 Irdandmekandja kahjurvarakontroll

SYS.4.5.M7 Andmekandja turvaline kustutus enne ja pärast kasutamist

SYS.4.5.M13 Irdandmekandja märgistamine andmekandja transpordil

SYS.4.5.M17 Andmete pikaajaline säilitamine irdandmekandjal

Lisanduvad kõrgmeetmed

SYS.4.5.M10 Andmekandja krüpteerimine

SYS.4.5.M11 Tervikluse kaitse kontrollkoodi või digitaalsignatuuriga

SYS.4.5.M14 Turvaline transport ja pakend

SYS.4.5.M15 Sertifitseeritud irdandmekandjad

SYS.4.5.M16 Spetsialiseeritud andmelüüsid

3.2 Põhimeetmed

SYS.4.5.M1 Töötajate teadlikkuse tõstmine

a. Töötajaid on teavitatud irdandmekandjate liikidest ja otstarbest.

b. Töötajad teavad, milliseid andmeid on lubatud irdandmekandjatele salvestada.

c. Töötajaid on koolitatud, kuidas nad peavad irdandmekandjatega (ingl *removable storage device, removable media*) ümber käima, et vältida nende kaotamist või vargust ja tagada andmekandjate pikk kasutusiga.

d. IT-süsteemidega on keelatud ühendada tundmatutest allikatest pärinevaid irdandmekandjaid.

e. Töötajad oskavad irdandmekandjaid turvaliselt kasutusest kõrvaldada.

SYS.4.5.M2 Irdandmekandja kaotamisest või manipulatsioonist teatamine [kasutaja]

a. Organisatsioon on määranud irdandmekandjaga seotud intsidentidest teavitamiseks selged teavituskanalid ja kontaktisikud.

b. Kasutaja on kohustatud irdandmekandja vargusest, kaotusest või manipuleerimiskahtlusest koheselt kontaktisikut teavitama.

c. Kasutaja täpsustab sündmuseteates, millist teavet irdandmekandjal talletati.

d. Pärast kaotamist üles leitud või taasloodud andmekandjat kontrollitakse võimaliku andmemanipulatsiooni ja kahjurvara leidumise suhtes.

SYS.4.5.M12 Irdandmekandja kahjurvarakontroll [kasutaja]

a. Enne irdandmekandjale salvestamist kontrollitakse andmekandjat kahjurvara leidumise suhtes.

b. Enne irdandmekandjal olevate andmete käitlust tehakse andmekandjale kahjurvarakontroll.

3.3 Standardmeetmed

SYS.4.5.M4 Irdandmekandjate kasutamise eeskiri

a. Organisatsioonis on koostatud irdandmekandjate kasutamise eeskiri.

b. Irdandmekandjate kasutamise eeskiri määrab vähemalt järgmist:

- milliseid irdandmekandjaid tohib kasutada;
- mis andmeid ei ole irdandmekandjatele lubatud salvestada;
- kuidas kaitsta andmeid lubamatu juurdepääsu, manipuleerimise ja kaotamise eest;
- kuidas irdandmekandjal olevaid andmeid krüpteerida;
- kuidas irdandmekandjaid turvaliselt hoida;
- kas irdandmekandjat on lubatud ühendada kolmandate poolte IT-süsteemidega;
- kuidas tuleb andmeid irdandmekandjatelt kustutada;

- kas ja kuidas on lubatud kasutada isiklikke andmekandjaid;
- milliste väliste töötajate või teenuseandjatega on andmekandjaid lubatud vahetada ja millistel tingimustel;
- kuidas tuleb andmekandjaid transportida;
- kuidas vältida kahjurvara levimist irdandmekandjate kaudu.

c. Irdandmekandjatele omavad juurdepääsu ainult volitatud kasutajad.

d. Regulaarselt kontrollitakse irdandmekandjate kasutamise turvanõuete ajakohasust ja nõuete täitmist.

SYS.4.5.M5 Irdandmekandjate kaasavõtmise kord

a. Irdandmekandjate väljaviimise kohta on kehtestatud kord, mis määrab:
- kas, millal ja milliseid irdandmekandjaid tohib organisatsiooni territooriumilt välja viia;
- kes ja kuidas tohivad irdandmekandjaid välja viia;
- milliseid turvameetmeid (eelkõige andmete krüpteerimist) tuleb seejuures rakendada.

SYS.4.5.M6 Irdandmekandjate halduse kord [vastutav spetsialist]

a. Irdandmekandjate halduseks on kehtestatud ühtsed reeglid.

b. Organisatsioonis kasutatavad irdandmekandjad:
- on ühtsel viisil ja kõrvalistele isikutele liigset teavet andmata märgistatud;
- on kantud organisatsiooni inventari nimekirja;
- on varundatud ja arhiveeritud;
- ei sisalda liigseid andmeid.

SYS.4.5.M7 Andmekandja turvaline kustutus enne ja pärast kasutamist [vastutav spetsialist]

a. Enne korduvkirjutatavate andmekandjate edasiandmist, taaskasutamist või kasutuselt kõrvaldamist on andmekandjatelt andmed ettenähtud viisil kustutatud.

b. Andmete turvaliseks kustutamiseks on koostatud juhised. Töötajatel on juurdepääs turvalist kustutamist võimaldavatele vahenditele.

c. Kõrgema kaitsetarbe korral tohib iga andmekandjat kasutada vaid ühe korra.

SYS.4.5.M13 Irdandmekandja märgistamine andmekandja transpordil [kasutaja]

a. Saadetav andmekandja ja selle pakend on märgistatud saajale ja saatjale arusaadavalt.

b. Tundlikku teavet sisaldava andmekandja märgistus ei anna kõrvalistele isikutele vihjeid andmete sisu kohta.

SYS.4.5.M17 Andmete pikaajaline säilitamine irdandmekandjal

a. Andmete pikaajaliseks säilitamiseks kasutatakse selleks otstarbeks sobivaid irdandmekandjaid.

b. Andmete käideldavuse ja tervikluse kontrollimiseks testitakse andmete loetavust irdandmekandjalt regulaarselt.

3.4 Kõrgmeetmed

SYS.4.5.M10 Andmekandja krüpteerimine (C-I)

a. Irdandmekandjal olevad andmed on täielikult krüpteeritud (vt CON.1 Krüptokontseptsioon).

b. Krüpteerimise protseduur on turvaline ja krüpteerimisvahendid on piisavalt kaitstud.

SYS.4.5.M11 Tervikluse kaitse kontrollkoodi või digitaalsignatuuriga (I)

a. Konfidentsiaalse teabe tervikluse tagamiseks on irdandmekandjal olevate andmete terviklus kaitstud CRC-koodidega või piisavalt tugeva digitaalsignatuuriga.

SYS.4.5.M14 Turvaline transport ja pakend (C-I-A)

a. Kasutatav transpordiviis on piisavalt turvaline ja vastab kaitsetarbele.

b. Andmekandjate transpordiks kasutatakse turvalisi saatmispakendeid, mis võimaldavad manipuleerimise kohe avastada.

c. Töötajad teavad, millist pakendit ja transporti tuleb andmekandjate saatmiseks kasutada.

SYS.4.5.M15 Sertifitseeritud irdandmekandjad (C-I-A)

a. Organisatsioonis kasutatakse ainult sertifitseeritud irdandmekandjaid.

b. Sertifitseerimine arvestab andmete pikaajalist ja terviklikku säilitamist ning krüpteerimise võimaldamist.

SYS.4.5.M16 Spetsialiseeritud andmelüüsid (C-I)

a. Organisatsioonis kasutatakse spetsialiseeritud andmelüüsi süsteemi, mis loeb andmed ühelt andmekandjalt, kontrollib andmeid kahjurvara suhtes ja kirjutab andmed teisele andmekandjale.

SYS.EE: Eesti IT-süsteemid

SYS.EE.1 X-tee turvaserver

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed X-tee turvaserveri kaitseks. X-tee turvaserveri omanik on organisatsioon või vastutav struktuuriüksus, kes võimaldab infosüsteemidel kasutada turvaserverit X-teel suhtlemiseks.

X-tee turvaserveriga liidestatud IT-süsteemid ei tohi ohustada X-tee taristut ega sattuda X-teega liidestatuse tõttu ise haavatavasse olukorda. Korrektne X-tee turvaserveri rakendamine tagab andmevahetuse tõendusväärtuse ja X-teega seonduvate äriprotsesside usaldusväärtuse.

1.2 Vastutus

X-tee turvaserveri meetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Vastutav spetsialist, organisatsiooni juhtkond.

1.3 Piirangud

X-tee turvaserveri teenuse tarbija meetmed on esitatud moodulis APP.EE.1 *X-tee andmeteenus*.

Turvaserveri kasutamise ja andmeteenuste kokkulepped toetuvad moodulitele CON.9 *Teabevahetus* ning OPS.3.1 *Teenuseandja infoturve*.

Serveri ja Linux operatsioonisüsteemi üldise halduse meetmed on esitatud moodulites SYS.1.1 *Server üldiselt* ja SYS.1.3 *Linuxi ja Unixi server*.

2 Ohud

2.1 Turvaserveri andmete väärkasutus

Turvaserveris vahendatakse ja säilitatakse nii teenuseandjate kui -tarbijate andmeid. Andmete väärkasutus, leke või volitamata muutmine mõjutab andmeteenuse osapooli ning andmeomanikke (sh eraisikuid).

2.2 E-templi väärkasutus

Turvaserver moodustab andmetele tõendusväärtuse tagamiseks e-templi. Turvaserveri omaniku valduses on enda ning teenuse osutamisel ka teiste organisatsioonide e-templid.

E-templi väärkasutus, leke või riknemine mõjutab kõiki andmeteenuse osapooli ka väljaspool X-tee keskkonda. Tõendusväärtuse või tõendatavate andmete (nt sõnumilogi) puudumine põhjustab äriprotsesside usaldusväärsuse vähenemist või kadu.

2.3 Turvaserveri haldusvead

Turvaserveri omanik vastutab andmeteenustele juurdepääsude korrektsuse eest. Turvaserveri haldamisel tehtud vead võivad põhjustada andmetele volitamata juurdepääsu või põhjuseta takistada volitatud kasutajate juurdepääsu andmeteenustele.

2.4 Turvaserveri käideldavushäire

Turvaserveri käideldavusest sõltub andmeteenuste ja sellest sõltuvate äriprotsesside (sh organisatsioonivälistе äriprotsesside) toimimine. Turvaserveri käideldavushäire võib kaasa tuua regulatsioonide ja lepingute rikkumisest tulenevad sanktsioonid ja tekitada organisatsioonile mainekahju.

2.5 Vead turvaserveri liidestamisel andmeteenusega

Turvaserveri ja andmeteenuse liidestamisel tehtud vead võivad põhjustada andmelekkeid ning volitamata juurdepääsu andmeteenustele.

3 Meetmed

3.1 Elutsükkel

Kavandamine

SYS.EE.1.M1 Turvaserveri paigalduse kavandamine

SYS.EE.1.M2 Turvaserveri krüptomooduli valik

Evitus

SYS.EE.1.M3 X-tee liitumisleping X-tee keskusega

SYS.EE.1.M4 Usaldusteenuste lepingud

Käitus

SYS.EE.1.M5 Turvaserveri sertifikaatide haldus

SYS.EE.1.M6 X-tee usaldusankru kasutamine turvaserveris

SYS.EE.1.M7 Ajatempliteenuse turvaline kasutamine

SYS.EE.1.M8 X-tee andmeteenuste turvaline liidestamine

SYS.EE.1.M9 Turvaserveri ja andmeteenuse testimine

SYS.EE.1.M10 X-tee turvaserveri sõnumilogi turvaline arhiveerimine

SYS.EE.1.M11 Turvaserveri krüptomoodulite turvaline käitus

SYS.EE.1.M12 Turvaserveri võrguturve

SYS.EE.1.M13 Turvaserveri tarkvara uuendamine

SYS.EE.1.M14 Turvaserveri kellaaja sünkroniseerimine

SYS.EE.1.M16 Turvaserveri ainuotstarbeline kasutus

SYS.EE.1.M17 Turvaserveri halduse API kasutamine

SYS.EE.1.M18 Turvaserveri logimine ja seire

SYS.EE.1.M21 Turvaserveri haldus turvaserveri omanikuna

Avariivalmendus

SYS.EE.1.M15 Turvaserveri seadistuste varundamine ja taastamine

SYS.EE.1.M22 Turvaserveri taasteplaan

Kõrvaldamine

SYS.EE.1.M19 Turvaserveri kasutuselt kõrvaldamine

SYS.EE.1.M20 Turvaserveri tarbimise turvaline lõpetamine/muutmine

Lisanduvad kõrgmeetmed

SYS.EE.1.M23 Isikustatud kontode ja rollide kasutamine turvaserveri halduses

SYS.EE.1.M24 Andmevahetuse laiendatud seire

SYS.EE.1.M25 Turvaserveri väliste võrguühenduse piiramine

SYS.EE.1.M26 Turvaserveri kõrgkäideldavus

SYS.EE.1.M27 Kvalifitseeritud e-templite kasutamine

3.2 Põhimeetmed

SYS.EE.1.M1 Turvaserveri paigalduse kavandamine

a. Turvaserveri suutvus- ning võrguühenduse omadused on tuletatud vahendatavate andmeteenuste käideldavuse ja läbilaskevõime nõuetest.

b. Turvaserveri sõnumilogi arhiveerimine on kavandatud vastavalt andmeteenuste eesmärkidele.

c. Turvaserveri tegevuslogide seire ja töötlus on kavandatud vastavalt organisatsiooni reeglitele (vt OPS.1.15 *Logimine*) ja turvaserveri teenuse eesmärkidele.

d. Turvaserveri tööks vajalikud ressursid (võrk, krüptomoodulid, andmebaasid, sõnumilogi arhiveerimisteenus) vastavad turvaserveri teenuse eesmärkidele.

SYS.EE.1.M2 Turvaserveri krüptomooduli valik

a. Signeerimisvõtmete jaoks kasutatava riistvaralise krüptomooduli (ingl *hardware security module*, HSM) valikul on lähtutud vahendatavate andmeteenuste turvagarantiide nõuetest (vt APP.EE.M1 *X-tee andmeteenuse kasutamise või andmise kavandamine*).

b. Krüptomooduli valikul on arvestatud järgmist:

- kvalifitseeritud e-templi moodustamise ja privaatvõtme turvalise hoiustamise nõuded;
- signeerimisvõtmete sertifitseerimiskeskuse (ingl *certification authority*, CA) seatud tingimused HSM-ile ning selle turvasertifikaatidele;
- planeeritava võtmeseadme jõudlus ning liidestusviis;
- krüptomooduli suutvus, tõrkekindlus ning asendatavus avariiolukorras vastavad TS teenuse eesmärkidele.

c. Krüptomooduli aktiveerimisvahendid või -salasõnad vastavad turvaeesmärkidele ning tunnustatud heale tavale.

SYS.EE.1.M3 X-tee liitumisleping X-tee keskusega [organisatsiooni juhtkond]

a. X-tee keskusega on sõlmitud X-tee liitumisleping.

b. X-tee keskuse iseteeninduses on registreeritud volitatud administratiivsed ja tehnilised kontaktisikud. Volitatud isikute muutumisel uuendatakse kontaktandmeid viivitamatult.

c. Teavituste saamise e-posti aadress on suunatud eraldiseisvale aadressile /meiligruppi, mille saajaid on rohkem kui üks inimene.

SYS.EE.1.M4 Usaldusteenuste lepingud [organisatsiooni juhtkond]

a. Organisatsioon on sõlminud usaldusteenuste lepingud.

b. Eksisteerib kord lepingute ülevaatuseks. Vajadusel lepingud uuendatakse.

c. Organisatsiooni volitatud administratiivsed ja tehnilised kontaktisikud on usaldusteenuste (ajatempliteenus, sertifitseerimiskeskus, OCSP) osutaja juures registreeritud. Volitatud isikute muutumisel uuendatakse kontaktandmeid viivitamatult.

d. Teavituste saamise e-posti aadress on suunatud eraldiseisvale aadressile/meiligruppi, mille saajaid on rohkem kui üks inimene.

SYS.EE.1.M5 Turvaserveri sertifikaatide haldus

a. Turvaserveri signeerimis- ja autentimissertifikaatide kehtivusaega seiratakse ning sertifikaadid uuendatakse õigeaegselt.

b. Sertifikaatide uuendamisel genereeritakse uued privaatvõtmed (ingl *private key*). Privaatvõtme korduv- ja mitmikkasutamine on keelatud.

c. Kasutuselt eemaldatud sertifikaatide tühistamise taotlus esitatakse usaldusteenuse pakkujale viivitamatult.

SYS.EE.1.M6 X-tee usaldusankru kasutamine turvaserveris

a. Usaldusankur (ingl *trust anchor*) laetakse X-tee keskuse määratud allikast.

b. Usaldusankru allalaadimisel kontrollitakse terviklust e-allkirja verifitseerimisega.

c. Turvaserverisse laadimisel võrreldakse turvaserveri kasutajaliideses nähtavat räsi (ingl hash) X-tee keskuse poolt publitseeritud räsiga.

d. Usaldusankru ajakohasust kontrollitakse regulaarselt (võrreldakse X-tee keskuse viimati publitseeritud usaldusankrut või selle räsi turvaserveris rakendatud usaldusankruga).

e. Kui X-tee keskus teavitab turvaserveri omanikke usaldusankru uuendamisvajadusest, rakendatakse uus usaldusankur ettenähtud ajaperioodil.

SYS.EE.1.M7 Ajatempliteenuse turvaline kasutamine

a. Turvaserveri ajatempliteenused on seadistatud vastavalt usaldusteenuste kokkulepetele ja vastavad andmeteenuste turvaeesmärkidele (käideldavus, ajatempliteenuse tase (kvalifitseeritud vs mittekvalifitseeritud)).

b. Võimalusel rakendatakse turvaserveris rohkem kui ühte ajatempliteenust.

c. Kui X-tee keskus teavitab turvaserveri omanikke ajatempliteenuse detailide uuendamisvajadusest, rakendatakse uus seadistus ettenähtud ajaperioodil.

d. Ajatempliteenused, mille kasutamise kokkulepe on lõppenud, eemaldatakse seadistusest viivitamatult.

SYS.EE.1.M8 X-tee andmeteenuste turvaline liidestamine

a. Turvaserveri ja andmeteenuse vahel on rakendatud vastastikku autenditud TLS ühendus, mille turvaserveri ja infosüsteemi TLS sertifikaate verifitseeritakse.

b. Autentimata ja/või krüpteerimata protokollide kasutamisel rakendatakse täiendavaid konfidentsiaalsust ja terviklust tagavaid turvameetmeid.

c. Andmeteenuse kasutamine on võimalik ainult volitatud turvaserveri vahendusel.

SYS.EE.1.M9 Turvaserveri ja andmeteenuse testimine

a. Turvaserveri ja andmevahetuse liidestuse arendus- ning testimistööd teostatakse arendus- või testkeskkonnas.

b. Arendus- ja testkeskkondades ei tohi kasutada käidukeskkonna (ingl *production environment, operational environment*) andmeid ega teenuseid.

c. Arendus- ja testkeskkondade turvaserveri ja andmeteenuste turvameetmed takistavad nende keskkondade väärkasutamist ja ründeobjektiks saamist.

SYS.EE.1.M10 X-tee turvaserveri sõnumilogi turvaline arhiveerimine

a. Sõnumilogi arhiveeritakse ja säilitatakse turvalisel viisil. Sõnumilogide säilitustähtajad tulenevad õigusaktidest ning andmeomanike määratud eesmärkidest.

b. Turvaserveris ei hoita sõnumilogi kauem kui see on hädavajalik.

c. Juurdepääs sõnumilogile (nii turvaserveris kui arhiivis) on piiratud andmeomanike eesmärkidest lähtuvalt.

SYS.EE.1.M11 Turvaserveri krüptomoodulite turvaline käitus

a. Krüptomooduli aktiveerimiseks vajalikud vahendid (tooken, PIN vms) on juudepääsetavad ainult volitatud isikutele.

b. Krüptomooduli aktiveerimise võimekus on tagatud ka töövälisel ajal ning avariiolukorras.

c. Krüptomooduli aktiveerimiseks vajalikud vahendid ning nende turvaomadused (sh PIN keerukus) vastavad kaitsetarbele.

d. Võrgu vahendusel kasutatava krüptomooduli juurdepääs on kaitstud tulemüüriga, lubades ainult ülesande täitmiseks vajalikke lähteaadresse.

e. Krüptomooduli või võtme kompromiteerimise tuvastamisel või võtme kasutuselt eemaldamisel teavitatakse viivitamatult usaldusteenuse andjat asjassepuutuvate sertifikaatide tühistamiseks.

SYS.EE.1.M12 Turvaserveri võrguturve

a. Turvaserver on eraldatud avalikust ning kasutajavõrkudest tulemüüriga, lubades sisenevat liiklust Internetist ainult X-tee transpordiprotokollile (vaikimisi: TCP 5500 ning 5577).

b. Turvaserveri administreerimisliidestele (vaikimisi: TCP 4000 [webui] ning 22[ssh]) on juurdepääs ainult volitatud võrkudest.

c. Turvaserveri teenusliidestele (vaikimisi: TCP 443, 8443, 80, 8080) on juurdepääs ainult turvaserveri teenuse tarbijatele üksik- või võrguaadresside alusel. Muutused (sh kasutusel mitteolevate aadresside eemaldamine) nimetatud aadresside pääsuloendites tehakse viivitamatult.

SYS.EE.1.M13 Turvaserveri tarkvara uuendamine

a. Turvaserveri X-Road tarkvara parandus- või uuendusversioonide välja laskmisel uuendatakse turvaserveri tarkvara X-tee keskuse määratud perioodi jooksul.

b. Uuendite hankimiseks kasutatakse X-tee keskuse heakskiidetud repositooriumit.

c. Regulaarselt kontrollitakse repositooriumi aadresside ning autentimisvõtmete ajakohasust.

d. Operatsioonisüsteemi uuendeid paigaldatakse vastavalt moodulile OPS.1.1.3 *Paiga- ja muudatusehaldus*.

SYS.EE.1.M14 Turvaserveri kellaaja sünkroniseerimine

a. Turvaserveri arvutikell on sünkroniseeritud usaldatud NTP serveritega (vt NET.1.2.M8. *Kellaaja sünkroniseerimine*).

SYS.EE.1.M15 Turvaserveri seadistuste varundamine ja taastamine

a. Turvaserveri seadistusi varundatakse regulaarselt.

b. Varukoopiate tegemise sagedus ning säilitustähtajad vastavad turvaserveri teenuse tingimustele.

c. Juurdepääs varukoopiatele on ainult volitatud isikutel.

d. Varukoopiast taastamisel veendutakse, et varundusest kasutusele võetud konfiguratsioon vastab tegelikule vajadusele ning selles pole aegunud või puuduolevaid elemente (nt tarbijate definitsioonid, pääsunimekirjad, teenuste seadistused).

SYS.EE.1.M16 Turvaserveri ainuotstarbeline kasutus

a. Turvaserveris käivitatakse ainult turvaserveri tööks vajalikke programme ja teenuseid.

SYS.EE.1.M17 Turvaserveri halduse API kasutamine

a. Turvaserveri halduse rakendusliidese (ingl *application programming interface*, API) võtmete haldus vastab organisatsiooni nõuetele.

b. API võtmetele kinnistatud rollid vastavad minimaalsuse printsiibile.

c. API väljakutseid tegevas süsteemis tagatakse tegevuse seostamine tegeliku kasutaja identifikaatoriga.

d. API võtmed, mille salajasus on kaheldav või mille kasutust enam ei vajata, kõrvaldatakse kasutuselt viivitamatult.

SYS.EE.1.M18 Turvaserveri logimine ja seire

a. Turvaserveri logisid töödeldakse ja säilitatakse vastavalt organisatsiooni poliitikatele.

b. Turvaserveri operatsioonisüsteemi tööd, ressursikasutust ning sõnumivahetuse metaandmeid seiratakse vastavalt organisatsiooni eesmärkidele.

SYS.EE.1.M19 Turvaserveri kasutuselt kõrvaldamine

a. Enne turvaserveri kasutuselt kõrvaldamist teavitatakse turvaserveri tarbijaid.

b. Esitatakse taotlus X-tee eksemplari vastavate konfiguratsioonielementide (turvaserveri sertifikaadid, aadressid, kasutuseta jäävad alamsüsteemid jms) tühistamiseks.

c. Tagatakse kõikide (sh veel arhiveerimata) sõnumilogide säilitamine või üle andmine vastavatele turvaserveri tarbijatele.

d. Tagatakse turvaserveri töölogide säilitamine.

e. Tühistatakse turvaserveri ning Turvaserveri tarbijate sertifikaadid.

f. Krüptovõtmed hävitatakse vastavalt krüptomooduli olemusele ning tootja juhistele.

SYS.EE.1.M20 Turvaserveri tarbimise turvaline lõpetamine/muutmine

a. Kõrvaldatava turvaserveri tarbijatega seotud konfiguratsioonielemendid (teenuse kirjeldus, pääsuloendid, TLS võtmed, X-tee alamsüsteem jms) eemaldatakse kasutuselt.

b. Turvaserveri tarbimise lõpetamisel tagatakse sõnumilogide säilitamine vastavalt turvaserveri tarbija nõuetele.

3.3 Standardmeetmed

SYS.EE.1.M21 Turvaserveri haldus turvaserveri omanikuna [vastutav spetsialist]

a. On kehtestatud turvaserveri teenuse standardtingimused, mis sisaldavad vähemalt järgmist:
   - kvalifitseeritud e-templite koostamise (nõuetekohase HSM olemasolu ning vastavate usaldusteenuste kasutamine) võimekus;
   - ajatembelduse täpsus (sagedus) ning lubatud viivitus (maksimaalne ajavahemik mil sõnumid on ajatembeldamata;
   - teenustaseme, sh käideldavuse eesmärgid;
   - X-tee turvaserveri sõnumilogi talletamise, arhiveerimise, säilitamise, juurdepääsu, hävitamise tavatingimused;
   - teenussoovide vastuvõtmise ja töötlemise kord.

b. Teenussoovid ning tehtud muutused teenuse tarbijat puudutavates seadistustes dokumenteeritakse.

c. Tagatud on teenuse tarbijate teenussoovidele reageerimine vastavalt teenuse standardtingimustele ja/või tarbijaga sõlmitud kokkuleppele.

d. Teenuse tarbijat teavitakse õigeaegselt:

- organisatsiooni signeerimissertifikaatide uuendamisvajadusest,
- tehniliste parameetrite muutustest.

e. Teenuskokkuleppe lõppemisel, krüptovõtme või võtmete konfidentsiaalsuse rikke või volitamatu kasutamise korral viivitamatult:
   - takistatakse (nt desaktiveerimise, süsteemist eemaldamise teel) vastava võtme kasutamist,
   - teavitatakse vastavat usaldusteenuse andjat sertifikaadi tühistamiseks,
   - teavitatakse teenusetarbijat teda puudutavatest asjaoludest ja läbiviidud tegevustest.

SYS.EE.1.M22 Turvaserveri taasteplaan

a. X-tee keskuse ja usaldusteenuste avarii- ja halduskontaktid ning vajalikud autentimisvahendid on avariiolukorras kiirelt kättesaadavad.
b. Krüptomoodulite asendamine on tagatud tagavaraseadmete, hooldusleping ute ja vastavate avariijuhenditega.
c. On dokumenteeritud turvaserveri taasteplaan. Taasteplaani toimimist testitakse regulaarselt.

3.4 Kõrgmeetmed

SYS.EE.1.M23 Isikustatud kontode ja rollide kasutamine turvaserveri halduses (C-I)

a. Turvaserveri halduses kasutatakse isikustatud kontosid.
b. Isikustatud kontodele määratakse rollid õiguste minimaalsuse printsiibist lähtuvalt.

SYS.EE.1.M24 Andmevahetuse laiendatud seire (I)

a. Võimalike kõrvalekallete tuvastamiseks seiratakse andmevahetuste metaandmeid ja kasutusmustreid.

SYS.EE.1.M25 Turvaserveri väliste võrguühenduse piiramine (C-A)

a. Sisenev liiklus X-tee transpordiprotokollile (vaikimisi TCP 5500 ja TCP 5577) on avatud ainult volitatud turvaserverite aadressidele. Volitatud turvaserveriteks võivad olla kas kõik vastavas X-tee eksemplaris registreeritud või eraldi kokkuleppes määratletud klient-turvaserverid.

SYS.EE.1.M26 Turvaserveri kõrgkäideldavus (A)

a. Turvaserveri teenuse tõrkekindluse tagamiseks ja/või koormusjaotuseks käitatakse turvaservereid mitmes eksemplaris.
b. Alamsüsteemide, teenuste ja pääsunimekirjade sünkroonsus eksemplaride vahel tagatakse tehniliste või protseduuriliste meetmetega.

SYS.EE.1.M27 Kvalifitseeritud e-templite kasutamine (C-I)

a. Kõik signeerimisvõtmed on loodud ning hoitakse ainult eIDAS määruse kvalifitseeritud võtmeseadme nõuetele vastavas krüptomoodulis.
b. Signeerimissertifikaadid on hangitud kvalifitseeritud usaldusteenuse pakkujalt.
c. Ajatembelduseks kasutatakse kvalifitseeritud ajatempli teenust.

4 Lisateave

4.1 Kasutatud lühendid ja mõisted

Usaldusteenuse osutaja

Sertifitseerimiskeskuse (ingl *Certificate Authority*, CA), kehtivuskinnituse (ingl *Online Certificate Status Protocol*, OCSP) ja/või ajatempliteenuse (ingl *Time Stamping Authority*, TSA) osutaja, Eestis SK ID Solutions ja Riigi Infosüsteemi Amet (RIA)

X-tee

Eestis töötav X-tee eksemplar/eksemplarid. Peamiselt käidukeskkonna (ingl *production environment, operational environment*) tähenduses.

X-Road

Tarkvara, mis realiseerib X-tee turvaserveri / keskserveri funktsioone.

X-tee keskus

X-tee eksemplari valitseja, Eestis Riigi Infosüsteemi Amet (RIA).

Turvaserver

X-tee turvaserver (ingl *X-Road Security Server*).

Turvaserveri omanik

Organisatsioon või vastutav struktuuriüksus, kes võimaldab infosüsteemidel kasutada turvaserverit X-teel suhtlemiseks (ka turvaserveri teenuse andja).

Turvaserveri tarbija

Organisatsioon või vastutav struktuuriüksus, kes omab infosüsteemi mis kasutab turvaserveri teenust. Üldnimetus X-tee andmeteenuse andja ja andmeteenuse tarbija kohta (ka turvaserveri teenuse tarbija).

X-tee andmeteenuse andja

X-teega liidestatud infosüsteem või vastava äriprotsessi omanik andmeteenuse andja rollis (ootab andmeteenuse tarbijalt päring-sõnumit ning koostab vastus-sõnumi).

X-tee andmeteenuse tarbija

X-teega liidestatud infosüsteem või vastava äriprotsessi omanik andmeteenuse tarbija rollis (koostab ja edastab päring-sõnumi ning ootab andmeteenuse andjalt vastus-sõnumit).

4.2 Publikatsioonid

Lühend	Publikatsioon
[RT]	Infosüsteemide andmevahetuskiht ("X-tee määrus") https://www.riigiteataja.ee/akt/106082019017?leiaKehtiv
[RIA]	RIA X-tee leht https://ria.ee/x-tee
[RIA]	X-tee abimaterjalid ja juhendid: https://abi.ria.ee
[X-TEE]	X-tee iseteeninduskeskkond, X-Road juhendid jm: https://x-tee.ee

SYS.EE.2 eID komponendid

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed eID (st. ID-kaart, Mobiil-ID, SmartID jmt ning nendega seotud teenuste) rakendamiseks organisatsioonides.

eID teenuskomponentide ja kliendikomponentide korrektne käsitlus tagab andmete tõendusväärtuse ja seonduvate äriprotsesside usaldusväärsuse.

1.2 Vastutus

eID komponentide turvameetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Organisatsiooni juhtkond.

1.3 Piirangud

Organisatsioonide teabevahetus toetub moodulile CON.9 *Teabevahetus.*

Lisaks rakendatakse eID komponente kasutatavale tarkvarale meetmeid moodulist OPS.1.1.6 *Tarkvara testimine ja kasutuselevõtt*.

2 Ohud

2.1 eID komponentide väärkasutus

eID vahendite väärkasutus või tehinguandmete valideerimata jätmine ohustab äriprotsesside usaldusväärsust ning võib kaasa tuua märkimisväärse majandusliku kahju. Samuti saab kahjustada organisatsiooni maine.

2.2 eID vahendite rakendamisvead

Meetmete eiramine võib tuua kaasa privaatsuse, tervikluse, konfidentsiaalsuse rikkeid. Meetmete rakendamata jätmine võib põhjustada organisatsiooni protsesside toimepidevust.

2.3 eID komponentide haldusvead

eID komponentide haldamisel tehtud vead (nt komponentide uuendamata jätmine) võivad põhjustada isikuandmete lekkimist, andmetele volitamata juurdepääsu või põhjuseta takistada volitatud kasutajate juurdepääsu andmeteenustele.

3 Meetmed

3.1 Elutsükkel

Kavandamine

SYS.EE.2.M1 eID vahendite kasutamise üldine kavandamine

SYS.EE.2.M2 eID-l põhineva autentimise kavandamine

SYS.EE.2.M3 E-allkirjastamise ja e-tembeldamise kavandamine

SYS.EE.2.M4 E-allkirjade või e-templite valideerimise kavandamine

SYS.EE.2.M5 eID tarkvaraliidestuse, -mooduli ja -konfiguratsiooni kavandamine

Evitus

SYS.EE.2.M6 eID teenuste lepingud

Käitus

SYS.EE.2.M7 E-tembeldamis- ja dekrüpteerimisvahendite turvaline kasutamine

SYS.EE.1.M8 ID-kaardi turvaline liidestamine (veebi)rakendusega

SYS.EE.2.M9 eID liidese (SmartID, Mobiil-ID), teenuse (SiVa, SiGa vm) või vahendaja (TaRa vm) turvaline liidestamine

SYS.EE.2.M10 eID klienditarkvara paigaldamine ja uuendamine

SYS.EE.2.M11 Andmete valmendus e-allkirjastamiseks, e-tembeldamiseks või krüpteerimiseks

SYS.EE.2.M12 E-allkirjastatud/e-tembeldatud andmete turvaline vastuvõtt

SYS.EE.2.M13 CDOC vormingus krüpteeritud andmete turvaline vastuvõtt

SYS.EE.2.M14 eID kasutajakoolitus

SYS.EE.2.M15 Usaldusankrute ning konfiguratsioonide regulaarne ülevaatus

SYS.EE.2.M16 E-allkirjade/e-templite ületembeldamine

SYS.EE.2.M17 ID-kaardi lugeja turvalisus

Avariivalmendus

SYS.EE.2.M18 eID avariivalmendus

Lisanduvad kõrgmeetmed

SYS.EE.2.M19 Sisemajutatud teenus vanemate (DDOC, BDOC jmt) ja teistes vormingutes (PDF, X-tee jmt) e-allkirjade/e-templite valideerimiseks

SYS.EE.2.M20 Õngitsuskindlate autentimisvahendite kasutamine

3.2 Põhimeetmed

SYS.EE.2.M1 eID vahendite kasutamise üldine kavandamine

a. Äriprotsessis on tuvastatud eID kasutamise vajadus ning määratletud:
   - eeldatavad kasutusmahud ja -mustrid;
   - vajadus subjekti eristada tunnuse (kodanik, e-resident, EU-resident jm) või kasutatava eID vahendi (ID-kaart, Digi-ID jne) alusel.

b. Kui on vajadus toetada peale Eesti riiklike eID vahendite ka Euroopa (eIDAS nõuetele vastavaid) ning teisi eID vahendeid, siis määratletakse toetatavate eID vahendite minimaalne turvagarantiide tase:
   - autentimisel (kõrge, märkimisväärne või madal);
   - e-allkirjade/e-templite moodustamisel või valideerimisel (kvalifitseeritud, täiustatud või muu).

c. Eestis riiklikult tunnustatud isiklike eID vahendite tasemed on vastavalt kõrge ning kvalifitseeritud.
d. Arvestatud on, et eID (peamiselt eIDAS raames toetatavad) vahendid esitavad subjekti identifikaatoreid erinevalt ning ühel subjektil võib eksisteerida mitu identifikaatorit.
e. eID vahendite valikul on lähtutud järgmistest kriteeriumitest:
    - kulude suurus organisatsioonile ja kasutajale;
    - vahendi levik sihtgrupis;
    - juurdepääsetavus ja sihtgrupi kogemus;
    - lisaseadmete kasutamise vajadus;
    - töökindlus;
    - infosüsteemiga liidestuse keerukus ja liidestuse modulaarsus/asendatavus;
    - vahendi asendatavus ja/või alternatiivvahendi võimalikkus avariiolukorras.

SYS.EE.2.M2 eID-l põhineva autentimise kavandamine

a. Määratud on autentimisvahendi nõutav minimaalne tase (kõrge, märkimisväärne, madal).
b. IT-süsteemi lubatav autentimistaseme on "kõrge" juhul kui IT-süsteem:
    - töötleb eriliiki isikuandmeid või võimaldab eriliiki isikuandmetele juurdepääsu;
    - annab juurdepääsu isikustatud hüvedele;
    - võimaldab tekitada olulist majanduslikku kahju.
c. eID vahendi kehtivust kontrollitakse kehtivusinformatsiooni, sertifikaatide puhul OCSP (Online Certificate Status Protocol) abil.
d. eID vahendi kehtivusinfo (sh puhverdatud OCSP vastus) on värskem kui 1 tund.
e. Autentimistegevuste tulemid koos vastavate tõenditega logitakse vastavalt organisatsiooni ja äriprotsessi eesmärkidele.

SYS.EE.2.M3 E-allkirjastamise ja e-tembeldamise kavandamine

a. Äriprotsessi nõuetest lähtuvalt on määratud:
    - e-allkirja/e-templi aktsepteeritavad tasemed (kvalifitseeritud, täiustatud, muu);
    - väljastatava e-allkirja/e-templi vormingud;
    - e-allkirjastamiseks/e-tembeldamiseks sobivad eID vahendid.
b. Organisatsiooni nimel e-tembeldamiseks kasutatakse sobivat e-tembeldamise vahendit.
c. Töötajatel on sobivad eID vahendid ning nad on varustatud ajakohaste juhenditega.
d. E-allkirjastamise/e-tembeldamise töövoogude juures on arvestatud kehtivuskinnituste (OCSP) ja ajatembeldamise teenuste tehniliste piirangutega (sh päringute arvuga ja autentimisnõuetega) ja kasutamisega kaasnevate kuludega.
e. Organisatsioonivälised e-allkirjastamise/e-tembeldamise teenuste kasutamise kavandamisel on arvestatud allkirjastavate andmete/dokumentide kolmandatele osapoolele (nt e-allkirja moodustamise teenuseandjale) edastamise lubatavust ning teenusetingimusi.

SYS.EE.2.M4 E-allkirjade või e-templite valideerimise kavandamine

a. Organisatsioonivälised valideerimissüsteemide kasutamisel on arvestatud valideeritavate andmete kolmandale osapoolele (valideerimisteenuse andja) edastamise lubatavust ning teenusetingimusi.

b. Äriprotsessi nõuetest lähtuvalt on määratud valideerimisprotsessi tulemuste logimise ja säilitamise nõuded.

SYS.EE.2.M5 eID tarkvaraliidestuse, -mooduli ja -konfiguratsiooni kavandamine

a. eID tarkavaraliidestus, -moodul ja -konfiguratsioon on uuendatav ning asendatav.

b. Asendamise, seadistamise ja uuendamise protseduurid on dokumenteeritud ja taaskorratavad.

c. Liidestusprotokollide puhul eelistatakse tuntud ja toetatud standardeid.

d. Usalduskonfiguratsioon on konfigureeritav, sh:

- sertifikaadi väljastanud lubatud sertifitseerimiskeskuste (ingl *certification authority*, CA) sertifikaatide valge nimekiri (ingl *whitelist*) või välise usaldusnimekirja (ingl *Trust Service List*, TSL) allikas ning autentsuse (sertifikaadi) seadistus;
- kehtivusinformatsiooni (sh OCSP, CRL) allikate ja nende autentsuse (sh teenuste sertifikaadid) seadistused;
- kehtivusinformatsiooni uuendamise perioodi ning kehtivusinfo värskuse piirangute seadistused;
- kasutatavate ajatembeldusteenuste ja nende autentsuse seadistused;
- Vajadusel: subjekti sertifikaadis lubatud väljastuspoliitikate (ingl *certificate issuance policy*) ning subjekti privaatvõtme (ingl *private key*) lubatud kasutuspiirangute (ingl *key usage*) valged nimekirjad.

SYS.EE.2.M6 eID teenuste lepingud [organisatsiooni juhtkond]

a. Organisatsioon on sõlminud eID komponentide kasutamiseks vajalikud teenuselepingud.

b. Teenuseandja juures on registreeritud administratiivsed ja tehnilised volitatud kontaktisikud.

c. Kontaktandmeid uuendatakse viivitamatult, kui neis on muudatusi.

d. Teavituste saamise e-posti aadress on suunatud aadressile/gruppi, mille saajaid on rohkem kui üks inimene.

SYS.EE.2.M7 E-tembeldamis- ja dekrüpteerimisvahendite turvaline kasutamine

a. E-tembeldamiseks ja dekrüpteerimiseks kasutatava krüptovahendi ja sertifikaadi turvatasemed vastavad äriprotsessi nõuetele.

b. Sertifikaadi väljastaja nõuded krüptovahendi turvalisusele ja sertifitseeritusele on täidetud.

c. Kehtestatud on kord e-tembeldamis- ja dekrüpteerimisvahendite ning nende aktiveerimiseks vajalike füüsiliste turvamoodulite hoidmiseks, juurdepääsuks ning kasutamiseks.

d. Rakendatud turvameetmed välistavad e-tembeldamis- ja dekrüpteerimisvahendite volitamata kasutamise, kopeerimise või hävitamise.

SYS.EE.1.M8 ID-kaardi turvaline liidestamine (veebi)rakendusega

a. Kliendisertifikaati verifitseeritakse krüptograafiliselt. Veendutakse, et kliendisertifikaat on väljastatud vahetult (st ei kasutata vahesertifikaate) valgesse nimekirja kuuluva CA poolt.

b. Kliendisertifikaadi kehtivust kontrollitakse kehtivusteenuse OCSP päringute abil.

c. Vajadusel piiratakse seansi loomist kliendisertifikaadis esitatud väljastuspoliitika ning kasutuspiirangute kontrollide abil.

d. Autentimispöördused ning nende vastused koos vastavate tõenditega logitakse vastavalt organisatsiooni ja äriprotsessi eesmärkidele.

e. Autenditud seansi kehtivus on ajaliselt piiratud. Seansi aegumisel korratakse autentimist.

SYS.EE.2.M9 eID liidese (SmartID, Mobiil-ID), teenuse (SiVa, SiGa vm) või vahendaja (TaRa vm) turvaline liidestamine

a. eID liidese (SmartID, Mobiil-ID), teenuse (SiVa, SiGa vm) või vahendaja (TaRa vm) liidestused on teostatud tehniliste juhendite kohaselt.

b. Teenuste ning eID liidese otspunktide vaheliseks andmesideks kasutatakse turvalist TLS protokolli. Vastavate otspunktide sertifikaadid on kinnistatud (ingl *certificate pinning*).

c. Teenuspöörduses sisalduv (sh kasutajale kuvatav) teave on kasutajale arusaadav ja sooritatava eID toiminguga üheselt seostatav ning arvestab kasutaja privaatsuse ning andmete konfidentsiaalsuse nõuetega.

d. Teenuspöörduse vastused valideeritakse liidese tehnilises kirjelduses näidatud viisil. Vastuses esitatud andmed (sh subjekti sertifikaat) on autentsed, terviklikud ja ajakohased ning vastavuses IT-süsteemi/äriprotsessi nõuetega.

e. Vajadusel piiratakse seansi loomist kliendisertifikaadis esitatud väljastuspoliitika ning kasutuspiirangute kontrollide abil.

f. Teenuspöördused ning nende vastused koos vastavate tõenditega logitakse vastavalt organisatsiooni ja äriprotsessi eesmärkidele.

g. Autenditud seansi kehtivus on ajaliselt piiratud. Seansi aegumisel korratakse autentimist.

SYS.EE.2.M10 eID klienditarkvara paigaldamine ja uuendamine

a. eID lahenduste klienditarkvara ja -teegid hangitakse heakskiidetud allikatest.

b. Tarkvara autentsust kontrollitakse digitaalse signatuuri verifitseerimise abil.

c. Klienditarkvara uusversiooni testitakse enne kasutuselevõttu vajalikes kombinatsioonides operatsioonisüsteemide ja rakendustega.

d. Tarkvarauuendus paigaldatakse kõigile eID kasutajatele ja teenustele ajaperioodi jooksul, mille määrab RIA või mida soovitab vastav tarkvaratarnija.

SYS.EE.2.M11 Andmete valmendus e-allkirjastamiseks, e-tembeldamiseks või krüpteerimiseks

a. Kasutatakse failivormingud, mis ei toeta aktiivsisu (JavaScript, makrod jm) rakendamist ning dokumendiväliste objektide dünaamilist kaasamist.

b. Vajadusel lisatakse e-allkirja konteinerisse dokumendi metaandmed (koostamise kuupäev/kellaaeg, allkirjastajate rollid jms).

c. Andmed/dokumendid ohutustatakse (eemaldatakse aktiivsed osised, kontrollitakse kahjurvara jms) enne e-allkirjastamist/e-tembeldamist.

d. Kasutatakse dokumendihaldusprotsesse, mille korral dokument enne selle edastamist teistele (organisatsioonivälistele) osapooltele allkirjastatakse (vältimaks olukorda, kus teine osapool muudab dokumenti enne e-allkirja lisamist).

SYS.EE.2.M12 E-allkirjastatud/e-tembeldatud andmete turvaline vastuvõtt

a. Valideerimist teostavad töötajad on varustatud sobivate töövahendite ning ajakohaste juhenditega.
b. Veendutakse e-allkirjastatud/e-tembeldatud andmekonteineri failivormingu sobivuses.
c. Vastuvõetud andmete e-allkirjad/e-templid valideeritakse tarkvara või teenuse abil.
d. Valideerimise tulemused koos tõenditega logitakse ning säilitatakse vastavalt organisatsiooni ja äriprotsessi eesmärkidele.
e. Enne andmete kasutamist või talletamist IT-süsteemides tehakse andmete ohutuse (kahjurvara, aktiivsed osad jmt) kontroll.
f. E-allkirjastatud/e-tembeldatud andmekonteiner säilitatakse vastavuses organisatsiooni ja äriprotsessi eesmärkidega.

SYS.EE.2.M13 CDOC vormingus krüpteeritud andmete turvaline vastuvõtt

a. Äriprotsessis on tuvastatud vajadus võtta vastu CDOC vormingus (sh kui dekrüpteerimiseks kasutatakse DigiDoc tarkvara) krüpteeritud dokumendikonteinereid.
b. On otsustatud kuidas andmete krüpteerijale edastatakse isiku isikukood või organisatsiooni registrikood, kelle nimele dokumendikonteiner krüpteeritakse või krüpteerimiseks vajalik autentimissertifikaat.
c. Vastuvõetud andmed dekrüpteeritakse esimesel võimalusel ning dekrüpteeritud andmed talletatakse vastavuses andmekaitse nõuetega.
d. Enne dekrüpteeritud andmete kasutamist on tagatud andmete ohutuse (kahjurvara, aktiivsed osad jmt) kontroll.

3.3 Standardmeetmed

SYS.EE.2.M14 eID kasutajakoolitus

a. Kasutajaid koolitatakse eID vahendite turvalise käitlemise osas järgmistel teemadel:
   - manipuleerimiskatsete äratundmine ning manipuleerimiskahtlustest teavitamise kord;
   - PIN-koodide valik, vahetamine ning turvaline säilitamine;
   - eIDga seotud mobiilseadmete turvalisus;
   - juhised eID vahendi varguse või hävimise puhuks;
   - eID vahendite ja sertifikaatide kehtivus (sh mõju krüpteeritud konteinerite dekrüpteerimisele) ja vahendite õigeaegne uuendamine;
   - eID vahendite olemasolu ja korrasoleku regulaarne kontrollimine (sh Mobiil-ID ja SmartID, mis võivad eksisteerida mitmes seadmes samaaegselt);
   - eID vahendite turvaline kasutusest kõrvaldamine (sh Mobiil-ID ja SmartID, mis võivad eksisteerida mitmes seadmes samaaegselt);
   - e-allkirjastamise, e-tembeldamise, e-allkirjade/e-templite valideerimise ning krüpteeritud konteinerite dekrüpteerimise töökorraldus organisatsioonis;

- kiipkaartide kiipkaardist eemaldamine toimingu või kasutusseansi lõppedes;
- vastavalt töötaja tööülesannetele: e-allkirjade erinevad vormingud ja tasemed ning nende tasemete tuvastamise töövahendid.

SYS.EE.2.M15 Usaldusankrute ning konfiguratsioonide regulaarne ülevaatus

a. eID liidestustes kasutatavate usaldusankrute (ingl *trust anchor*) (CA sertifikaadid, sertifikaatide väljastamispoliitikad jm) loendid on regulaarselt kontrollitud ning õigeaegselt ajakohastatud.

b. Aegunud, tühistatud või kasutuseta usaldusankrud eemaldatakse konfiguratsioonidest.

c. Kasutusele võetavad usaldusankrud lisatakse konfiguratsioonidesse.

d. Otspunktide kinnistatud sertifikaadid on uuendatud õigeaegselt.

e. eID komponentide kasutamiseks mõeldud teenuste seadistused on uuendatud teenuseandja nõuetele vastavalt.

SYS.EE.2.M16 E-allkirjade/e-templite ületembeldamine

a. Tulevikus tõestusväärtust vajavatele aegunud vormingutes e-allkirjadele ning e-templitele on lisatud täiendav ajatempel või ajakohases vormingus e-allkiri. Ületembeldamine tõendab, et algne allkirjakonteiner eksisteeris enne täiendava ajatempli/e-allkirja lisamist.

SYS.EE.2.M17 ID-kaardi lugeja turvalisus

a. Kiipkaardi lugeja on arvutiga ühendatud vahetult (välditakse lugeja ühendamist USB jaoturite ja -dokkide kaudu).

b. Avalikus kasutuses, mitme kasutaja või kõrgendatud turbevajadusega töökohal kasutatakse PIN-sõrmistikuga ja sertifitseeritud kiipkaardi lugejaid.

c. Kiipkaart eemaldatakse lugejast vajaliku toimingu lõpetamisel ning arvuti juurest lahkumisel.

SYS.EE.2.M18 eID avariivalmendus

a. Toetatud on rohkem kui üks eID vahend või valmisolek lülituda alternatiivse vahendi kasutamisele.

b. IT-süsteemides kasutatava sertifikaatide kehtivuskinnitusteenuse (OCSP) tõrke puhuks on ettevalmistatud seadistused ja juhendid tühistusnimekirjade (CRL) põhiseks töökorralduseks.

c. Ajatempliteenused on kas dubleeritud või on valmisolek ümberlülituseks alternatiivsele teenusele.

d. Alternatiivseid vahendeid, alternatiivseid teenuseid ning nende kasutusjuhendite korrektsust kontrollitakse regulaarselt.

3.4 Kõrgmeetmed

SYS.EE.2.M19 Sisemajutatud teenus vanemate (DDOC, BDOC jmt) ja teistes vormingutes (PDF, X-tee jmt) e-allkirjade/e-templite valideerimiseks (C)

a. Vältimaks tundlike dokumentide edastamist välisele osapoolele, käitatakse sisemajutuses sobivat valideerimise (SiVa vm) teenust.

b. Valideerimist teostavates kasutaja- ja serverrakendustes (DigiDoc jt) on valideerimisteenuse teenusaadressid asendatud siseteenuse andmetega kõigi kasutajate jaoks.
c. Avaliku valideerimisteenuse poole pöördumine on takistatud asjakohaste meetmetega (nt tulemüüri reeglitega).
d. Usaldusnimekirju ning valideerimistarkvara uuendatakse õigeaegselt.
e. E-allkirjade/e-templite valideerimist ei teostata RIA DigiDoc mobiilrakendusega ega muude organisatsioonivälistе valideerimisteenustega.

SYS.EE.2.M20 Õngitsuskindlate autentimisvahendite kasutamine (C-I)

a. Kriitilistes IT-süsteemides kasutatakse autentimisvahendina õngitsuskindlaid (ingl *phishing-resistant*) vahendeid, milleks on kas D-kaart, mis on vastastikku autenditud TLS-ühendusega, või sertifitseeritud füüsiline tooken (ingl *token*) WebAuthn protokolliga.

4 Lisateave

Eestis kasutatavad riiklikult tunnustatud eID vahendid vastavad kõrgele (autetimisvahendina) ning kvalifitseeritud (digitaalsel allkirjastamisel) tasemetele. Euroopas on kasutusel erineva tasemega eID vahendid ning infosüsteemides tuleb alati kontrollida, millise tasemega vahendit kasutaja kasutab.

Publikatsioonid

Lühend	Publikatsioon
[EUTS]	E-identimise ja e-tehingute usaldusteenuste seadus (EUTS) https://www.riigiteataja.ee/akt/125102016001?leiaKehtiv
[ID]	eID üldine info ja klienditarkvara https://id.ee
[RIA]	RIA eID informatsioon ning teenused riigiasutustele https://www.ria.ee/et/riigi-infosusteem/elektrooniline-identiteet-eid.html
[RIA]	Teave Eesti usaldusnimekirja kohta https://sr.riik.ee/

Kasulikud viited

eID teenuste (peamiselt SmartID ja ID-kaardi) turvalise liidestamise juhend:
https://github.com/SK-EID/smart-id-documentation/wiki/Secure-Implementation-Guide

e-allkirja moodustamise rakendus:
https://github.com/open-eid/SiGa

e-allkirja valideerimise rakendus:

https://open-eid.github.io/SiVa

eID sertifikaatide profiilid:

https://www.skidsolutions.eu/repositoorium/CP/

eIDAS raamistikus teavitatud Euroopa autentimisvahendite mittetäielik nimekiri koos tasemetega:

https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS

Euroopa Liidu usaldusnimekiri:

https://webgate.ec.europa.eu/tl-browser/#/

IND: TÖÖSTUSE IT

IND.1 Käidu- ja protsessijuhtimissüsteemid

1 Kirjeldus

1.1 Eesmärk

Esitada korralduslikud ja kontseptuaalsed meetmed käidutehnoloogia (ingl *operational technology,* OT) süsteemide, sh protsessijuhtimissüsteemide (ingl *industrial control system,* ICS) ja SCADA süsteemide turvaliseks kasutamiseks organisatsioonis.

1.2 Vastutus

Käidu- ja protsessijuhtimissüsteemide turvameetmete täitmise eest vastutab käidutehnoloogia talitus.

Lisavastutajad

IT-talitus, töötaja, infoturbejuht, arhitekt.

1.3 Piirangud

Käidu- ja protsessijuhtimissüsteemide tehniline teostus võib süsteemide otstarbe, komponentide ja tehnoloogiate erinevuse tõttu tugevasti varieeruda. Turvameetmete kujundamisel selle mooduli meetmete järgi tuleb neid erisusi arvestada.

Töötajate infoturbe teadlikkuse tõstmiseks rakendatakse täiendavalt moodulit ORP.3 *Infoturbe teadlikkuse tõstmine ja koolitus*. Protsessijuhtimissüsteemide puhul lisanduvad meetmed moodulitest ORP.4 *Identiteedi ja õiguste haldus* ja OPS.1.1.5 *Logimine*.

2 Ohud

2.1 Keskkonnamõjust tingitud kahjustused

Tööstuslikes tingimustes puutuvad käidu- ja protsessijuhtimissüsteemide komponendid kokku kahjulike keskkonnamõjudega. Kahjulikud keskkonnamõjud (nt äärmuslik kuumus, külm, niiskus, tolm, vibratsioon, söövitavad ained) võivad oluliselt mõjutada ICS-komponentide toimimist.

Sageli ilmnevad mitmed tegurid üheaegselt. Pidevas ebasoodsas keskkonnas võib ICS-komponentide eluiga olla lühem, nad võivad kiiremini kuluda ja varem rikki minna.

2.2 Käidutehnoloogia puudulik integreerimine turbekorraldusse

Kontori-IT ja tööstusautomaatika süsteemide (ingl *industrial automation and control system*) tehniliste või korralduslike erinevuste tõttu ei pruugi organisatsiooni üldised turvanõuded olla käidutehnoloogia juures piisavad või täies mahus rakendatavad. Kui infoturbe eest vastutajad ei tea tööstusautomaatika süsteemidele omaseid infoturbe ja talitlusohutuse aspekte, võivad käidutehnoloogia kasutamisega seotud ohud realiseeruda.

2.3 Puudulik käidu- ja protsessijuhtimissüsteemide haldus

Standardsete IT-halduse protseduuride kasutamine käidutehnoloogia seadmete puhul ei ole piisav kõikide käidutehnoloogia turvanõrkuste kompenseerimiseks. Kui muudatuste ja intsidentide halduses, seadmete seadistamises, rikete kõrvaldamises või turvauuendite (ingl *security update*) paigaldamises ei arvestata käidutehnoloogia eripäradega, võib see kaasa tuua käidu- ja protsessijuhtimissüsteemide tõrgetest tingitud tootmiskatkestusi, varalist kahju, vigastusi või keskkonnakahju. Volitamata muudatused ICS-komponentides võivad lisaks süsteemi funktsionaalsele toimele mõjutada ka selle turvalisust.

2.4 Puudulik juurdepääsu turve

Kui käidu- ja protsessijuhtimissüsteemide integreerimiseks organisatsiooni kesksete tootmisjuhtimise- ja ERP-süsteemidega kasutatakse ebapiisava turvalisusega sidekanalit, võidakse seda ühendust kasutada käidu- ja protsessijuhtimissüsteemide ründamiseks. Kui ICS-võrk ei ole kontorivõrgust eraldatud, ohustavad kõik organisatsiooni arvutivõrgule suunatud ründed koheselt ka protsessijuhtimissüsteemide toimimist. Ka sissetungitõrje süsteemi (ingl *intrusion prevention system*, IPS) ja kahjurvaratõrje tarkvara kasutamine käidutehnoloogia keskkondades on raskesti teostatav, kuna tarkvara aktiivne sekkumine süsteemi töösse võib ohustada tööprotsesside täitmist.

2.5 Ebaturvaline rakenduste arendusprotsess

Käidutehnoloogia rakenduste ja juhtprogrammide läbimõtlemata muudatused ja arendused võivad põhjustada tõrkeid käidutehnoloogia kasutamisel. Täiendavaid ohte põhjustavad ebaturvaline arenduskeskkond, vigane lähtekood, sisendite valideerimata jätmine või ebaturvalised andmeedastusliidesed.

2.6 Ebaturvaline kaugadministreerimine

Protsessijuhtimissüsteemide kaughaldus üle avalike võrkude (mobiilsidevõrk, Internet) võib kaasa tuua volitamata juurdepääsu käidutehnoloogia komponentidele või taristule. Ebaturvaliste konfiguratsioonidega või puudulike seirevõimalustega kaugpääsud võimaldavad ründajatel vältida võrguperimeetri turvamehhanisme.

2.7 Puudulikud seire- ja avastusprotseduurid

Protsessijuhtimissüsteemide seirefunktsioonid (protsessiga seotud hoiatused, tehniliste parameetrite näidud) vajavad toimimiseks toetavat IT-taristut. Kontrolli puudumine võrgus toimuvatest sündmuste, ründekatsete ja võrgu ummistuste üle võib kaasa tuua tõrkeid infovahetuses juhtimissüsteemiga. Intsidendid võivad jääda õigeaegselt avastamata.

2.8 Puudulik testimine

Kui käidu- ja protsessijuhtimissüsteemide muudatusi hoolikalt ei kavandata, kooskõlastata ega tegelikkusele sarnases keskkonnas ei testita, võivad märkamata jäänud loogika- või tarkvaratehnilised vead ja tõrked tööstusautomaatika süsteemides tekitada olulist kahju. Tootja poolt väljastatud testimata uuend võib väära parameetriväärtuse tõttu põhjustada tõrke protsessijuhtimissüsteemis.

2.9 Puudulik elutsükli kontseptsioon

Kuna käidutehnoloogia komponentide elutsükkel on kontori IT-seadmetega võrreldes märgatavalt pikem, siis võib käidu- ja protsessijuhtimissüsteemide võrkudes olla kasutusel riistvara- ja tarkvarakomponente (nt. operatsioonisüsteeme), millel ei ole enam tootja tuge. Kui tarkvara nõrkuste kõrvaldamiseks uuendeid ei väljastata, kasutatakse teadaolevaid nõrkusi süsteemide ründamiseks. Sama oht on ka siis, kui uuendeid ei installita või installitakse suure hilinemisega.

Kui enne uuendite paigaldamist ei tehta olemasolevast tarkvarast varukoopiat, ei saa vigase uuendi korral tarkvara vana seisu taastada.

Käidu- ja protsessijuhtimissüsteemide pikk elutsükkel võib põhjustada raskusi varuosade hankimisel, kui tootja on lõpetanud komponentide valmistamise. Sama kehtib ka vanade süsteemide hoolduse ja korrashoiu oskusteabe kohta, mida uutel töötajatel ei pruugi olla.

2.10 Ebaturvaline hankimine

Kui käidutehnoloogia seadmete hanke koostamisel ei ole esitatud piisavaid infoturbe nõudeid, võivad hangitud käidu- ja protsessijuhtimissüsteemid sisaldada turvanõrkusi, mida ei ole hiljem võimalik parandada.

Hanketingimustes liiga detailse süsteemikirjelduse esitamine võib paljastada liigset teavet organisatsiooni protsesside ja ärisaladuste kohta.

2.11 Ebaturvaliste protokollide kasutamine

Käidutehnoloogia komponentides kasutatakse tuntud võrguprotokollide (nt *Ethernet*, TCP/IP, GSM) kõrval spetsiifilisi tööstusautomaatika protokolle, mille väljatöötamisel ei ole alati infoturbe nõudeid arvestatud. Seetõttu võivad turvamehhanismid kohati üldse puududa või olla ainult piiratult rakendatavad. Teavet võidakse edastada avatekstina või turvalist autentimist kasutamata. Võrgule juurdepääsu omav ründaja saab lugeda või muuta suhtluse sisu ning sel viisil mõjutada protsesse, simuleerides näiteks andurisignaale või võltsides juhtkäske.

2.12 Ebaturvaline konfiguratsioon

Käidutehnoloogia komponentide vaikimisi konfiguratsioonis ei ole turvafunktsionaalsus alati aktiveeritud. Ebaturvalise konfiguratsiooniga komponent võib ohustada terve süsteemi turvalisust (nt kui juurdepääsuks kasutatakse vaikimisi parooli). Ebaturvalise konfiguratsiooni näide on ka mittevajalike teenuste ja turvamata liideste (nt USB- ja *Firewire*-portide) kasutamine.

2.13 Käidutehnoloogia sõltuvus IT-võrkudest

Kui käidu- ja protsessijuhtimissüsteemid pole kavandatud toimima muust võrgust täiesti eraldatutena, siis mõjutavad sisevõrgu katkestused ja muud IT-intsidendid otseselt ka käidutehnoloogia kasutamist. Kuna arvutivõrgud üldjuhul ei ole organisatsiooni käidutehnoloogia taristu käitaja kontrolli all, saab intsidente lahendada ainult välise abiga. Sellise sõltuvuse näideteks on internetiühendused (nii kaabel- kui ka mobiilsideühendused), ühiskasutatavad taristukomponendid ja pilveteenused.

3 Meetmed

3.1 Elutsükkel

Kavandamine

IND.1.M1 Integreerimine turbekorraldusse

IND.1.M11 Turvaline hankimine ja süsteemiarendus

IND.1.M12 Nõrkuste halduse korra kehtestamine

Evitus

IND.1.M3 Kahjurprogrammide tõrje

IND.1.M4 Käidutehnoloogia taristu dokumenteerimine

IND.1.M5 Sobiva tsoonikontseptsiooni väljatöötamine

IND.1.M6 Käidu- ja protsessijuhtimisüsteemide muudatuste haldus

IND.1.M7 Keskne õiguste haldus

IND.1.M20 Laiendatud süsteemidokumentatsioon

IND.1.M21 Suhtlusteede dokumenteerimine

Käitus

IND.1.M8 Käidutehnoloogia komponentide turvaline haldus

IND.1.M9 Ird-andmekandjate ja mobiilseadmete kasutamise kitsendamine

IND.1.M10 Sündmuste seire, logimine ja avastamine

IND.1.M18 Käidu- ja protsessijuhtimissüsteemi logimine

IND.1.M19 Varukoopiate tegemine

IND.1.M22 Keskne logimine ja seire

Kõrvaldamine

IND.1.M23 Käidutehnoloogia komponentide kõrvaldamine

Lisanduvad kõrgmeetmed

IND.1.M13 Käidu -ja protsessijuhtimissüsteemide avariivalmendus

IND.1.M14 Käidutehnoloogia komponentide tugev autentimine

IND.1.M15 Õiguste kontroll ja järelevalve

IND.1.M16 Tsoonide tugev isoleerimine

IND.1.M17 Regulaarne turbe läbivaatus

IND.1.M24 Kommunikatsioon rikke korral

3.2 Põhimeetmed

IND.1.M1 Integreerimine turbekorraldusse [infoturbejuht]

a. Käidutehnoloogia ja protsessijuhtimisüsteemide turbe halduseks on loodud iseseisev infoturbe halduse süsteem või on see integreeritud terviklikku infoturbe halduse süsteemi (vt ISMS.1 *Turbehaldus*).

b. Turbekorraldusse on kaasatud kõik käidutehnoloogia ja protsessijuhtimisüsteemide huvipooled.

c. Organisatsioonis on määratud käidutehnoloogia ja protsessijuhtimisüsteemide valdkonna infoturbe eest vastutav isik.

d. Infoturbe halduses on arvestatud käidutehnoloogia valdkonnaspetsiifiliste õigusaktide, eeskirjade ja erinõuetega.

IND.1.M3 Kahjurprogrammide tõrje

a. Kahjurprogrammide suhtes kontrollitakse järgmisi käidutehnoloogia ja protsessijuhtimissüsteemi komponente:
   - välisliidesed;
   - ühendused sisevõrgu, Interneti ja partnerivõrkudega;
   - ird-andmekandjad;
   - hooldus-, häälestus- ja programmeerimisterminalid;
   - uued komponendid (näiteks kettad, tarkvara).

b. Arvestatakse käidutehnoloogia komponentide tootja juhistega viirusetõrje tarkvara kasutamiseks, vajadusel rakendatakse alternatiivseid kaitsemeetmeid.

c. Teadaolevate viirusekäekirjade faili (ingl *virus signature file*) hankimine käidutehnoloogia süsteemidesse ei tohi toimuda otse Internetist.

IND.1.M4 Käidutehnoloogia taristu dokumenteerimine

a. Käidutehnoloogia taristu halduseks on koostatud täielik, ajakohane ja praktiliselt kasutatav dokumentatsioon, sh varade loend.

b. Varade loendisse on kantud ajakohased andmed kõigi tarkvara- süsteemi- ja võrgukomponentide kohta:
   - nimetus, tähis, otstarve;
   - asukoht, füüsiline turvatsoon;
   - vastutaja (koos kontaktandmetega);
   - toote mudel, tüüp, versioon, tarkvara paikamisseis, konfiguratsioon;
   - toote keskkond/platvorm, liidestusandmed, andmevahetus;
   - võrgu andmed (võrguskeem tsoonidega, aadressid, pordid, protokolliversioon);
   - valmistaja/tarnija andmed, litsentsid, sertifikaadid, teabevahetus tarnijaga;
   - varundusandmed, varunduse seis;
   - haldus- ja hooldusandmed.

c. Käidutehnoloogia ja protsessijuhtimissüsteemide dokumentatsiooni haldus on automatiseeritud.

d. Dokumentide turve vastab andmete kaitsetarbele.

IND.1.M18 Käidu- ja protsessijuhtimissüsteemide logimine

a. Kõik käidutehnoloogia ja protsessijuhtimissüsteemi komponentides tehtavad muudatused logitakse.

b. Kõik õnnestunud ja ebaõnnestunud juurdepääsukatsed protsessijuhtimissüsteemile logitakse.

IND.1.M19 Varukoopiate tegemine [töötaja]

a. Käidutehnoloogia ja protsessjuhtimissüsteemi tarkvarast ning andmetest tehakse perioodiliselt varukoopiaid.

b. Täiendavalt tehakse varukoopiate enne ja pärast käidutehnoloogia ja protsessjuhtimissüsteemi komponentide muudatust.

3.3 Standardmeetmed

IND.1.M5 Tsoonimispõhimõtete väljatöötamine [arhitekt]

a. Turvatsoonide loomisel on arvestatud käidutehnoloogia ja protsessijuhtimissüsteemide objekte ja funktsioone ning nende erinevat kaitsetarvet võrreldes kontorivõrguga.

b. Käidutehnoloogia ja protsessijuhtimissüsteemide võrgud on projekteeritud tõrke- ja ründekindlatena.

c. Käituse võrgusegmendid on teineteisest võimalikult sõltumatud. Tsoonid, millest tehnoloogilist protsessi juhitakse, peavad olema muu tsooni rikke või eraldamise korral endiselt käideldavad, nõutav ajavahemik määratakse avariikäsitluse korras.

d. Teostatakse perioodilisi kontrolle dokumenteerimata ühendusteede avastamiseks ja kõrvaldamiseks.

IND.1.M6 Käidu- ja protsessijuhtimissüsteemide muudatuste haldus

a. Organisatsioonis on määratletud, dokumenteeritud ja rakendatud käidu- ja protsessijuhtimissüsteemide muudatuste läbiviimise protsess.

b. Käidu- ja protsessijuhtimissüsteemide muudatuste halduses järgitakse üldisi muudatusehalduse meetmeid (vt OPS.1.1.3 *Paiga- ja muudatusehaldus*).

IND.1.M7 Keskne õiguste haldus [infoturbejuht]

a. Käidu-ja protsessijuhtimissüsteemide kasutajate pääsuõiguste haldus (õiguste taotlemine, kontrollimine, kehtestamine, tühistamine ja dokumenteerimine) lähtub kehtestatud pääsuõiguste halduse eeskirjast (vt ORP.4 *Identiteedi ja õiguste haldus*).

b. Õigusi antakse rollipõhiselt ning vastavalt vähima vajaduse põhimõttele. Kõigi rolli- ja personalimuudatuste korral viiakse läbi mõjutatud isikute pääsuõiguste ülevaatus.

c. Tööjaamapõhiseid juurdepääsuõigusi tulemüüri või marsruuteri pääsuloendite kaudu käsitletakse kui kasutajaõiguste andmist vastavalt pääsuõiguste halduse korrale.

d. Õiguste seis ja õiguste ajalugu on läbivaatuskõlblikult dokumenteeritud.

e. Käidu -ja protsessijuhtimissüsteemide kasutamist on võimalik tuvastada (vt IND.1.M10 *Seire, logimine ja avastamine*).

f. Pääsuõigusi kontrollitakse regulaarselt, õiguste kuritarvituse korral on võimalik rakendada sanktsioone.

IND.1.M8 Käidutehnoloogia komponentide turvaline haldus [IT-talitus]

a. Käidutehnoloogia komponentide esmaseks konfigureerimiseks on koostatud kontrollloend, mis sõltuvalt komponendist määrab:
   - tarbetute või ebaturvaliste funktsioonide, liideste jm elementide desaktiveerimise;
   - turvafunktsioonide aktiveerimise;
   - pääsu reguleerimise ja autentimise;
   - algparoolide asendamise;
   - kaugpääsu ja kaughoolduse;
   - aja sünkroniseerimise;
   - logimise.

b. Käidutehnoloogia komponentide kaughoolduseks kasutatakse eraldatud haldusvõrkusid, kus on kasutusel turvalised protokollid ja rakendatud turvaline autentimine.

c. Juurdepääs hooldeliidestele on piiratud selleks õigusi omavate isikutega.

d. Juurdepääs on antud ainult nendele süsteemidele ja funktsioonidele, mida vajatakse konkreetse administreerimisülesande täitmiseks.

e. Rakendused ja sidekanalid, mida komponentide kaughooldusel kasutatakse, on vähemalt sama kaitsetarbe tasemega kui hallatavad käidu-ja protsessijuhtimissüsteemid.

f. Kaughooldus- ja haldustoimingute volitamine, järelevalve ja juhtimine toimub reguleeritult. Juurdepääs kaughoolduseks aktiveeritakse ainult konkreetseks kasutuskorraks ja pärast seda uuesti desaktiveeritakse. Hooldustoimingud dokumenteeritakse.

g. Kaugpääsuks ei ole võimalik luua lisajuurdepääsuteid.

h. Kõrgemat turvalisust nõudvaid ja ärikriitilisi haldustoiminguid saab teha ainult mitme administraatori koostöös.

IND.1.M9 Ird-andmekandjate ja mobiilseadmete kasutamise kitsendamine

a. On kehtestatud käidutehnoloogia valdkonna ird-andmekandjate ja mobiilseadmete kasutamise eeskiri.

b. Käidutehnoloogia toodangukeskkonnas (ingl *production environment*) on ird-andmekandjate ja mobiilseadmete ühendamine piiratud, erandjuhud dokumenteeritakse.

c. Teenuseandjate omanduses olevate andmekandjate ja seadmete kasutamine lubatakse ainult kirjaliku kooskõlastusega. Vastavad nõuded on teenuseandjate poolt kirjalikult kinnitatud.

d. Käidutehnoloogia komponentide tarbetud liidesed on desaktiveeritud. Võimalusel piiratakse aktiveeritud liidestes andmekandjate ja mobiilseadmete kasutamist.

IND.1.M10 Sündmuste seire, logimine ja avastamine

a. Organisatsioonis on kehtestatud käidu- ja protsessijuhtimissüsteemide logi- ja sündmustehalduse protseduur, mis sisaldab turvasündmuste tuvastamise ja nendest teavitamise meetmeid ning intsidentide käsitlemise plaani.

b. Intsidentide käsitlemise plaani koostamisel lähtutakse organisatsiooniülesest turvaintsidentide halduse protsessist (vt DER.2.1 *Turvaintsidentide käsitlus*). Intsidentide käsitlemise plaan hõlmab sündmuste liigitamist, teatamisteid, asjassepuutuvaid struktuuriüksusi, sündmuste analüüsi ning dokumenteerimist, süsteemide taastet ja intsidendi järelkäsitlust.

c. Intsidentide käsitlemise plaani toimivust ja ajakohasust kontrollitakse regulaarselt (vähemalt kord aastas), vajadusel korrigeeritakse plaani.

d. Käidu- ja protsessijuhtimissüsteemi kasutamisel logitakse vähemalt alljärgnevad sündmused:
   - süsteemi käivitus ja restart,
   - olulised sündmused käidutehnoloogia platvormis;
   - teenuse käivitus;
   - sisselogimised ja sisselogimiskatsed;
   - haldus- ja hooldustoimingud;
   - kahjurvaratõrje tulemused;
   - võrgusündmused (ühenduse katkemised, sõnumite blokeerimised, ummistused);
   - turvalisust puudutavad vea- ja tõrketeated.

e. Käidutehnoloogia komponentide süsteemiaeg võetakse usaldusväärsetest allikatest, see on pidevalt sünkroonne välise etaloniga ja standardses vormingus (ajavöönd, suve- ja talveaeg).

f. Suure kaitsetarbe korral kasutatakse käidutehnoloogia võrgus sissetungi tuvastuse süsteemi (IDS).

IND.1.M11 Turvaline hankimine ja süsteemiarendus [infoturbejuht]

a. Käidu -ja protsessijuhtimissüsteemide hankimiseks, arendamiseks ja integreerimiseks on kehtestatud ja dokumenteeritud vajalikul kaitsetarbel põhinevad ühilduvus-, töökindlus- ja turvanõuded. Need nõudeid käsitletakse osana pakkumiskutse dokumentidest.

b. Infoturvameetmed kavandatakse käidu-ja protsessijuhtimissüsteemide arenduse varases järgus.

c. Lepingupartneritega (arendajad, tarnijad või organisatsioonivälised käitajad) on sõlmitud konfidentsiaalsuslepped.

d. Järgitakse tootjate või integreerijate soovitusi käidutehnoloogia komponentide turvaliseks kasutamiseks.

e. On määratud meetmed tegevuse jätkamiseks juhul, kui käidutehnoloogia partner lõpetab teenuse andmise (vt OPS.2.3 *Väljasttellimine*).

IND.1.M12 Nõrkuste halduse korra kehtestamine

a. Käidu -ja protsessijuhtimissüsteemide turvalisuse tagamiseks on kehtestatud nõrkuste halduse kord. Kord käsitleb käidutehnoloogia komponentide tarkvara, protokollide ja väliste liideste nõrkuste tuvastamist ja edasiste tegevuste kavandamist.

b. Nõrkuste tuvastamiseks jälgitakse asjakohaste huvigruppide (nt tootjate ning CERT-i) avaldatud nõrkuste aruandeid.

c. Tuvastatud nõrkuste hindamise (nt CVSS kriteeriumitega) järgselt kavandatakse ja rakendatakse parandusmeetmed (nt turvapaikade paigaldamine).

d. Käidutehnoloogia komponentide nõrkuste prognoosimiseks ja ennetuseks peetakse komponentide toe ja tööea lõpu arvestust.

e. Käidu- ja protsessijuhtimissüsteemide nõrkuste tuvastamiseks korraldatakse perioodiliselt läbivaatusi ja auditeid.

IND.1.M20 Laiendatud süsteemidokumentatsioon

a. Käidu- ja protsessijuhtimissüsteemid on dokumenteeritud nende kasutamiseks ja haldamiseks piisava detailsusega.

b. Süsteemidokumentatsioon sisaldab vähemalt:
   - võimalikke kasutusjuhte (nt korraline hooldus, komponentide vahetus ja remont, välised teenused);
   - organisatsioonipõhiste erisuste kirjeldust;
   - juhiseid süsteemi haldamiseks (sealhulgas kaughaldus);
   - tööstusautomaatika komponentide muudatuste kronoloogiat.

c. Kõik käidutehnoloogia komponentide muudatused dokumenteeritakse esimesel võimalusel.

d. Dokumentatsioon on kaitstud lubamatu juurdepääsu eest.

e. Dokumentatsioon on tõrgete korral kättesaadav.

IND.1.M21 Suhtlusteede dokumenteerimine

a. Tööstusautomaatika komponentide andmevahetuspartnerid, andmekategooriad ja andmevahetuse tehniline spetsifikatsioon on dokumenteeritud.

b. Uute komponentide lisamisel täiendatakse andmevahetusseoste dokumentatsiooni.

IND.1.M22 Keskne logimine ja seire

a. Käidu- ja protsessijuhtimissüsteemi logiandmed saadetakse kesksesse logisüsteemi.

b. Logiandmeid analüüsitakse regulaarselt.

c. Automaatseire käigus tuvastatud võimalikest turvakriitilistest sündmustest teavitatakse vastutavaid töötjaid automaatselt.

IND.1.M23 Käidutehnoloogia komponentide kõrvaldamine

a. Vanade või defektsete käidutehnoloogia komponentide kõrvaldamisel kustutatakse automaatikakomponendist turvaliselt kõik tundlikud andmed.

b. Automaatikakomponendi kasutuselt kõrvaldamisel veendutakse, et kõik kasutajate pääsuandmed on seadmest kustutatud.

3.4 Kõrgmeetmed

IND.1.M13 Käidu- ja protsessijuhtimisssüsteemide avariivalmendus (A)

a. Iga turvatsooni kohta on kehtestatud ja dokumenteeritud avariikäsitluse plaan (vt moodul DER.4 *Avariihaldus*), mis arvestab vähemalt järgmiste avariistsenaariumitega:
   - internetiühenduse pikaajaline (üle ühe nädala) katkestus;
   - kontori-IT täielik väljalangemine teatud ajaks (nt 2 päeva);
   - käidutehnoloogia elutähtsate IT-komponentide ajutine väljalangemine;

- käidutehnoloogia elutähtsate IT-komponentide turvarike ründe või kahjurprogrammi tõttu.

b. Käidu- ja protsessijuhtimissüsteemide jaoks on välja töötatud varundamise ja taastamise kord, milles esitatakse:
   - varundamise, taastamise ja varukoopiate regulaarse testimise protseduurid;
   - süsteemide taastamise protseduurid;
   - defektsete komponentide parandamine;
   - varuosade vajadus ning hoidmine;
   - alternatiivsed side- ja juhtimisvõimalused tõrgete korral.
c. Käidutehnoloogia avariihalduse toimimist hinnatakse regulaarselt (vähemalt kord aastas). Selleks kasutatakse avariikäsitluse testimist, avariide simuleerimist ja taastetegevuste harjutamist.
d. Kasutatakse käidu- ja protsessijuhtimissüsteemide ja käidutehnoloogia komponentide tööks vajalike tugisüsteemide (nt elektritoide, võrgukomponendid, haldusteed) dubleerimist ja liiasust.
e. Väga suure käideldavustarbe puhul on teise asukohta rajatud varujuhtimiskeskus, mille saab peamise juhtimiskeskuse väljalangemisel määratud aja jooksul kasutusele võtta.

IND.1.M14 Käidutehnoloogia komponentide tugev autentimine (C-I-A)

a. Kõikjal, kus võimalik, nõutakse komponentide (sealhulgas võrguseadmete) ja teenuste kasutamiseks ja hoolduse läbiviimiseks kasutaja identifitseerimist ja autentimist.
b. Turvaliseks autentimiseks kasutatakse multiautentimist (ingl *multifactor authentication*).
c. Avariide puhuks on loodud lokaalsed süsteemide ja rakenduste kontod, mida hoitakse turvaliselt.
d. Autentimislahenduse kavandamisel arvestatakse turvatsoonide omavahelist sõltumatust.
e. Autentimissüsteemide konfiguratsioon ja muudatused dokumenteeritakse ning süsteeme kontrollitakse intsidentide avastamiseks.

IND.1.M15 Õiguste kontroll ja seire (C-I-A)

a. Organisatsioon on koostanud varade ülevaate, mis sisaldab kõigi oluliste käidu- ja protsessijuhtimissüsteemide pääsuõiguste hetkeseisu ja muutmise ajalugu (vt IND.1.M7 *Keskne õiguste haldus*).
b. Varade ülevaade võimaldab vaadata konkreetse kasutaja õigusi kõigis süsteemides, ja teistpidi, iga süsteemi üksikute kasutajate õigusi.
c. Olulise tähtsusega haldustoimingud logitakse (vt IND.1.M10 *Sündmuste seire, logimine ja avastamine*).
d. Logid on kohustuste lahususe põhimõttel kaitstud lubamatu kustutuse ja muutmise eest.

IND.1.M16 Tsoonide tugev isoleerimine (I-A)

a. Süsteemi ja võrgu tasandil raskesti kaitstavate käidu-ja protsessijuhtimissüsteemide kaitseks kasutatakse preventiivsete turbekontrolli funktsioonidega liidestussüsteeme.
b. Riskide vähendamiseks on käidu- ja protsessijuhtimissüsteemi kohandatud või on loodud P-A-P-struktuuriga (paketifilter - rakenduslüüs - paketifilter) demilitaartsoon(id), mis võimaldavad viirusetõrjet, andmevormingute kontrolli ning sõnumisisu kontrolli ja filtreerimist.

c. Turvalisest perimeetrist tahtliku või juhusliku möödumise (nt ird-andmekandjate ja mobiilseadmete kasutamise kaudu) tõkestamiseks on rakendatud täiendavaid korralduslikke ja tehnilisi infoturbe meetmeid.

IND.1.M17 Regulaarne turbe läbivaatus [infoturbejuht] (I)

a. Käidutehnoloogia komponentide turbe kontseptsiooni vastavust turvapoliitikale ja komponentide konfiguratsiooni asjakohasust vaadatakse läbi perioodiliselt ja/või vastavalt vajadusele, näiteks uute ohtude ilmnemisel.

b. Turbe läbivaatus hõlmab vähemalt neid süsteeme, mis on välisliideste või otsese kasutajate juurdepääsu tõttu ohtudele rohkem avatud.

c. Läbivaatused sisaldavad nõrkuste hindamist ja praktilist testimist. Läbistustestide läbiviimisel arvestatakse selle võimalike mõjudega süsteemi käideldavusele.

IND.1.M24 Kommunikatsioon rikke korral [töötaja] (A)

a. Käidu- ja protsessijuhtimissüsteemide käitamiseks sidesüsteemide rikke korral on loodud alternatiivsed ja teist tehnoloogiat kasutavad varusidekanalid.

4 Lisateave

Lühend	Publikatsioon
[ISO27019]	EVS-EN ISO/IEC 27019:2020 “ Information technology - Security techniques - Information security controls for the energy utility industry”

IND.2: Tööstusautomaatika

IND.2.1 Tööstusautomaatika komponendid üldiselt

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed tööstusautomaatika süsteemide (ing *industrial automation and control system*), sh protsessijuhtimissüsteemide (ingl *industrial control system*, ICS) ja SCADA (Supervisory Control and Data Acquisition) süsteemide komponentide turbeks, olenemata komponentide valmistajast, arhitektuurist, otstarbest ja paigalduskohast.

1.2 Vastutus

„Tööstusautomaatika komponendid üldiselt“ meetmete täitmise eest vastutab käidutehnoloogia talitus.

Lisavastutajad

Töötaja, arhitekt, hooldepersonal.

1.3 Piirangud

Meetmed on üldistatud kõikidele automaatikakomponentidele. Spetsiifiliste tööstusautomaatika komponentide tehnilised meetmed on esitatud teistes mooduligrupi IND.2 *Tööstusautomaatika* moodulites. Käidutehnoloogia korralduslikud meetmed esitatakse moodulis IND.1 *Käidu- ja protsessijuhtimissüsteemid*.

2 Ohud

2.1 Süsteemi ebaturvaline konfiguratsioon

Tööstusautomaatika (ing *industrial automation and control system*) komponendi vaikeseadetes pole komponendi kasutusvõimalused piiratud. Kui tööstusautomaatika komponendi konfiguratsioonis on kogu funktsionaalsus sisse lülitatud ning teenused aktiivsed ka siis, kui neid ei kasutata, on ründajal lihtsam seadmele juurde pääseda. Muutmata jäetud vaikeparooli või seadme konfiguratsioonivea tõttu ülevõetud seadet saab ära kasutada tööstusautomaatika süsteemi edasiste rünnete lähtekohana.

2.2 Puudulik kasutajate ja õiguste haldus

Osal tööstusautomaatika komponentidel on autonoomne kasutajate ja õiguste halduse funktsioon. Kui pääsuõigusi keskselt ei hallata, võivad juurdepääsu tööstusautomaatika komponentidele saada selleks volitamata isikud. Kui pääsuõigustest puudub ülevaade, võivad töötajad kasutada jagatud kasutajakontot või jäävad teenuseandjate kontod sulgemata.

2.3 Puudulik logimine

Kui logitakse ainult automatiseeritud protsessiga seotud sündmusi, jäävad infoturbe seisukohast olulised tööstusautomaatika komponentide andmed ja sündmused tähelepanuta. See teeb turvasündmused raskesti avastatavaks ning toimunud intsidente ei ole võimalik tagantjärele analüüsida.

2.4 Automaatikakomponentide manipuleerimine ja sabotaaž

Tööstusautomaatika komponentide mitmekesiste liidestusvõimalustega kaasneb süsteemide, tarkvara ja edastatava teabe manipuleerimise oht. Automaatikakomponendis võib ründaja blokeerida või muuta oleku- ja tõrketeateid või muid mõõtetulemusi. Manipuleeritud mõõtetulemused võivad põhjustada teiste komponentide või teenindava personali valeotsuseid. Manipuleeritud süsteeme võidakse ära kasutada uute manipulatsioonide varjamiseks või muude süsteemide ja asukohtade ründamiseks.

2.5 Ebaturvalised protokollid

Tööstusautomaatika süsteemides kasutatakse sageli protokolle, mille turvamehhanismid kas üldse puuduvad või on puudulikud. Tehnilist teavet edastatakse lihttekstina, ilma tervikluse kontrollita ja eelneva autentimiseta. Sidekanalile juurdepääsu omav ründaja saab muuta suhtluse sisu või sekkuda juhtkäskudesse ning seeläbi mõjutada seadmete tööd. Protokollitasandil on rünne võimalik ka juhul, kui komponentide muu konfiguratsioon on turvaline ja ilma nõrkusteta.

2.6 Ummistusründed (DoS)

Ründaja saab tööstusautomaatika komponentide kasutamist mõjutada ummistusrünnetega (ingl *denial of service attack*). Reaalajas toimuvate protsesside korral võib juba lühiajaline häiring põhjustada teabekao või juhtimise kontrolli kadumise.

2.7 Kahjurprogrammid

Ka isoleeritud tööstusautomaatika võrkudes esineb kahjurprogrammide oht. Nakatumise võimalused tulenevad liidestest väliskeskkonna ja kontori-IT-ga. Suureks ohuks on hoolduses kasutatavad sülearvutid ja tööstusautomaatika komponentide programmeerimisel ja hooldamisel kasutatavad ird-andmekandjad. Viimaste kaudu saab kahjurprogramme üle kanda ka isoleeritud keskkondades.

2.8 Teabe luure

Tööstusautomaatika komponendid sisaldavad üksikasjalikku teavet protsessi või toimingu kohta. Ka edastatud näitudest (nt mõõte- või juhtsignaalide andmetest ja juhtimisprogrammidest) on võimalik tuletada ärisaladuseks liigitatavat teavet. Ründaja võib saada ligipääsu ärisaladustele (tööstusspionaaž) või intellektuaalomandile. Samuti hangitakse teavet tööstusautomaatika komponentide tööpõhimõtte ja turvamehhanismide kohta, et seda kasutada edasiste rünnete sooritamiseks.

2.9 Manipuleeritud püsivara

Tööstusautomaatika komponentidel saab lisaks rakendusprogrammidele muuta ka püsivara (ingl *firmware*). Manipuleeritud püsivara kasutamisel on võimalik programmeerida lokaalseid liideseid (nt USB-porti) või mõjutada komponendi toimimist olemasoleva võrguühenduse kaudu. Ka tarkvarauuendit on võimalik teekonnal tootjast kasutajani manipuleerida. Ebaturvalisest allikast tehtud ostu kaudu võib käitajani jõuda juba kompromiteeritud püsivaraga komponent. Ründaja saab võimaluse protsesside ja protseduuride muutmiseks ja võltsimiseks.

3 Meetmed

3.1 Elutsükkel

Kavandamine

IND.2.1.M13 Automaatikakomponentide nõuetekohane kasutuselevõtmine

Evitus

IND.2.1.M4 Tarbetute teenuste, funktsioonide ja liideste desaktiveerimine või desinstallimine

IND.2.1.M6 Võrgu segmentimine

Käitus

IND.2.1.M1 Konfigureerimis- ja hooldeliideste juurdepääsu kitsendamine

IND.2.1.M2 Turvaliste protokollide kasutamine konfigureerimiseks ja hoolduseks

IND.2.1.M7 Andmete varundamine

IND.2.1.M8 Kahjurvara tõrje

IND.2.1.M11 Automaatikakomponentide hooldus

IND.2.1.M16 Välisliideste turve

IND.2.1.M17 Turvaliste protokollide kasutamine infoedastuseks

Lisanduvad kõrgmeetmed

IND.2.1.M18 Avariiside

IND.2.1.M19 Turvatestimine

IND.2.1.M20 Usaldusväärne programmikood

3.2 Põhimeetmed

IND.2.1.M1 Konfigureerimis- ja hooldeliideste juurdepääsu kitsendamine

a. Tööstusautomaatika (ing *industrial automation and control system*) komponentide konfigureerimis- ja hooldeliidestele on juurdepääs ainult volitatud töötajatel.

b. Seadmete tüüpkasutajakontod on blokeeritud ja vaikeparoolid on vahetatud (vt ORP.4 *Identiteedi ja õiguste haldus*). Uusi paroole hoitakse turvaliselt.

c. Tööstusautomaatika komponentide konfiguratsiooni saab muuta selleks volitatud ja autenditud töötaja. Konfiguratsioonimuudatused dokumenteeritakse.

IND.2.1.M2 Turvaliste protokollide kasutamine konfigureerimiseks ja hoolduseks [hooldepersonal]

a. Tööstusautomaatika komponentide konfigureerimiseks ja hooldamiseks kasutatakse turvalisi protokolle.

b. Konfigureerimise ja hoolduse käigus edastatavad andmed on kaitstud.

IND.2.1.M4 Tarbetute teenuste, funktsioonide ja liideste desaktiveerimine või desinstallimine [hooldepersonal]

a. Kõik tööstusautomaatika komponentide tarbetud teenused, funktsioonid ja liidesed on desaktiveeritud või desinstallitud.

IND.2.1.M6 Võrgu segmentimine [arhitekt]

a. Tööstusautomaatika komponendid on lahutatud kontori IT-süsteemidest.

b. Tööstusautomaatika komponentide töö sõltuvused võrguteenustest on dokumenteeritud.

c. Tööstusautomaatika komponentide suhtlus teiste komponentidega on vajaduspõhine ja võimalikult minimaalne.

3.3 Standardmeetmed

IND.2.1.M7 Andmete varundamine

a. Programmidest ja andmetest tehakse regulaarselt varukoopiaid.

b. Varukoopia tehakse alati ka pärast süsteemi muudatusi.

IND.2.1.M8 Kahjurvara tõrje

a. Tööstusautomaatika komponendid on kaitstud kahjurvara eest (vt OPS.1.1.4 *Kaitse kahjurprogrammide eest*).

b. Kahjurvaratõrje tarkvara ja viirusekäekirjad on uuendatud viimase versioonini.

c. Kui kahjurvaratõrje tarkvara ei saa komponendi ressursi nappuse või reaalajanõuete tõttu kasutada, rakendatakse kompenseerivaid meetmeid (nt käidutehnoloogia tootmisvõrgu isoleerimine).

IND.2.1.M11 Automaatikakomponentide hooldus [hooldepersonal]

a. Uued ja kinnitatud turvauuendid installitakse tööstusautomaatika komponentide korralise hoolduse käigus.

b. Operatsioonisüsteemi uuendid installitakse töökeskkonna komponendile ainult pärast komponendi valmistajalt kinnituse saamist ning testimist oma testimiskeskkonnas.

c. Kriitiliste turvauuendite ilmnemisel tehakse nende paigaldamiseks hooldus esimesel võimalusel.

IND.2.1.M13 Automaatikakomponentide käikuandmise kord

a. Tööstusautomaatika komponendid kinnitatakse kasutamiseks ainult siis, kui nende püsivara, tarkvara ja turvauuendid vastavad hetkenõuetele.

b. Tööstusautomaatika komponendid on integreeritud käituse, seire ja infoturbe halduse protsessidesse. Eelkõige hõlmab see:

- muudatuste ja õiguste haldust;
- nõrkuste haldust;
- kahjurvaratõrjet;
- käituse seiret ja avariivalmendust;
- regulaarset süsteemide turvaläbivaatust.

IND.2.1.M16 Välisliideste turve

a. Välise juurdepääsuga liidesed, nt võrguliidesed, USB-pordid ja jadaühendused, on kaitstud väärkasutuse eest.

IND.2.1.M17 Turvalised andmesideprotokollid

a. Mõõte- ja juhtimisandmed on kaitstud lubamatu juurdepääsu ja muutmise eest.

b. Reaalajarakenduste puhul kaitstakse andmeid vastavalt vajadusele ja võimalusele.

c. Avalikes võrkudes edastatavad mõõte- ja juhtandmed on nõuetekohaselt kaitstud.

3.4 Kõrgmeetmed

IND.2.1.M18 Avariiside [töötaja] (A)

a. Tegevusvõime säilitamiseks tõrgete korral on loodud alternatiivsed ja sõltumatud sidekanalid.

IND.2.1.M19 Turvatestimine (C-I-A)

a. Tehniliste turvameetmete toimivust kontrollitakse regulaarsete turvatestimistega.

b. Testimised plaanitakse hooldusaegadele ja neid ei tehta töötavatel seadmetel.

c. Testimistulemused dokumenteeritakse, tuvastatud riske analüüsitakse ja käsitletakse.

IND.2.1.M20 Usaldusväärne programmikood (I-A)

a. Püsivara uuendeid ja uusi juhtprogramme installitakse alles pärast uuendite tervikluses ja autentsuses veendumist.

4 Lisateave

Lühend	Publikatsioon
[NIST]	NIST Special Publication 800-82 , „Guide to Industrial Control Systems (ICS) Security“

IND.2.2 Programmeeritavad kontrollerid

1 Kirjeldus

1.1 Eesmärk

Tagada programmeeritavate kontrollerite (ingl *programmable logic controller*, PLC) turve olenemata nende valmistajast, otstarbest, arhitektuurist või asukohast.

1.2 Vastutus

Programmeeritavate kontrollerite meetmete täitmise eest vastutab käidutehnoloogia talitus.

1.3 Piirangud

Tööstusautomaatika komponentide turbe üldised meetmed on esitatud moodulis IND.2.1 *Tööstusautomaatika komponendid üldiselt*. Talitlusohutuse (ingl *functional safety*) automaatika valdkonna meetmed on kirjeldatud moodulis IND.2.7 *Ohutusautomaatika*. Käidutehnoloogia korralduslikud meetmed esitatakse moodulis IND.1 *Käidu- ja protsessijuhtimissüsteemid.*

2 Ohud

2.1 Puudulik dokumentatsioon

Kui programmeeritavate kontrollerite dokumentatsioon on puudulik, võivad olulised liidesed ja turvafunktsioonid jääda tähelepanuta. Kui dokumentatsioonis ei kirjelda piisavalt kasutatavaid funktsioone, ühendusporte ning õiguste haldust, võib juhtuda et turvanõrkused jäävad parandamata. Puuduliku dokumentatsiooni korral võib tekkida probleem kontrolleritega tegeleva töötaja lahkumisel.

3 Meetmed

3.1 Elutsükkel

Käitus

IND.2.2.M1 Programmeeritavate kontrollerite (PLC) täielik dokumentatsioon

IND.2.2.M3 Aja sünkroniseerimine

3.2 Põhimeetmed

Antud moodulis põhimeetmed puuduvad.

3.3 Standardmeetmed

IND.2.2.M1 Programmeeritavate kontrollerite (PLC) täielik dokumentatsioon

a. Juhtimisprogrammid ja kontrolleri konfiguratsioon arhiveeritakse pärast iga muudatust.
b. Konfiguratsioonimuudatused ja komponentide väljavahetamine dokumenteeritakse.

IND.2.2.M3 Aja sünkroniseerimine

a. Süsteemiaegade sünkroniseerimine on tsentraliseeritud ja automaatne.

3.4 Kõrgmeetmed

Antud moodulis kõrgmeetmed puuduvad.

IND.2.3 Andurid ja täiturid

1 Kirjeldus

1.1 Eesmärk

Tagada nutikate andurite (ingl *sensor*) või anduritena töötavate seadmekogumike turve sõltumata nende valmistajast, otstarbest, arhitektuurist või asukohast.

1.2 Vastutus

Andurite ja täiturite (ingl *actuator*) meetmete täitmise eest vastutab käidutehnoloogia talitus.

Lisavastutajad

Hooldepersonal.

1.3 Piirangud

Tööstusautomaatika komponentide turbe üldised meetmed on esitatud moodulis IND.2.1 *Tööstusautomaatika komponendid üldiselt*. Moodul ei käsitle traadita andurivõrke (vt SYS.4.4 *Esemevõrgu (IoT) seade üldiselt*). Käidu- ja juhtimistehnika üldised turvameetmed on esitatud moodulis IND.1 *Käidu- ja juhtimistehnika*.

2 Ohud

2.1 Puudulikud turvanõuded toodete hankimisel

Kui puuduliku riskiteadlikkuse ja lisakulude tõttu ei pöörata andurite hankimisel infoturbele piisavat tähelepanu, võivad need sisaldada nõrkusi, mida on hiljem väga kulukas kõrvaldada.

Tööstuskeskkonnas kasutatavad andurid võivad asuda ekstreemsete temperatuuridega, niiskust, tolmu, vibratsiooni sisaldavas või söövitava toimega keskkonnas. Kahjulike keskkonnamõjude tõttu võivad tööstusautomaatika komponentide andurid kiiremini kuluda, varem rikki minna või anda ebaõigeid mõõtetulemusi.

2.2 Väär kalibreerimine

Kui andurid on kalibreeritud vääralt või kui andurite kalibreerimisele on lubamatu juurdepääs, ei pruugi andurite näidud olla usaldusväärsed ja anda ebaõigeid mõõtetulemusi.

3 Meetmed

3.1 Elutsükkel

Evitus

IND.2.3.M1 Andurite õige valimine ja paigaldamine

Käitus

IND.2.3.M2 Andurite kalibreerimine

Lisanduvad kõrgmeetmed

IND.2.3.M3 Traadita side vältimine

3.2 Põhimeetmed

IND.2.3.M1 Andurite õige valimine ja paigaldamine [hooldepersonal]

a. Andurite valimisel ja hankimisel on arvestatud valmistaja usaldusväärsust ning andurite sobivust antud keskkonnatingimustele (temperatuur, tolm, vibratsioon, korrosioon jms).

b. Andurid on paigaldatud ja installitud vastavalt valmistaja nõuetele.

3.3 Standardmeetmed

IND.2.3.M2 Andurite kalibreerimine [hooldepersonal]

a. Andureid kalibreeritakse regulaarselt, kalibreerimine dokumenteeritakse.

b. Lubamatu juurdepääs kalibreerimisele on tõkestatud.

3.4 Kõrgmeetmed

IND.2.3.M3 Traadita side vältimine (C)

a. Suurema kaitsetarbe korral ei kasutata raadiovõrke (nt raadiokohtvõrku (WLAN), lähiväljasidet (NFC) või *Bluetooth*'i).

b. Tarbetud sideliidesed desaktiveeritakse.

IND.2.4 Robotseadmed

1 Kirjeldus

1.1 Eesmärk

Esitada elektrooniliselt juhitavate pool- või täisautomaatsete robotseadmete (nt masinjuhitavate tööpinkide) turbe meetmed, sõltumata nende valmistajast, otstarbest, arhitektuurist või asukohast. paigalduskohast.

1.2 Vastutus

Mooduli „Robotseadmed“ meetmete täitmise eest vastutab käidutehnoloogia talitus.

1.3 Piirangud

Meetmed on suunatud robotseadmetele, mille sisemisele konfiguratsioonile puudub organisatsioonil juurdepääs. Tööstusautomaatika komponentide turbe üldised meetmed on esitatud moodulis IND.2.1 *Tööstusautomaatika komponendid üldiselt*. Käidutehnoloogia üldised korralduslikud turvameetmed esitatakse moodulis IND.1 *Käidu- ja protsessijuhtimissüsteemid.*

2 Ohud

2.1 Puudulikust hooldusest põhjustatud tõrge või häiring

Kui robotseadmeid regulaarselt ei hooldata, ei tööta seadmed enam õigesti või langevad rivist välja. Robotseadme tõrked ja ebastabiilne töötamine võivad ohustada töötajaid ja häirida tootmist.

2.2 Sihilikud manipulatsioonid

Kui robotseadme liidesed on ebapiisavalt kaitstud, saab ründaja lokaalsete programmeerimisliidese või võrgu kaudu manipuleerida masina parameetreid. Sel viisil on võimalik töödeldavaid detaile tahtlikult kahjustada või muuta defektseks terve tooteseeria. Ründaja saab rikkuda ka seadme enda.

3 Meetmed

3.1 Elutsükkel

Käitus

IND.2.4.M1 Valmistaja tehtava kaughoolduse turve

IND.2.4.M2 Protseduur käituseks pärast garantiiaja lõppu

3.2 Põhimeetmed

IND.2.4.M1 Valmistaja tehtava kaughoolduse turve

a. On kehtestatud keskne kaughalduse eeskiri, mis määrab, milliseid kaughoolduslahendusi kasutatakse, kuidas kaitstakse sideühendusi ja tehakse kaughoolduse seiret.

b. Robotseadme kaughoolduse tegemisel ei pääse hoolduse tegija juurde organisatsiooni muudele süsteemidele või robotseadmetele.

c. Robotseadmesse salvestatud andmete kasutamise protseduurid on hoolduse tegijaga koos-kõlastatud.

IND.2.4.M2 Protseduur käituseks pärast garantiiaja lõppu

a. On kehtestatud protseduur robotseadme turvaliseks käituseks pärast garantiiaja lõppu.

b. Robotseadme tarnijaga on sõlmitud tugiteenuseleping.

3.3 Standardmeetmed

Antud moodulis standardmeetmed puuduvad.

3.4 Kõrgmeetmed

Antud moodulis kõrgmeetmed puuduvad.

IND.2.7 Ohutusautomaatika

1 Kirjeldus

1.1 Eesmärk

Esitada infoturbe meetmed ohutusautomaatika süsteemi rajamiseks.

Selles mooduli kontekstis hõlmab ohutusautomaatika andureid, täitureid, ohutustehnilist programmeeritavat juhtimist (loogikasüsteemi), rakendustarkvara ning juurdekuuluvaid programmeerimisseadmeid, konfigureerimispulte ja visualiseerimisvahendeid.

1.2 Vastutus

Ohutusautomaatika meetmete täitmise eest vastutab käidutehnoloogia talitus.

Lisavastutajad

Infoturbejuht, arhitekt, hooldepersonal.

1.3 Piirangud

Moodul täiendab ohutusautomaatika vaatest mooduleid IND.1 *Käidu- ja protsessijuhtimissüsteemid* ja IND.2.1 *Tööstusautomaatika komponendid üldiselt.* Hoolduseks ja halduseks programmeerimisseadmetena ja visualiseerimisvahenditena kasutatavate IT-süsteemide turve on esitatud moodulis SYS.2.1 *Klientarvuti üldiselt*.

2 Ohud

2.1 Loogikasüsteemi manipuleerimine

Loogikasüsteemi rakendusprogrammi manipuleerimine võib kahjustada ohutusautomaatika terviklust. Erinevalt käidutehnoloogia tavakomponendist võib ohutusautomaatika komponendi manipuleerimisest tulenev oht inimestele, keskkonnale ja tehnilistele süsteemidele olla palju suurem.

2.2 Puudulikud seire- ja tuvastusprotseduurid

Kui automatiseeritava protsessi tööseisundite näitusid, seisu jälgimisega seotud hoiatusi (nt täitetaseme ületamise korral) ja tehnilisi parameetreid (temperatuur, ventiilide asend) saab manipuleerida, võib see kaasa tuua väga raskeid tagajärgi, sealhulgas ohu inimeste elule ja tervisele. Manipuleerimise teeb võimalikuks ründetuvastussüsteemide puudumine ja ohutusautomaatika komponentide puudulik seire. Seire puudumisel pole ründeid võimalik aegsasti avastada.

3 Meetmed

3.1 Elutsükkel

Kavandamine

IND.2.7.M6 Ohutusautomaatika tervikluse turve

IND.2.7.M4 Infoturbe sidumine talitlusohutuse haldusega

Evitus

IND.2.7.M1 Arvelevõtt ja dokumenteerimine

IND.2.7.M7 Ohutusautomaatika eraldamine ja sõltumatus keskkonnast

Käitus

IND.2.7.M2 Riistvara- ja tarkvarakomponentide sihtotstarbeline kasutamine

IND.2.7.M3 Loogikasüsteemi turve

IND.2.7.M5 Ohutusautomaatika intsidendihaldus

IND.2.7.M8 Tehniliste andmete turvaline edastus ohutusautomaatikale

IND.2.7.M9 Andme- ja signaaliühenduste turve

IND.2.7.M10 Simuleeritud või sillatud muutujate esitus ja alarmeerimine

IND.2.7.M11 Integreeritud süsteemide ohutuse reguleerimine

Lisanduvad kõrgmeetmed

IND.2.7.M12 Rakendusprogrammide ja konfiguratsiooniandmete tervikluse ja autentsuse tagamine

3.2 Põhimeetmed

IND.2.7.M1 Arvelevõtt ja dokumenteerimine [arhitekt, hooldepersonal]

a. Ohutusautomaatika süsteemidesse kuuluvad riist- ja tarkvarakomponendid, andmed ja ühendused on dokumenteeritud.

b. Ohutusautomaatika süsteemi dokumentatsioon sisaldab järgmist:
   - andmeühendustes kasutatavate signaalide spetsifikatsioon;
   - andmetüüp;
   - andmevahetuse protokoll ja suund;
   - turvateave (autentimine, sertifikaadid, krüpteerimine);
   - ohutusautomaatika kavandamise, teostuse, hoolduse, seire, kontrolli ja muutmise protsesside eest vastutavad allüksused ja rollid.

c. Dokumentatsiooni ajakohastatakse muudatuste korral ja kontrollitakse vähemalt kord aastas.

IND.2.7.M2 Riistvara- ja tarkvarakomponentide sihtotstarbeline kasutamine [hooldepersonal]

a. Ohutusautomaatika süsteemidesse kuuluvaid ja koos nendega kasutatavaid tark- ja riistvarakomponente ei kasutata muuks otstarbeks.

IND.2.7.M3 Loogikasüsteemi turve [hooldepersonal]

a. Loogikasüsteemi turvamehhanismid on aktiveeritud. Kui see pole tehtav või kui kaitsetarve on suurem, lisatakse korralduslikke meetmeid.

b. Loogikasüsteemide rakendusprogramme saavad muuta ja süsteemi installimise kinnitada ainult selleks volitatud isikud.

c. Ohutusautomaatika komponente kaitstakse lubamatu füüsilise juurdepääsu eest.

d. Programmeerimisseadmeid ühendatakse süsteemiga ainult vajaduse korral ja seansipõhiselt.

3.3 Standardmeetmed

IND.2.7.M4 Infoturbe sidumine talitlusohutuse haldusega [käidutehnoloogia talitus]

a. Ohutusautomaatika infoturbega seotud protsessid, õigused ja kohustused on selgelt määratletud ja integreeritud talitlusohutuse halduse protsessiga.

b. Ohutusautomaatika seadmeid hallatakse vastavalt õigusnormidele ja ohutusstandarditele.

IND.2.7.M5 Ohutusautomaatika intsidendihaldus [infoturbejuht]

a. On kehtestatud ohutusautomaatika intsidendikäsitlusplaan, mis määrab vajalikud rollid ja kohustused;

b. Intsidendikäsitlusplaanis arvestatakse vähemalt järgmiste stsenaariumitega:
   - ohutusautomaatika side katkemine, sidepartneri turvarike;
   - anduri, täituri või loogikasüsteemi turvarike (nt kahjurvara hooldepuldis).

c. Tegutsemist intsidendistsenaariumide korral harjutatakse regulaarselt.

IND.2.7.M6 Ohutusautomaatika tervikluse turve [arhitekt, hooldepersonal]

a. Spetsifikatsiooni, teostuse ja tehniliste parameetrite juhusliku ja volitamata muutmise võimalused on tõkestatud.

IND.2.7.M7 Ohutusautomaatika eraldamine ja sõltumatus keskkonnast [arhitekt, hooldepersonal]

a. Ohutusautomaatika seadmeid kaitstakse keskkonnast tulenevate kahjulike mõjude (sh vigased või ummistavad andmed) eest.

b. Keskkonnaga side või andmevahetuse katkemise puhuks on asendusväärtuste kasutamise protseduur.

c. Ohutusautomaatikat mõjutada võivate protsesside muudatused tehakse talitlusohutuse halduse kaudu.

IND.2.7.M8 Tehniliste andmete turvaline edastus ohutusautomaatikale [arhitekt, infoturbejuht, hooldepersonal]

a. Rakendatakse tehnilisi ja korralduslikke meetmeid ohustusautomaatikale edastatavate andmete autentsuse ja tervikluse kaitseks.

b. Tööseadmete kasutamine isiklikuks otstarbeks on keelatud.

c. Andmete edastus ird-andmekandjatel on piiratud (vt CON.9 *Teabevahetus*).

IND.2.7.M9 Andme- ja signaaliühenduste turve [arhitekt, infoturbejuht, hooldepersonal]

a. On rakendatud meetmed ühesuunaliste ühenduste turvalisuse tagamiseks (näiteks suundlüüs).

b. Andme- ja signaaliühendused, mis vajavad tagasisidet (kahesuunalisust), on turvatud. Kahesuunaliste ühenduste puhul rakendatakse sõltuvalt vajadusest ja füüsilisest turbest alljärgnevaid meetmeid:
   - ohutusautomaatika sidepartner tõendab turvalisust turva- või riskianalüüsiga;
   - edastatavad andmed krüpteeritakse, sidepartner on autenditud;
   - ühendused algatatakse alati ohutusautomaatika keskkonnast;
   - andmeliiklus on piiratud määratud portide ja aadressidega;
   - edastatavate sõnumite sisu seire võimalike anomaaliate leidmiseks.

IND.2.7.M10 Simuleeritud või sillatud muutujate esitus ja alarmeerimine [arhitekt]

a. Asendusväärtustega simuleeritud või väljast sillatud muutujaid seiratakse ning väärtused esitatakse kasutajale pidevalt ja ühetähenduslikult.

b. Nende muutujate väärtusepiirid on määratletud ja piirini jõudmisest alarmeeritakse.

IND.2.7.M11 Integreeritud süsteemide ohutuse haldus [arhitekt, hooldepersonal]

a. On välja töötatud strateegia ohutusega seotud komponentide kasutamiseks integreeritud süsteemides.

b. Ühiskasutus ei tekita ohutussüsteemile turvariske, ühiskasutuslike komponentide hulgas on turvalised piisavalt lahus ebaturvalistest.

3.4 Kõrgmeetmed

IND.2.7.M12 Rakendusprogrammide ja konfiguratsiooniandmete tervikluse ja autentsuse tagamine [arhitekt] (I)

a. Hangitakse ainult selliseid ohutusautomaatika vahendeid, millele tootja on välja töötanud piisavad terviklus- ja autentsuskontrolli mehhanismid.

b. Loogikasüsteemi või sellega seotud andurite ja täiturite konfiguratsiooniandmete ja rakendusprogrammide terviklus- ja autentsuskontrolli mehhanismid on aktiveeritud ja turvaliselt konfigureeritud.

c. Tervikluse rikked tuvastatakse ja tehakse teatavaks automaatselt.

d. Allalaaditavana väljastatav tarkvara on kaitstud manipuleerimise eest. Püsivara ja selle uuendid saadakse valmistajalt signeeritult.

e. Ohutusautomaatika programmeerimise ja halduse seadmeid ei kasutata muuks otstarbeks (ei ühendata võrku).

f. Vajadusel kasutatakse kompenseerivaid turvamehhanisme, näiteks ohutusautomaatika lahutamist demilitaartsooni.

4 Lisateave

Lühend	Publikatsioon

[ISO61508]	EVS-EN 61508-2:2010 „Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronicsafety-related systems“
[ISO61511]	EVS-EN 61511-1:2017 „Functional safety - Safety instrumented systems for the process industry sector - Part 1: Framework, definitions, system, hardware and application programming Requirements“
[ISO62443]	IEC 62443-2-1:2010 „Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program“

IND.3 Käidutehnoloogia võrgud

IND.3.2 Käidutehnoloogia komponentide kaughooldus

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed käidutehnoloogia (ingl *operational technology*, OT) komponentide turvaliseks kaughoolduseks. Käidu -ja protsessijuhtimissüsteemid koosnevad tavaliselt erinevate tootjate riistvara- ja tarkvarakomponentidest, mille käigushoiuks ja hoolduseks on vajalik tagada volitatud hoolduspersonali kaugjuurdepääs.

1.2 Vastutus

Käidutehnoloogia komponentide kaughoolduse meetmete täitmise eest vastutab käidutehnoloogia talitus.

Lisavastutajad

IT-talitus, arhitekt, hooldepersonal, andmekaitsespetsialist, töötaja.

1.3 Piirangud

Moodulis esitatakse ainult käidutehnoloogia spetsiifikat arvestavad meetmed. Konkreetse käidutehnoloogia süsteemi eripärast tingituna võivad OT komponendile rakendatavad meetmed antud moodulis kirjeldatust erineda.

Käidutehnoloogia süsteemidele rakendatakse lisaks üldised kaughoolduse meetmed moodulist OPS.1.2.5 *Kaughooldus* ning turvalise võrguarhitektuuri meetmed moodulist NET.1.1 *Võrgu arhitektuur ja lahendus*.

Antud moodul ei käsitle protsessijuhtimissüsteemide (ingl *industrial control systems*, ICS) tavakasutust ja kaugseiret käidukeskkonnas (nt protsesside käivitamist või seiskamist). Meetmed protsessijuhtimissüsteemide turvaliseks kasutamiseks on esitatud moodulites IND.1 *Käidu- ja protsessijuhtimissüsteemid* ja IND.2.7 *Ohutusautomaatika*.

Sõltuvalt käidutehnoloogia komponentide kaughoolduse korraldusest rakendatakse täiendavalt meetmeid järgmistest moodulitest: OPS.1.1.4 *Logimine*, OPS.2.3 *Väljasttellimine*, OPS.2.2 *Pilvteenuste kasutamine*, APP.3.1 *Veebirakendused*.

2 Ohud

2.1 Kaughoolduse pääsuõiguste puudulik dokumenteerimine

Organisatsiooni käidutehnoloogia komponentidele vajavad juurdepääsu organisatsiooni töötajad, komponentide tootjad ja väliseid partnerettevõtted. Praktikas kasutatakse kaugjuurdepääsu andmiseks erinevaid tehnilisi lahendusi, mistõttu on risk teha vigu pääsuõiguste halduses. Kontori arvutivõrguga võrreldes on käidutehnoloogia süsteemide pääsuõiguste halduse protsess sageli oluliselt halvemini reguleeritud ja dokumenteeritud.

Puudused pääsuõiguste regulatsioonis suurendavad käidutehnoloogia komponentidele volitamata juurdepääsu riski. Manipuleerides üksikut komponenti on võimalik otseselt mõjutada ICS-i füüsilisi protsesse ning põhjustada häireid kogu tootmisprotsessis. Raskemal juhul võib ohtu sattuda töötajate elu ja tervis. Kuna üksiku kaughoolduse komponendi toimimine võib mõjutada terve käidutehnoloogia süsteemi tööd, tuleb kõiki tehtavaid muudatusi hallata komplekselt. Teadmise puudumine sellest, kes ja millal komponenti uuendas või konfigureeris, vähendab oluliselt süsteemi töökindlust.

2.2 Käidutehnoloogia võrgu sõltuvus organisatsiooni arvutivõrgust

Käidutehnoloogia süsteemid vajavad erinevalt organisatsiooni arvutivõrgust reaalajas andmeid ning katkestuseta andmesideühendusi. Pelgalt lühiajaline käideldavushäire võib ICS süsteemis tekitada kriitilisi vigu.

Kui arvutivõrk ja käidutehnoloogia võrk on eraldamata, võib arvutivõrgu turvanõrkuste ärakasutamine mõjutada ka käidutehnoloogia komponentide turvalisust.

Kui käidutehnoloogia kaughooldus toimub arvutivõrgu komponentide ja teenuste kaudu, võib arvutivõrgu halduprotseduuridest tingitud viivituste tõttu viibida ICS kriitiliste vigade kõrvaldamine.

2.3 Puudulikud nõuded kaughoolduse teostajatele

Organisatsiooni arvutivõrgu haldusele esitatavad üldised turvanõuded on käidutehnoloogia võrgu jaoks sageli sobimatud, kuna teenusele esitatavad nõudeid ei ole piisavalt kitsendatud. Arvutivõrgu jaoks sobivad konfiguratsiooni- ja muudatusehalduse nõuded ei pruugi olla käidutehnoloogia võrkudes kasutamiseks piisavalt detailsed.

Poolte vahel kokku leppimata pääsuhaldusreeglid ei võimalda üksikute kasutajate õigusi käidutehnoloogia süsteemis piisava täpsusega hallata. Välise partneri või tootjaettevõtte töötajad on käidutehnoloogia talitusele tundmatud, seetõttu on detailne ülevaade pääsuõigustest äärmiselt oluline.

Kaughoolduse eeskirja puudumisel ei saa käidutehnoloogia haldur kaugjuurdepääsude kasutamist adekvaatselt kontrollida. Turvaintsidendi toimumisel on intsidendi põhjuste ja süüdlaste väljaselgitamine raskendatud. Intsidendist põhjustatud tootmisseisakud võivad pikeneda.

2.4 Kontrolli puudumine kaughoolduse toimingute üle

Kaughoolduse läbiviijatel peavad olema hooldatava süsteemi kohta vajalikud eelteadmised. Sageli ei ole väliseid partnereid piisavalt informeeritud konkreetsete käidutehnoloogia süsteemide ohutus- ja turvanõuetest.

Kui käidutehnoloogia talitus ei saa kaughoolduse seansside kulgu ja sisu kontrollida, ei ole võimalik suure riskipotentsiaaliga konfiguratsioonivigu ega hooldustöötaja poolt tehtud eksimusi piisavalt kiiresti märgata ja neile reageerida. Halvemal juhul võib see kaasa tuua tootmisseisakust tingitud rahalisi kaotusi, rikkuda käidutehnoloogia süsteemi komponente või ohustada inimeste elu ja tervist.

Kaughoolduse üle kontrolli puudumine võib viia ärisaladuste lekkeni. Tootmissüsteemi konfigureerimisel tehtud viga võib põhjustada defekte lõpptoodangus ja langetada toodete kvaliteeti. See võib oluliselt kahjustada organisatsiooni mainet.

2.5 Juurdepääs käidutehnoloogia komponendile ebaturvalisest võrgusegmendist

Juurdepääs käidutehnoloogia võrgule tööks või halduseks mittevajalikest võrkudest või võrgusegmentidest ohustab käidutehnoloogia süsteemi turvalisust. Ka organisatsiooni sisevõrgu segmendid ei ole sama usaldusväärsusega. Lõppkasutaja seadmete võrgusegmendis leviv kahjurvara võib sealt levida ka käidutehnoloogia võrku. Käidutehnoloogia komponendid ei pruugi olla kahjurvara vastu olla nii hästi kaitstud kui kahjurvaratõrje tarkvaraga varustatud lõppseadmed.

Juurdepääsu teistest võrgusegmentidest on võimalik kasutada ICS-süsteemi vastu korraldatud sihtründe (ingl *targeted attack*) sooritamiseks.

Võrguülene perioodiline paigahaldus võib olla ohtlik ICS-süsteemidele, kuna puudub teave, kuidas konkreetsed muudatused võivad mõjutada käidutehnoloogia võrgu toimimist.

2.6 Ebaturvalised varuvõimalused kaugjuurdepääsuks

Võimalikele käidutehnoloogia komponentide riketele reageerimiseks peab OT komponentide juurdepääs olema alati võimaldatud. Seetõttu on käidutehnoloogia võrkudes vajalik luua varulahendus juhuks, kui põhiliselt kasutatav tehnoloogiline lahendus ei toimi. Selline alternatiivne kaughooldusjuurdepääs võib olla ründaja poolt haavatav. Näiteks varulahendusena otse käidutehnoloogia võrku paigaldatud GSM-modem võib olla vastuolus organisatsioonis kehtestatud turvapoliitikatega.

2.7 Kaughoolduslahenduste ebaturvaline teostus

Käidutehnoloogia süsteemi komponendid on sageli loodud erinevate tootjate poolt. Detsentraliseeritud süsteemi kaughoolduse läbiviimiseks on vaja mitmeid erinevaid kaughoolduslahendusi. Erinevate tootjate poolt eelistatud ja erinevaid tehnoloogiaid kasutatavad juurdepääsulahendused muudavad käidutehnoloogia talitusel keeruliseks nii kaughoolduse haldamise kui turvalisuse tagamise.

Avalikust võrgust algatatavaid juurdepääsulahendusi saab ründaja käidutehnoloogia võrkudesse tungimiseks ja komponentide manipuleerimiseks hõlpsasti ära kasutada.

Käidutehnoloogia kaughoolduslahendusele tootja poolt pakutavad turvameetmed ei pruugi vastata tegelikule kaitsetarbele ja organisatsioonis kehtestatud turvanõuetele.

2.8 Kaughoolduslahenduse tehnoloogiline mahajäämus ja aegumine

Käidutehnoloogia süsteemide pika elutsükli tõttu on tavaline, et üht süsteemi kasutatakse kümme aastat või kauemgi. Kaughoolduseks kasutatavad juurdepääsusüsteemid ei saa oma vanuse tõttu enam turvauuendeid.

Käidutehnoloogia süsteemidesse integreeritud kaughoolduse võimalused, mida aktiivselt ei kasutata, muutuvad riskiks, mille kohta süsteemi haldajal puudub teadmine.

Juurdepääsusüsteemi teadaolevate turvanõrkuste kasutamine teeb võimalikuks volitamata juurdepääsu käidutehnoloogia süsteemidesse. Tehnoloogia üldise arengu taustal muutub selliste tagauste ära kasutamine ICS-süsteemide ründamiseks üha tõenäolisemaks.

3 Meetmed

3.1 Elutsükkel

Kavandamine

IND.3.2.M1 Käidutehnoloogia komponentide kaughoolduse kavandamine

IND.3.2.M4 Kokkulepped kaughoolduse teostamiseks väljastpoolt organisatsiooni

Evitus

IND.3.2.M5 Hooldusprotseduuride kooskõlastamine IT-talitusega

Käitus

IND.3.2.M2 OT komponentide pääsuõiguste järjepidev dokumenteerimine

IND.3.2.M3 OT kaughoolduse pääsuõiguste kontroll ja erandite haldus

IND.3.2.M6 Kaughoolduslahenduste turve käidutehnoloogia võrgus

IND.3.2.M7 IT-süsteemide lahtisidestus käidutehnoloogia võrgust

IND.3.2.M8 Kaughooldusseansi kontrollitud algatamine

IND.3.2.M9 Turvaline failide edastamine kaughoolduse käigus

IND.3.2.M10 Kaughoolduse seire ja kontroll

IND.3.2.M11 OT kasutajakontode keskhaldus

Lisanduvad kõrgmeetmed

IND.3.2.M12 Käidutehnoloogia kaughoolduse erilahendus

IND.3.2.M13 Kaughoolduse tegevuste laiendatud logimine

IND.3.2.M14 Kaughoolduse seansi tehniline kontroll

3.2 Põhimeetmed

IND.3.2.M1 Käidutehnoloogia komponentide kaughoolduse kavandamine [arhitekt]

a. On kehtestatud organisatsiooniülene kord käidutehnoloogia (ingl *operational technology*, OT) komponentide kaughoolduse tellimiseks ja läbiviimiseks.

b. Käidutehnoloogia kaughoolduse kord arvestab järgmisi aspekte:
   - seadusandlusest tulenevad nõuded, sh isikuandmete kaitse;
   - OT komponentide spetsifikatsioonid ja tootjate soovitused;
   - võrkude eraldatusest tulenevad turvanõuded;
   - nõuded liidestusele ja andmesideühendustele;
   - kaughoolduse käideldavusnõuded;
   - keskkonnatingimustest tulenevad erinõuded;
   - koostoime olemasolevate süsteemidega.

c. Kaughoolduse korda järgivad kõik asjakohased organisatsiooni töötajad ja välised partnerid.

d. Kõik kaughoolduseks kasutatavad tehnilised lahendused on keskselt dokumenteeritud.

e. Lisanduvate OT komponentide puhul lepitakse eelnevalt tarnijaga kokku infoturbe nõuded.

f. Võimalusel kasutatakse kõigi OT komponentide kaughoolduseks standardseid ja ühtseid lahendusi.

IND.3.2.M2 OT komponentide pääsuõiguste järjepidev dokumenteerimine [IT talitus, hooldepersonal]

a. Käidutehnoloogia süsteemide kaughoolduse pääsuõigusi hallatakse järjepidevalt.

b. Kaughoolduse juurdepääsuõigused on dokumenteeritud. Dokumenteerimine on korraldatud analoogiliselt arvutivõrgu IT-süsteemide kaugjuurdepääsude dokumenteerimisega.

c. OT süsteemi integreeritud kaughoolduslahenduse puhul desaktiveeritakse mittevajalikud süsteemikontod. Ka desaktiveeritud juurdepääsud dokumenteeritakse.

IND.3.2.M3 OT kaughoolduse pääsuõiguste kontroll ja erandite haldus [IT-talitus]

a. Käidutehnoloogia komponentide kaughoolduslahenduste ja seotud juurdepääsuõiguste vastavust käidutehnoloogia kaughoolduse korrale (vt IND.3.2.M1 *Käidutehnoloogia komponentide kaughoolduse kavandamine*) kontrollitakse regulaarselt.

b. On kehtestatud protseduurid käidutehnoloogia kaughoolduse korrast erandite heakskiitmiseks ja kinnitamiseks.

IND.3.2.M4 Kokkulepped kaughoolduse teostamiseks väljastpoolt organisatsiooni

a. Kõigi organisatsioonivälise pooltega (OT komponentide tootjad, integraatorid ja hooldusteenuste osutajad) on kokku lepitud kaughoolduse läbiviimise tingimused. Kokkulepped tagavad, et välised kasutajad kasutavad OT-kaughoolduse juurdepääsu ainult kontrollitult ja kooskõlastatult.

b. On määratud, kellel organisatsioonis ja kui suures ulatuses on õigus välistele kasutajatele juurdepääse anda. Täiendavalt on määratud töötajad, kellel on volitused vajadusel seirata ja kontrollida välise hooldepersonali tegevusi.

c. Kaughooldust tehes tagatakse käidutehnoloogia süsteemiga töötavate inimeste turvalisus.

d. Organisatsiooni käidutehnoloogia spetsialist võib OT komponentide kaughooldust teha juhul, kui ta on selleks saanud vastava volituse.

IND.3.2.M5 Hooldusprotseduuride kooskõlastamine IT-talitusega [IT talitus, arhitekt]

a. Käidutehnoloogia talitus on kooskõlastanud IT-talituse ja teiste asjakohaste organisatsioonisiseste üksustega kõik OT komponentide kaughooldusel kasutatavad liidesed, süsteemid ja süsteemide tehnilised parameetrid.

b. On määratud kõik käidutehnoloogia talituse välised rollid, protseduurid ja kohustused, mis on kaughoolduse läbiviimiseks vajalikud (sh kasutuslubade taotlemine).

IND.3.2.M6 Kaughoolduslahenduste turve käidutehnoloogia võrgus [IT-haldus]

a. Kui käidutehnoloogia komponendi kaugjuurdepääs toimub läbi arvutivõrgus oleva seadme või serveri, vastutab käidutehnoloogia talitus vähemalt ühe juurdepääsuks vajaliku turvakomponendi seadistuse ja pääsuõiguste andmise eest.

b. Võimaluse korral kasutatakse käidutehnoloogia komponentide kaughoolduseks standardseid, keskselt hallatud autentimislahendusi.

c. Kui OT komponendi kaughoolduse juurdepääsusüsteem pole organisatsiooni poolt keskselt hallatav, kaitstakse juurdepääse täiendavalt tüüpse (vaikimisi pakutava) kaugjuurdepääsulahenduse koosseisu mittekuuluva turvamehhanismiga.

3.3 Standardmeetmed

IND.3.2.M7 IT-süsteemide lahtisidestus käidutehnoloogia võrgust [arhitekt]

a. Kaugjuurdepääsud mis tahes OT komponendile on käidutehnoloogia võrgust lahti sidustatud (ingl *decoupling*). Enne kaughoolduse sessiooni algatamist ühendatakse kaugjuurdepääsuks kasutatav IT-süsteem lahti teistest võrkudest. Kaughoolduseks luuakse uus sessioon.

b. Kaughooldustööriistad ja rakendused on hooldusarvutise eelnevalt installitud.

c. Kaughoolduse IT-süsteem toetab erinevaid kasutajakontosid.

d. Kaughoolduseks kasutatakse hüppeserverit (ingl *jump server*) või demilitaartsoonis (DMZ) paiknevat rakenduslüüsi (ingl *Application Layer Gateway*, ALG).

e. Võimaluse korral vastutab kaugjuurdepääsu lahtisidumise eest ja haldab vastavat DMZ-d käidutehnoloogia talitus.

IND.3.2.M8 Kaughooldusseansi kontrollitud algatamine [töötaja]

a. Kõik kaughoolduse seansid kooskõlastatakse käidutehnoloogia süsteemi opereeriva organisatsiooni poolt määratud süsteemi omanikuga (ingl *system owner*). Alles pärast seda aktiveerib vastutav käidutehnoloogia talituse spetsialist kaughoolduse juurdepääsu. Kaughooldusseansside eelnev kooskõlastamine süsteemi omanikuga on vajalik nii eelnevalt kokku lepitud hooldusaegade raames tehtava korralise hoolduse kui erakorralise kaughooldusvajaduse puhul.

b. Kaughooldusseanss kestab piiratud aja. Vastutav käidutehnoloogia talituse spetsialistil on otsustusõigus kaughoolduse ajastuse ja kestvuse üle (vt IND.3.2.M3 *OT kaughoolduse pääsuõiguste kontroll ja erandite haldus*).

c. Väline kaughooldusjuurdepääs luuakse vaid seestpoolt väljapoole (algatatakse käidutehnoloogiavõrgust).

d. Kaughoolduseks avatud pordid ei ole juurdepääsetavad ebausaldusväärsetest võrkudest.

IND.3.2.M9 Turvaline failide edastamine kaughoolduse käigus [arhitekt, IT-talitus]

a. Turvaliseks failivahetuseks OT kaughoolduse käigus (nt. konfiguratsioonifailide, süsteemiuuendite või juhendite saatmiseks) on kehtestatud turvameetmeid sisaldavad protseduurid.

b. Failide edastamisel kontrollitakse faile võimaliku kahjurvara avastamiseks.

c. Failide edastamine saab toimuda ainult eelnevalt autenditud kasutajate vahel. Failiedastus ei ole automaatne, vaid vajab algatamiseks eelnevat luba.

d. Failide edastamine logitakse.

IND.3.2.M10 Kaughoolduse seire ja kontroll [töötaja]

a. Käidutehnoloogia süsteemides tehtav kaughooldus ei kahjusta tootmisprotsessi ega riku käidutehnoloogia süsteeme ja seadmeid.

b. Kaughooldus ei ohusta otseselt ega kaudselt inimesi, kes käidutehnoloogia süsteeme kasutavad või viibivad seadmete läheduses.

c. Kui eksisteerib oht võimaliku kehavigastuse või varalise kahju tekitamiseks, valideeritakse kõiki kaughooldustoiminguid nelja silma põhimõttel (ingl *four-eyes principle*).

d. Kohapeal kaughoolduse toiminguid jälgiv käidutehnoloogia talituse spetsialist saab vajadusel kaughoolduse käiku sekkuda või kaughoolduse seansi katkestada.

IND.3.2.M11 OT kasutajakontode keskhaldus [IT-talitus]

a. Käidutehnoloogia komponentide kaughooldus toimub ainult käidutehnoloogia talituse või keskselt hallatavas kataloogiteenuses (ingl *directory service*) registreeritud kasutajakontodelt.

3.4 Kõrgmeetmed

IND.3.2.M12 Käidutehnoloogia kaughoolduse erilahendus [arhitekt] (C-I-A)

a. Kaughoolduseks kasutatakse spetsiaalset OT komponentide kaughoolduslahendust, mis on sõltumatu organisatsiooni arvutivõrgust ja IT-arhitektuurist. Kõik muud võimalused käidutehnoloogia komponentide kaugjuurdepääsuks on desaktiveeritud või blokeeritud.

b. Käidutehnoloogia komponentide kaughoolduseks kasutatakse organisatsiooni arvutivõrgust sõltumatut, eraldiseisvat internetiühendust.

IND.3.2.M13 Kaughoolduse tegevuste laiendatud logimine [arhitekt, andmekaitsespetsialist] (C-I)

a. Käidutehnoloogia süsteemide kaughoolduse tegevused on täielikult ja koheselt jälgitavad.

b. Lisaks sündmustele (ingl *event*) ja seansiandmetele logitakse täiendavalt kaughoolduse toimingute sisu.

IND.3.2.M14 Kaughoolduse seansi tehniline kontroll [arhitekt, andmekaitsespetsialist] (C-I-A)

a. Kõiki käsutasandi tegevusi ehk käsitsi või automaatselt antud käsklusi on võimalik vajadusel tehniliselt takistada.

b. OT kaughoolduse seansside automaatseirelahendus käivitab alarmi mitte ainult konkreetsete tehniliste reeglite rikkumise, vaid ka kasutusmustris toimuvate anomaaliate (nt ootamatult suurenenud andmesidemaht) esinemisel.

NET: VÕRGUD JA SIDE

NET.1: Võrgud

NET.1.1 Võrgu arhitektuur ja lahendus

1 Kirjeldus

1.1 Eesmärk

Esitada võrgu arhitektuuri ja võrgulahenduse infoturbe meetmed.

1.2 Vastutus

Võrgu arhitektuuri ja võrgulahenduse meetmete täitmise eest vastutab arhitekt.

Lisavastutajad

Infoturbejuht, IT-talitus.

1.3 Piirangud

Võrguhaldusega seotud teemasid käsitletakse moodulis NET.1.2 *Võrguhaldus*.

Võrgukomponentide turvalisust käsitletakse moodulirühmas NET.3 *Võrgukomponendid*.

Võrgulahenduste (nt raadiokohtvõrk ja salvestusvõrk) meetmed esitatakse spetsiifilistes moodulites (nt raadiokohtvõrgu turvameetmed mooduligrupis NET.2 *Raadiovõrgud* ja salvestusvõrgu meetmed moodulis SYS.1.8 *Salvestussüsteemid*).

Virtuaalsete privaatpilvede ja hübriidpilvede meetmed on esitatud moodulis OPS.2.2 *Pilvteenuste kasutamine*. Sidevahendite infrastruktuuri meetmeid käsitletakse moodulis NET.4.2 *IP-telefon (VoIP*).

2 Ohud

2.1 Sideühenduse tõrge või puudulik sooritusvõime

Sidekanalite ebapiisav läbilaskevõime või sideühenduse tehniline tõrge võib tugevalt häirida äriprotsesse, kuna on häiritud neid toetavate pilvteenuste kasutamine. Sideühenduse nõrkusi ära kasutav teenusetõkestusrünne (ingl distributed denial-of-service attack, DDoS attack) võib sideühendusest sõltuva teenuse muuta täiesti kättesaamatuks.

Sideühenduse puudulik sooritusvõime raskendab väliste klientarvutite (klientide) pöördumist organisatsiooni sisevõrgu serverite poole. Selle tulemusena halveneb võrguteenuste kättesaadavus klientidele.

2.2 Sisevõrgule juurdepääsu puudulik turve

Kui sisevõrgu ja Interneti vaheline üleminek ei ole piisavalt turvaline (nt kui tulemüür (ingl *firewall*) puudub või on valesti seadistatud), võivad ründajad organisatsiooni tundlikele andmetele juurde pääseda, andmeid varastada või manipuleerida.

2.3 Võrgu asjatundmatu teostus

Võrgu ebaturvalisena kavandatud arhitektuur ja võrgu asjatundmatu laiendamine lihtsustavad ründajal võrgu kohta teavet hankida ja turvanõrkusi tuvastada. Võrgu kaootiline topoloogia

või läbimõtlemata konfiguratsioon teevad võrku tunginud ründaja avastamise keeruliseks. Ründaja võib võrgus nähtamatuks jäädes organisatsiooni võrguliiklust jälgida, andmeid varastada ja manipuleerida.

3 Meetmed

3.1 Elutsükkel

Kavandamine

NET.1.1.M1 Võrgu turvapoliitika

NET.1.1.M3 Võrgu tehniliste nõuete spetsifitseerimine

NET.1.1.M13 Võrgu teostuskava

NET.1.1.M16 Võrgu arhitektuuri dokumenteerimine

NET.1.1.M17 Võrgulahenduse spetsifitseerimine

NET.1.1.M22 Segmentimise eeskiri

NET.1.1.M25 Võrgu arhitektuuri ja võrgulahenduse detailplaneerimine

NET.1.1.M26 Võrgu käitusprotsesside spetsifitseerimine

NET.1.1.M27 Võrgu arhitektuuri arvestamine avariivalmenduses

Evitus

NET.1.1.M2 Võrgulahenduse dokumentatsioon

NET.1.1.M4 Võrgu tsoneerimine

NET.1.1.M10 Demilitaartsoon (DMZ)

NET.1.1.M14 Võrgu kavakohane teostus

NET.1.1.M18 Internetiühenduse P-A-P-struktuuri (paketifilter-rakenduslüüs-paketifilter) kasutamine

NET.1.1.M21 Haldusalade eraldamine

NET.1.1.M23 Turvasegmentide eraldamine

Käitus

NET.1.1.M5 Klientide ja serverite võrgusegmentide eraldamine

NET.1.1.M6 Lõppseadmete segmendid sisevõrgus

NET.1.1.M7 Tundliku teabe turve võrgus

NET.1.1.M8 Internetti pääsu alusturve

NET.1.1.M9 Turvaline andmevahetus ebausaldusväärsete võrkudega

NET.1.1.M11 Siseneva andmeliikluse turve

NET.1.1.M12 Väljuva andmeliikluse turve

NET.1.1.M15 Võrgu vastavuskontroll

NET.1.1.M19 Taristuteenuste eraldamine

NET.1.1.M20 Alamvõrgud IPv4/IPv6 lõppseadmetele

NET.1.1.M24 Võrkude loogiline eraldamine VLAN-iga

Lisanduvad kõrgmeetmed

NET.1.1.M28 Kõrgkäideldavad võrgu- ja turvakomponendid

NET.1.1.M29 Võrguühenduste kõrgkäideldav teostus

NET.1.1.M30 Hajusa ummistusründe tõrje

NET.1.1.M31 Võrgusegmentide füüsiline eraldamine

NET.1.1.M32 Haldusvõrgu segmentide füüsiline eraldamine

NET.1.1.M33 Võrgu alamsegmendid

NET.1.1.M34 Krüpteerimisprotseduuride rakendamine võrgutasemel

NET.1.1.M35 Võrgupõhise lekketõrje rakendamine

NET.1.1.M36 Virtuaalse kohtvõrguga eraldamise keeld väga suure kaitsetarbe korral

3.2 Põhimeetmed

NET.1.1.M1 Võrgu turvapoliitika [IT-talitus, infoturbejuht]

a. Võrgu turvapoliitika on kehtestatud lähtuvalt üldisest infoturvapoliitikast. Võrgu turvapoliitika esitab nõuded ja juhised võrgu turvaliseks kavandamiseks ja teostuseks.
b. Võrgu turvapoliitika määrab:
   - millistel juhtudel tuleb võrk segmentida ja kasutajarühmad ning IT-süsteemid üksteisest loogiliselt ja füüsiliselt eraldada;
   - millised andmesidekanalid ning võrgu- ja rakendusprotokollid on konkreetsetel juhtudel lubatud;
   - kuidas eraldatakse võrguhalduse ja -seire andmeliiklus muust liiklusest;
   - millistel tingimustel ja kuidas andmeliiklus krüpteeritakse;
   - kuidas korraldatakse andmevahetus teiste organisatsioonidega.
c. Võrgu halduse ja turvalisusega tegelevad töötajad tunnevad võrgu turvapoliitikat ja järgivad seda.
d. Võrgu turvapoliitika muudatusettepanekud ja turvapoliitikast lahknevused dokumenteeritakse ning nendest informeeritakse infoturbejuhti.
e. Võrgu turvapoliitika nõuetekohast rakendamist kontrollitakse regulaarselt. Kontrolli tulemused dokumenteeritakse.

NET.1.1.M2 Võrgulahenduse dokumentatsioon [IT-talitus]

a. Võrgulahendus on dokumenteeritud ja sisaldab vähemalt järgmist:
   - võrgu loogilist ülesehitust esitavat võrguskeemi;
   - alamvõrkude, tsoonide ja segmentide kirjeldust;
   - võrgus tehtud muudatusi.
b. Võrgulahenduse dokumentatsiooni (sh võrguskeemi) hoitakse ajakohasena.

NET.1.1.M3 Võrgu tehniliste nõuete spetsifitseerimine

a. Võrgule esitatavad tehnilised nõuded on välja töötatud lähtuvalt võrgu turvapoliitikast (vt NET.1.1.A1 *Võrgu turvapoliitika*).

b. Turvapoliitika või ärivajaduste muutumisel võrgu tehniliste nõuete spetsifikatsiooni ajakohastatakse.

c. Võrgu arhitektuuri ja komponentide valikul ning võrgulahenduse teostusel arvestatakse võrgule esitatavaid tehnilisi nõudeid.

NET.1.1.M4 Võrgu tsoneerimine

a. Võrk on jagatud füüsiliselt eraldatud (eraldi seadmetega teostatud) tsoonideks:
   - sisevõrk;
   - demilitaartsoon (vajadusel, vt NET.1.1.M10 *Demilitaartsoon (DMZ)*);
   - välisühendused Interneti ja ebausaldusväärsete võrkudega.

b. Tsoonidevahelised üleminekud on turvatud tulemüüridega (ingl *firewall*), mis võimaldavad ainult lubatud andmeliiklust.

c. Ebausaldusväärsed võrgud (nt Internet) ja usaldusväärsed võrgud (nt sisevõrk) on eraldatud dünaamilist pakettide filtreerimist ja valgefiltreerimist (ingl *whitelisting*) teostavate tulemüüridega.

d. Kui turvapoliitika või võrgunõuete spetsifikatsioon nõuab tsoneerimisel spetsiaalset tulemüüriarhitektuuri, siis on arhitektuur nii ka realiseeritud.

NET.1.1.M5 Klientide ja serverite võrgusegmentide eraldamine [IT-talitus]

a. Kliendid (serverilt teenuseid saavad funktsionaalüksused) ja serverid asuvad eraldi võrgusegmentides.

b. Andmesidet nende segmentide vahel reguleeritakse dünaamilise paketifiltriga (ingl *dynamic packet filter*). Rakenduse- ja süsteemispetsiifilised erandid, mis lubavad kliente ja servereid paigutada ühisesse võrgusegmenti, on dokumenteeritud.

NET.1.1.M6 Lõppseadmete segmendid sisevõrgus

a. Ühes võrgusegmendis on ainult sarnase turbevajadusega ja -funktsionaalsusega lõppseadmed (ingl *endpoint*).

b. Välise juurdepääsuga võrgusegmendid, milles asuvate lõppseadmete turvameetmed ei ole piisavad, paiknevad eraldi tsoonis.

NET.1.1.M7 Tundliku teabe turve võrgus

a. Tundlike andmete edastamisel kasutatakse ajakohaseid ja turvalisi võrguprotokolle või usaldusväärseid ning turvatud sidekanaleid ((vt NET.3.3 *Virtuaalne privaatvõrk (VPN)*).

NET.1.1.M8 Internetti pääsu alusturve

a. Võrgutsoonid on eraldatud Internetist tulemüüridega.

b. Internetiliiklus on suunatud läbi tulemüüri, mis filtreerib liiklust protokolle ja võrguühendusi piiravate tulemüürireeglite alusel.

NET.1.1.M9 Turvaline andmevahetus ebausaldusväärsete võrkudega

a. Iga võrgu jaoks, millega andmeid vahetatakse, on määratud usaldatavustase.

b. Ebausaldusväärne võrk loetakse usaldustaseme poolest samaväärseks Internetiga.

NET.1.1.M11 Siseneva andmeliikluse turve

a. Pääs välistelt IP-aadressidelt sisevõrku on suunatud läbi turvalise sidekanali ja on lubatud ainult usaldatavatele IT-süsteemidele ja kasutajatele (vt NET.3.3 *Virtuaalne privaatvõrk (VPN)*).

b. Siseneva liikluse VPN-lüüsid asuvad eraldi aadressiruumis (soovitavalt välises demilitaartsoonis (ingl *demilitarized zone*, DMZ)).

c. VPN-lüüsi kaudu autenditud pöördumine sisevõrku käib läbi sisemise tulemüüri.

d. Välised IT-süsteemid ei saa juurdepääsu sisevõrgule otse Internetist ega välisest demilitaartsoonist.

NET.1.1.M12 Väljuva andmeliikluse turve

a. Sisevõrgust Internetti suunatud andmeside on suunatud läbi väljaspool sisevõrku asuva turvaproksi või vastavat võimekust omava keskse tulemüüri.

b. P-A-P-struktuuri (paketifilter-rakenduslüüs-paketifilter) kasutamise korral on väljaminev andmeside suunatud läbi P-A-P turvaprokside.

NET.1.1.M13 Võrgu teostuskava

a. On koostatud võrgu teostuskava, mis põhineb võrgu turvapoliitikal ja nõuete spetsifikatsioonil.

b. Võrgu teostuskavas on arvestatud vähemalt järgmist:
   - ühendus Internetiga ja usaldatud partnerivõrkudega;
   - võrgu, võrgutsoonide ja -segmentide topoloogia;
   - võrgu- ja turvakomponentide dimensioneerimine ja dubleerimine, edastusteed ja välisühendused;
   - kasutatavad protokollid ning nende põhikonfiguratsioon (eelkõige lõppseadmete IPv4/IPv6 alamvõrkude puhul);
   - haldus ja seire (vt NET.1.2 *Võrguhaldus*).

NET.1.1.M14 Võrgu kavakohane teostus

a. Võrk on rajatud asjatundlikult ning teostuskava kohaselt.

b. Võrgu vastuvõtmisel kontrollitakse selle vastavust teostuskavale.

NET.1.1.M15 Võrgu vastavuskontroll [infoturbejuht]

a. Võrgu vastavust turvapoliitikale ja võrgunõuete spetsifikatsioonile kontrollitakse regulaarselt.

b. On määratud vastavuskontrolli teostajad ja kriteeriumid, millest kontrollimisel lähtuda.

3.3 Standardmeetmed

NET.1.1.M10 Demilitaartsoon (DMZ)

a. Organisatsioon on loonud füüsilise ja/või loogilise alamvõrgu, mis eraldab usaldatava võrgu ebausaldatavast ja milles asuvad proksid serverite mõlemapoolse kättesaadavuse võimaldamiseks (demilitaartsoon (ingl *demilitarized zone*, DMZ)).

b. Organisatsioon on kehtestanud demilitaartsoonide kasutamise korra vastavalt IT-süsteemide ja andmete kaitsetarbele.

c. Internetist juurdepääsetavad teenused ja rakendused paiknevad demilitaartsoonis ja on kaitstud demilitaartsooni tulemüüriga (ingl *firewall*).
d. Demilitaartsooni segmente võib sõltuvalt IT-süsteemide kaitsetarbest olla rohkem kui üks.

NET.1.1.M16 Võrgu arhitektuuri dokumenteerimine

a. Arhitektuuri dokumentatsioonis on esitatud kõik olulised võrgu arhitektuuri komponendid, sealhulgas:
   - sisevõrgu arhitektuur sh virtualiseerimislahendus;
   - sisevõrgu liiasusega komponendid;
   - väliste liidestuste, sh tulemüüri ja demilitaartsooni arhitektuur;
   - laivõrgu ja raadiovõrgu komponendid;
   - turvaseadmete (tulemüürid, sissetungituvastuse ja sissetungitõrje süsteemid) asukohad ja turvafunktsioonid;
   - spetsiifiliste IT-süsteemide võrguühenduste nõuded;
   - virtualiseeritud hostide arhitektuur, sh NVO (*Network Virtualization Overlay*);
   - ühendused privaatpilvega;
   - ühendused pilvteenustega (vt OPS.2.2 *Pilvteenuste kasutamine* ja OPS.3.1 *Teenuseandja infoturve*);
   - IT-taristu halduse ja seire jaoks kasutatavate komponentide arhitektuur.
b. Arhitektuuri dokumentatsiooni ajakohastatakse regulaarselt.

NET.1.1.M17 Võrgulahenduse spetsifitseerimine

a. Võrgu arhitektuuri alusel on koostatud võrgu tehnilise lahenduse kava, milles on esitatud arhitektuuri elementide üksikasjad:
   - tsoneerimise kava;
   - *Network Virtualization Overlay* komponendid, sh virtualiseeritud võrgukomponendid;
   - laivõrgu ja raadiovõrgu turve;
   - lõppseadmete (ingl *endpoint*) ühendused võrguseadmetega, võrguelementide ühendused, sideprotokollid;
   - kõigi võrguelementide liiasusmehhanismid;
   - IPv4- ja IPv6-adresseerimise, kommuteerimise ja marsruutimise põhimõtted;
   - virtualiseeritud hostide turve;
   - privaatpilve komponentide turve;
   - IT-taristu turvalise halduse ja seire realisatsiooni määrangud.

NET.1.1.M18 Internetiühenduse P-A-P-struktuuri (paketifilter-rakenduslüüs-paketifilter) kasutamine

a. On kasutusel kahetasemeline tulemüürisüsteem. Tulemüüride vahel on proksipõhine rakenduslüüs (ingl *application level gateway*) või turvaproksid, mis on liiasusega siirdevõrguga ühendatud välise ja sisemise tulemüüriga.

b. Siirdevõrgus ei ole muid seadmeid peale proksipõhiste rakenduslüüside ja vastavate turvaprokside. Mistahes andmeliiklus on rakenduslüüsi või turvaproksiga välisvõrgust lahti sidestatud.
c. Otseühendus läbi rakenduskihi tulemüüri (konfigureerida transmissioonivõrku) on blokeeritud. Sisemine tulemüür on konfigureeritud vähendama rakenduslüüside ja turvaprokside siseründeid.
d. VPN-lüüsist sisevõrku suunatud autenditud ja usaldusväärsed võrkupääsud ei läbi rakenduslüüsi ega P-A-P-struktuuri turvaproksisid.

NET.1.1.M19 Taristuteenuste eraldamine

a. IT-taristule baasteenuseid andvad serverid asuvad eraldatud võrgusegmendis.
b. IT-taristu teenuse serverite andmeside on kaitstud dünaamilise paketifiltriga.

NET.1.1.M20 Alamvõrgud IPv4/IPv6 lõppseadmetele

a. Lõppseadmed (ingl *endpoint*) on jagatud alamvõrkudesse vastavalt sellele, kas seadmed kasutavad IPv4, IPv6 või mõlemat protokolli.

NET.1.1.M21 Haldusvõrkude eraldamine

a. Võrgutaristu halduseks kasutatakse üldisest andmesidest eraldatud sidekanalit (ingl *out-of-band management*).
b. Võrgutaristu halduseks kasutatavad haldustööjaamad on paigutatud eraldi võrgusegmenti.
c. Haldustööjaamade ja haldusalade vaheline side on kaitstud dünaamilise paketifiltriga.
d. Haldusvõrgu segmentidest väljuvat ja nendesse sisenevat andmeliiklust on võrguhaldusmeetmetega kitsendatud ainult vajalike sihtkohtadeni.
e. Haldusvõrgud hõlmavad vähemalt järgmisi võrgusegmente:
    - õigustega ja haldusside autentimisega tegelevate IT-süsteemide segment;
    - IT-süsteemide haldus;
    - võrguseire;
    - keskne logimine;
    - haldusvõrgu põhiteenuste IT-süsteemid;
    - hallatavad IT-süsteemid.
    - IT-süsteemide haldusliidesed on kaitstud dünaamilise paketifiltriga.
    - IT-süsteemide haldusliidesed on kaitstud tulemüüridega kui IT-süsteemid:
    - on Internetist juurdepääsetavad;
    - on mõeldud üksnes sisevõrgus kasutamiseks;
    - on ise turvakomponendiks Internetist juurdepääsetavate IT-süsteemide ja sisevõrgu vahel.
f. IT-süsteemi haldusliidese kaudu ei saa võrku segmentida ega teha segmentide sildamist (ingl *bridging*).

NET.1.1.M22 Segmentimise eeskiri

a. Enne segmentimist on koostatud võrgu segmentimise eeskiri, mis arvestab kavandatavaid arhitektuuri- ja võrgulahendusi (sh ka virtualiseeritud võrke).

b. Segmentimise eeskirjas on kirjeldatud vähemalt järgnev:
   - kavandatavad võrgusegmendid, uute võrgusegmentide loomine ja lõppseadmete võrgusegmentidesse paigutamine;
   - arendus- ja testimiskeskkondade segmendid;
   - klientarvutite võrgusegmendist võrkupääsu reguleerimine;
   - raadioühendused ja spetsialiseeritud sidekanalid;
   - virtualiseerimishostid ja virtuaalmasinad;
   - mitut võrgusegmenti teenindavate seadmete (nt koormusejaotur) integreerimine;
   - võrgusegmentide vaheliste sidestuskomponentide (nt dünaamilise paketifiltriga tulemüür) turvafunktsioonid.
   - segmentide võrgutehniline teostus.

NET.1.1.M23 Võrgusegmentide eraldamine

a. Erineva kaitsetarbega IT-süsteemid asuvad erineva turvatasemega võrgusegmentides.
b. IT-süsteemide ühte võrgusegmenti paigutamisel määrab turbe suurima kaitsetarbega IT-süsteem.
c. Segmendid on jaotatud alamsegmentideks lähtuvalt segmentimise eeskirjas määratud parameetritest.
d. Võrgusegmente ega -tsoone ei saa sillata.
e. Kui kommutaatoriga (ingl *switch*) seotud virtuaalsed kohtvõrgud (ingl *virtual LAN,* VLAN) kuuluvad eri organisatsioonidele, on need täielikult lahutatud või on kogu võrguliiklus andmetele lubamatu juurdepääsu kaitseks krüpteeritud.

NET.1.1.M24 Võrkude loogiline eraldamine VLAN-iga

a. Virtuaalse kohtvõrgu kaudu ei saa luua ühendusi rakenduslüüsi (ingl *application level gateway*) ees või P-A-P-turvaprokside ees oleva tsooni ja selle taga oleva sisemise võrgu vahel.
b. Virtuaalsest kohtvõrgust pole võrgutsoonide sildamine lubatud.
c. Kõik VLAN-ide vahelised ühendused on suunatud läbi tulemüüri.

NET.1.1.M25 Võrgu arhitektuuri ja võrgulahenduse detailplaneerimine

a. Võrgu arhitektuuri ja võrgulahenduse jaoks on koostatud detailne teostusplaan.

NET.1.1.M26 Võrgu käitusjuhend [IT-talitus]

a. Võrgu haldusprotseduurid on dokumenteeritud võrgu käitusjuhendis.
b. Võrgu käitusjuhend arvestab IT-halduse korraldamisel võrgusegmentide ja tsoonide võimalikke erisusi.

NET.1.1.M27 Võrgu arhitektuuri arvestamine avariivalmenduses [IT-talitus]

a. Võrgu kavandamisel või enne olulisi arhitektuurimuudatusi analüüsitakse võrgu arhitektuuri mõju IT-süsteemide avariivalmendusele.

3.4 Kõrgmeetmed

NET.1.1.M28 Kõrgkäideldavad võrgu- ja turvakomponendid (A)

a. Sisevõrgu olulised võrgu- ja turvakomponendid on avarii-ümberlülituse (ingl *failover*) võimekusega ning teostatud liiasusega (ingl *redundancy*).

NET.1.1.M29 Võrguühenduste kõrgkäideldav teostus (A)

a. Võrguühendused (kaasa arvatud internetiühendus) on kavandatud liiasusega (ingl *redundancy*).

b. Teenuseandja andmeühenduste liiasuse rakendamisel on lähtutud vajadustest ja võrgutehnoloogiast, mis tagab andmeühenduste sarnase sooritusvõime.

c. Võrguühenduste kavandamisel on arvestatud võimalikke ohtusid ja ebasoodsaid keskkonnatingimusi.

d. Kahe sõltumatu ISP (ingl *Internet service provider*, ISP) kasutamisel jälgitakse, et mõlemad ühendused ei kasutaks sama füüsilist edastusmeediumi.

NET.1.1.M30 Hajusa ummistusründe tõrje (A)

a. Hajusate ummistusrünnete (ingl *distributed denial-of-service attack*, *DDoS attack)* mõju vähendamiseks on võrgu ribalaiused jaotatud eri tarbijate ja protokollide vahel.

b. Suuremahuliste teenusetõkestusrünnete leevendamiseks on Interneti tarnijalt (*ingl Internet service provider*, ISP) lepinguga tellitud ummistusründe tõrje teenus.

NET.1.1.M31 Võrgusegmentide füüsiline eraldamine (C-I-A)

a. Erineva turvatasemega võrgusegmendid on kommutaatoritega (ingl *switch*) ja/või ruuteritega (ingl *router*) üksteisest füüsiliselt eraldatud, üksnes loogiline eraldamine pole lubatud.

NET.1.1.M32 Haldusvõrgu segmentide füüsiline eraldamine (C-I-A)

a. Haldusvõrgu segmendid on põhivõrgust kommutaatoritega ja/või ruuteritega füüsiliselt eraldatud, üksnes loogiline eraldamine pole lubatud.

NET.1.1.M33 Võrgu alamsegmendid (C-I-A)

a. Lõppseadmete (ingl *endpoint*) ründamise tõkestamiseks on võrk jaotatud väikesteks, sarnase nõuete profiili ja sarnase turbega alamsegmentideks.

NET.1.1.M34 Võrgupõhised krüptograafilised vahendid (C-I)

a. Sisevõrgus, partnerivõrgus ja demilitaartsoonis on turvasegmendid loodud võrgutaseme krüptograafiliste vahenditega, näiteks VPN-tehnoloogiaga või turvastandardile IEEE 802.1AE vastava tehnoloogiaga.

b. Kui andmeid sisevõrgus, partnerivõrgus või demilitaartsoonis vahetatakse ebaturvalise sidekanali kaudu, siis krüpteeritakse kogu andmeside.

NET.1.1.M35 Võrgupõhise lekketõrje rakendamine [infoturbejuht] (C-I)

a. Andmelekke riski vähendamiseks on kasutusel võrgu tasemel lekketõrje (ingl *data leakage prevention*, DLP) süsteemid.

NET.1.1.M36 Virtuaalse kohtvõrguga eraldamise keeld väga suure kaitsetarbe korral (C-I-A)

a. Väga suure kaitsetarbega võrgusegmendi puhul pole seal võrgusegmendis virtuaalse kohtvõrgu (VLAN) kasutamine lubatud.

4 Lisateave

Lühend	Publikatsioon
[ISO27033]	EVS-ISO/IEC 27033-3:2013 “Infotehnoloogia. Turbemeetodid. Võrguturve. Osa 3: Tüüpsed võrgustsenaariumid. Riskid, kavandamismeetodid ja reguleerimisküsimused”

NET 1.2 Võrguhaldus

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed turvalise võrguhalduse rajamiseks ja käigus hoidmiseks ning turvalise andmeside tagamiseks.

1.2 Vastutus

Võrguhalduse meetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Arhitekt, ülemus.

1.3 Piirangud

Moodul esitab võrguhalduse turbe üldmeetmed. Võrgukomponentide turbe meetmed esitatakse detailsemalt mooduligruppides NET.2 Raadiovõrgud ja NET.3. Võrgukomponendid. Võrgutaristu haldust käsitletakse moodulikihis INF. Pääsuõiguste andmist käsitleb moodul ORP.4 Identiteedi ja õiguste haldus. Võrgusündmuste (sh haldustegevuste) logimist ja arhiveerimist käsitletakse moodulites OPS.1.1.5 Logimine ja CON.3 Andmevarunduse kontseptsioon.

2 Ohud

2.1 Lubamatu juurdepääs kesksetele võrguhalduskomponentidele

Kui ründaja saab võrgu puuduliku segmentimise või paikamata turvanõrkuste tõttu juurdepääsu võrguhalduse süsteemile, saab ta volitamata ümberseadistamise kaudu (nt võrguliiklust ümber suunates) võrgu toimimist häirida.

2.2 Lubamatu juurdepääs võrgukomponentidele

Kui ründajal õnnestub võrgu kaudu juurde pääseda võrgukomponendile, saab ta seda komponenti kontrollida ja manipuleerida. Ründajal on võimalik häirida konkreetset

komponenti läbivat andmeliiklust. Lisaks saab ründaja niimoodi ette valmistada edasisi ründeid.

2.3 Lubamatu sekkumine võrguhalduse sidesse

Võrguhalduse andmeside pealtkuulamise ja manipuleerimise teel on võimalik võrgukomponentide konfiguratsiooni muuta ja niimoodi neid kontrollida. See võib kahjustada võrgu käideldavust. Peale selle võib ründaja vaadata ja salvestada edastatavaid andmeid.

2.4 Võrgukomponentide süsteemiaja puudulik sünkroniseerimine

Võrgukomponentide süsteemiaja puuduliku sünkroniseerimise korral ei pruugi logiandmed omavahel korreleeruda või võivad kaasa tuua ekslikke sündmuseteateid, kuna eri sündmuste ajatemplitel puudub ühtne alus. Seetõttu on raske aset leidvatele sündmustele kiiresti reageerida ja probleeme õigeaegselt kõrvaldada. Turvaintsidendid, näiteks andmelekked, võivad jääda märkamata.

3 Meetmed

3.1 Elutsükkel

Kavandamine

NET.1.2.M1 Võrguhalduse kavandamine

NET.1.2.M2 Võrguhalduse nõuete spetsifitseerimine

NET.1.2.M11 Võrguhalduse juhend

NET.1.2.M13 Võrguhalduse kontseptsioon

NET.1.2.M14 Võrguhalduse rakendusplaan

NET.1.2.M15 Võrguhalduse taristu turvalise käituse kontseptsioon

NET.1.2.M16 Võrguhalduslahenduste turvaline konfigureerimine

NET.1.2.M27 Võrguhalduse avariivalmendus

Evitus

NET.1.2.M9 Võrguhalduse side turve

NET.1.2.M12 Võrguhalduse dokumenteerimine

NET.1.2.M18 Võrguhalduse koolitus

NET.1.2.M21 Võrguhalduse side lahusus

NET.1.2.M22 Haldusfunktsioonide piiramine

NET.1.2.M28 Haldusklientide paigutus ainukanaliga halduse puhul

NET.1.2.M29 Virtuaalsed kohtvõrgud (VLAN) haldustsoonis

Käitus

NET.1.2.M7 Sündmuste logimine

NET.1.2.M8 Kellaaja sünkroniseerimine

NET.1.2.M10 SNMP-side piiramine

NET.1.2.M17 Regulaarne võrguhalduse ülevaatus

NET.1.2.M24 Võrgukomponentide keskne konfiguratsioonihaldus

NET.1.2.M25 Võrgukomponentide seire

NET.1.2.M26 Sündmuste teavitus, alarmeerimine ja logimine

Avariivalmendus

NET.1.2.M6 Regulaarne andmevarundus

Lisanduvad kõrgmeetmed

NET.1.2.M30 Halduslahenduse kõrgkäideldav teostus

NET.1.2.M31 Üksnes turvaliste protokollide kasutamine

NET.1.2.M32 Haldusvõrgu füüsiline eraldamine

NET.1.2.M33 Haldussegmendi füüsiline eraldamine

NET.1.2.M35 Asitõendite turve

NET.1.2.M36 Võrguhalduse logimise liidestamine turvateabe ja -sündmuste halduse (SIEM) lahendusega

NET.1.2.M37 Kõiki asukohti hõlmav aja sünkroniseerimine

NET.1.2.M38 Avariitöökorralduse kehtestamine võrguhaldustaristu jaoks

3.2 Põhimeetmed

NET.1.2.M1 Võrguhalduse kavandamine

a. Võrguhalduse kavandamisel on lähtutud infoturvapoliitikast, nõuete spetsifikatsioonist (vt NET.1.2.M2 *Võrguhalduse nõuete spetsifitseerimine),* võrguhalduse tööülesannetest ja tööülesannete täitmiseks vajalikest pääsuõigustest.

b. Võrguhalduse kavandamisel on käsitletud vähemalt järgmist:
   - võrguhalduseks eraldatavad võrgualad;
   - juurdepääs haldusserverile;
   - halduse andmeside;
   - andmeside protokollid (nt IPv4 ja IPv6);
   - liidesed sündmuse- ja alarmiteadete edastuseks;
   - logimine, sh keskse logimislahenduse liidesed;
   - aruandlus ja selle liidestus.

NET.1.2.M2 Võrguhalduse nõuete spetsifitseerimine

a. Võrguhalduse kavandamise käigus on dokumenteeritud võrguhalduse taristule ja protsessidele kehtestatud nõuded.

b. Võrguhalduse nõuded sisaldavad nõudeid haldusvahenditele, olulistele võrgukomponentidele ja võrguhalduse protsessi etappidele.

NET.1.2.M6 Regulaarne andmevarundus

a. Võrguhalduslahendustes varundatakse regulaarselt järgmised andmed:
   - hallatavate objektide süsteemiandmed;
   - sündmuse- ja võrguteated;

- logid;
- keskse võrguhalduslahenduse seadistused.

NET.1.2.M7 Sündmuste logimine

a. Võrguhalduslahenduses logitakse vähemalt järgmisi sündmusi:
   - volitamata või ebaõnnestunud pääsukatsed;
   - konfiguratsioonimuudatused;
   - võrgu sooritusvõime ja käideldavuse kõikuvus;
   - automaatprotsesside veateated (nt konfiguratsiooni levitamise korral);
   - võrgukomponentide kättesaadavushäired.

NET.1.2.M8 Kellaaja sünkroniseerimine

a. Kõigis võrguhalduse komponentides ja nendega seotud võrgukomponentides on kellaaeg sünkroniseeritud ning kasutatakse sama ajavööndit.
b. Kohtvõrgu kõigis kohtades sünkroniseeritakse kellaega NTP-teenusega.
c. Eraldi haldusvõrgu korral on soovitatav haldusvõrku paigutada eraldi NTP-server.

NET.1.2.M9 Võrguhalduse side turve

a. Kui võrguhalduse andmesideks kasutatakse põhivõrgu taristut, toimub andmevahetus ainult turvalisi protokolle kasutades.
b. Spetsiaalse haldusvõrguga lahendatud andmeside korral järgitakse meetmeid moodulist NET.1.1 *Võrgu arhitektuur ja lahendus.*

NET.1.2.M10 SNMP-side piiramine

a. Võrguhalduseks kasutatakse SNMP (*Simple Network Management Protocol*) turvalisi versioone (2020 a. SNMPv3).
b. Ebaturvaliste, VPN-i või TLS-iga kaitsmata SNMP versioonide puhul kasutatakse eraldatud haldusvõrku.
c. Juurdepääs SNMP protokolli andmestikule on lubatud ainult vajalikele haldusserveritele.
d. Kui SNMP protokolli võrguhalduseks ei kasutata, on SNMP blokeeritud.

NET.1.2.M11 Võrguhalduse juhend

a. Võrguhalduseks on koostatud kirjalik juhend, vajadusel juhendit ajakohastatakse.
b. Võrguhalduse juhendis on määratud:
   - kasutatavad võrguteenused ja võrguhaldusvahendid;
   - võrguhaldustegevused (kaasaarvatud kõik keskselt tehtavad ja automatiseeritud toimingud);
   - logimise, andmeside ja pääsu reguleerimise turbe meetmed.
c. Võrguhaldusega seotud töötajad järgivad võrguhalduse juhendit. Juhendi järgimist kontrollitakse regulaarselt.

3.3 Standardmeetmed

NET.1.2.M12 Võrguhalduse dokumenteerimine

a. Võrguhalduse dokumentatsioonis on kirjeldatud:
   - hallatavad võrgukomponendid;
   - võrguhaldusvahendid, terminalid ja töökohad;
   - võrguhaldusega seotud andmebaasid ja haldusandmed;
   - liidesed väliste rakenduste ja teenustega.

b. Võrguhalduse dokumentatsioon on vastavuses võrgutaristu dokumentatsiooniga (vt NET.1.1 *Võrgu arhitektuur ja lahendus*).

c. Võrguhalduse taristu arhitektuuri dokumentatsioon on täielik ja ajakohane.

NET.1.2.M13 Võrguhalduse kontseptsioon

a. On välja töötatud võrguhalduse kontseptsioon, mis lisaks võrguhalduse juhendis kirjeldatule (vt NET.1.2.M11 *Võrguhalduse juhend*) määrab:
   - võrguhalduse meetodid ja tehnoloogiad;
   - juurdepääsu ja andmeside turbe;
   - võrgu segmentimise;
   - võrguhalduse komponentide paigutuse turvatsoonides;
   - võrgukomponentide seire ja tegevuste logimise;
   - alarmeerimise korralduse;
   - võrguhalduse automatiseerimise;
   - tõrgetest ja turvaintsidentidest teatamise korralduse;
   - võrguhalduse avariivalmenduse.

NET.1.2.M14 Võrguhalduse rakendusplaan

a. Võrguhalduse kontseptsiooni ja võrguhalduse juhendi alusel on koostatud üksikasjalik võrguhalduse rakendusplaan.

NET.1.2.M15 Võrguhalduse taristu turvalise kasutamise kord

a. Võrguhalduse taristu turvalise kasutamise kord on välja töötatud lähtuvalt võrgu turvapoliitikast, võrguhalduse juhendist ja võrguhalduse kontseptsioonist.

NET.1.2.M16 Võrguhalduslahenduste turvaline konfigureerimine

a. Võrguhalduslahenduste seadistamisel lähtutakse kehtestatud nõuetest (vt NET.1.2.M2 *Võrguhalduse nõuete spetsifitseerimine*) ning võrguhalduse kontseptsioonist (vt NET.1.2.M13 *Võrguhalduse kontseptsioon*).

b. Võrguhalduslahenduse konfiguratsioon ja kasutuselevõtt on turvalised.

NET.1.2.M17 Regulaarne võrguhalduse ülevaatus

a. Võrguhaldusele esitatud nõuetele vastavust kontrollitakse regulaarselt.

b. Ülevaatuse käigus kontrollitakse võrguhalduse dokumentatsiooni ajakohasust, vastavust hetkeseisule ning tegelikele protseduuridele.

c. Ülevaatuse käigus hinnatakse, kas olemasolev võrguhalduse taristu on turvaline ja jätkusuutlik.

NET.1.2.M18 Võrguhalduse koolitus [ülemus]

a. Võrguhalduse koolitusprogramm sisaldab konfiguratsiooni haldust (ingl *configuration management*) ja suutvuse haldust (ingl *capacity management*) ning arvestab konkreetse võrguhalduslahenduse iseärasusi.

b. Võrguhalduse koolitusprogramm sisaldab käitumisjuhiseid tüüpiliste tõrgete ning turvaintsidentidega toimetulekuks.

c. Koolitusi ja väljaõpet tehakse regulaarselt. Koolitust korratakse pärast võrguhalduslahendustes oluliste tehniliste või korralduslike muudatuste tegemist.

NET.1.2.M21 Võrguhalduse side lahusus

a. Võimalusel välditakse halduspääsu andmist võrgukomponentidele välisest võrgust.

b. Kui juurdepääs võrgukomponentidele välisest võrgust ning ilma keskse haldusvahendita on vajalik, kasutatakse selleks eraldi andmesidekanalit.

c. Vastavad hüppeserverid (ingl *jump server*) on osa haldusvõrgust ning need on paigutatud eraldi pääsusegmenti.

NET.1.2.M22 Haldusfunktsioonide piiramine

a. Aktiveeritud on üksnes vajalikud haldusfunktsioonid, muud funktsioonid on blokeeritud.

NET.1.2.M24 Võrgukomponentide keskne konfiguratsioonihaldus

a. Haldusvõrgu võrgukomponentide tarkvara, püsivara (ingl *firmware*) ning konfiguratsiooniandmeid jagatakse ja paigaldatakse keskselt, automatiseeritult ning ilma märgatavat katkestust tekitamata.

b. Konfiguratsioonid on turvaliselt hoitud ning volitatud töötajatele vajadusel kättesaadavad.

c. Konfiguratsioonihaldus on kooskõlas versioonihalduse ja varunduse protsessidega.

d. Keskse konfiguratsioonihalduse toimimist kontrollitakse regulaarselt.

NET.1.2.M25 Võrgukomponentide seire

a. Oluliste võrgukomponentide käideldavus- ja sooritusparameetreid seiratakse regulaarselt.

b. Seire tulemuste hindamiseks on eelnevalt määratletud käideldavus- ja sooritusparameetrite läviväärtused (ingl *network baselining*).

NET.1.2.M26 Sündmuste teavitus, alarmeerimine ja logimine

a. Võrgukomponentide ja võrguhaldusvahenditega seotud olulised sündmused logitakse kesksesse haldussüsteemi.

b. Võrgukomponentide ja võrguhaldusvahenditega seotud olulistest sündmustest teavitatakse automaatselt kohe pärast sündmuse toimumist vastutavat IT-personali.

c. Logitakse vähemalt järgmist:

- võrgu- ja halduskomponentide tõrge või käideldavusrike;
- riistvara väärtalitus;
- ebaõnnestunud sisselogimiskatsed;
- IT-süsteemide piirilähedane koormus või ülekoormus.

NET.1.2.M27 Võrguhalduse avariivalmendus

a. Võrguhalduse avariivalmendus on osa organisatsiooni üldisest avariivalmenduse kontseptsioonist.

b. Võrguhaldusvahendite ja võrgukomponentide konfiguratsioonid on varundatud ja nende taaste on lisatud taasteplaanidesse.

NET.1.2.M28 Haldustööjaamade turvaline paigutus ainukanaliga halduse puhul

a. IT-süsteemide haldamiseks ainukanaliga (ingl *in-band*) haldusvõrgus on kasutusel spetsialiseeritud haldustööjaamad.

b. Kui organisatsioon kasutab nii Internetist juurdepääsetavaid kui sisevõrgu IT-süsteeme, on nende halduseks kohandatud eraldi haldustööjaamad.

NET.1.2.M29 Virtuaalsed kohtvõrgud (VLAN) haldustsoonis

a. Kui kasutatakse virtuaalseid haldusvõrke, asuvad väline paketifilter ja sellega ühendatud seadmed eraldiseisvas võrgusegmendis.

b. Kogu liiklus läbib rakenduslüüsi (ingl *application level gateway*).

3.4 Kõrgmeetmed

NET.1.2.M30 Halduslahenduse kõrgkäideldavus (A)

a. Kesksed halduslahendused ja neid toetavad võrgukomponendid on teostatud kõrgkäideldavalt.

b. On tagatud oluliste halduslahenduse komponentide liiasus (ingl *redundancy)*, näiteks komponentide dubleerimise kaudu.

NET.1.2.M31 Turvalised protokollid (C-I-A)

a. Kasutatakse üksnes turvalisi võrguhaldusprotokolle.

b. Võrguhaldusprotokollide kõik turvafunktsioonid on kasutusel.

NET.1.2.M32 Haldusvõrgu füüsiline eraldamine [arhitekt] (C-I-A)

a. Haldusvõrk on muust sisevõrgust võrguseadmetega füüsiliselt eraldatud.

NET.1.2.M33 Haldussegmendi füüsiline eraldamine [arhitekt] (C-I-A)

a. Haldusvõrk on jaotatud eraldi võrguseadmetega haldussegmentideks.

b. Kohtvõrgu komponente, turvakomponente ja välisühenduste komponente hallatakse erinevatest, võrguseadmetega füüsiliselt eraldatud haldussegmentidest.

NET.1.2.M35 Asitõendite turve (C-I-A)

a. IT-kriminalistika (ingl *computer forensics*) vajadustest lähtuvalt on kehtestatud kord võrguhaldust käsitlevate asitõendite õigusnormi kohaseks ning muutmiskindlaks arhiveerimiseks (vt DER.2.2 *IT-kriminalistika võimaldamine*).

NET.1.2.M36 Võrguhalduse logimise liidestamine turvateabe ja -sündmuste halduse (SIEM) lahendusega (C-I-A)

a. Võrguhalduse logimine on ühendatud turvateabe ja -sündmuste halduse (ingl *security information and event management*, SIEM) lahendusega.

b. Nõudeid võrguhalduslahendusele (vt NET1.2.M2 *Võrguhalduse nõuete spetsifitseerimine*) on täiendatud SIEM lahenduste liideste ja edastusviisidega.

NET.1.2.M37 Kõiki asukohti hõlmav aja sünkroniseerimine (C-I)

a. Organisatsiooni kõigis asukohtades on seadme aja sünkroonsus tagatud ühise alusaja (nt kõrgema taseme NTP-serveri) järgi.

NET.1.2.M38 Võrguhalduse taristu asenduslahendused (A)

a. Võrgukomponentide tarkvara ja püsivara (ingl *firmware*) paigaldamiseks ja konfiguratsiooni taastamiseks on olemas tõhusad alternatiivlahendused.

4 Lisateave

Lühend	Publikatsioon
[ISO27033]	EVS-ISO/IEC 27033-3:2013 “Infotehnoloogia. Turbemeetodid. Võrguturve. Osa 3: Tüüpsed võrgustsenaariumid. Riskid, kavandamismeetodid ja reguleerimisküsimused”

a.

b.

NET.2: Raadiovõrgud

NET.2.1 Raadiokohtvõrgu käitamine

1 Kirjeldus

1.1 Eesmärk

Esitada juhised raadiokohtvõrgu ((ingl *wireless local area network*, WLAN) rajamiseks ja turvaliseks käituseks.

1.2 Vastutus

Raadiokohtvõrgu käitamise meetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Arhitekt, tehnikatalitus.

1.3 Piirangud

Raadiokohtvõrkude turvalist kasutamist käsitletakse moodulis NET.2.2 *Raadiokohtvõrgu kasutamine*. Raadiokohtvõrgu autentimisteenuste (nt RADIUS) kasutamisel rakendatakse lisaks meetmeid moodulitest *NET.1.1 Võrgu arhitektuur ja lahendus* ning SYS.1.1 *Server üldiselt*. Raadiokohtvõrgu intsidentide halduseks rakendatakse meetmeid moodulist DER.2.1 *Turvaintsidentide käsitlus*.

2 Ohud

2.1 Raadiokohtvõrgu ühenduse tõrge või häiring

Raadiokohtvõrgu (ingl *wireless local area network*, WLAN) sidet võivad häirida ka teised sama sagedusvahemiku elektromagnetilise kiirguse allikad (muud raadiovõrguseadmed, Bluetooth-seadmed, mikrolaineahjud, teised raadiokohtvõrgud). Ummistusründe tegemiseks on võimalik edastada samas sagedusalas signaale, mis häirivad raadiokohtvõrkude kasutamist.

2.2 Raadiokohtvõrgu kavandamisvead

Raadiokohtvõrgu kavandamisel tehtud vead võivad kaasa tuua olulisi turvanõrkusi. Kui kasutatakse teadaolevate turvanõrkustega kohtvõrgu standardeid (nt turvaalgoritmi WEP puhul on võimalik krüptovõti hõlpsasti murda), on ründajal võimalik võrku tungida, võrguliiklust pealt kuulata ja konfidentsiaalseid andmeid kopeerida.

Raadiolainete ebapiisav leviulatus või vähene andmeedastuskiirus võib kaasa tuua teenuse kvaliteedi languse. Oluliste rakenduste kasutamine võib olla häiritud. Teatud asukohtades ei saa raadiokohtvõrku kasutada.

2.3 Raadiokohtvõrgu kasutamise korra puudumine

Ilma raadiokohtvõrgu taristu keskse halduseta on raske tagada turvaline seadistus kõikides raadiokohtvõrgu pääsupunktides (ingl *wireless access point*). Vaikeseadistuses on võrguseadmed enamasti puudulike turvamehhanismidega ja lihtsalt tuvastatavate paroolidega.

Raadiovõrkude kasutamise korra puudumisel võib töötaja teadmatusest ühendada kohtvõrku lubamatu pääsupunkti. Lisatud lubamatu pääsupunkti kaudu, eriti kui selle turvalisus on nõrk, võivad kõik lähedalasuvad seadmed saada kohtvõrgu juurdepääsu.

2.4 Ebaturvalised autentimisprotseduurid

Raadiokohtvõrgu puuduvad või ebapiisavad autentimisprotseduurid ja -mehhanismid võivad kaasa tuua turvanõrkusi. Näiteks standardi IEEE 802.1x käsitletud Extended Authentication Protocol (EAP) raamistiku mõni meetod sisaldab teadaolevaid turvanõrkusi (nt on EAP-MD5 kaitsetu vahendusrünnete (ingl *man-in-the-middle attack*) ja sõnastikrünnete (ingl *dictionary attack*) vastu. Nii on EAP-MD5 kasutamise korral võimalik kasutaja parooli ära arvata ja andmesidet pealt kuulata.

2.5 Raadiokohtvõrgu taristu seadistusvead

Raadiokohtvõrgu pääsupunktides ja muudes raadiovõrgu komponentides (nt raadiokohtvõrgu kontroller) on arvukalt seadistusvõimalusi, mis hõlmavad ka turvafunktsioone. Vale seadistuse puhul ei ole pääsupunkti kaudu andmeside võimalik või on pääsupunkt liiga madala kaitsetasemega.

2.6 Puuduvad või ebapiisavad raadiokohtvõrgu turvamehhanismid

Raadiokohtvõrgu komponendid on sageli eelseadistatud ilma turvamehhanisme aktiveerimata või on turvamehhanismid rakendatud ainult osaliselt. Isegi tänapäeval kasutatakse veel raadiokohtvõrgu komponente, mis toetavad üksnes puudulikke turvamehhanisme (nt WEP). Üldjuhul ei ole vanematele seadmetele saadaval turvalisust parandavaid püsivara uuendeid (ingl *firmware update*). Sellist teadaoleva turvnõrkusega seadet on ründajal võimalik ära kasutada andmeside pealtkuulamiseks ja konfidentsiaalsele teabele juurde pääsemiseks.

2.7 Raadiokohtvõrgu side pealtkuulamine

Raadiolainete edastuskeskkonda ei ole võimalik kontrollida (jagatud meedium), seda saavad korraga kasutada paljud kasutajad. Seetõttu on võimalik raadiokohtvõrgu kaudu edastatavaid andmeid jälgida ja salvestada. Kui edastatavaid andmeid ei krüpteerita või kasutatakse ebaturvalist krüpteerimismehhanismi, on neid andmeid võimalik lugeda. Kuna raadiokohtvõrgu leviala ulatub sageli kaugemale nõutud piireist, ei saa võrgu omanik tervet levipiirkonda kontrollida ega turvata.

2.8 Tegeliku pääsupunkti matkimine (kahjurpääsupunkt)

Ründaja võib esineda ühe osana raadiokohtvõrgu taristust, kui ta on kasutaja lähedusse üles seadnud sobivalt valitud võrgunimega pääsupunkti. Sellist pääsupunkti nimetatakse kahjurpääsupunktiks (ingl *rogue access point*). Kui kahjurpääsupunkt saadab õigest pääsupunktist tugevamaid signaale ja vastastikust autentimist ei nõuta, siis hakkab kliendi seade kasutama tugijaamana kahjurpääsupunkti. Kasutaja logib sisse võrku, mille arvab olevat soovitud võrguks, kuid ründaja saab tema andmesidet pealt kuulata ja salvestada. Sageli kasutatakse seda meetodit avalike raadiovõrkude (ingl *public WiFi network*) ründeks.

Õigele pääsupunktile juurdepääsu tõkestades saab läbi viia teenusetõkestusrünnet. Ründaja võib mürgitusmeetodeid (ingl *poisoning*) või teesklusmeetodeid (ingl *spoofing*) kasutades teeselda kellegi teise identiteeti või suunata võrguliikluse läbi talle kuuluvate süsteemide, mis võimaldab ründajal andmesidet pealt kuulata.

2.9 Kaitsmata pääs pääsupunktist kohtvõrku

Kui pääsupunktid on paigaldatud kõigile nähtavalt ja ilma füüsilise kaitseta, saab ründaja võrguliikluse pealtkuulamiseks lisada oma seadme pääsupunktide ja kommutaatorite (ingl *switch*) vahele. Ka WPA2-ga andmeside krüpteerimine pole piisav, sest selline meetod kaitseb vaid raadioliidest ega arvesta Etherneti ühendust.

2.10 Riistvara kahjustused

Raadiokohtvõrgu toimimist võivad häirida riistvara tõrked. Väljaspool organisatsiooni turvaperimeetrit asuvaid raadiokohtvõrgu seadmeid võib ründaja tahtlikult kahjustada. Samuti on need seadmed avatud ka asukohast tulenevatele ohtudele (nt liigniiskusest või pikselöögist tingitud kahjustused).

2.11 Pääsupunkti vargus

Raadiokohtvõrgu pääsupunktide paigaldamine kergesti juurdepääsetavasse (nt käiguteede kohale lae alla) või rahvarohkesse asukohta suurendab seadmete varguse ohtu. Varastatud seadmes on ründajal võimalik ligi pääseda pääsupunkti salvestatud RADIUS-serveri autentimise ühisvõtmele või levialavõtmele (nt WPA2 Personal), mille abil on võimalik saada raadiokohtvõrgule lubamatu juurdepääs.

3 Meetmed

3.1 Elutsükkel

Kavandamine

NET.2.1.M1 Raadiokohtvõrkude kavandamine

NET.2.1.M2 Sobiv raadiokohtvõrgu standard

NET.2.1.M3 Turvaline krüptomehhanism

NET.2.1.M10 Raadiokohtvõrgu turvajuhend

Soetus

NET.2.1.M11 Sobivad raadiokohtvõrgu komponendid

Evitus

NET.2.1.M4 Pääsupunktide turvaline paigaldus

NET.2.1.M5 Pääsupunkti turvaline aluskonfiguratsioon

NET.2.1.M6 Raadiokohtvõrgu taristu turvaline seadistus

NET.2.1.M7 Turvaline raadiokohtvõrgu arhitektuur

NET.2.1.M9 Raadiokohtvõrgu turvaline ühendamine kaabelvõrguga

Käitus

NET.2.1.M12 Raadiokohtvõrgu sobiv haldus

NET.2.1.M13 Raadiokohtvõrgu regulaarne turvakontroll

NET.2.1.M14 Raadiokohtvõrgu komponentide regulaarne läbivaatus

Avariivalmendus

NET.2.1.M8 Raadiokohtvõrgu intsidendikäsitluse kord

Lisanduvad kõrgmeetmed

NET.2.1.M15 Raadiokohtvõrgu turve virtuaalse privaatvõrguga (VPN)

NET.2.1.M16 Raadiokohtvõrgu ja kaabelvõrgu vahelise ühenduse lisaturve

NET.2.1.M17 Pääsupunktide ühenduse turve

NET.2.1.M18 Raadiokohtvõrgu sissetungituvastuse ja -tõrje tööriistad

3.2 Põhimeetmed

NET.2.1.M1 Raadiokohtvõrkude kavandamine

a. Raadiokohtvõrgu (ingl *wireless local area network*, WLAN) kasutuselevõtuks organisatsioonis on koostatud kava, mis määrab:
   - mis eesmärgil ja millistes äriprotsessides raadiokohtvõrku rakendatakse ja mis on raadiokohtvõrgu lisandväärtus;
   - mis asukohtades raadiovõrku rakendatakse;
   - milliseid funktsioone ja rakendusi raadiokohtvõrk toetab;
   - milliste andmete edastamiseks raadiokohtvõrku kasutada ei tohi;
   - milliseid turvanõudeid raadiokohtvõrgu käitamisel arvestatakse.
b. Raadiokohtvõrgu kavandamisel määratakse raadiokohtvõrgu taristu halduse eest vastutajad ja teavitusteed ning töötatakse välja haldusprotseduurid.

NET.2.1.M2 Sobiv raadiokohtvõrgu standard [arhitekt]

a. Raadiokohtvõrgu häiringute vältimiseks on välja selgitatud, kui palju seadmeid on kavandatavates raadiokohtvõrgu sagedusalades (2,4 GHz ja 5 GHz) ja milliseid

raadiokanaleid (ingl *wireless channel*) need seadmed kasutavad. Muud häiringuallikad (Bluetooth-saatjad, kõrgepingekaablid, DECT-telefonid) võimalusel kõrvaldatakse.

b. Seadmete poolt toetatud raadiokohtvõrgu standarditest on valitud kasutamiseks kõige turvalisemad. Lubatud on IEEE 802.11i-2004 (krüptomehhanism WPA2) või uuem standard (WPA3). WEP ja WPA kasutamine on blokeeritud. Standardite valiku põhjused on dokumenteeritud.

c. Raadiokohtvõrgu kavandamisel välistatakse seadmed, mis toetavad ainult ebaturvalisi autentimis- ja krüpteerimismehhanisme.

NET.2.1.M3 Turvaline krüptomehhanism [arhitekt]

a. Raadiokohtvõrgu andmeliiklus on krüptograafiliselt kaitstud.

b. Lihtsalt murtavate krüpteerimisprotokollide (nt WEP-ga kasutatav TKIP) kasutamine on blokeeritud. Selle asemel kasutatakse WPA2 krüpteerimisprotokolle CCMP (kasutab AES krüptoalgoritmi) või EAP (Extensible Authentication Protocol).

c. Kui kasutusel on autentimismehhanism WPA2-Personal (WPA2-PSK, Pre Shared Key), kasutatakse paroolina vähemalt 20-märgilist keerukat võtit. Võtit muudetakse regulaarselt.

d. Parema turvalisuse tagab autentimismehhanism WPA2-Enterprise, mille puhul autentimine toimub kasutajanime ja parooliga autentimisprotokolli 802.1X ja keskselt hallatava RADIUS serveriga.

NET.2.1.M4 Pääsupunktide turvaline paigaldus [tehnikatalitus]

a. Raadiokohtvõrgu pääsupunktid (ingl *wireless access point*) ei ole kõrvalistele isikutele lihtsalt juurdepääsetavad. Vajadusel kasutakse kaitsekorpusi ja vargusvastaseid vahendeid.

b. Kasutatakse meetmeid (nt suundantennid või metallvarjestus) raadiolainete levi takistamiseks nõutavast levialast välja jäävatele aladele.

c. Välistes tingimustes asuvad antennid ja pääsupunktid on kaitstud ilmastikumõju (nt vihm või pikselöök) ja elektriliste häiringute eest. Võimalusel tuleks hooneväliste pääsupunktide paigaldamist vältida.

NET.2.1.M5 Pääsupunkti turvaline seadistus

a. Tootja poolt tehtud eelseadistused (sh võrgunimed, paroolid ja krüptovõtmed) muudetakse enne pääsupunkti võrku lisamist.

b. Sisekasutuseks ette nähtud raadiokohtvõrgu võrgunimi (SSID) ei võimalda teha järeldusi riistvara, organisatsiooni, teenuseandja või kasutusotstarbe kohta.

c. Tarbetud protokollid, pordid, teenused ja haldusjuurdepääsud (nt Telnet või HTTP) on suletud või desaktiveeritud.

d. DHCP- serveri kasutamisel on rakendatud vahendid (nt Dynamic ARP Inspection, DAI) ARP-pette (ingl *ARP spoofing*) avastamiseks ja tõrjeks.

e. Kogu raadiokohtvõrgu taristu ulatuses on paigaldatud püsivara uuendid (ingl *firmware update*) ja turvauuendid (ingl *security update*). Uuendid on enne paigaldamist testitud.

f. Administraatori kasutajakonto pääsuõigused on antud minimaalsuse printsiipi järgides. Avariivalmenduse tarbeks on pääsupunktil aktiveeritud ka lokaalne kasutajakonto.

g. Pääsupunktide halduse sideühendus on krüpteeritud.

NET.2.1.M6 Raadiokohtvõrgu taristu turvaline seadistus

a. Raadiokohtvõrgu klientide turvaliseks konfigureerimiseks rakendatakse meetmeid moodulitest SYS.2.1 *Klientarvuti üldiselt* ja NET.2.2 *Raadiokohtvõrgu kasutamine*.

b. Raadiokohtvõrgu kaudu ei saa ühendada omavahel eri turvatsoonides asuvaid klientseadmeid.

NET.2.1.M7 Turvaline raadiokohtvõrgu arhitektuur [arhitekt]

a. Kõrge käideldavuse tagamiseks ühendatakse pääsupunktid võrgutaristuga kaabliühendustega.

b. Raadiokohtvõrgu võrgusegmendid eraldatakse kohtvõrgust füüsiliselt või jagades võrgu loogilisteks virtuaalseteks kohtvõrkudeks (VLAN).

NET.2.1.M8 Raadiokohtvõrgu intsidendikäsitluse kord

a. Raadiokohtvõrgu intsidentide käsitlemiseks on olemas kord (vt DER.2.1 *Turvaintsidentide käsitlus*).

b. Raadiokohtvõrgu ründe korral on võimalik pääsupunktid ja raadioside määratud ulatuses blokeerida.

c. On olemas tegevuskava varastatud pääsupunkti abil sisevõrku tungimise takistamiseks (WPA2-PSK kasutamisel muudetakse võti, RADIUS-serveri puhul blokeeritakse varastatud pääsupunkt serveris).

d. Varastatud pääsupunkti sertifikaadipõhise autentimise puhul kliendisertifikaadid blokeeritakse.

e. Vajadusel on võimalik taastada pääsupunktide seadistused varukoopiast.

3.3 Standardmeetmed

NET.2.1.M9 Raadiokohtvõrgu turvaline ühendamine kaabelvõrguga [arhitekt]

a. Raadiokohtvõrgu ühenduskohad kaablipõhise kohtvõrguga on turvatud (nt paketifiltriga).

b. Iga võrgunime (SSID) jaoks on kasutusele võetud eraldi virtuaalne kohtvõrk.

c. Kohtvõrgule juurdepääsu raadiovõrgust käsitletakse ja turvatakse sarnaselt nagu juurdepääsu Internetist. Juurdepääs on lubatud ainult tulemüüri kaudu.

d. Raadiokohtvõrku liidetakse ainult organisatsiooni kehtestatud nõuetele vastavaid pääsupunkte (ingl *wireless access point*).

e. Pääsupunktide ühendamisel järgitakse meedet NET.2.1.M7 *Turvaline raadiokohtvõrgu arhitektuur.*

NET.2.1.M10 Raadiokohtvõrgu turvajuhend

a. Organisatsiooni üldise turvapoliitika alusel on dokumenteeritud, kehtestatud ja kõigile kasutajatele teatavaks tehtud raadiokohtvõrgu turvajuhend.

b. Raadiokohtvõrgu turvajuhend määrab muuhulgas:

- kes tohib installida, konfigureerida ja kasutada raadiokohtvõrgu komponente;
- millised peavad olema raadiokohtvõrgu komponentide turvameetmed ja tüüpkonfiguratsioon;
- kuidas toimub raadiokohtvõrgu komponentide haldus;

- kuidas toimub raadiokohtvõrgu tegevuste logimine ja seire;
- kuidas ja kellele teatada turvaprobleemidest (vt DER.2.1 *Turvaintsidentide käsitlus*).

c. Raadiokohtvõrgu turvajuhendi järgimist kontrollitakse regulaarselt. Tulemused dokumenteeritakse.

NET.2.1.M11 Sobivad raadiokohtvõrgu komponendid

a. Raadiokohtvõrgu taristu kavandamise (vt NET.2.1.M1 *Raadiokohtvõrkude kavandamine*) tulemuste alusel on raadiokohtvõrgu komponentide valimiseks koostatud nõuete spetsifikatsioon.

b. Kõik raadiokohtvõrgu komponendid on kokkusobivad võrgu-, turva-, autentimis-, seire- ja logitaristutega. Raadiokohtvõrgu komponentide hankimisel arvestatakse ühilduvusnõuetega.

c. Raadiokohtvõrgu kliendid, pääsupunktid, võrguhaldussüsteemid ja autentimisserverid toetavad turvalisi autentimismeetodeid.

NET.2.1.M12 Raadiokohtvõrgu sobiv haldus

a. Raadiokohtvõrku hallatakse kesksete haldusvahenditega.

b. Raadiokohtvõrgu haldamine hõlmab vähemalt järgmist:

- pääsupunktide ja raadiokohtvõrgu klientseadmete püsivaraversioonide uuendamine ja dokumenteerimine;
- konfiguratsioonimuudatused ja nende muudatuste dokumenteerimine;
- alarmteadete analüüs ja hindamine;
- rikkeotsingud;
- toimingud intsidendikahtluse korral;
- logimine ja logiandmete analüüs.

c. Halduslahendus vastab raadiokohtvõrgu turvajuhendi nõuetele.

NET.2.1.M13 Raadiokohtvõrgu regulaarne turvakontroll

a. Raadiokohtvõrku kontrollitakse teadaolevate turvanõrkuste suhtes regulaarselt.

b. Kontrolli käigus otsitakse raadiokohtvõrku lubamatult paigaldatud pääsupunkte.

c. Perioodiliselt mõõdetakse võrgu teenusekvaliteeti, sealhulgas:

- läbilaskevõime (ingl *bandwidth*);
- latentsus (ingl *latency*);
- paketikadu (ingl (*packet loss*).

d. Raadiokohtvõrgu turvanõrkuste avastamiseks viiakse perioodiliselt läbi raadiokohtvõrgu turvatestimine.

e. Turvakontrollide tulemused dokumenteeritakse, kõrvalekallete põhjusi analüüsitakse.

NET.2.1.M14 Raadiokohtvõrgu komponentide regulaarne läbivaatus

a. Raadiokohtvõrgu komponente (pääsupunktid, jaotussüsteem, raadiokohtvõrgu halduslahendus jms) hõlmavate turvameetmete rakendatust kontrollitakse regulaarselt.

b. Raadiokohtvõrgu komponentide konfiguratsiooni õigsust kontrollitakse regulaarselt.

c. Pisteliselt kontrollitakse, kas kergesti juurdepääsetavates asukohtades paiknevates pääsupunktides pole toimunud avamis- või manipuleerimiskatseid.

d. Läbivaatuste tulemused dokumenteeritakse, kõrvalekallete põhjuseid analüüsitakse.

3.4 Kõrgmeetmed

NET.2.1.M15 Raadiokohtvõrgu turve virtuaalse privaatvõrguga (VPN) (C-I)

a. Raadiokohtvõrgu (WLAN) taristu andmeside turbeks kasutatakse virtuaalset privaatvõrku (ingl *virtual private network*, VPN).

b. VPN rakendamisel järgitakse meetmeid moodulist NET.3.3 *Virtuaalne privaatvõrk (VPN)*.

NET.2.1.M16 Raadiokohtvõrgu ja kaabelvõrgu vahelise ühenduse lisaturve (C-I-A)

a. Raadiokohtvõrgu ja kaabelvõrgu vahelise ühenduse lisaturbeks on kasutusel täiendavad meetmed ja vahendid, nt sissetungituvastuse süsteem (ingl *intrusion detection system*, IDS) ja/või sissetungitõrje süsteem (ingl *intrusion prevention system*, IPS).

NET.2.1.M17 Pääsupunktide ühenduse turve (C)

a. Pääsupunktide vaheline side on andmete konfidentsiaalsuse tagamiseks krüpteeritud (vt NET.2.1.M3 *Turvalise krüptomehhanismi valimine*).

b. Andmeside pääsupunkti (ingl *wireless access point*) ja raadiokohtvõrgu haldussüsteemi vahel on turvatud IPSec, TLS v1.2 või TLS v1.3 protokollidega. Autentimiseks on nõutav sertifikaat.

c. Pääsupunkti ja raadiokohtvõrgu halduse mistahes elemente ei paigutata pilve.

d. Raadiokohtvõrgu taristus puudub pääsupunktide vahel otseside, andmeside toimub krüpteeritult läbi raadiokohtvõrgu keskse kontrolleri.

NET.2.1.M18 Raadiokohtvõrgu sissetungituvastuse ja -tõrje tööriistad (C-I-A)

a. Nõrkuste ja turvasündmuste avastamiseks raadiokohtvõrgus on kasutusel raadiovõrkude jaoks mõeldud sissetungituvastuse (ingl *wireless intrusion detection system*, WIDS) ja/või sissetungitõrje (ingl *wireless intrusion prevention system*, WIPS) süsteemid.

4 Lisateave

Lühend	Publikatsioon
[NIST]	NIST Special Publication 800-153 „Guidelines for Securing Wireless Local Area Network (WLANs)“
[NIST]	NIST Special Publication 800-97 „Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11“

NET.2.2 Raadiokohtvõrgu kasutamine

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed raadiokohtvõrkude (ingl *wireless local area network*, WLAN) turvaliseks kasutamiseks.

1.2 Vastutus

Mooduli meetmete rakendamise eest vastutab kasutaja.

Lisavastutajad

IT-talitus, ülemus.

1.3 Piirangud

Moodul sisaldab meetmeid raadiokohtvõrkude turvaliseks kasutamiseks. Raadiokohtvõrgu turvalise evituse ja käituse meetmed on kirjeldatud moodulis NET.2.1 *Raadiokohtvõrgu käitus*. Klientarvuti turbe üldpõhimõtteid käsitletakse moodulis SYS.2.1 *Klientarvuti üldiselt*. Raadiokohtvõrgu kasutajatele rakendatakse lisaks meetmeid moodulitest ORP.3 I*nfoturbe teadlikkuse tõstmine ja koolitus* ning DER.2.1 *Turvaintsidentide käsitlus.*

2 Ohud

2.1 Eeskirjade tundmise puudulikkus

Kui kasutaja ei järgi raadiokohtvõrgu turvalise kasutamise eeskirja (nt ühendub tundmatu võrguga), tekib ründajal võimalus võrguliiklust pealt kuulata. Ründaja saab juurdepääsu võrgu kaudu edastatavatele andmetele, näiteks külastatud veebilehetedele, seansiküpsistele (ingl *session cookie*) ja paroolidele.

2.2 Turvameetmete eiramine

Kui kehtestatud turvameetmeid eiratakse, nt kasutatakse raadiokohtvõrgu klienti *ad hoc* režiimis (ingl *ad hoc mode)*, võib mõni muu klientseade juhul, kui kliendi ressursid on välja jagatud, saada lubamatu juurdepääsu kasutaja konfidentsiaalsetele dokumentidele.

2.3 Raadiovõrgu andmeside pealtkuulamine

Krüpteerimata või ebapiisavalt krüpteeritud andmeid on võimalik andmevahetuse käigus kopeerida ja pealt kuulata. Organisatsioon ei oma täielikku kontrolli kõigi asukohtade üle, kus andmete vastuvõtt on tehniliselt võimalik.

2.4 Sideühenduse andmete analüüs

WLAN-liidese MAC-aadressi järgi on võimalik koostada mobiilse kasutaja profiil, näiteks teada saada, milliseid avalikke pääsupunkte (ingl *wireless access point*) ta kasutab.

2.5 Õige pääsupunkti teesklemine (kahjurpääsupunkt)

Ründaja võib oma kontrolli all olevaid seadmeid esitada raadiokohtvõrgu taristu osana, rajades kliendi läheduses kahjurpääsupunkti (ingl *rogue access point*), millele on sobivalt valitud võrgunimi (SSID). Kasutaja logib end sisse võrku, mis ainult näiliselt on kasutaja poolt soovitud sihtvõrk. Seeläbi võib ründaja sideühendust pealt kuulata.

Kahjurpääsupunktide kasutamine on eriti levinud avalikuks kasutuseks mõeldud raadiokohtvõrkudes.

3 Meetmed

3.1 Elutsükkel

Kavandamine

NET.2.2.M1 Raadiokohtvõrgu kasutamise eeskiri

Evitus

NET.2.2.M2 Raadiokohtvõrgu kasutajate teadlikkuse tõstmine ja koolitus

Käitus

NET.2.2.M3 Raadiokohtvõrgu kasutamine avalikes raadiokohtvõrkudes

Avariivalmendus

NET.2.2.M4 Raadiokohtvõrgu turvasündmuste puhul käitumise kord

3.2 Põhimeetmed

NET.2.2.M1 Raadiokohtvõrgu kasutamise eeskiri [IT-talitus]

a. Organisatsiooni üldise turvapoliitika alusel on kehtestatud raadiokohtvõrgu (ingl *wireless local area network*, WLAN) kasutamise eeskiri.
b. Raadiokohtvõrgu kasutamise eeskiri sätestab vähemalt järgmist:
   - milliste sisemiste ja väliste võrkudega tohib raadiokohtvõrgu klienti ühendada;
   - millist teavet ei tohi raadiokohtvõrgus vahetada;
   - klientseadmete turvavahendite rakendamine;
   - paroolide piisava tugevuse nõue;
   - juhuvõrgurežiimi keeld;
   - seadistuse muutmise keeld;
   - kataloogide ja teenuste lubatavuse tingimused;
   - keeld ühendada pääsupunkte (ingl *wireless access point*) organisatsiooni kohtvõrguga;
   - WLAN-liidese desaktiveerimine pikema kasutuspausi järel;
   - tegevused turvaintsidendi puhul.
c. Eeskirja järgimist kontrollitakse regulaarselt ja tulemused dokumenteeritakse.

NET.2.2.M2 Raadiokohtvõrgu kasutajate teadlikkuse tõstmine ja koolitus [ülemus, IT-talitus]

a. Raadiokohtvõrgu kasutajaid koolitatakse raadiokohtvõrguga seotud ohtude ja turbe alal. Koolitus sisaldab organisatsioonipõhiseid näiteid.
b. Kasutajaile selgitatakse olulisi raadiokohtvõrgu turvasätteid ning ohte, mis tulenevad nende sätete vältimisest või desaktiveerimisest.
c. Kasutajad tunnevad raadiokohtvõrgu kasutamise eeskirja ja järgivad seda.

NET.2.2.M3 Raadiokohtvõrgu kasutamine avalikes raadiokohtvõrkudes [IT-talitus]

a. Kasutajad teavad, kas ja mis tingimustel on avaliku pääsupunkti kasutamine lubatud (vt NET.2.2.M2 *Raadiokohtvõrgu kasutajate teadlikkuse suurendamine ja koolitus*).
b. Harva kasutatavad raadiokohtvõrgud kustutatakse klientseadme kasutusajaloost.
c. Võimalusel kasutatakse ebaturvalistes tingimustes kitsendatud õigustega kasutajakontot. Administraatori õigustega kasutajal on oma arvutist välistesse ebaturvalistesse raadiokohtvõrkudesse sisenemine keelatud.
d. Ebaturvalises raadiokohtvõrgus edastatakse tundlikke andmeid ainult krüpteeritult ja kasutades turvalisi protokolle.
e. Võõrast raadiokohtvõrgust saab kasutaja organisatsiooni siseressursside poole pöörduda ainult virtuaalse privaatvõrgu (VPN) kaudu (vt NET.3.3 *VPN*).

3.3 Standardmeetmed

NET.2.2.M4 Raadiokohtvõrgu turvasündmuste puhul käitumise kord

a. Raadiokohtvõrgu intsidendikahtluse või tõrke puhul on kasutaja kohustatud oma töötulemused varundama, raadiokohtvõrgust väljuma ja oma klientseadme WLAN-liidese desaktiveerima.
b. Kasutaja dokumenteerib veateated ja anomaaliad, kaasaarvatud tegevused, mida ta on teinud enne turvaintsidenti või selle ajal.
c. Tõrke või intsidendikahtluse korral WLAN võrgus teavitab kasutaja turvasündmusest koheselt IT-talitust kokku lepitud kontaktpunkti (nt IT-kasutajatoe) kaudu.

3.4 Kõrgmeetmed

Moodulil puuduvad kõrgmeetmed.

4 Lisateave

Lühend	Publikatsioon
[NIST]	NIST Special Publication 800-153 „Guidelines for Securing Wireless Local Area Network (WLANs)“

NET.3: Võrgukomponendid

NET.3.1 Ruuter ja kommutaator

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed ruuterite (ingl *router*) ja kommutaatorite (ingl *switch*) turvaliseks käituseks.

1.2 Vastutus

Ruuteri ja kommutaatori meetmete rakendamise eest vastutab IT-talitus.

Lisavastutajad

Infoturbejuht.

1.3 Piirangud

Moodulis ei kirjeldata konkreetsete seadmetootjate tootespetsiifilisi meetmeid.

Kuna tänapäeval on ruuteri (ingl *router*) ja kommutaatori (ingl *switch*) algselt erinevad funktsioonid sageli ühendatud ühte seadmesse, siis ka enamik selle mooduli meetmeid on kasutatavad nii ruuterite kui ka kommutaatorite puhul. Ruuterite ja kommutaatorite tulemüürifunktsioonide rakendamisel tuleks järgida meetmeid moodulist NET.3.2 *Tulemüür*.

Moodul ei käsitle virtuaalsete ruuterite ja kommutaatorite turvameetmeid ega arvutite operatsioonisüsteemides aktiveeritavaid marsruutimisfunktsioone.

Moodulis ei käsitleta taristu turvaaspekte (nt seadmete sobiv paigaldus, elektritoide või kaabeldus), need on esitatud kihi INF *Taristu* moodulites.

Võrkude rajamise ja halduse meetmed on esitatud moodulites NET.1.1 *Võrgu arhitektuur ja lahendus* ja NET.1.2 *Võrguhaldus*.

2 Ohud

2.1 Hajus ummistusrünne (DDoS)

Võrgu hajus ummistusrünne (ingl *distributed denial-of-service(DDoS) attack*) võib olla tekitatud SYN-tulva (ingl SYN-*flood*) või UDP-tulva (ingl UDP-*flood*) abil. Ohvriks valitud seadmele saadetakse massiliselt SYN-pakette või datagramme, millele vastamine koormab vastuvõtja üle. Ummistusründe tulemusel tekivad ruuterite töös häired. Selle tagajärjel halveneb kohtvõrgu teenuste käideldavus ja kohtvõrk võib muutuda kättesaamatuks.

2.2 Manipuleerimine

Kui ründajal õnnestub ruuterile või kommutaatorile saada lubamatu juurdepääs, on tal võimalik seadmeid manipuleerida (nt aktiveerida neis täiendavaid teenuseid). Ruuteri või kommutaatori konfiguratsiooni muutes saab blokeerida teenuseid, klientseadmeid või terveid võrgusegmente.

2.3 Ruuteri või kommutaatori konfigureerimisvead

Ruuterite ja kommutaatorite algses standardkonfiguratsioonis võib olla aktiveeritud tarbetuid ja ebaturvalisi teenuseid. Kui ruuterid ja kommutaatorid võetakse kasutusele ebaturvaliste vaikeseadetega, on seadmetele lihtsam lubamatult juurde pääseda, seadmeid manipuleerida ja/või teenuseid katkestada. See võib muuta võrguteenused kasutajale kättesaamatuks.

Ruuteri või kommutaatori haldaja võib seadme seadistamisel oskamatusest või tähelepanematusest teha seadistusvea, mille tulemusena tekib võimalus lubamatuks juurdepääsuks võrguressurssidele.

Kui sisselogimiskuva paljastab seadme mudeli ning versiooninumbri, siis osutub võimalikuks sihtotstarbeliselt ära kasutada just konkreetses versioonis leiduvaid nõrkusi.

2.4 Puudulik kavandamine

Ruuterite ja kommutaatorite kasutuselevõtu kavandamisel võidakse eksida seadmete portide arvu või sooritusvõime spetsifitseerimisel. Sageli juhtub see siis, kui peamiseks otsustuskriteeriumiks on võetud seadme maksumus. Seetõttu võib ruuter või kommutaator olla juba alguses üle koormatud. Selle tagajärjel ei pruugi võrguteenused olla kättesaadavad. Aladimensioneeritud seadmete puhul suureneb oluliselt ummistusründe oht.

2.5 Ühildumatud aktiivsed võrgukomponendid

Kui olemasolevaid võrke täiendatakse teiste tootjate aktiivsete võrgukomponentidega, võivad kergesti tekkida seadmevahelised ühilduvusprobleemid. Mitmete tootjate seadmeid koos kasutades võib langeda võrguteenuse kvaliteet (nt läbilaskevõime). Ka ühes võrgus samadel seadmemudelitel erinevaid põhivara- või tarkvaraversioone kasutades võivad tekkida ühilduvusprobleemid. Tulemuseks on raskesti lahendatavad tõrked ja häired võrgu toimimises.

2.6 MAC-tulv

MAC-tulva (ingl MAC-flooding) puhul edastab ründaja kommutaatorile suurel hulgal võltsitud MAC-lähteaadressidega päringuid. Niipea kui kommutaatoris saavutatakse salvestatavate MAC-aadresside piirväärtus, hakkab see päringuid edastama kõigile võrgus olevatele IT-seadmetele. See võimaldab ründajal võrguliiklust kaardistada ja tekitada tarbetut võrgukoormust.

2.7 Ründed STP protokolli vastu

STP (ingl spanning tree protocol, STP) ründe korral edastab ründaja sillaprotokolli andmeüksusi (ingl bridge protocol data unit, BPDU) eesmärgil, et kommutaatorid hakkaksid juursillana (ingl root bridge) kasutama kohtvõrku ühendatud kahjurkommutaatorit. Võrguliiklus suunatakse läbi kahjurkommutaatori, mistõttu ründaja saab salvestada selle kaudu edastatud informatsiooni. Ründaja saab algatada hajusaid ummistusründeid ja võltsitud sillaprotokolli andmeüksuste abil sundida võrku spanning tree topoloogiat uuesti rajama ja kutsuda esile võrgu tõrke.

2.8 GARP-ründed

GARP-ründe (ingl *gratuitous ARP attack, GARP attack*) korral edastab ründaja ARP (ingl *Address Resolution Protocol*, ARP) vastuse vormingus pakette valitud ohvrile või sama alamvõrgu kõigile IT-seadmetele. Võltsitud ARP-i päringuvastuses asendab ründaja kellegi teise IP-aadressi oma seadme MAC-aadressiga, mis sunnib rünnatavat seadet muutma oma ARP-i tabelit. Selle tulemusel võrguliiklus suunatakse tegeliku sihtaadressi asemel ründajale. Seeläbi võib ründaja ohvrite vahelist andmevahetust salvestada või manipuleerida.

3 Meetmed

3.1 Elutsükkel

Kavandamine

NET.3.1.M21 Pääsuõiguste ja identiteedi haldus võrgutaristus

Soetus

NET.3.1.M11 Ruuteri või kommutaatori valimine

Evitus

NET.3.1.M1 Ruuteri või kommutaatori turvaline baaskonfiguratsioon

NET.3.1.M4 Ruuteri või kommutaatori haldusliideste turve

NET.3.1.M9 Ruuteri või kommutaatori käidudokumentatsioon

NET.3.1.M10 Ruuterite ja kommutaatorite turvajuhend

NET.3.1.M18 Pääsuloendid

Käitus

NET.3.1.M5 Kaitse IP-pakettide fragmenteerimisrünnete eest

NET.3.1.M6 Ruuteri või kommutaatori avariijuurdepääs

NET.3.1.M7 Ruuterite ja kommutaatorite logimine

NET.3.1.M12 Konfiguratsiooni kontroll-loend

NET.3.1.M13 Eraldatud haldusvõrk

NET.3.1.M14 ICMP-sõnumite kaitsmine väärkasutuse eest

NET.3.1.M15 Võltsitud pakettide ja teeskluse tõkestamine

NET.3.1.M16 IPv6 „routing header type 0“ rünnete takistamine

NET.3.1.M17 Ummistusrünnete tõrje

NET.3.1.M19 Kommutaatori portide turve

NET.3.1.M20 Turvalised marsruutimisprotokollid

NET.3.1.M23 Läbivaatused ja läbistustestimised

Avariivalmendus

NET.3.1.M8 Andmete regulaarne varundamine

NET.3.1.M22 Ruuterite ja kommutaatorite avariivalmendus

Lisanduvad kõrgmeetmed

NET.3.1.M24 Võrkupääsu reguleerimine

NET.3.1.M25 Konfiguratsioonifailide tervikluse laiendatud kaitse

NET.3.1.M26 Kõrgkäideldavuse tagamine

NET.3.1.M27 Ärikriitiliste rakenduste jõudluse haldus

NET.3.1.M28 Sertifitseeritud tooted

3.2 Põhimeetmed

NET.3.1.M1 Ruuteri või kommutaatori turvaline baaskonfiguratsioon

a. Enne ruuteri (ingl *router*) või kommutaatori (ingl *switch*) kasutuselevõttu paigaldatakse sellesse turvaline baaskonfiguratsioon.

b. Vaikeseadistuse tüüpsed kasutajakontod ja paroolid muudetakse. Paroole hoitakse krüpteeritult (nt paroolihoidlas).Mittevajalikud kasutajakontod desaktiveeritakse.

c. Konfiguratsioonifailide juurdepääs on piiratud ja nende terviklus sobivate meetmetega tagatud.

d. Ruuterite ja kommutaatorite baaskonfiguratsioonis on tarbetud teenused, protokollid ja funktsioonilaiendused desaktiveeritud või desinstallitud.

e. Ruuterite ja kommutaatorite tarbetud võrguliidesed ja pordid on blokeeritud.

f. Ruuterite ja kommutaatorite funktsionaalsuse täiendamine on põhjendatud ja on vastavuses organisatsiooni turvapoliitikatega.

NET.3.1.M4 Ruuteri või kommutaatori haldusliideste turve

a. Halduspääs ruuterisse või kommutaatorisse on võimalik ainult määratud IP-aadressilt või IP-aadresside vahemikult.

b. Haldusliidestele ei ole juurdepääsu ebausaldatavaist võrkudest.

c. Ruuterite ja kommutaatorite haldusühenduste kaitseks kasutatakse turvalisi ja krüpteeritud protokolle. Krüpteerimata haldusside puhul kasutatakse eraldatud haldusvõrku (lisakanaliga haldus, (ingl out-of-band management)).

d. Haldusliideste kasutamiseks on seatud sobivad ajapiirangud.

e. Haldusliidese kõik tarbetud teenused on desaktiveeritud.

f. Lubamatu juurdepääs (sh füüsiline juurdepääs) võrguseadme spetsialiseeritud riistvaraliidesele on piiratud.

NET.3.1.M5 Kaitse IP-pakettide fragmenteerimisrünnete eest

a. IPv4- ja IPv6-fragmenteerimisrünnete tõrjeks on ruuteril ja 3nda võrgukihi (*Layer* 3) kommutaatoril aktiveeritud turvamehhanismid.

NET.3.1.M6 Ruuteri või kommutaatori avariijuurdepääs

a. Võrgu mittetoimimisel on haldajail võimalik ruutereid ja kommutaatoreid hallata lokaalse otsepääsu kaudu.

NET.3.1.M7 Ruuterite ja kommutaatorite logimine

a. Ruuteri ja kommutaatori sündmustest logitakse (võimaluse korral automaatselt) vähemalt:

- konfiguratsiooni muudatused;
- taaskäivitused;
- süsteemi tõrked;
- liideste, süsteemi ja võrgusegmentide seisundimuudatused;
- ebaõnnestunud sisselogimiskatsed.

NET.3.1.M8 Regulaarne andmevarundus

a. Ruuterite ja kommutaatorite konfiguratsioonifaile varundatakse regulaarselt.

b. Varukoopiaid hoitakse turvaliselt. Varukoopiad on avarii korral kättesaadavad.

NET.3.1.M9 Ruuteri või kommutaatori käidudokumentatsioon

a. Ruuteri ja kommutaatori olulised käidutööd (sh kõik turbe muudatustega seonduv) lisatakse käidudokumentatsiooni (ingl *operational documentation*).

b. Ruuteri ja kommutaatori konfiguratsioonid ja nendes tehtud muudatused on dokumenteeritud.

c. Käidudokumentatsioon on kaitstud lubamatu juurdepääsu eest.

3.3 Standardmeetmed

NET.3.1.M10 Ruuterite ja kommutaatorite turvajuhend [infoturbejuht]

a. Organisatsiooni üldise turvapoliitika alusel on kehtestatud ruuterite *(ingl router)* ja kommutaatorite (ingl *switch*) turvajuhend, milles on esitatud seadmete turvalise käituse spetsifikatsioonid ja juhised.

b. Seadmehaldurid on ruuterite ja kommutaatorite turvajuhendiga tutvunud ja järgivad seda.

c. Lahknevused turvajuhendist ja turvajuhendi muudatused kooskõlastatakse infoturbejuhiga ning dokumenteeritakse.

d. Turvajuhendi järgimist kontrollitakse regulaarselt.

NET.3.1.M11 Ruuteri või kommutaatori valimine

a. Ruuteri või kommutaatori hankimiseks on kehtestatud nõuete spetsifikatsioon.

b. Hangitav seade on kooskõlas infoturvapoliitikaga ja vastab võrgu kaitsetarbele.

NET.3.1.M12 Konfiguratsiooni kontroll-loend

a. Ruuterite ja kommutaatorite kasutusotstarbest tulenevalt on tähtsamate turvaseadete kontrolliks koostatud konfiguratsiooni kontroll-loend (ingl *checklist*).

NET.3.1.M13 Eraldatud haldusvõrk

a. Ruutereid ja kommutaatoreid hallatakse eraldatud haldusvõrgu kaudu (lisakanaliga haldus (ingl *out-of-band management*)).

b. Haldusliidesed ja -ühendused on kaitstud eraldi tulemüüriga (ingl *firewall*).

c. Põhivõrku ühenduvad haldusliidesed on desaktiveeritud.

d. Kõik haldusprotokollide autentimiseks, krüpteerimiseks ja tervikluse tagamiseks kasutatud turvamehhanismid on aktiveeritud. Kõik ebaturvalised haldusprotokollid on desaktiveeritud (vt NET.1.2 *Võrguhaldus*).

NET.3.1.M14 ICMP-sõnumite kaitsmine väärkasutuse eest

a. Protokollide ICMP (Internet Control Message Protocol, ICMP) ja ICMPv6 sõnumeid filtreeritakse väärkasutuse tõkestamiseks.

NET.3.1.M15 Võltsitud pakettide ja teeskluse tõkestamine

a. Juurdepääs ruuteritesse ja kommutaatoritesse määramata IP-aadressidelt on blokeeritud (ingl *bogon filtering*).

NET.3.1.M16 IPv6 „routing header type 0“ rünnete takistamine

a. Protokolli IPv6 kasutamisel rakendatakse turvamehhanisme, mis avastavad ja hoiavad ära marsruutimispäise (ingl *routing header*) *type 0* põhinevaid ründeid.

NET.3.1.M17 Ummistusrünnete tõrje

a. Teenusetõkestuse vältimiseks rakendatakse turvamehhanisme, mis avastavad ja tõrjuvad sõnumite suure hulgaga seotud ründeid (ingl *denial-of-service attack*) ning TCP olekukurnamisründeid (ingl *TCP state-exhaustion attack*).

NET.3.1.M18 Pääsuloendid

a. Juurdepääs ruuteritele ja kommutaatoritele on piiratud pääsuloendiga (ingl *access control list,* ACL), mis määrab, millistel IT-süsteemidel ja/või mis võrkudest on ruuteritele ja kommutaatorite juurdepääs lubatud.

b. Spetsiifiliste nõuete puudumisel on pääsuloend koostatud valge nimekirja (ingl *whitelisting*) põhimõttel.

NET.3.1.M19 Kommutaatori portide turve

a. Kommutaatori pordid on kaitstud lubamatu füüsilise juurdepääsu eest.

NET.3.1.M20 Turvalised marsruutimisprotokollid

a. Marsruutimisandmete vahetamise ja marsruutimistabeli (ingl *routing table*) uuendite edastamisel ruuterid autenditakse. Kõik kasutatavad marsruutimisprotokollid (ingl *routing protocols*) toetavad ruuterite autentimist.

b. Dünaamilise marsruutimise (ingl *dynamic routing*) protokolle kasutatakse üksnes turvalistes võrkudes. Demilitaartsoonides (ingl *demilitarized zone*, DMZ) kasutakse marsruutimistabelil tuginevaid staatilise marsruutimise (ingl *static routing*) protokolle.

NET.3.1.M21 Pääsuõiguste ja identiteedi haldus võrgutaristus

a. Ruuterite ja kommutaatorite pääsuõiguste haldus on osa kesksest identiteedi- ja õiguste haldusest (vt ORP.4 *Identiteedi ja õiguste haldus*).

NET.3.1.M22 Ruuterite ja kommutaatorite avariivalmendus

a. Diagnostikaks ja rikkeotsinguks on koostatud tüüpiliste tõrgete käsitluse juhend, mida regulaarselt ajakohastatakse.

b. Ruuterite ja kommutaatorite avariivalmendus on osa üldisest avariivalmenduse kontseptsioonist (vt DER.4. *Avariihaldus*).

c. Avariivalmenduse dokumentatsioon ja tegevusjuhendid on kättesaadavad ka paberkujul.

d. Avariiprotseduure harjutatakse regulaarselt.

NET.3.1.M23 Läbivaatused ja läbistustestimised

a. Teadaolevate turvaprobleemide suhtes kontrollitakse ja testitakse ruutereid ja kommutaatoreid regulaarselt.

b. Regulaarsete läbivaatuste käigus kontrollitakse, kas seadmed vastavad turvalisele baaskonfiguratsioonile.

c. Läbivaatuste ja läbistustestimiste tulemused dokumenteeritakse, tuvastatud puudustega tegeletakse esimesel võimalusel.

3.4 Kõrgmeetmed

NET.3.1.M24 Võrkupääsu reguleerimine (I-A)

a. Juurdepääs võrgule on reguleeritud standardile IEEE 802.1x vastava pordipõhise autentimismeetodiga EAP-TLS (Extensible *Authentication Protocol* (EAP) - *Transport Layer Security* (TLS)).

b. Eeltoodud meetodit ei tohi kasutada koos standardi ebaturvaliste versioonidega IEEE 802.1x-2001või IEEE 802.1x-2004.

NET.3.1.M25 Konfiguratsioonifailide tervikluse laiendatud kaitse (I)

a. Ruuteri (ingl *router*) või kommutaatori (ingl *switch*) avariijärgsel taastel või taaskäivitusel kasutatakse ainult viimast veatut konfiguratsiooni ja viimati uuendatud pääsuloendit.

NET.3.1.M26 Kõrgkäideldavuse tagamine (A)

a. Ruuterid ja kommutaatorid on kavandatud liiasusega (ingl *redundancy*).

b. Kõrgkäideldavuse tagamise mehhanismid vastavad organisatsiooni turvapoliitikale, ei takista ruuteri või kommutaatori turvafunktsioonide tööd ja ei vähenda turvataset.

NET.3.1.M27 Ärikriitiliste rakenduste jõudluse haldus (A)

a. Ärikriitiliste rakenduste piisava jõudluse tagamiseks teevad ruuterid ja kommutaatorid serverirakenduste ja võrguteenuste prioriseerimist ja vajaduspõhist ressursside jaotamist.

NET.3.1.M28 Sertifitseeritud tooted (C-I)

a. Ruuter või kommutaator on sertifitseeritud vähemalt *Common Criteria* (CC) tasemel EAL4 või sellega võrreldava muu turvahindamise alusel.

NET.3.2 Tulemüür

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed tulemüüri (ingl *firewall*) või tulemüürisüsteemi turvaliseks hankimiseks, rajamiseks, konfigureerimiseks ja käitamiseks.

1.2 Vastutus

Tulemüüri turvameetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Infoturbejuht.

1.3 Piirangud

Moodul täiendab moodulit „NET.1.1 *Võrgu arhitektuur ja lahendus“* tulemüürispetsiifiliste turvameetmetega. Tulemüüris kasutatava ruuteri või kommutaatori funktsionaalsuse turbeks rakendatakse lisaks meetmeid moodulist NET.3.1 *Ruuterid ja kommutaatorid.*

Moodulis ei käsitleta lisafunktsionaalsusega seadmete (nt. järgmise põlve tulemüür (ingl *next generation firewall*)) täiendavaid turvaaspekte, need on esitatud moodulites NET.3.3 *Virtuaalne privaatvõrk (VPN)*, ning OPS1.4 *Kaitse kahjurprogrammide eest*. Selles moodulis ei käsitleta välise serveriteenuse konkreetseid turbevõimalusi (nt pöördproksi (ingl *reverse proxy*) või veebitulemüür).

Taristu turvaaspektid (nt sobiv paigaldus või elektritoide) on esitatud mooduligrupis INF *Taristu*. Tulemüüride puhul rakendatakse täiendavalt üldisi turvameetmeid moodulitest ORP.4 *Identiteedi ja õiguste haldus*, OPS.1.1.2 *IT-haldus* ja OPS.1.1.3 *Paiga- ja muudatusehaldus*.

2 Ohud

2.1 Hajus ummistusrünne (DDoS)

Hajusa ummistusründe (ingl *distributed denial-of-service attack*, *DDoS attack*) puhul tekitab suur hulk töötlemist vajavaid pakette või sõnumeid häireid tulemüüri (ingl *firewall*) töös. Hajusa ummistusründe saab korraldada nt TCP SYN-tulva (ingl *SYN flood*) või UDP-tulva (ingl *UDP flood)* abil. Ummistusründe tagajärjel halveneb võrguteenuste kättesaadavus.

2.2 Manipuleerimine

Kui ründajal õnnestub saada tulemüürile või tulemüüri haldusliidesele juurdepääs, saab ta tulemüüri seadistust meelevaldselt manipuleerida. Ründaja saab muuta konfiguratsiooni (nt tulemüürireegleid muutes lubada Internetist juurdepääs sisevõrgule), käivitada täiendavaid teenuseid või paigaldada kahjurvara. Samuti saab ta manipuleeritavas süsteemis sideühendusi pealt kuulata või käivitada ummistusründe.

2.3 Tulemüürireeglite piirangust möödumine

Tulemüüriga kaitstud võrgusektsioonidele ligi pääsemiseks ja tulemüüri kaitsemehhanismidest läbitungimiseks võib ründaja algatada killuründe (ingl *fragmentation attack*) või kasutada ära võrguprotokollide nõrkusi.

2.4 Tulemüüri konfigureerimis- ja hooldusvead

Tulemüüri konfiguratsioonil ja tulemüüri haldusel on oluline tähtsus IT-süsteemide ja äriprotsesside turvalisuse tagamisel. Valesti seatud tulemüürireeglid võivad blokeerida IT-süsteemi võrkupääsu ja tekitada käideldavusprobleeme. Väär tulemüüri konfiguratsioon võib jätta sisevõrgu välise ründaja vastu täiesti ilma kaitseta. Halvimal juhul võib ründaja saada juurdepääsu sisevõrgu ressurssidele.

3 Meetmed

3.1 Elutsükkel

Kavandamine

NET.3.2.M1 Tulemüüride turvajuhend

Soetus

NET.3.2.M15 Tulemüüri hankimise kord

Evitus

NET.3.2.M4 Tulemüüri turvaline konfigureerimine

NET.3.2.M8 Dünaamilise marsruutimise keelamine

NET.3.2.M14 Tulemüüri käidudokumentatsioon

Käitus

NET.3.2.M2 Tulemüürireeglid

NET.3.2.M3 Sobivad filtreerimisreeglid paketifiltris

NET.3.2.M6 Haldusliideste turve

NET.3.2.M9 Tulemüüri logimine

NET.3.2.M10 Killuründe tõrje paketifiltris

NET.3.2.M16 Turvaline P-A-P-struktuur (paketifilter-rakenduslüüs-paketifilter)

NET.3.2.M17 IPv4 või IPv6 desaktiveerimine

NET.3.2.M18 Tulemüüri haldusvõrgu eraldamine

NET.3.2.M19 UDP-tulva ja TCP SYN-tulva ning järjenumbri äraarvamise tõrje paketifiltris

NET.3.2.M22 Tulemüüri kellaaja sünkroniseerimine

NET.3.2.M23 Tulemüüri seire ja seiretulemuste analüüs

NET.3.2.M24 Läbivaatused ja läbistustestimised

Avariivalmendus

NET.3.2.M7 Tulemüüri avariijuurdepääs

NET.3.2.M32 Tulemüüri avariivalmendus

Lisanduvad kõrgmeetmed

NET.3.2.M20 Põhiliste Interneti protokollide turve

NET.3.2.M21 Andmeliikluse ajutine dekrüpteerimine

NET.3.2.M25 Tervikluskaitstud konfiguratsioonifailid

NET.3.2.M26 Funktsioonilaienduste väljasttellimine

NET.3.2.M27 Erinevad operatsioonisüsteemid ja tulemüüritooted mitmeastmelises tulemüüri arhitektuuris

NET.3.2.M28 Aktiivsisu keskne filtreerimine

NET.3.2.M29 Kõrgkäideldavuse tagamise vahendid

NET.3.2.M30 Ärikriitiliste rakenduste jõudluse haldus

NET.3.2.M31 Sertifitseeritud tooted

3.2 Põhimeetmed

NET.3.2.M1 Tulemüüride turvajuhend [infoturbejuht]

a. Organisatsiooni üldise turvapoliitika alusel on kehtestatud tulemüüride (ingl *firewall*) turvajuhend, milles on esitatud tulemüüride turvalise käituse nõuded.

b. Kõik tulemüüride eest vastutajad tunnevad ja järgivad tulemüüride turvajuhendit.

c. Lahknevused turvajuhendist ja turvajuhendi muudatused kooskõlastatakse infoturbejuhiga ning dokumenteeritakse.

d. Tulemüüride turvajuhendi järgimist kontrollitakse regulaarselt.

NET.3.2.M2 Tulemüürireeglid

a. Kogu sisevõrgust väljuv andmeliiklus on suunatud läbi tulemüüri. Lubamatute ühenduste loomine turvatud võrgust väljapoole on blokeeritud.

b. Väljastpoolt kaitstavasse võrku tehtud lubamatud ühendumiskatsed blokeeritakse. Ühelgi välisel IT-süsteemil ei ole tulemüüri kaudu juurdepääsu otse sisevõrku (vt NET.1.1 *Võrgu arhitektuur ja lahendus*).

c. Tulemüüride tarbeks on kehtestatud selged reeglid, mis määravad, milline sisevõrgu liiklus ja millised ühendused sisevõrgust välja (nt erinevatele teenusserveritele) on

lubatud. Kõik võrguühendustaotlused on tulemüüris lubatud valge nimekirja (ingl *whitelisting*) põhimõttel.

d. Kõik erandid ja muudatused tulemüürireeglites dokumenteeritakse koos põhjendustega. Erandid ja muudatused kooskõlastatakse enne tulemüürireeglite rakendamist.

e. Organisatsioonis on määratud isikud, kes tohivad tulemüürireegleid muuta ning on määratud vastutaja, kes kinnitab tulemüürireeglite muudatused.

f. Võimalikud tulemüürireeglite eranditest tulenevad turvanõrkused korvatakse konkreetsete rakenduste või IT-süsteemide spetsiifiliste turvameetmetega.

NET.3.2.M3 Sobivad filtreerimisreeglid paketifiltris

a. Paketifiltri (ingl *packet filter*) pakettide filtreerimisreeglid on kehtestatud ja kasutusele võetud lähtuvalt meetmest NET.3.2.M2 *Tulemüürireeglid.*

b. Paketifilter tõkestab kõik vigased TCP-lippude (ingl *TCP flag*) kombinatsioonid.

c. Tulemüüris on rakendatud reeglid TCP andmevoo, UDP datagrammide ja ICMP sõnumite filtreerimiseks dünaamilise paketifiltriga (ingl *dynamic packet filtering, stateful packet inspection*).

NET.3.2.M4 Tulemüüri turvaline konfigureerimine

a. Enne kasutuselevõttu on tulemüür konfigureeritud turvaliseks, lubatud on ainult vajalikud teenused.

b. Kõik konfiguratsioonimuudatused dokumenteeritakse (vt NET.3.2.A14 *Käidudokumentatsioon*).

c. On kasutusel meetmed konfiguratsioonifailide tervikluse tagamiseks.

d. Tulemüürile juurdepääsu paroolid on hoolikalt turvatud, nt. kaitstud krüptovahenditega (vt CON.1 *Krüptokontseptsioon*).

e. Tarbetud teenused ja tarbetu lisafunktsionaalsus on tulemüüris desaktiveeritud või desinstallitud. Tulemüüri lisafunktsionaalsuse kasutuselevõtt toimub põhjendatud vajaduse alusel, vastavad otsused on dokumenteeritud.

f. Tulemüüride konfiguratsiooniandmed ja seadistuse dokumentatsioon on kaitstud väliste isikute juurdepääsu eest.

NET.3.2.M6 Tulemüüri haldusliideste turve

a. Halduspääs tulemüüri on võimalik ainult määratud IP-aadressilt või IP-aadresside vahemikult.

b. Tulemüüri haldusliidestele ei ole juurdepääsu ebausaldatavaist võrkudest.

c. Tulemüüri kohtvõrgu haldusühenduste (ingl *in-band management*) protokollid on turvalised. Alternatiivina võib kasutada haldusotstarbeks eraldatud (lisakanaliga) haldusvõrku (ingl *out-of-band management*)).

d. Haldusliideste kasutamiseks on seatud sobivad ajapiirangud.

NET.3.2.M7 Tulemüüri avariijuurdepääs

a. Võrgu mittetoimimisel on haldajail võimalik tulemüüri hallata lokaalse otsepääsu kaudu.

NET.3.2.M8 Dünaamilise marsruutimise keelamine

a. Tulemüüri dünaamiline marsruutimine on desaktiveeritud (välja arvatud siis, kui paketifiltrit kasutatakse mooduli NET.3.1 *Ruuterid ja kommunikaatorid* kohaselt ruuterina).

NET.3.2.M9 Tulemüüri logimine

a. Tulemüüris logitakse vähemalt järgmised turvasündmused:
   - tulemüüri haldusliidesesse sisselogimised;
   - tulemüüri konfiguratsioonimuudatused;
   - blokeeritud võrguühendustaotlused (IP-lähteaadressid ja IP-sihtaadressid, lähte- ja sihtpordid või ICMP/ICMPv6 tüüp, kuupäev, kellaaeg);
   - ebaõnnestunud juurdepääsukatsed süsteemiressurssidele (autentimisvigade või õiguste puudumise tõttu);
   - tulemüüriteenuste veateated;
   - üldised tulemüüri veateated.
b. Tulemüüris tehtud toimingud logitakse võimalusel automaatselt.
c. Turvaprokside kasutamisel logitakse vähemalt protokolli või pääsuloendi (ingl *access control list,* ACL) nurjunud autentimiskatsed, sh teenus, IP-lähteaadressid ja IP-sihtaadressid, lähte- ja sihtpordid, kuupäev ja kellaaeg.

NET.3.2.M10 Killuründe tõrje paketifiltris

a. Protokollide IPv4 ja IPv6 killuründe (ingl *fragmentation attack*) tõrjeks on paketifiltris rakendatud turvamehhanismid.

NET.3.2.M14 Tulemüüri käidudokumentatsioon

a. Kõik tulemüüri turvalisust mõjutavad toimingud (sh tulemüüri reeglid, konfiguratsiooni ja süsteemiteenuste muudatused) lisatakse käidudokumentatsiooni (ingl *operational documentation*).
b. Kõik muudatused tulemüürireeglites dokumenteeritakse koos muudatuse põhjendusega.
c. Dokumentatsioon on kaitstud lubamatu juurdepääsu eest.

NET.3.2.M15 Tulemüüri hankimise kord

a. Enne hankimist on tulemüüri sobivuse hindamiseks koostatud nõuete spetsifikatsioon.
b. Tulemüüri valikul arvestatakse infoturvapoliitikast ja kaitsetarbest tulenevaid nõudeid.
c. IPv6 protokolli kasutamisel võimaldab paketifilter IPv6 laiendpäiste (ingl *IPv6 extention header*) kontrolli ja IPv6 konfigureerimist protokollile IPv4.

NET.3.2.M22 Tulemüüri kellaaja sünkroniseerimine

a. Tulemüüri kellaaeg sünkroniseeritakse turvalise NTP-serveriga.
b. Kellaaja sünkroniseerimine muude väliste allikatega on tulemüüris blokeeritud.

3.3 Standardmeetmed

NET.3.2.M16 Turvaline P-A-P-struktuur (paketifilter-rakenduslüüs-paketifilter)

a. P-A-P-struktuur (paketifilter-rakenduslüüs-paketifilter) on rajatud omavahel riist- ja tarkvaraliselt ühilduvatest komponentidest.

b. Põhilised protokollid kasutavad OSI rakenduskihi tasemel turvaproksit (ingl *application level proxy*). TCP ja UDP puhul kasutatakse vähemalt üldist turvaproksit (ingl *generic proxy*).

NET.3.2.M17 IPv4 või IPv6 desaktiveerimine

a. Võrgusegmendis IPv4 või IPv6 protokolli mittekasutamisel on vastav protokoll tulemüüri liideses desaktiveeritud.

NET.3.2.M18 Tulemüüri haldusvõrgu eraldamine

a. Tulemüüre hallatakse üksnes eraldi haldusvõrgu kaudu (lisakanaliga haldus (ingl *out-of-band management*)). Tulemüüri haldusliidesed andmesidevõrgus (ingl *in-band management*) on desaktiveeritud.

b. Halduse andmeside on tulemüüris piiratud haldusprotokolli ja määratud lähte- ja sihtaadressidega. Kõik ebaturvalised haldusprotokollid on desaktiveeritud (vt NET.1.2 *Võrguhaldus*).

c. Tulemüüris on aktiveeritud haldusühenduste kasutajate autentimise, andmete tervikluse tagamise ja krüpteerimise turvamehhanismid.

NET.3.2.M19 UDP-tulva ja TCP SYN-tulva ning järjenumbri äraarvamise tõrje paketifiltris

a. Ebausaldusväärsest võrgust juurdepääsetavaid serveriteenuseid kaitstakse poolavatud ja avatud kätluskatsete (ingl *handshake)* tulva (ingl *flood*) eest UDP-andmevooge piirava paketifiltriga.

b. Paketifiltris on väljuvate ühenduste tarbeks aktiveeritud TCP protokolli algse järjenumbri (ingl *initial sequence number*, ISN) genereerimine (välja arvatud siis, kui see on teostatud turvaproksis).

NET.3.2.M23 Tulemüüri seire ja seiretulemuste analüüs

a. Organisatsiooni IT-süsteemide seire kontseptsioon sisaldab tulemüüride seiret.

b. On määratud, milliseid logisid analüüsitakse ja kas seda tehakse regulaarselt, pisteliselt või üksnes juhtumipõhiselt.

c. Tulemüüri haldajaid teavitatakse automaatselt järgmistel juhtudel:

- eelnevalt määratletud piirväärtuste ületamisel;
- vigade ja tõrgete esinemisel;
- eelnevalt määratletud sündmuste toimumise korral.

d. Tulemüüri logiandmeid ja olekuteateid edastatakse üksnes turvaliste edastusteede kaudu.

NET.3.2.M24 Läbivaatused ja läbistustestimised

a. Tulemüüri (või tulemüürisüsteemi) testitakse teadaolevate turvaprobleemide suhtes regulaarselt.

b. Tulemüüri turbe läbivaatusi tehakse regulaarselt, läbivaatuse tulemused dokumenteeritakse.

NET.3.2.M32 Tulemüüri avariivalmendus

a. Tulemüüri avariivalmendus on osa organisatsiooni üldisest avariivalmenduse kontseptsioonist (vt DER.4. *Avariihaldus*).

b. Tulemüüri konfiguratsioonid on varundatud ja nende taaste on lisatud taasteplaanidesse.

c. Avariivalmenduse dokumentatsioon ja tegevusjuhendid on kättesaadavad ka paberkujul.

d. Tulemüüri avariiprotseduure harjutatakse regulaarselt.

3.4 Kõrgmeetmed

NET.3.2.M20 Põhiliste Interneti protokollide turve (C)

a. Protokollide HTTP, SMTP ja DNS ja nende krüpteeritud versioonide andmeliiklus on marsruuditud läbi protokollispetsiifiliste turvaprokside.

NET.3.2.M21 Andmeliikluse ajutine dekrüpteerimine (C-I)

a. Krüpteeritud ühendused ebausaldusväärsetesse võrkudesse dekrüpteeritakse ajutiselt protokolli verifitseerimiseks ja edastavate andmete kontrollimiseks kahjurvara suhtes.

b. Dekrüpteeritud andmete kasutamisel järgitakse õiguslikke raamtingimusi.

c. Andmeliiklust ajutiselt dekrüpteeriv komponent tõkestab aegunud ja/või ebaturvalised krüpteerimistehnoloogiad (nt SSL) ja aegunud ja/või ebaturvalised krüptoalgoritmid (nt DES, MD5, SHA1).

d. TLS-proksi kontrollib sertifikaatide usaldusväärsust. Kui kasutatud sertifikaat ei ole usaldusväärne, tõkestatakse ühendus.

NET.3.2.M25 Tervikluskaitstud konfiguratsioonifailid (C-I)

a. Pärast tulemüüri avariijärgset taastet või taaskäivitust kasutatakse ainult viimast veatut konfiguratsiooni ja viimati uuendatud pääsuloendit.

b. Ülaltoodu kehtib ka siis kui tulemüüri on taaskäivitanud ründaja.

NET.3.2.M26 Funktsioonilaienduste väljasttellimine (C-I-A)

a. Tulemüüri funktsioonilaiendused tellitakse ainult spetsialiseeritud riist- ja tarkvarana.

NET.3.2.M27 Erinevad operatsioonisüsteemid ja tulemüüritooted mitmeastmelises tulemüüri arhitektuuris (C-I)

a. Et vähendada ühe toote võimaliku nõrkuse mõju, kasutatakse mitmeastmelise tulemüüri puhul väliste ja sisemiste tulemüüride juures erinevaid operatsioonisüsteeme ja tulemüüritooteid.

NET.3.2.M28 Aktiivsisu keskne filtreerimine (C-I)

a. Veebiliikluse aktiivsisu (ingl *active content*) filtreeritakse keskselt, krüpteeritud andmeliikluse kontrollimiseks andmed ajutiselt dekrüpteeritakse.

b. Turvaproksid võimaldavad aktiivsisu filtreerimist.

NET.3.2.M29 Kõrgkäideldavuse tagamise vahendid (A)

a. Paketifiltrid, rakenduslüüsid, ruuterid ja muud aktiivkomponendid (nt kommutaatorid) on kavandatud piisava liiasusega.

b. Välisvõrguühendusteks kasutatakse kahte üksteisest sõltumatut lahendust (nt erinevate Interneti teenuse pakkujate lahendusi).

c. Pärast avarii-ümberlülitust säilitab tulemüür vastavuse turvajuhendis esitatud nõuetele.

d. Käideldavuse seire põhineb rohkem kui ühel parameetril ja kriteeriumil. Logiandmeid ja hoiatusteateid kontrollitakse regulaarselt.

NET.3.2.M30 Ärikriitiliste rakenduste jõudluse haldus (A)

a. Võrgulüüsides ja võrgusegmentide vahelistes üleminekutes kasutatakse jõudluse halduse võimekusega paketifiltreid.

NET.3.2.M31 Sertifitseeritud tooted (C-I)

a. Tulemüürid on sertifitseeritud vähemalt *Common Criteria* tasemel EAL4 või sellega võrreldava muu turvahindamise põhjal.

4 Lisateave

Lühend	Publikatsioon
[NIST]	NIST Special Publication 800-41 „Guidelines on Firewalls and Firewall Policy“

NET.3.3 Virtuaalne privaatvõrk (VPN)

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed virtuaalse privaatvõrgu (ingl *virtual private network*, VPN) turvaliseks kavandamiseks, rakendamiseks ja käituseks.

1.2 Vastutus

Virtuaalse privaatvõrgu (VPN) meetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Infoturbejuht.

1.3 Piirangud

Moodulis käsitletakse üksnes OSI mudeli kihtidel 2 (lülikiht (ingl *data link layer*)) kuni 4 (transpordikiht (ingl *transport layer*)) põhinevaid virtuaalse privaatvõrgu süsteeme.

Turvalise võrgu loomist käsitletakse moodulis NET.1.1 *Võrgu arhitektuur ja lahendus*. Virtuaalse privaatvõrgu käitusega seotud protsesse kirjeldatakse moodulites OPS.1.1.3 *Paiga- ja muudatusehaldus*, ORP.3 *Infoturbe teadlikkuse suurendamine ja koolitus*, CON.1

Krüptokontseptsioon, CON.3 *Andmevarunduse kontseptsioon*, DER.4 *Avariihaldus* ja OPS.1.2.5 *Kaughooldus*.

VPN otspunktide operatsioonisüsteemide turvalist seadistamist esitavad moodulid SYS.1.1 *Server üldiselt* või SYS.2.1 *Klientarvuti üldiselt*.

2 Ohud

2.1 Virtuaalse kohtvõrgu rakenduskava puudumine või puudulikkus

Hooletult kavandatud, rajatud või seadistatud virtuaalne privaatvõrk võib sisaldada turvanõrkusi. Ründaja saab nõrkusi ära kasutada organisatsiooni konfidentsiaalsele teabele juurde pääsemiseks.

Ebapiisava kasutajakoolituse tõttu kasutatakse VPN-i ebaturvalises keskkonnas või luuakse ühendus VPN-iga ebaturvalisest klientarvutist. See võimaldab ründajal saada juurdepääsu organisatsiooni võrgule.

Kui IT-talitusel puudub VPN-i ühenduste üle kontroll, ei suudeta VPN-i väärkasutust või VPN-i kaudu tehtud rünnet õigeaegselt avastada ja ründaja võib pikaks ajaks märkamatuks jääda.

2.2 Ebaturvaline virtuaalse kohtvõrgu teenuseandja

Kui organisatsioon kasutab VPN-lahenduseks teenuseandjat, on võimalik, et teenuseandja IT-süsteemide ründaja saab juurdepääsu ka teenuseandja klientseadmete sisevõrgule ning kasutab juurdepääsu klientseadmetes olevate andmete sihipäraseks varastamiseks.

2.3 VPN klientrakenduse ebaturvaline seadistus

Kui VPN klientrakendus ei ole turvaliselt konfigureeritud, võib juhtuda, et selle turvamehhanisme kasutatakse puudulikult või ei kasutata üldse. Kui kasutaja saab muuta VPN klientrakenduse konfiguratsiooni või kasutada VPN-lahenduseks oma valitud tarkvara, muudab see ühenduse ebaturvaliseks.

2.4 VPN-komponentide ebaturvaline tüüpseadistus

VPN-komponentide tüüpseadistus ei pruugi vastata andmete kaitsetarbele. Kui esikohale seatakse lahenduse kasutusmugavus ja lihtne paigaldus (nt jäetakse muutmata tootja vaikeparoolid), võib tüüpseadistus sisaldada ründaja jaoks lihtsalt ära kasutatavaid nõrkusi. Ründajal võib tekkida võimalus juurdepääsuks organisatsiooni kohtvõrgule.

3 Meetmed

3.1 Elutsükkel

Kavandamine

NET.3.3.M1 Virtuaalse privaatvõrgu rakendamise kava

NET.3.3.M6 Virtuaalse privaatvõrgu nõuete analüüs

NET.3.3.M7 Virtuaalse privaatvõrgu tehnilise teostuse kava

NET.3.3.M8 Virtuaalse privaatvõrgu turvalise kasutamise juhend

Soetus

NET.3.3.M2 Virtuaalse privaatvõrgu teenuseandja valimine

NET.3.3.M9 Virtuaalse privaatvõrgu toodete valimise kord

Evitus

NET.3.3.M3 Virtuaalse privaatvõrgu seadmete turvaline installimine

NET.3.3.M4 Virtuaalse privaatvõrgu turvaline seadistus

NET.3.3.M10 Virtuaalse privaatvõrgu turvaline käitus

NET.3.3.M13 VPN-komponentide integreerimine tulemüüriga

Käitus

NET.3.3.M5 Tarbetute virtuaalse privaatvõrgu juurdepääsude tõkestamine

NET.3.3.M11 Välisvõrgu turvaline ühendamine

NET.3.3.M12 Virtuaalse privaatvõrgu kasutajate pääsuhaldus

Lisanduvad kõrgmeetmed

NET.3.3.M13 VPN-komponentide integreerimine tulemüüriga

3.2 Põhimeetmed

NET.3.3.M1 Virtuaalse privaatvõrgu rakendamise kava

a. Enne virtuaalse privaatvõrgu (ingl *virtual private network*, VPN) kasutuselevõttu on organisatsioon hinnanud virtuaalse privaatvõrgu vajadust.

b. Enne virtuaalse privaatvõrgu kasutuselevõttu on määratud:

- virtuaalse privaatvõrgu käitusega seotud töötajate kohustused;
- VPN-i kasutajarühmad ja nende õigused;
- Pääsuõiguste andmise, muutmise ja tühistamise kord.

NET.3.3.M2 Virtuaalse privaatvõrgu teenuseandja valimine [infoturbejuht]

a. Virtuaalse privaatvõrgu teenuseandjaga on sõlmitud teenustasemelepped (ingl *service level agreement*, SLA) ja need on dokumenteeritud.

b. VPN-teenuseandjaga kokkulepitud teenusetasemelepingu täitmist kontrollitakse regulaarselt.

NET.3.3.M3 Virtuaalse privaatvõrgu seadmete turvaline installimine

a. Kui kasutatakse spetsiaalseid VPN-seadmeid, on seadmetel kehtiv hooldusleping.

b. VPN-komponente installivad üksnes töötajad, kellel on installimiseks vajalik kvalifikatsioon.

c. VPN-komponentide installimise käik ja kõrvalekalded installijuhendist dokumenteeritakse.

d. Virtuaalse privaatvõrgu funktsionaalsust ja turvamehhanismide toimimist testitakse enne virtuaalse kohtvõrgu kasutuselevõttu.

NET.3.3.M4 Virtuaalse privaatvõrgu turvaline seadistus

a. Kõigi virtuaalse privaatvõrgu klientseadmete, serverite ja ühenduste jaoks on spetsifitseeritud ja dokumenteeritud turvaline konfiguratsioon.

b. Virtuaalse privaatvõrgu haldaja kontrollib regulaarselt IT-süsteemide VPN seadistuse turvalisust. Vajadusel muudetakse VPN-i konfiguratsiooni.

NET.3.3.M5 Tarbetute virtuaalse privaatvõrgu juurdepääsude tõkestamine

a. Regulaarselt kontrollitakse, kas virtuaalsesse kohtvõrku pääsevad üksnes volitatud IT-süsteemid ja kasutajad.

b. Tarbetud virtuaalse kohtvõrgu juurdepääsud desaktiveeritakse võimalikult kiiresti.

c. Virtuaalse kohtvõrgu juurdepääs on lubatud ainult ettenähtud kasutusajaks.

3.3 Standardmeetmed

NET.3.3.M6 Virtuaalse privaatvõrgu nõuete analüüs

a. Virtuaalse privaatvõrgu vajaduse hindamisele (vt NET.3.3.M1 *Virtuaalse privaatvõrgu rakendamise kava*) tuginedes on läbi viidud virtuaalse privaatvõrgu riist- ja tarkvarakomponentide nõuete analüüs.

b. Virtuaalse privaatvõrgu nõuete analüüsis on arvesse võetud järgmist:

- hõlmatavad äriprotsessid;
- juurdepääsukanalid;
- identifitseerimis- ja autentimisprotseduurid;
- kasutajad ja kasutajaõigused;
- vastutused ja kohustused;
- teatamisteed.

NET.3.3.M7 Virtuaalse privaatvõrgu tehnilise teostuse kava

a. On koostatud virtuaalse privaatvõrgu tehnilise teostuse kava, mis määrab:

- võrgu topoloogia;
- VPN pääsupunktid;
- krüpteerimismeetodid ja -vahendid;
- lubatavad pääsuprotokollid,
- teenused ja ressursid.

b. On määratletud alamvõrgud, millele on VPN-i kaudu juurdepääs.

NET.3.3.M8 Virtuaalse privaatvõrgu turvalise kasutamise juhend [infoturbejuht]

a. Virtuaalse privaatvõrgu kasutajate jaoks on koostatud virtuaalse privaatvõrgu turvalise kasutamise juhend.

b. Kasutajad on virtuaalse privaatvõrgu turvalise kasutamise osas koolitatud.

c. Töötajale VPN-pääsu loomisel õpetatakse teda VPN-i kasutama.

d. Kõik virtuaalse privaatvõrgu kasutajad on kohustatud virtuaalse privaatvõrgu turvalise kasutamise juhendit järgima.

NET.3.3.M9 Virtuaalse privaatvõrgu toodete valimise kord

a. Virtuaalse privaatvõrgu toodete valimisel on arvestatud organisatsiooni vajadusi erinevates asukohtades ja allüksustes, sealhulgas mobiilkasutajate ja kaugtöötajate vajadusi.

NET.3.3.M10 Virtuaalse privaatvõrgu turvaline käitus

a. On dokumenteeritud virtuaalse privaatvõrgu turvalise käituse (ingl *operation*) põhimõtted, milles on sätestatud virtuaalse privaatvõrgu:
   - kvaliteedihaldus;
   - järelevalve;
   - hooldus;
   - koolitus;
   - õiguste haldus.

NET.3.3.M11 Välisvõrgu turvaline ühendamine

a. VPN ühenduse loomisel kasutatakse piisavalt turvalist autentimist. Võimalusel kasutatakse mitmikautentimist (ingl *multifactor authentication*).

b. VPN-ühenduse saab luua ainult määratud IT-süsteemide ja teenuste vahel.

c. VPN-ühenduse andmevahetusprotokollid on sobivad ja turvalised.

NET.3.3.M12 Virtuaalse privaatvõrgu kasutajate pääsuhaldus

a. Virtuaalse privaatvõrgu kasutajate pääsuhaldus on tsentraliseeritud ja sellega tegeletakse järjepidevalt.

b. Pääsuõiguste halduse servereid hallatakse turvaliselt ning kaitstult lubamatu juurdepääsu eest.

3.4 Kõrgmeetmed

NET.3.3.M13 VPN-komponentide integreerimine tulemüüriga (C-I)

a. Virtuaalse privaatvõrgu andmeliiklust on võimalik kontrollida ja filtreerida.

b. VPN-i komponentide integratsioon tulemüüriga (ingl *firewall*) on dokumenteeritud.

4 Lisateave

Lühend	Publikatsioon
[ISO]	ISO/IEC 27033-5:2013 „Information technology – Security techniques – Network security – Part 5: Securing communications across networks using Virtual Private Networks (VPNs)“

NET.3.4 Võrkupääsu reguleerimine (NAC)

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed klientseadmete võrkupääsu reguleerimiseks (ingl *network access control*, NAC). turvaliseks kavandamiseks, rakendamiseks ja käituseks.

NAC võimaldab võrgule juurdepääsu läbi turvalise autentimise ja volitamise. Selleks kasutatakse standardil IEEE 802.1X (keskne autentimisserver või RADIUS-server) või MAC-aadressidel põhinevat autentimist.

1.2 Vastutus

Võrkupääsu reguleerimise (NAC) meetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Organisatsiooni juhtkond.

1.3 Piirangud

Moodul käsitleb NAC-lahenduse üldise seadistamise, autentimise, volitamise ja haldamise meetmeid. Kui meede käsitleb konkreetset IT-komponenti (nt RADIUS-server), siis on komponent meetmes nimetatud.

Moodulit täiendavad meetmed moodulitest APP.2.1 *Kataloogiteenus üldiselt* ja NET.1.1 *Võrgu arhitektuur ja lahendus*. Raadiokohtvõrgu (WLAN) seadmeid käsitletakse moodulites NET.2.1 *Raadiokohtvõrgu käitamine* ja NET.2.2 *Raadiokohtvõrgu kasutamine*.

Moodul ei hõlma järgmist:

- võrgukomponentide üldised aspektid ja võrguportide turvalisus (vt. NET.3.1 *Ruuter ja kommutaator*);
- IEEE 802.1X protokolli mittekasutavad NAC erilahendused;
- RADIUSe rakendamine võrgukomponentides (kommutaatorid, WLAN-i pääsupunktid või WLAN-i kontrollerid);
- lõppseadmete turve (vt mooduligruppe SYS.2 *Klientarvutid*, SYS.3 *Mobiilseadmed* ja SYS.4 *Muud süsteemid*);
- serverite (vt SYS.1.1 *Server üldiselt*) ja virtualiseerimise üldine turve (vt SYS.1.5 *Virtualiseerimissüsteem*);
- Identiteedi ja volituste haldamise üldaspektid (vt ORP.4 *Identiteedi- ja õiguste haldus*).

2 Ohud

2.1 NAC-lahenduse puudulik kavandamine

Võrguühendust omavatest seadmetest ülevaadet omamata võivad vajalikud seadmed jääda võrguühenduseta või suunatakse nad valesse võrgusegmenti. Puuduliku kavandamise tõttu ei pruugi kasutatavad kommutaatorid toetada NAC-lahenduse nõudeid. RADIUS-serveri ebapiisava jõudluse tõttu ei suuda server üheaegselt teenindada piisavat hulka lõppseadmeid.

Kui autentimise ja volitamise protseduurid on ülemäära piiravad, võib volitatud seadmete võrkupääs olla takistatud. Sama on ka vastupidi, kui protseduurid on ülemäära lubavad, jäävad võimalikud turvameetmed rakendamata.

2.2 Lõppseadmete koordineerimata lisamine NAC-lahendusse

Sobivate orkestreerimistööriistade, protseduurijuhiste puudumine ning mittetäielikud seadmeloendid raskendavad lõppseadmete integreerimist NAC-lahendusega.

Erinevate lahenduste kooskasutus vähendab autentimise kasutajasõbralikkust. Ebatüüpsed ja NAC-lahenduse nõuetele mittevastavad seadmed toovad kaasa ebaturvalised autentimisviisid, kuigi tugevate autentimismeetodite rakendamine oleks võimalik.

Suureneb tõenäosus, et seadmete paigutamisel võrgusegmentidesse tehakse vigu.

2.3 Ebaturvaliste protokollide kasutamine

EAP (Extensible Authentication Protocol) toe puudumisel kasutatakse ebaturvalisi autentimisprotokolle, nt EAP-MD5 või MAC autentimine. Kui nõrkade autentimisprotokollidega lõppseadmetel ei piirata, milliste seadmetega on ühendus lubatud ja milliseid protokolle selleks võib kasutada, lihtsustub võltsimis-, taasesitus- või vahendusrünnete läbiviimine.

2.4 NAC-lahenduse väär konfigureerimine

NAC-lahenduse seadistamisel lõppseadmetes ja kommutaatorites või RADIUS-serveri NAC-reeglite valesti konfigureerimisel võib tekkida viga. Inimlik eksimus võib olla põhjustatud puudulikust protsessijuhendist, töötaja teadmatusest või ajanappusest. Viga võib põhjustada häireid NAC-lahenduse töös, nt lõppseadmed ei pääse ligi vajalikele ressurssidele või neil puudub juurdepääs võrgule.

MAC-aadressi registreerimine valesse võrgusegmenti või eksimine volituste andmisel võib tekitada juurdepääsu andmetele, millele juurdepääsu antud lõppseadme kasutajale pole ette nähtud.

2.5 Konfiguratsioonimuudatuste ebapiisav valideerimine

Kui muudatuste läbiviimisel konfiguratsioonimuudatusi ei kontrollita ega valideerita, võivad tekkida konfiguratsioonivead. Näiteks võib juhtuda, et lõppseadmetel on juurdepääs liiga paljudele ressurssidele või vastupidi, juurdepääsu vajalikele ressurssidele puudub.

Kui kommutaatori portides lülitatakse NAC ilma mõjuva põhjuseta välja, võivad volitamata lõppseadmed saada juurdepääsu võrguressurssidele. Ebapiisav lõppseadmete tarkvarakomponentide valideerimine võib põhjustada häireid andmevahetuses ja mõjutada tarkvara funktsionaalsust.

2.6 Kaitsmata juurdepääs võrgule

Kommutaatori portides NAC-i funktsionaalsuse ajutiselt või püsivalt välja lülitamine mõjutab võrgujuurdepääsu turvalisust. Volitamata isikud või IT-süsteemid võivad saada liigseid õigusi, pääseda loata juurde konfidentsiaalsele teabele ning seda manipuleerida või kustutada.

NAC-i desaktiveerimine ebapiisava kahjurvaratõrje võimekusega seadmetes võimaldab pahavara levimist üle erinevate IT-süsteemide ja võrgusegmentide.

2.7 Keskse NAC-lahenduse komponendi rike

Kesksete NAC-lahenduse komponentide rikkeid põhjustavad vigased NAC-komponendid, väär võrguseadistus, protsesside puudumine või teenusetõkestusründed (ingl *denial-of-service attack*). Lõppseade võib muutuda juurdepääsmatuks. RADIUS-serveri rikke korral oleneb kommutaatori konfiguratsioonist, kas lõppseadmetele antakse seejärel võrgule piiramatu juurdepääs või puudub võrkupääs üldse.

2.8 Ebapiisav isikuandmete kaitse

Isikuandmete kaitse puudulik rakendamine (nt ülemäära pikkade andmesäilitustähtaegade määramine või andmekaitsespetsialisti kooskõlastuse puudumine) võib soodustada

isikuandmete väärkasutust. Näiteks on võimalik lõppseadmeid kasutavaid töötajaid profileerida kasutajaprofiilidesse või nende toiminguid pika aja jooksul jälgida.

3 Meetmed

3.1 Elutsükkel

Kavandamine

NET.3.4.M1 NAC-i kasutuselevõtu otsustamine

NET.3.4.M2 NAC-i kasutuselevõtu kavandamine

NET.3.4.M3 NAC-lahenduse nõuete loend

NET.3.4.M4 NAC-lahenduse rakendusplaan

Evitus

NET.3.4.M8 NAC-spetsiifiliste rollide ja õiguste määratlemine RADIUS-serveris

NET.3.4.M9 NAC pääsuõiguste andmise reeglid

Käitus

NET.3.4.M5 Lõppseadmete halduse kohandamine NAC-lahendusega

NET.3.4.M7 Turvalise autentimise kasutamine lõppseadmetes

NET.3.4.M10 NAC-lahenduse identiteedihaldus

NET.3.4.M11 NAC-lahenduse turvaline konfiguratsioon

NET.3.4.M12 NAC-lahenduse seire

NET.3.4.M13 NAC-lahenduse konfiguratsiooni valideerimine

NET.3.4.M14 Täiendavad meetmed seadme MAC-aadressil põhineval autentimisel

NET.3.4.M15 Kahjurvaratõrje integreerimine NAC-lahendusega

NET.3.4.M16 NAC-lahenduse komponentide sündmuste logimine

NET.3.4.M17 RADIUS-serveri turvaline asukoht võrgus

NET.3.4.M18 NAC-lahenduse üksikasjalik dokumenteerimine

NET.3.4.M19 Turvaline NAC-i identiteedihaldus

Avariivalmendus

NET.3.4.M6 NAC-lahenduse avariivalmendus

Lisanduvad kõrgmeetmed

NET.3.4.M20 MACsec-i kasutamine

NET.3.4.M21 Lõppseadmete vastavuskontroll

NET.3.4.M22 NAC-i kasutamine volituste andmisel

NET.3.4.M23 Autonoomsete RADIUS-serverite kasutamine

NET.3.4.M24 Turvaliste andmesideprotokollide ainukasutus

NET.3.4.M25 NAC-lahenduse integreerimine turvaseirega

NET.3.4.M26 Kesksete NAC-lahenduse komponentide kõrgkäideldavuse tagamine

NET.3.4.M27 MAC-aadressil põhineva autentimise vältimine

3.2 Põhimeetmed

NET.3.4.M1 NAC-i kasutuselevõtu otsustamine [organisatsiooni juhtkond]

a. Organisatsioon on teinud põhjendatud otsuse, kas ja millisel määral NAC organisatsioonis kasutusele võetakse.

b. Enne otsustamist on arvestatud järgnevaga:
   - võrgusegmendid ja võrgukomponendid, millele NAC rakendub;
   - võrgusisesed ja võrguvälised lõppseadmed, mis NACi kasutavad;
   - NAC-i mõju IT-süsteemide toimimisele.

3.3 Standardmeetmed

NET.3.4.M2 NAC-i kasutuselevõtu kavandamine

a. NAC kasutuselevõtu kavandamisel on arvestatud vähemalt järgmisi aspekte:
   - lõppseadmetele, kommutaatoritele (ingl *switch*) ja RADIUS-serverile esitatavad nõuded;
   - seadmeloendite ajakohastamine ja täiendamine;
   - NAC-komponentide hankimise, käituse ja intsidentide halduse protsesside määratlemine;
   - seadmete ümberpaigutamise ja asendamise võimaldamine;
   - NAC-lahenduse seire ja logimine;
   - väliste turvakomponentidega liidestamine (nt tulemüürid, kahjurvaratõrje rakendused, turvanõrkuste skannerid, kesksed turvasündmuste tuvastamise ja raporteerimise süsteemid);
   - täiendavate turvafunktsioonide vajadus (nt profiilianalüüs, lõppseadmete vastavuskontroll, MACsec krüpteerimine).

NET.3.4.M3 NAC-lahenduse nõuete loend

a. NAC-lahenduse komponentide funktsionaalsed nõuded on koondatud ühtsesse NAC nõuete loendisse.

b. NAC nõuded on kõigi mõjutatud osapooltega kooskõlastatud. NAC-komponentide hankimisel, testimisel ja kasutuselevõtuks kinnitamisel arvestatakse esitatud nõudeid.

c. NAC nõuete loendit vaadatakse regulaarselt üle ning uuendatakse vastavalt vajadusele.

NET.3.4.M4 NAC-lahenduse rakendusplaan

a. NAC-lahenduse rakendusplaanis on kirjeldatud lahendusele esitatud nõuetele vastavad käitusprotseduurid ja NAC-komponentide tehnilised spetsifikatsioonid.

b. NAC-lahenduse rakendusplaan on kooskõlas võrgu segmenteerimise põhimõtetega (vt NET.1.1 *Võrgu arhitektuur ja lahendus*).

c. NAC-lahenduse rakendusplaanis on määratletud:
   - võrgusegmendid, kus NAC-i kasutatakse;

- mõjutatud lõppseadmete, kommutaatorite, WLAN-i pääsupunktide (ingl *wireless access point*) ning WLAN-kontrollerite seadete spetsifikatsioonid;
- RADIUSe rakendamine ja NAC-i reeglid;
- integreerimine kasutavate kataloogiteenustega;
- kasutajate autentimine ja volitamine;
- liidestused väliste turvakomponentidega (nt tulemüürid, kahjurvaratõrje rakendused, turvanõrkuste skannerid, kesksed turvasündmuste tuvastamise ja raporteerimise süsteemid);
- lisafunktsioonide kasutamine;

NET.3.4.M5 Lõppseadmete halduse kohandamine NAC-lahendusega

a. Lõppseadmete kasutuselevõtu, asendamise, muudatuste ja rikete halduse protsessid arvestavad NAC-i kasutuselevõtust tulenevaid piiranguid.

b. Lõppseadmete keskse halduse protsess hõlmab NAC-lahenduse toimimiseks vajaliku tarkvara, konfiguratsioonimuudatuste ja autentsustõendite (nt sertifikaatide) paigaldamist ja haldust.

NET.3.4.M6 NAC-lahenduse avariivalmendus

a. NAC-i turvamehhanisme on vastava vajaduse tekkimisel võimalik ajutiselt ning soovitud ulatuses desaktiveerida.

b. RADIUS-serveri mittetoimimise puhuks on koostatud avariivalmenduse stsenaariumid ning kavandatud meetmed negatiivsete toimete maandamiseks.

c. NACi avariivalmenduseks on kaalutud järgmisi võimalusi:
   - aktiivsed võrguühendused säilitatakse (nt korduvautentimise nõude ajutise peatamisega), kuid kõik uued sisselogimiskatsed lükatakse tagasi;
   - dünaamiline võrkulogimine peatatakse. Selle asemel kasutatakse vähemalt kriitiliste vajaduste ulatuses võrgusegmentide vahelisi fikseeritud ühendusi, mis realiseeritakse eeldefineeritud kommutaatoriseadistuste abil;
   - NAC-i kasutamine desaktiveeritakse kas kõigis võrguseadmetes või kommutaatorite üksikutes portides, et võrguühendus saaks jätkuda piiranguteta.

d. RADIUSe avariivalmenduse stsenaariumid on vastavuses organisatsiooni turvapoliitikatega.

NET.3.4.M7 Turvalise autentimise kasutamine lõppseadmetes

a. Lõppseadmetes kasutatakse turvalisi ja ajakohaseid autentimismeetodeid (nt lõppseadme autentimine toimub automaatselt sertifikaatide või juurdepääsulubade alusel).

b. Ebaturvalisi autentimismeetodeid kasutatakse ainult põhjendatud erandjuhtudel. Vastav otsus on dokumenteeritud.

NET.3.4.M8 NAC-spetsiifiliste rollide ja õiguste määratlemine RADIUS-serveris

a. RADIUS-serveri pääsuõiguste andmisel on arvestatud RADIUS-serveri haldamiseks vajalike kasutajarühmade vajadusi.

b. NAC-spetsiifiline juurdepääs RADIUS-serverile on antud järgnevatele kasutajarühmadele:
   - kasutajad, mis haldavad oma võrgupiirkonna kommutaatoreid (RADIUS-kliendid).

- lõppseadmete halduse eest vastutavad kasutajad, kes haldavad seadmeidentiteete (nt MAC-aadresse);
- esmatasandi tugiüksus, mis analüüsib vigaseid RADIUSe taotlusi ja teeb sellest tulenevaid korrektuure.

NET.3.4.M9 NAC pääsuõiguste andmise reeglid

a. NAC-lahenduse jaoks on koostatud reeglid lõppseadmete võrkupääsu lubamiseks.

b. Iga lõppseadme või lõppseadmete grupi kohta on määratletud, kas
   - võrgule on lubatud piiramatu juurdepääs;
   - juurdepääs võrgule on keelatud;
   - seade pääseb ligi ainult piiratud võrgusegmentidele.

c. NAC reeglites on määratud kasutatavad autentimismeetodid, eduka autentimise tingimused ja juurdepääsukontrolli teostamise viis.

NET.3.4.M10 NAC-lahenduse identiteedihaldus

a. NAC-i autentimiseks kasutatakse individuaalseid identiteete. Rohkem kui ühe lõppseadme jaoks loodud identiteedid on lubatud ainult põhjendatud erandjuhtudel.

b. NAC-i autentimiseks vajalik teave on kaitstud volitamata juurdepääsu eest.

NET.3.4.M11 NAC-lahenduse turvaline konfiguratsioon

a. NAC-lahenduse komponentide turvaliseks konfigureerimiseks on välja töötatud turvalised standardkonfiguratsioonid ja protseduurijuhendid.

b. NAC-i lahenduse komponentide seadistuste aja- ja asjakohasust kontrollitakse regulaarselt.

c. Lõppseadmete kasutajate volitused on piiratud määral, et nad ei saaks manipuleerida suplikandi (ingl *supplicant*) ehk ühendust taotleva seadme konfiguratsiooni, seda desaktiveerida ega lugeda NAC-i võtmeid või paroole.

d. NAC-autentimine on kommutaatoris või kommutaatori üksikutes portides desaktiveeritud ainult põhjendatud ja eelnevalt määratletud erandjuhtudel.

NET.3.4.M12 NAC-lahenduse seire

a. Keskne RADIUS-server, kõik autentija (ingl *authenticator*) rollis olevad kommutaatorid ning muud NAC-lahenduse jaoks vajalikud kesksed teenused on integreeritud kesksesse seirelahendusse.

b. Seirelahendusse on lisatud:
   - kõik NAC-spetsiifilised parameetrid, mis tagavad NAC-lahenduse või vastavate teenuste funktsionaalsuse.
   - RADIUS protokolli kasutatavuse kontroll (nt genereerides RADIUS-päringuid kogu NAC-i ahela, sh väliste kataloogiteenuste, kontrollimiseks).
   - kommutaatorite oleku seire NAC-i desaktiveerimise tuvastamiseks.

c. Kõrvalekalletest määratletud olekutest ja piirväärtustest teavitatakse volitatud IT-halduse töötajaid.

NET.3.4.M13 NAC-lahenduse konfiguratsiooni valideerimine

a. NAC-lahenduse konfiguratsiooni õigsuse kontrollimiseks on koostatud valideerimiseesmärgid. Valideerimiseesmärgid arvestavad erinevate NAC-lahenduse komponentide funktsionaalsust ja spetsifikatsioone.

b. NAC-lahenduse komponentide tegeliku konfiguratsiooni võrdlemist soovitud seadistusega viiakse läbi regulaarselt.

NET.3.4.M14 Täiendavad meetmed seadme MAC-aadressil põhineval autentimisel

a. Lõppseadmeid, kus ei ole võimalik kasutada turvalist EAP autentimist ja mis on tuvastatud MAC-aadressi järgi, ei klassifitseerita usaldusväärseteks lõppseadmeteks. Selliste seadmete juurdepääs võrgule on piiratud minimaalselt vajalikuga.

b. Vajadusel rakendatakse andmete kaitseks täiendavaid meetmeid, nt lõppseadmete andmeside piiramine või seadmeprofiilide koostamine.

NET.3.4.M15 Kahjurvaratõrje integreerimine NAC-lahendusega

a. Kõiki lõppseadmeid kontrollitakse kahjurvara avastamiseks enne seadmete organisatsiooni võrku ühendamist ja IT-süsteemidele juurdepääsu võimaldamist.

b. Sobiv kahjurvaratõrje lahendus on seotud NAC-i autentimisega. Kahjurvara avastamisel võetakse NAC-lahenduses kasutusele meetmed kahjurvara leviku tõkestamiseks.

NET.3.4.M16 NAC-lahenduse komponentide sündmuste logimine

a. NAC-lahenduses logitakse NAC-komponentide olekumuudatused ja muud turvalisuse seisukohast olulised sündmused.

b. Täiendavalt logitakse NAC-i kesksete komponentide konfiguratsioonimuudatused.

c. On määratletud kogutavate logide detailsus ja keskses logitaristus talletatavad logid.

d. Logiandmeid edastatakse üle turvaliste andmesidekanalite.

e. Turvakriitilised sündmused (nt RADIUSe katkestus või ebatavaline arv RADIUSe päringuid) käivitavad automaatse alarmeerimise.

NET.3.4.M17 RADIUS-serveri turvaline asukoht võrgus

a. RADIUS-server on paigaldatud kaitstud võrgusegmenti (vt NET.1.1 *Võrguarhitektuur ja lahendus*).

b. Päringud RADIUS-serverisse on lubatud ainult usaldusväärsetest allikatest.

c. RADIUS-server ei suhtle lõppseadmetega otse, vaid ainult kommutaatori autentija (ingl *authenticator*) vahendusel. Kommutaatorite päringuid võetakse vastu ainult määratud haldusvõrgu segmendist.

NET.3.4.M18 NAC-lahenduse üksikasjalik dokumenteerimine

a. NAC-lahendus koos kõigi lahendusse kuuluvate komponentidega on asjakohaselt dokumenteeritud.

b. Dokumentatsioonis on kirjeldatud NAC-lahenduse komponentide ja lõppseadmete konfiguratsioonid ning komponentide vahelised sõltuvused. Dokumentatsiooni on parema arusaamise eesmärgil sobivalt liigendatud.

c. Dokumentatsioon sisaldab NAC-lahendusse sisseehitatud autentimisreeglite lihtsustatud kirjeldust.

d. Dokumentatsiooni hoitakse ajakohasena ja uuendatakse pärast iga muudatuse toimimist.

e. Dokumentatsiooni ajakohasust kontrollitakse regulaarselt.

NET.3.4.M19 Turvaline NAC-i identiteedihaldus

a. NAC-i võrkupääsude kaitseks rakendatakse sobivat identiteedihalduse lahendust.
b. Identiteedihalduse käigus tehakse vähemalt järgmist:
    - sertifikaatide käsitlemine ja kaitse;
    - identiteetide sulgemine ja kustutamine;
    - identiteedi sulgemise protsessi ja kasutatavate liideste kirjeldamine.

3.4 Kõrgmeetmed

NET.3.4.M20 MACsec-i kasutamine (C-I)

a. Andmete terviklikuse ja konfidentsiaalsuse tagamiseks kasutatakse võrgustandardil IEEE 802.1AE põhinevat MACsec (Media Access Control Security) lahendust.
b. On registreeritud kommutaatorid ja lõppseadmed, mis ei toeta MACsec-i või kus ei tohiks MACsec-i kasutada. Välistamise põhjendatust kontrollitakse regulaarselt.

NET.3.4.M21 Lõppseadmete vastavuskontroll (C)

a. Enne lõppseadme ühendamist organisatsiooni võrku ja IT-süsteemidele juurdepääsu andmist kontrollima, kas lõppseade vastab organisatsiooni turvanõuetele.
b. Iga lõppseadme tüübi jaoks on koostatud spetsifikatsioon, millele lõppseade peab vastama. Nõuetele mittevastavate seadmete juurdepääs võrgule on piiratud.
c. NAC-lahendus on integreeritud vastavuskontrolli tööriistaga, mis automaatselt hindab lõppseadmete vastavust. Saadud tulemuse põhjal otsustab NAC-lahendus, kas ja millises ulatuses lõppseade võrku lubatakse.

NET.3.4.M22 NAC-i kasutamine volituste andmisel (C)

a. NAC-lahendus jagab lõppseadmed seadmeprofiili ja kaitsenõuetega alusel eraldi võrgusegmentidesse.
b. On kaalutud, kas NAC-i abil teha lõppseadmete mikrosegmentimist (ingl *microsegmentation*).

NET.3.4.M23 Autonoomsete RADIUS-serverite kasutamine (A)

a. NAC-i rakendamiseks kasutatakse spetsiaalseid ja autonoomseid RADIUS-servereid. RADIUS-server ei paku peale NAC-funktsionaalsuse muid teenuseid, nt VPN-i juurdepääsu reguleerimist.
b. Erinevates võrkudes kasutatakse eraldiseisvaid RADIUS-servereid. On kaalutud vajadust rakendada eraldi RADIUS-serverid kontori -ja tootmisvõrgu tarbeks või paigutada eraldi RADIUS-serverid LAN- ja WLAN võrkudesse.
c. On kaalutud autonoomsete RADIUS-serverite kasutamist eraldiseisvates võrgusegmentides.

NET.3.4.M24 Turvaliste andmesideprotokollide ainukasutus (C)

a. Kesksete NAC-lahenduse komponentide vahelises andmevahetuses ning RADIUS-serveri ja kataloogiteenuse vahelises suhtluses kasutatakse ainult turvalisi protokolle.

b. On analüüsitud, kas RADIUS-serveri ja kommutaatorite vahelises andmevahetuses on võimalik kasutada ainult turvalisi protokolle.

NET.3.4.M25 NAC-lahenduse integreerimine turvaseirega (A)

a. Kesksed NAC-lahenduse komponendid ja NAC-lahenduse poolt kasutatavad kesksed teenused on integreeritud turvaseire lahendusega.

b. NAC-spetsiifilised turvasündmused (nt ühendustaotluste sagedane tagasilükkamine või identiteedi korduv kasutamine) käivitavad automaatse teavituse.

c. Kui organisatsioon kasutab automatiseeritud süsteeme sissetungi tunnuste avastamiseks ja neist alarmeerimiseks (ingl *intrusion detection system*, IDS), on sellesse integreeritud ka NAC-lahenduse komponendid.

NET.3.4.M26 Kesksete NAC-lahenduse komponentide kõrgkäideldavuse tagamine (A)

a. Kesksed NAC-lahenduse komponendid on paigaldatud liiasusega. Ka muud NAC-lahenduse funktsionaalsuse jaoks olulised kesksed teenused on kõrgkäideldavad.

b. Kõrge käideldavuse jaoks olulised parameetrid on integreeritud seire- ja logimissüsteemidega. Oluliste parameetrite oleku muutumisel saadetakse automaatteavitus.

c. RADIUS-serveri mittetoimimise puhuks koostatud avariivalmenduse stsenaariumid ei alanda võrgu turvataset.

NET.3.4.M27 MAC-aadressil põhineva autentimise vältimine (I)

a. MAC-aadressil põhinevat autentimist kasutatakse ainult juhul, kui see on tehniliselt vältimatu, erandi tegemine on põhjendatult vajalik ja võrgu turvapoliitika seda lubab.

NET.4: Side

NET.4.1 Telefonikeskjaam

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed sidesüsteemide turvaliseks kasutamiseks välisvõrguga ühendatud organisatsioonisisese telefonikeskjaama (ingl *private branch exchange*, PBX) ja sellega seotud klientseadmete (lauatelefonide) abil.

Telefonikeskjaama abil saab ühendada organisatsiooni telefone organisatsioonisiseseste ja organisatsioonivälistе abonentidega (nt analoogtelefonivõrgu kaudu).

1.2 Vastutus

Telefonikeskjaama meetmete täitmise eest vastutab vastutav spetsialist.

Lisavastutajad
IT-talitus, ülemus.

1.3 Piirangud

IP-telefoni komponentide ja IP-telefoni kaudu toimuva kõneedastuse turvaaspekte käsitletakse täpsemalt moodulis NET.4.2 *IP-telefon (VoIP)*.

Telekommunikatsioonisüsteemide puhul arvestatakse täiendavalt mooduleid ORP.4 *Identiteedi ja õiguste haldus*, OPS.1.2.5 *Kaughooldus*, CON.3 *Andmevarunduse kontseptsioon* ja OPS.1.1.5 *Logimine*.

2 Ohud

2.1 Sidesüsteemi pealtkuulamine

Kui telefonikõnesid edastatakse krüpteerimata kujul, kaasneb oht, et ründaja võib kõnesid pealt kuulata. Telefonikeskjaamal on olemas funktsionaalsus, mis võimaldab telefonikõnesid märkamatult pealt kuulata. Selliste tavaolekus blokeeritud funktsioonide aktiveerimine nõuab süsteemist täpsemaid teadmisi, kuid Internetis vabalt kättesaadavate juhiste tõttu ei ole see keerukas.

2.2 Ruumide pealtkuulamine sidesüsteemi kaudu

Ruumides toimivat on võimalik sideseadmete mikrofonide kaudu pealt kuulata.

Seadmesse integreeritud mikrofoniga intelligentseid klientseadmeid, nagu näiteks automaatvastajaid, aga ka arvuteid, pihuarvuteid ja mobiiltelefone, on võimalik avaliku võrgu või kohtvõrgu kaudu manipuleerida. Sisse ehitatud mikrofoni saab aktiveerida ilma selle omaniku teadmata (nt käivitada telefoni „beebimonitori“ funktsioon).

Olemasolevasse sidesüsteemi võib ründaja lisada spetsiaalse pealtkuulamisseadme. Sellisel viisil täiendatud sidesüsteemi on võimalik ära kasutada näiteks ruumides toimuva vestluse pealtkuulamiseks.

2.3 Sideteenuse vargus

Sideteenuse varguse eesmärk on kanda tehtud telefonikõnede või andmeedastuse kulud üle kolmandale isikule. Sidesüsteemi kuritarvitamiseks on võimalik väärkasutada sidesüsteemi olemasolevaid funktsioone. Selleks sobivad näiteks kaugprogrammeeritavad kõnesuunamised või sissehelistusvalikud.

Telefonikeskjaama on võimalik seadistada nii, et sissetulevad „välisliinid“ ühendatakse väljaminevate „välisliinidega“ ja pahatahtlik ründaja saab vastavale telefoninumbrile sisse helistades sidesüsteemi operaatori kulul automaatselt ühenduda välise telefonivõrguga.

2.4 Telefoniühenduse kuritarvitus

Kui organisatsioonis on telefone, mis asuvad külastajatele juurdepääsetavates kohtades või ei ole konkreetse kasutajaga seotud, on oht, et telefone kasutatakse ära kas kahju tekitamise või isikliku kasusaamise otstarbel. Pahatahtlikud kasutajad saavad teha organisatsiooni lauatelefonidelt kõnesid tasulistele teenusenumbritele. Endaga seotud tasulistele numbritele helistamist võib ründaja korraldada ka otsese finantskasu saamise eesmärgil.

Lauatelefonidesse on integreeritud elektroonilised telefoniraamatud, kuhu on salvestatud kõik organisatsiooni sisenumbrid. Sellise telefoniraamatu lekkimine väljapoole organisatsiooni võib olla mittesoovitav.

3 Meetmed

3.1 Elutsükkel

Kavandamine

NET.4.1.M1 Telefonikeskjaama kasutuselevõtu kava

NET.4.1.M6 Telefonikeskjaama turvajuhend

Soetus

NET.4.1.M2 Sideteenuste tarnija valimine

NET.4.1.M13 Telefonikeskjaama hankimise kord

Evitus

NET.4.1.M7 Telefonikeskjaama turvaline paigutus

NET.4.1.M8 Tarbetute või turvakriitiliste funktsioonide piiramine ja blokeerimine

NET.4.1.M16 Sidesüsteemi klientseadmete turve

Käitus

NET.4.1.M5 Telefonikeskjaama logimine

NET.4.1.M9 Sidesüsteemi turvalise kasutamise koolitus

NET.4.1.M10 Telefonikeskjaama konfiguratsiooni dokumenteerimine ja läbivaatus

NET.4.1.M12 Konfiguratsioonifailide varundus

Kõrvaldamine

NET.4.1.M11 Telefonikeskjaama ja sideseadmete kasutuselt kõrvaldamise kord

Avariivalmendus

NET.4.1.M14 Telefonikeskjaama avariivalmendus

NET.4.1.M15 Hädaabikõned telefonikeskjaama tõrke puhuks

Lisanduvad kõrgmeetmed

NET.4.1.M17 Telefonikeskjaama hoolduse turve

NET.4.1.M18 Täiendav füüsiline turve

NET.4.1.M19 Dubleerivad ühendused

3.2 Põhimeetmed

NET.4.1.M1 Telefonikeskjaama kasutuselevõtu kava [IT-talitus]

a. Enne telefonikeskjaama hankimist või laiendamist on tehtud sidesüsteemi nõuete analüüs.

b. Nõuete analüüsi aluseks on võetud telefonikeskjaama kasutamise otstarve ja oodatavad funktsioonid.

c. Nõuete analüüsi tulemusena on määratud:

- klientseadmete liik ja arv;
- laiendatavus;
- ühendused ühtse telefonivõrguga;

- välisliinide arv;
- õiguste kontseptsioon;
- haldus ja konfigureerimine;
- turvanõuded;
- logimine;
- varundus;
- avariivalmendus;
- klienditoe- ja hooldelepingud.

d. Telefonikeskjaama kasutuselevõtu kava on dokumenteeritud ja kooskõlastatud IT-talitusega.

NET.4.1.M2 Sideteenuste tarnija valimine [IT-talitus]

a. On määratud lepinguline sideteenuste tarnija, kes ühendab telefonikeskjaama abonendid ühtsesse telefonivõrku, et oleks võimalik helistada ka organisatsioonile kuuluvast telefonikeskjaamast väljapoole.
b. Sideteenuste tarnija valikul on arvestatud järgmist:
   - sidesüsteemi nõudeid;
   - turvanõudeid;
   - tarnija kogemusi;
   - teeninduskvaliteeti;
   - maksumust ja tariife.
c. Kõigi tarbitavate sideteenuste kohta on tarnijaga sõlmitud kirjalik leping.

NET.4.1.M5 Telefonikeskjaama logimine

a. Telefonikeskjaamas logitakse vähemalt järgmised kõneandmed:
   - kõne või ühenduse kellaaeg ja kuupäev;
   - lähte- ja sihttelefoninumber;
   - kõne kestus.
b. Telefonikeskjaama haldustoimingud ja pääsuõiguste muutused logitakse.
c. Telefonikeskjaama logisid analüüsitakse regulaarselt.

NET.4.1.M15 Hädaabikõned telefonikeskjaama tõrke puhuks

a. Sidesüsteemi tõrke korral on tagatud organisatsioonivälised hädaabikõnede tegemise võimalus (nt kasutades mobiiltelefoni).
b. Hädaabikõne tegemine on võimalik kõikidest ruumidest.

3.3 Standardmeetmed

NET.4.1.M6 Telefonikeskjaama turvajuhend [IT-talitus]

a. Organisatsiooni turvapoliitikate alusel on kehtestatud telefonikeskjaama turvajuhend.
b. Kõik telefonikeskjaama hankimise, paigaldamise ja käitusega seotud isikud järgivad turvajuhendit.

c. Telefonikeskjaama turvajuhendis esitatakse vähemalt järgmised turvalise käituse aspektid:
   - halduse turve ja haldustoimingute logimine;
   - lubatud käitus- ja hooldustööriistad;
   - juurdepääsuvõimaluste kitsendamine;
   - õiguste andmise kord;
   - tarkvarauuendite paigaldamine ja konfiguratsioonimuudatused;
   - andmevarundus ja -taaste;
   - tõrgetele ja turvaintsidentidele reageerimise kord.

NET.4.1.M7 Telefonikeskjaama turvaline paigutus

a. Telefonikeskjaam on paigutatud ruumi, mille turvalisus vastab serveriruumile kehtivatele nõuetele.
b. Sideteenuste käideldavuse tagamiseks on telefonikeskjaama infrastruktuuri puhul arvestatud järgmisi aspekte:
   - stabiilne elektritoide/liigpingekaitse;
   - sobiv mikrokliima;
   - kaitse veekahjustuste eest;
   - tuleohutus;
   - turvauste ja -akende kasutamine;
   - ühenduvus valvesüsteemiga.
c. Telefonikeskjaama seadmed ja seadmete liidesed on kaitstud füüsilise juurdepääsu eest (nt lukustatud ja plommitud).

NET.4.1.M8 Tarbetute või turvakriitiliste funktsioonide piiramine ja blokeerimine

a. Aktiveeritud on ainult vajalikud funktsioonid.
b. Tarbetud või väärkasutust võimaldavad telefonikeskjaama funktsioonid on keskselt desaktiveeritud.
c. Klientseadmetes olevad konfidentsiaalsed andmed on piisavalt turvatud. Vajadusel kasutatakse spetsiaalsete programmeeritavate turvafunktsioonidega klientseadmeid.

NET.4.1.M9 Sidesüsteemi turvalise kasutamise koolitus [ülemus]

a. Sidesüsteemi kasutajad on läbinud sideteenuste ja seadmete kasutamise koolituse.
b. Klientseadmete kasutusjuhendid on sidesüsteemi kasutajatele kättesaadavad.
c. Kasutajad teavad, kelle poole sidesüsteemi häiringu või turvasündmuse puhul pöörduda.

NET.4.1.M10 Telefonikeskjaama konfiguratsiooni dokumenteerimine ja läbivaatus [IT-talitus]

a. Telefonikeskjaama konfiguratsioon ja telefoninumbrite loend on dokumenteeritud ja ajakohastatud.
b. Telefonikeskjaama konfiguratsiooni kontrollitakse regulaarselt. Läbivaatuse käigus kontrollitakse kas:
   - telefoninumbrid ja kasutajad on täielikus vastavuses;

- määramata telefoninumbrid on ka tegelikult kasutusse võtmata;
- desaktiveeritud funktsioone ja sideliideseid ei saa kasutada;
- konfiguratsioon vastab dokumentatsioonile;
- haldusprotseduurid on piisavad ja nende tulemused on dokumenteeritud;
- täidetakse andmekaitsenõudeid.

c. Läbivaatuse tulemused esitatakse lisaks otsestele vastutajatele ka infoturbejuhile, andmekaitsespetsialistile ja antud valdkonna eest vastutajale juhtkonnas.

NET.4.1.M11 Telefonikeskjaama ja sideseadmete kasutuselt kõrvaldamise kord [IT-talitus]

a. Telefonikeskjaama või sideseadmete kasutuselt kõrvaldamine toimub vastavalt üldise infoturvapoliitika nõuetele.

b. Enne telefonikeskjaama või sideseadmete kõrvaldamist kustutatakse nendest turvaliselt kõik andmed.

c. Edasiseks tööks olulised andmed varundatakse välisele andmekandjale või arhiveeritakse.

d. Kõrvaldatud seadmetel ei ole tundlikku teavet sisaldavaid silte ega märgiseid (kiirvalikunuppude selgitusi vms).

NET.4.1.M12 Konfiguratsioonifailide varundus

a. On koostatud sidesüsteemide andmevarunduse kontseptsioon, mis on osa serverite ja võrgukomponentide üldisest andmevarunduse kontseptsioonist.

b. Telefonikeskjaama konfiguratsiooni- ja käiduandmete esmane varundus on tehtud kohe pärast algset konfigureerimist.

c. Andmeid (sh abonentide nimekirja) varundatakse regulaarselt või kohe pärast konfiguratsiooni- ja käiduandmete muudatusi.

d. Telefonikeskjaama andmete taastamist varukoopialt testitakse regulaarselt.

NET.4.1.M13 Telefonikeskjaama hankimise kord

a. Telefonikeskjaama hankimisel arvestatakse sidesüsteemi kavandamise ja nõuete analüüsi tulemusi (vt NET.4.1.M1 *Telefonikeskjaama kasutuselevõtu kava*).

b. Hankimisel arvestatakse organisatsioonis olemasolevaid sidesüsteeme ja nende komponente. Sidesüsteemi osalise uuendamise või täiendamise korral jälgitakse, et vanad ja uued seadmed omavahel ühilduksid.

c. Sidesüsteemi uuendamisel (nt kui laiendatakse või asendatakse analoogsidesüsteeme IP-süsteemide ja -seadmetega) arvestatakse täiendavaid logimis- ja turvanõudeid.

NET.4.1.M14 Telefonikeskjaama avariivalmendus

a. On dokumenteeritud telefonikeskjaama avariivalmenduse plaan, mis on osa organisatsiooni üldisest avariivalmenduse kontseptsioonist (vt DER.4. *Avariihaldus*).

b. On välja töötatud juhised tegutsemiseks tüüpsete tõrkesituatsioonide puhul.

c. Sidesüsteemi kriitiliste komponentide asendamiseks on olemas varuseadmed.

d. Telefonikeskjaama avariivalmenduse plaani testitakse stsenaariumipõhiselt ja regulaarselt, testimise tulemused dokumenteeritakse.

NET.4.1.M16 Sidesüsteemi klientseadmete turve

a. Klientseadmete mittekasutavad andmevahetusliidesed (nt Bluetooth) ja tarbetud funktsioonid on desaktiveeritud.
b. Vaba juurdepääsuga ruumides asuvate telefoniseadmete funktsioonid on sobivalt piiratud ja telefoniseadmete konfigureerimine on kaitstud parooli või PIN-koodiga.
c. Klientseadmetes olev tundlik teave on piisavalt turvatud.
d. Klientseadmete turvalisuse tagamise eest vastutavad seadmete kasutajad. Kasutajad on saanud vastava koolituse.

3.4 Kõrgmeetmed

NET.4.1.M17 Telefonikeskjaama hoolduse turve (C-I)

a. Telefonikeskjaama hoolduse ja konfigureerimise vahendid (spetsiaalne riist- või tarkvara) on paroolidega kaitstud.
b. Juurdepääs telefonikeskjaamale on ainult spetsialiseeritud hooldusarvutitest, mis asuvad eraldi turvatsoonis.
c. Kui IP-põhiseks juurdepääsuks ei kasutata eraldi kaablit, on IP-andmeside krüpteeritud.
d. Remonti antav seade ei sisalda tundlikku teavet.

NET.4.1.M18 Täiendav füüsiline turve (C-I)

a. Telefonikeskjaam asub eraldiseisvas ja turvalises ruumis.
b. Sissepääs telefonikeskjaama ruumi on lubatud vaid piiratud isikuteringile.
c. Organisatsioonivälised isikud pääsevad telefonikeskjaama juurde ainult koos määratud saatjaga.
d. Organisatsioonivälise isikute ruumis viibimine (nimi, ettevõte, ajavahemik) registreeritakse.

NET.4.1.M19 Dubleerivad ühendused (A)

a. Telefonikeskjaama välisühendus on dubleeritud.
b. IP-põhine sidesüsteem on täiendavalt ja turvaliselt ühendatud analoogtelefonivõrguga.

NET.4.2 IP-telefon (VoIP)

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed VoIP-põhise sidesüsteemi (ingl Voice over IP,VoIP) komponentide ja IP-telefoni kõneedastuse turvalisuse tagamiseks.

1.2 Vastutus

IP-telefoni meetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Kasutaja, infoturbejuht.

1.3 Piirangud

Traditsioonilise telefonikeskjaama turvameetmeid käsitletakse moodulis NET.4.1 *Telefonikeskjaam*.

Andmeside turvet käsitletakse moodulites NET.1.1 *Võrgu arhitektuur ja lahendus*, NET.1.2 *Võrguhaldus* ja NET.3.2 *Tulemüür*.

Kui IP-telefoni kasutatakse klientarvutis paikneva tarkvaratelefonina, rakendatakse mooduli SYS.2.1 *Klientarvuti üldiselt* ja operatsioonisüsteemidega seotud moodulite meetmeid.

Kui VoIP-põhise sidesüsteemi tarkvara kasutatakse serveris, järgitakse peale operatsioonisüsteemidega seotud moodulite ka mooduli SYS.1.1 *Server üldiselt* meetmeid.

VoIP-põhise sidesüsteemi puhul arvestatakse täiendavalt mooduleid ORP.4 *Identiteedi ja õiguste haldus*, OPS.1.1.2 *IT-haldus*, OPS.1.1.3 *Paiga- ja muudatusehaldus* ja OPS.1.1.5 *Logimine*.

2 Ohud

2.1 VoIP-põhise sidesüsteemi vahetarkvara seadistusvead

Enamasti on IP-telefoniga ühendumiseks kaasatud mitu IT-süsteemi. Kui alustusprotokollina kasutatakse SIP-i, on andmeside jaoks vaja süsteeme nagu registraatorid (ingl *registrar*), SIP-i vaheserverid (ingl *proxy server*) ja asukohaserverid (ingl *location server*). VoIP-põhise sidesüsteemi infrastruktuuri muutmisel võivad kergesti tekkida konfigureerimisvead (nt võidakse kogemata teha vigu telefoninumbrite sisestamisel).

VoIP-põhise sidesüsteemi vahetarkvara (ingl *middleware*) väära seadistuse tulemusel võib telefoniside lakata töötamast.

2.2 VoIP-põhise sidesüsteemi komponentide väär konfiguratsioon

Olenemata sellest, kas VoIP-põhine sidesüsteem põhineb spetsialiseeritud riistvaral või tarkvarapõhisel süsteemil, on õige konfiguratsioon telefonisüsteemi nõuetekohase töö jaoks ülioluline. Peale signaalimisseadistuse on olulised meediaedastuse ja andmepakkimise meetodid ja seaded. Kui kasutatakse ebasobivat meetodit või kõneandmeid pakitakse liigselt kokku, halveneb kõnekvaliteet. Kui valitakse meetod, mille korral pakitakse liiga vähe, on oht andmesidevõrk üle koormata.

2.3 Kõnede pealtkuulamine

Kui telefonikõnesid või andmeid edastatakse krüpteerimata kujul, on ründajal võimalik kõnesid pealt kuulata või andmeid salvestada. VoIP-põhises sidesüsteemis on telefonikõnede ja andmeedastuse pealtkuulamine lihtsam kui traditsioonilises telefonisidesüsteemis, kuna kõne voogedastatakse (ingl *media streaming*) protokolliga RTP (ingl *Real Time Transport Protocol*, RTP). Ründajal on teeskluse (ingl *spoofing*) või nuuskimise (ingl *sniffing*) tehnikaid kasutades palju võimalusi andmesidevõrgu ründamiseks.

2.4 Telefoniühenduse kuritarvitus

Kui organisatsioonis on IP-telefone, mis asuvad külastajatele juurdepääsetavates kohtades või ei ole konkreetse kasutajaga seotud, võib IP-telefone kuritarvitada kahju tekitamise või isikliku kasusaamise otstarbel. Ründaja võib seadmele juurde pääsedes kasutada ära IP-telefoni tarkvara nõrkusi ning paigaldada sinna pahavara. Samuti on võimalik IP-telefoni

võrguühenduse kaudu ühenduda teiste sidesüsteemi komponentidega ja saada juurdepääs sisevõrgule.

Pahatahtlikud kasutajad võivad organisatsioonile kuuluvatelt telefoninumbritelt teha kõnesid tasulistele teenusenumbritele. Kui IP-telefonides on sisenumbrite salvestuseks kasutusel e-telefoniraamat, võib selle sisu lekkida.

3 Meetmed

3.1 Elutsükkel

Kavandamine

NET.4.2.M1 VoIP-põhise sidesüsteemi kasutuselevõtu kava

NET.4.2.M7 VoIP-põhise sidesüsteemi turvajuhend

NET.4.2.M8 VoIP-side krüpteerimine

Soetus

NET.4.2.M9 VoIP-põhise sidesüsteemi komponentide valimise kord

Evitus

NET.4.2.M4 VoIP-põhisele sidesüsteemile juurdepääsu kitsendamine

NET.4.2.M5 Vahetarkvara turvaline seadistamine

NET.4.2.M11 IP-telefonide turvaline kasutamine

NET.4.2.M13 VoIP-põhise sidesüsteemi tulemüür

Käitus

NET.4.2.M3 VoIP-põhise sidesüsteemi turvaline haldus

Kõrvaldamine

NET.4.2.M12 VoIP-põhise sidesüsteemi komponentide turvaline kõrvaldamine

Lisanduvad kõrgmeetmed

NET.4.2.M14 Signaalimise krüpteerimine

NET.4.2.M15 SRTP protokolli turve

NET.4.2.M16 Andmesidevõrgu ja VoIP-võrgu eraldamine

3.2 Põhimeetmed

NET.4.2.M1 VoIP-põhise sidesüsteemi kasutuselevõtu kava

a. Enne IP-telefonide kasutuselevõttu on koostatud VoIP-põhise sidesüsteemi kasutuselevõtu kava.

b. On otsustatud, kas IP-telefone hakatakse kasutama täielikult või osaliselt ning kuidas VoIP-põhine sidesüsteem ühendatakse avaliku (andme)sidevõrguga.

c. VoIP-põhise sidesüsteemi kasutuselevõtu kavas määratakse:

- soovitavad funktsioonid;
- nõuded käideldavusele, terviklusele ja konfidentsiaalsusele;

- signaalimis- ja transpordiprotokollid;
- eeldatava kasutajate arv;
- krüpteerimise ulatuse ja krüptomehhanismid;
- komponentide valimise põhimõtted;
- konfigureerimine ja haldus;
- logimise korraldus.

d. Kasutuselevõtu kavas on arvestatud olemasolevate andmesidevõrkude jõudlust ja ülesehitust.

NET.4.2.M3 VoIP-põhise sidesüsteemi turvaline haldus

a. VoIP-põhise sidesüsteemi tarbetud funktsioonid on desaktiveeritud.

b. VoIP-põhise sidesüsteemi konfiguratsioon on kaitstud lubamatute muudatuste eest.

c. Kõik VoIP-põhise sidesüsteemi turvamehhanismid on aktiveeritud. Turvamehhanismide toimimist testitakse enne IP-telefonide kasutuselevõttu.

d. Rakendatud turvamehhanismid ja konfiguratsioon on dokumenteeritud.

NET.4.2.M4 VoIP-põhisele sidesüsteemile juurdepääsu kitsendamine

a. Ebaturvalistest võrkudest ei saa IT-süsteemid luua otseühendusi organisatsiooni VoIP-põhise sidesüsteemi komponentidega.

b. Kui VoIP-põhisest sidesüsteemist ühendutakse otse avalikku andmesidevõrku, edastatakse kõik signaalimis- ja kõneandmed üksnes demilitaartsoonis asuva kontsentraatori kaudu.

NET.4.2.M5 Vahetarkvara turvaline seadistamine

a. VoIP-põhise sidesüsteemi komponentide ja vahetarkvara (ingl *middleware*) vaikekonfiguratsioon on enne kasutuselevõttu kohandatud lähtuvalt teabevahetuse kaitsetarbest.

b. Kõik installimis- ja konfigureerimisetapid on dokumenteeritud selliselt, et pädev kolmas isik on võimeline vahetarkvara seadistama, tuginedes ainult dokumentatsioonile.

c. Konfigureerimise automatiseerimise makrod on põhjalikult testitud ja dokumenteeritud.

d. Kõik VoIP-põhise sidesüsteemi vahetarkvara tarbetud teenused on desaktiveeritud.

3.3 Standardmeetmed

NET.4.2.M7 VoIP-põhise sidesüsteemi turvajuhend [infoturbejuht]

a. Organisatsiooni üldise turvapoliitika alusel on kehtestatud VoIP-põhise sidesüsteemi turvajuhend, mis esitab VoIP-põhise sidesüsteemi komponentide käitus- ja kasutusnõuded.

b. VoIP-põhise sidesüsteemi turvajuhend sisaldab vähemalt järgmist:
   - VoIP-põhise sidesüsteemi kasutamise võimalikud riskid;
   - IP-telefonide turvalise kasutamise nõuded;
   - lubatavad funktsioonid, teenused, protokollid ja ühendused;
   - rollid, õigused ja kohustused;
   - VoIP-põhise sidesüsteemi halduse, hoolduse ja auditeerimise korraldus;

- komponentide hankimise ja uuendamise nõuded;
- toimingute dokumenteerimise nõuded.

c. Kõik VoIP-põhise sidesüsteemi haldajad järgivad VoIP-põhise sidesüsteemi turvajuhendit.

NET.4.2.M8 VoIP-side krüpteerimine

a. On määratud, millistel juhtudel on VoIP-side krüpteerimine kohustuslik.

b. Kogu turvalisest kohtvõrgust väljuv IP-telefoni side on krüpteeritud sobivate turvamehhanismidega (SRTP, TLS).

c. Kui VoIP-sidet ei krüpteerita, on kasutajad sellest teadlikud ja väldivad konfidentsiaalse teabe edastamist.

NET.4.2.M9 VoIP-põhise sidesüsteemi komponentide valimise kord

a. VoIP-põhise sidesüsteemi komponentide valimiseks on koostatud nõuete spetsifikatsioon.

b. Nõuete spetsifikatsioon sisaldab vähemalt järgmist:

- üldnõuded (taristu, ühilduvus, protokollide tugi, suutvus);
- logimisnõuded (detailsus, turve, andmekaitsenõuded);
- uuendus- ja paikamisnõuded;
- haldusnõuded (protokollide tugi, haldusliidestus);
- krüpteerimisnõuded.

c. On kehtestatud protseduur VoIP-põhise sidesüsteemi komponentide võrdlemiseks.

NET.4.2.M11 IP-telefonide turvaline kasutamine [kasutaja]

a. IP-telefoni kasutajad teavad peamisi VoIP side ohte ja turvameetmeid.

b. Järelevalveta jäetud IP-telefon on lukustatud. Lahtilukustamine nõuab piisava tugevusega parooli sisestamist.

c. Hädaabinumbritele helistamine on võimalik ka aktiveeritud paroolkaitse puhul.

d. Kasutajad teavad, keda ja kuidas tuleb turvasündmusest teavitada.

NET.4.2.M12 VoIP-põhise sidesüsteemi komponentide turvaline kõrvaldamine

a. Enne VoIP-põhise sidesüsteemi komponentide kasutuselt kõrvaldamist kustutatakse neist turvaliselt kõik tundlikud andmed.

b. Pärast andmete kustutamist ja/või komponentide tehaseseadete taastamist kontrollitakse, kas andmete kustutamine õnnestus.

c. Enne IP-telefonide kõrvaldamist eemaldatakse nendelt tundlikku teavet sisaldavad sildid ja märgised.

NET.4.2.M13 IP-telefoni tulemüür

a. VoIP-põhise sidesüsteemi kavandamisel otsustatakse, kas piisab olemasoleva tulemüüri (ingl *firewall*) VoIP-side tarbeks kohandamisest või hangitakse ja paigaldatakse täiendav tulemüür.

b. RTP-liikluse filtreerimiseks kasutatakse rakenduslüüsi (ingl *application level gateway*) funktsionaalsusega tulemüüri.

3.4 Kõrgmeetmed

NET.4.2.M14 Signaalimise krüpteerimine (C-I)

a. VoIP-põhise sidesüsteemi tervikluse ja konfidentsiaalsuse tagamiseks edastatakse signaalimisteave krüpteeritud VPN-kanalite kaudu või selliste signaalimisprotokollidega (ingl *signaling protocol*), millel on oma turvamehhanismid (SIP, H.225).

b. Kui signaalimisprotokollil pole piisavaid turvamehhanisme, rakendatakse rakenduskihist madalamate kihtide (transpordi- või võrgukihi) turvamehhanisme.

c. Suure kaitsetarbe korral kasutatakse SIP signaalimisprotokolli (ingl *session initialization protocol*, SIP) koos TLS protokolliga.

d. Krüpteerimine vastab moodulile CON.1.*Krüptokontseptsioon*.

NET.4.2.M15 SRTP protokolli turve (C-I)

a. VoIP-põhise sidesüsteemi transpordiprotokollid RTP (ingl *real-time transport protocol*, RTP) ja RTCP (ingl *RTP Control Protocol,* RTCP) on kaitstud protokollide krüpteeritud versioonidega SRTP ja SRTCP.

b. SRTP (ingl *secure real-time transport protocol*, SRTP) krüpteerimise ja autentimise alusvõti (ingl *master key*) on vähemalt 128-bitine ja on genereeritud turvaliste vahenditega (nt MIKEY võtmehaldusprotokolliga).

c. RTP-sõnumite autentsust ja terviklust kaitseb piisavalt tugev räsifunktsioon (nt HMAC-SHA2).

d. On kasutusel autentsete SRTP-pakettide loendur. Taasesitusründe (ingl *replay attack*) puhul jäetakse korduvad paketid kõrvale.

e. Krüptomehhanismide ja -parameetrite ning räsialgoritmi valik ja põhjendus on dokumenteeritud.

NET.4.2.M16 Andmesidevõrgu ja VoIP-võrgu eraldamine (C-I-A)

a. VoIP-võrk on andmesidevõrgust tulemüüridega füüsiliselt või vähemalt VLAN-iga (virtuaalse kohtvõrguga) lahutatud.

b. On otsustatud, kuidas toimida seadmetega, millel on vaja juurdepääsu nii VoIP- kui ka andmesidevõrgule (nt arvutid, milles on tarkvaraline IP-telefoni klientrakendus).

c. VoIP-võrgu kommutaatori IP-telefoniga ühendatud pordis on lubatud ainult IP-telefoni ühendused.

d. Olenevalt kaitsetarbest rakendatakse VoIP-võrgu turbeks täiendavaid meetmeid (nt IEEE 802.1X vastavat autentimist).

INF: TARISTU

INF.1 Hoone üldiselt

1 Kirjeldus

1.1 Eesmärk

Esitada organisatsiooni tüüpilise hoone tehnilisi ja organisatoorseid turvaaspekte käsitlevad meetmed. Seejuures võetakse arvesse hoonete kogu elutsüklit, alustades nõuete koostamisest, kavandamisest, rajamisest, kasutamisest kuni remondi ja väljakolimiseni.

1.2 Vastutus

„Hoone üldiselt“ meetmete täitmise eest vastutab tehnikatalitus.

Lisavastutajad

Infoturbejuht, organisatsiooni juhtkond, töötaja, arhitekt, haldusosakond, tuleohutusspetsialist.

1.3 Piirangud

Hoone side- ja elektrikaabeldust käsitletakse moodulis INF.12 Kaabeldus, eriruume (nt serveri- ja arhiiviruumid) käsitletakse mooduligrupi INF:Taristu vastavates moodulites. Väliste töötajate kaasamist käsitletakse moodulis ORP.1 Infoturbe korraldus.

2 Ohud

2.1 Tuli

Tulekahju kahjustab hoonet ja sisustust olulisel määral. Tulekahju käigus võivad inimesed saada raskelt kannatada või hukkuda. Inimestel tekitab suitsuving vingumürgistust. Tulekahjuga kaasnev suits ja kõrge temperatuur kahjustavad IT-seadmeid, hoones ladustatavat kaupa ja hoone sisustust.

2.2 Äike

Äikese ajal võib välgu voolutugevus mitmesaja tuhande voldise pinge korral ulatuda kuni kahesaja tuhande amprini. See tohutu energia vabaneb ja hajub 50–100 mikrosekundi jooksul. Kui välk tabab hoonet vahetult, võib välgu energia hoonet oluliselt kahjustada. Välgutabamus võib tuua kaasa tulekahju ja hävitada läheduses asuvad elektriseadmed.

Välguga kaasnev elektromagnetväli mõjub ka eemalasuvatele elektrikaablitele ja elektritarvititele, kaablites indutseeritud liigpinge mõju on laiaulatuslik. Kui välgutabamus on hoonele lähemal, on tundlike elektroonikaseadmete hävinemine tõenäolisem.

2.3 Vesi

Vesi kahjustab hoonete osiseid tugeva vihma, kõrgvee või üleujutuse tagajärjel. Samuti võivad veekahjustused olla põhjustatud veeavariist hoone sees, mis võib juhtuda näiteks defektsete veetorude või veekraanide hooletu kasutamise tõttu.

2.4 Ilmastikust ja loodusõnnetustest tulenevad ohud

Olenevalt geograafilisest asukohast on hoone avatud ilmastikust ja loodusõnnetustest tulenevatele riskidele. Äärmuslikud ilmastikunähtused on näiteks tormid, orkaanid ja tsüklonid. Loodusõnnetusi võivad põhjustada seismilised või klimaatilised või nähtused. Eestis on arvestatavad üleujutuste ja maalihetega seotud ohud.

2.5 Keskkonnaohud

Hooneid võivad kahjustada läheduses asetleidvad, tihti täiesti ootamatud sündmused (nt keemiliste ainete hoidla plahvatus või mürgiste ainete leke). Õnnetuskoha lähedusest tuleb määramata ajaks evakueerida kogu töötajaskond. Piirkonnas toimuvate päästetööde või teede blokeerimise tõttu ei ole võimalik hoonele ligi pääseda või saab hoonet kasutada üksnes piiratud ulatuses.

2.6 Lubamatu sissepääs

Hoonesse ebaseaduslikult sisenenud isikud võivad tahtlikult rikkuda või varastada organisatsiooni vara. Sissetungijad võivad IT- seadmeid varastada, andmeid kustutada või manipuleerida. Ainuüksi sisse murdmine põhjustab varalist kahju akende või uste lõhkumisest tingitud kahjustuste näol. Sissemurdmise eesmärk on enamasti kergesti edasi müüdavate toodete vargus. Ette kavandatud rünne andmete loata kopeerimiseks või manipuleerimiseks võib põhjustada palju suuremat kahju kui IT-seadmete hävitamine. Ründaja võib hoonesse paigaldada lubamatu pealtkuulamisseadme, mille abil hilisemaid manipulatsioone läbi viia.

2.7 Ehituseeskirja rikkumine

Kui hoone rajamisel ei järgita tuleohutuse või konstruktsioonide ohutuse nõudeid (nt kui kasutatakse spetsifikatsioonile mittevastavaid ehitusmaterjale), võib see ühel hetkel kaasa tuua väga raskeid tagajärgi. Riski suurendab asjaolu, et selliseid rikkumisi on keeruline märgata.

2.8 Puudulikud tuletõkked

Hoonetes on palju erinevaid ruume läbivaid torusid ja kaableid (nt vee- ja heitveetorustik, küttesüsteem, elektri- ja sidekaablid). Kui seejuures ei paigaldata sobivaid tuletõkkeid, võivad tuli ja suitsugaasid läbi läbiviikude kontrollimatult levida.

Piirdekonstruktsioonide tuletõkete ümberehitamisel või muutmisel tootja ettekirjutusi eirates võib juhtuda, et tuletõke oma otstarvet ei täida.

2.9 Elektrikatkestus

Elektrikatkestuse korral võivad terved hooned või hooneosad kasutuks muutuda. Elektrivarustuse olemasolust ei sõltu mitte üksnes tavapärased elektritarvitid, nagu näiteks IT-seadmed või valgustus, vaid tänapäevase taristu kõik komponendid (nt liftid, kliimaseadmed, ohutuvastussüsteemid, turvaväravad, uste automaatlukustussüsteemid, veepumbad, sprinkler- või telefonisüsteemid). Elektrikatkestuste tekkimist soodustavad kaabelduse projekteerimisel tehtud vead, mistõttu kaablid asetsevad lihtsalt ligipääsetavates kohtades.

3 Meetmed

3.1 Elutsükkel

Kavandamine

INF.1.M1 Hoone turbe kavandamine
INF.1.M4 Hoone tulekahjusignalisatsioon
INF.1.M5 Käsikustutid
INF.1.M9 Hoonete turbe programm
INF.1.M14 Piksekaitsesüsteem
INF.1.M15 Juhtistike ja torustike asendiplaanid
INF.1.M16 Kaitset vajavate hooneosade otstarbe mittenäitamine
INF.1.M17 Suitsutõkestus

Evitus

INF.1.M3 Tuleohutusnõuete järgimine
INF.1.M7 Sissepääsu reguleerimine ja -kontroll
INF.1.M8 Suitsetamiskeeld
INF.1.M10 Standardite ja eeskirjade järgimine
INF.1.M13 Tehnosüsteemidele juurdepääsu reguleerimine
INF.1.M27 Sissemurdmiskaitse

Käitus

INF.1.M2 Elektrisüsteemi sobivus
INF.1.M6 Akende ja uste sulgemine
INF.1.M12 Võtmete ja pääsmike haldus
INF.1.M18 Tuleohutuse läbivaatused
INF.1.M19 Tuleohutuse eest vastutava töötaja õigeaegne teavitamine
INF.1.M36 Taristu dokumentatsiooni regulaarne uuendamine

Avariivalmendus

INF.1.M20 Tulekahju korral tegutsemise plaan ja tuleohutusõppused

Lisanduvad kõrgmeetmed

INF.1.M22 Turvalised uksed ja aknad
INF.1.M23 Turvatsoonid
INF.1.M24 Automaatne vee-eemaldus
INF.1.M25 Sobiva asukoha valimine
INF.1.M26 Valve- ja turvateenistus
INF.1.M30 Sobiva hoone valimine
INF.1.M31 Turvaline väljakolimine
INF.1.M34 Häire- ja hoiatussüsteem

3.2 Põhimeetmed

INF.1.M1 Hoone turbe kavandamine [arhitekt, infoturbejuht]

a. Hoone turvameetmed on kavandatud hoone kasutusotstarbest tulenevalt ning vastavuses äriprotsesside vajaduste ja kaitsetarbega.

b. Hoones asuvate inimeste, varade ja IT-süsteemide kaitseks on arvestatud turvaaspektidega alates tuleohutusest ja elektrisüsteemist kuni pääsukontrollini.

c. Turvameetmete valimise käigus on vastutajatega konsulteeritud ja valdkondade turvanõuded ühildatud.

INF.1.M2 Elektrisüsteemi sobivus

a. Elektrisüsteemi tehnilised parameetrid vastavad tegelikele vajadustele.

b. Elektrisüsteemis tarbitav võimsus jaotub ühtlaselt vooluvõrgu kolme faasi vahel.

c. Elektrijuhistik ja kaitsmed vastavad juhistiku projektile.

d. Ruumide kasutuse ja tehnilise varustuse (IT, kliimaseadmete, valgustuse jms) muutumisel kontrollitakse ja vajadusel kohandatakse elektrisüsteemi.

INF.1.M3 Tuleohutusnõuete järgimine [tuleohutusspetsialist]

a. Organisatsiooni töötajad järgivad tuleohutuseeskirju.

b. Hoone on projekteeritud ja ehitatud nii, et tulekahju puhkemisel:
   - säilib hoone kandevõime ettenähtud aja jooksul;
   - on tule ja suitsu teke ning levik hoones piiratud;
   - on tule levimine naaberehitistele piiratud;
   - on tagatud ohutu evakuatsioon;
   - on arvestatud päästemeeskonna ohutuse ja tegutsemisvõimalustega.

c. Tuleohutusnõuded on täidetud hoone kasutusea vältel.

d. Evakuatsiooniteed on selgelt ja nõuetekohaselt tähistatud ning takistusteta kasutatavad. Evakuatsiooniteede kasutatavust kontrollitakse regulaarselt.

e. Tuletõkkeuksed on püsivalt suletud asendis või sulguvad häire korral automaatselt.

f. Tuleohutuse tõstmiseks eemaldatakse ruumidest mittevajalikud paberdokumendid, pakkematerjal ja tuleohtlikud jäätmed.

g. On määratud tuleohutuse eest vastutaja. Vastutajal on vajalik väljaõpe.

INF.1.M4 Hoone tulekahjusignalisatsioon [arhitekt, tuleohutusspetsialist]

a. Hoonesse on paigaldatud suitsuandurid.

b. Suitsuandurite paigaldamiseks on valitud vähemalt järgmised asukohad:
   - koridorid;
   - serveriruumid, tehnilised ruumid ja kilbiruumid;
   - koosolekuruumid;
   - õhukonditsioneerimissüsteemi olemasolul ka ventilatsioonikanalid.

c. Suitsuandurid on ühendatud kesksesse tulekahjusignalisatsiooni süsteemi.
d. Suitsu tuvastamise korral rakendub häire, mis on kuuldav kõigile hoones viibivatele isikutele.
e. Suitsuandurite ja tulekahjusignalisatsiooni korrasolekut kontrollitakse regulaarselt.

INF.1.M5 Käsikustutid [tuleohutusspetsialist]

a. Hoonesse on tuleohutusnõuete kohaselt paigaldatud piisaval hulgal, sobivat tüüpi ja piisavas suuruses käsikustuteid.
b. Käsikustutid on paigutatud kohtadesse, kust nad on tulekahju korral kergesti kättesaadavad.
c. Elektri- ja elektroonikaseadmeid ning andmekandjaid sisaldavates ruumides paiknevad üksnes gaaskustutid.
d. Käsikustuteid kontrollitakse ja hooldatakse regulaarselt, kontrollimisaeg ja hooldusvälp on dokumenteeritud.
e. Töötajad oskavad käsikustuteid kasutada, kustutite praktilist kasutamist harjutatakse regulaarselt.

INF.1.M6 Akende ja uste sulgemine [töötaja, haldusosakond]

a. Kui hoones ei ole inimesi, hoitakse aknad suletud ja välisuksed (ka rõdu- või terrassiuksed) lukustatud.
b. Uste ja akende sulgemise kord on töötajaile teada ja selle täitmist kontrollitakse regulaarselt.

INF.1.M7 Sissepääsu reguleerimine ja -kontroll [haldusosakond, infoturbejuht]

a. Hoone, hooned või hooneosad on vajadusel jaotatud eri kaitsetarbega turvatsoonideks (vt INF.1.M23 *Turvatsoonid*).
b. Pääs ruumidesse on reguleeritud tehniliste meetmetega (nt turvaväravad, iselukustuvad uksed, pääsmikuga avatavad lukusüsteemid) ja korralduslike meetmetega (nt külastajate registreerimine) vastavalt ruumide kaitsetarbele.
c. Külastajate lubamine hoonetesse ja ruumidesse toimub kehtestatud korra alusel.
d. Suure kaitsetarbega hoonetesse ja ruumidesse on sissepääs piiratud. Sisenemise õigus on ainult volitatud isikutel, kehtestatud pääsuloendi alusel. Külastajad liiguvad suure kaitsetarbega ruumides ainult koos saatjaga.
e. Külastajatel on kohustus kanda kõigile nähtavalt töötajate kaardist eristatavat külalisekaarti.
f. Sissepääsu reguleerimise meetmete tõhusust kontrollitakse regulaarselt.

INF.1.M8 Suitsetamiskeeld [töötaja, haldusosakond]

a. Suitsetamine on lubatud ainult hoonest eemal.
b. IT-seadmeid või andmekandjaid sisaldavates ruumides (nt serveriruumid, arhiivid), kus tulekahju ja saaste põhjustab suurt kahju, on suitsetamine rangelt keelatud.
c. Suitsetamisalale viivad välisuksed on kaitstud pääsukontrollisüsteemiga ja neid ei jäeta lahti.

INF.1.M10 Standardite ja eeskirjade järgimine [haldusosakond]

a. Hoonete kavandamisel, rajamisel, sisustamisel, remontimisel ning tehnosüsteemide paigaldamisel järgitakse kohaldatavaid ehitusnorme.

INF.1.M27 Sissemurdmiskaitse

a. Sissemurdmise takistamiseks rakendatakse meetmeid, mis on piisavad ja ühtlasi vastavad kohalikele tingimustele:
   - uksed ja aknad on turvalised;
   - vajadusel on aknad kaitstud turvakile või trellidega ning uksed ja aknad metallruloodega;
   - vajadusel on ustele paigaldatud lisalukud ja -riivid;
   - mittekasutatavad lisasissepääsud on suletud, avariiväljapääsud on sissemurdmiskindlad;
   - ventilatsiooniavad ja muud tehnilised avad on kaetud võredega;
   - väljaspool tööaega on liftid avatavad uksekaardiga.
b. Sissemurdmiskaitse meetmete tõhusust kontrollitakse regulaarselt.
c. Töötajad on teadlikud sissemurdmiskaitse meetmetest ja nendega seonduvatest kohustustest.

3.3 Standardmeetmed

INF.1.M9 Hoonete turbe programm [arhitekt, infoturbejuht]

a. Organisatsiooni üldise turbekontseptsiooni alusel on kehtestatud hoonete turbe programm, mis sätestab muuhulgas:
   - suure kaitsetarbega ruumide paigutuse põhimõtted;
   - ruumidesse pääsu reguleerimise;
   - valvesüsteemide kasutamise;
   - vee- ja tuleõnnetuste mõju vähendamise meetmed;
   - hoone asukohast tulenevad lisameetmed;
   - IT-taristu tulekaitse meetmed;
   - tehnoteenuste turbe.
b. Pärast turvaintsidendi toimumist või muudatusi hoonete kasutusotstarbes turbe programm ajakohastatakse.
c. Kaitset vajavad ruumid ja hooneosad asuvad eemal suure ohuga aladest (nt esimene korrus, keldriruumid). Kaitset vajavad ruumid paiknevad soovitavalt hoone siseosas.

INF.1.M12 Pääsmike ja võtmete haldus [haldusosakond]

a. Pääsmike ja võtmete haldamist ja väljaandmist korraldatakse tsentraalselt.
b. Pääsmikke ja võtmeid väljastatakse ainult põhjendatud juhtudel ja volitatud isikutele, väljastused ja tagastused dokumenteeritakse.
c. Töötaja on kohustatud hoidma ja kasutama talle väljastatud pääsmikku ja võtmeid turvaliselt. Võtmete ja pääsmike lubamatu kopeerimine on keelatud.

d. Varuvõtmeid hoitakse turvalises kohas, avariiolukorras on varuvõtmed kättesaadavad.
e. On olemas protseduurid pääsmiku või võtme kaotamise korral tegutsemiseks (teatamiseks, asendamiseks, kulude katmiseks, lukkude vahetamiseks jms).
f. Töötaja töölt lahkumise korral tagastab töötaja talle väljastatud pääsmiku ja võtmed.

INF.1.M13 Tehnosüsteemidele juurdepääsu reguleerimine

a. Tehnosüsteemide jaotusseadmed on paigutatud viisil, mis välistab volitamata isikute juurdepääsu.
b. Kappide ja seadmete lukud on töökorras. Jaotuskappe tohivad avada ainult konkreetse tehnosüsteemi eest vastutavad isikud (vt INF.1.M12 *Pääsmike ja võtmete haldus*).
c. Varuvõtmeid hoitakse turvaliselt ja need on vajadusel saadaval.
d. Jaotusseadme komponendid on selgelt ja püsivalt märgistatud.
e. Sulavkaitsmete kasutamisel puhul on seadmekapis vajalik arv varukaitsmeid.

INF.1.M14 Piksekaitsesüsteem

a. Hoone piksekaitsesüsteemi kaitseklassi valikul on lähtutud asjakohase standardi alusel koostatud riskianalüüsi tulemustest (standardid EN 62305, EVS-HD 60364 ja EVS-EN 60099).
b. Lisaks välisele piksekaitsesüsteemile on paigaldatud sisemised elektritarvitite liigpingepiirikud (vt INF.12 *Kaabeldus*).
c. Piksekaitsesüsteemi kontrollitakse ja hooldatakse regulaarselt.

INF.1.M15 Juhistike ja torustike paigutusskeemid

a. On määratud isikud, kes juhistike ja torustike paigutusskeeme haldavad ja ajakohastavad.
b. Paigutusskeemid on ajakohased ja täpsed, vajadusel koos lisatud selgitava tekstiga.
c. Paigutusskeemidel on vähemalt järgmised andmed:
    - Juhistike ja torustike täpsed kulgemisteed igal korrusel;
    - täpsed tehnilised andmed (juhtme või toru tüüp, dimensioonid);
    - otstarve ja tarbijad;
    - märgistus.
d. Juhistike ja torustike hooldustööd on dokumenteeritud.
e. Paigutusskeemid on kaitstud lubamatu juurdepääsu eest. Vajaduse korral on paigutusskeemid kiiresti kättesaadavad.

INF.1.M16 Kaitset vajavate hooneosade otstarbe mittenäitamine

a. Avalikel majajuhtidel ei ole viidatud kaitset vajavate hooneosade (serveriruumide, andmekeskuste, arhiivide jms) asukohale.
b. Kaitset vajavate hooneosade asukoht ei ole väljastpoolt maja tuvastatav.
c. Kaitset vajavate ruumide uksesildid ei näita ruumide tegelikku otstarvet.

INF.1.M17 Suitsutõkestus [arhitekt]

a. Konstruktsiooni suitsutõkestuse toimimist testitakse koheselt pärast paigaldus- või remonditööde lõppemist.
b. IT-seadmeid sisaldavatest ruumidest saab suitsu kiiresti eemaldada.

c. Tuletõkkeuksed on ühtlasi ka suitsukindlad (tüübitähisega RS).

INF.1.M18 Tuleohutuse läbivaatused [tuleohutusspetsialist]

a. Tuleohutuse läbivaatuseid tehakse regulaarselt, vähemalt ühel korral aastas.

b. Läbivaatuse käigus hinnatakse vähemalt järgmist:
   - tule- ja plahvatusohtlike materjalide hoidmist;
   - põlevate materjalide olemasolu tehno- ja serveriruumides;
   - suitsuandurite ja tulekustutite olemasolu ja hooldust;
   - tuletõkkeuste kasutamist;
   - evakuatsiooniteede läbipääsetavust.

c. Tuleohutuse läbivaatuse käigus tuvastatud puudused kõrvaldatakse esimesel võimalusel.

INF.1.M19 Tuleohutuse eest vastutava töötaja õigeaegne teavitamine [tuleohutusspetsialist]

a. Tuleohutuse eest vastutavat töötajat teavitatakse aegsasti kõigist eelseisvatest töödest, mis mõjutavad tuleohutust.

b. Tuleohutuse eest vastutav töötaja kontrollib nii hoone ehitustööde käigus kui pärast ehitustööde lõppemist tuleohutusmeetmete nõuetekohast rakendamist (vt INF.1.M3 *Tuleohutusnõuete järgimine*).

INF.1.M20 Tulekahju korral tegutsemise plaan ja tuleohutusõppused [tuleohutusspetsialist]

a. Tuleohu korral tegutsemiseks on koostatud tulekahju korral tegutsemise plaan.

b. Töötajatele korraldatakse tulekahju korral tegutsemise plaanil põhinevaid ja regulaarseid häire- ja tuleohutusõppuseid.

INF.1.M36 Taristu dokumentatsiooni regulaarne uuendamine

a. Taristu dokumentatsioon (rajatise-, trassi- ja kaabliskeemid, torustike paigutusskeemid, evakuatsiooniteede kirjeldused ja tuletõrjeplaanid) on ajakohane.

b. Töötajatel on dokumentatsioonile vajaduspõhine juurdepääs.

c. Tulekahju korral tegutsemise plaani ja evakuatsiooniteede skeemi vaadatakse üle regulaarselt. Vajadusel korrigeeritakse plaani.

d. Kõik töötajad on teadlikud tuleohutus- ja hoonete kasutamise juhendites tehtud muudatustest.

e. Taristu dokumentatsiooni ajakohasust kontrollitakse vähemalt kord kolme aasta jooksul.

3.4 Kõrgmeetmed

INF.1.M22 Turvalised uksed ja aknad (C-I-A)

a. Hoonete uksed ja aknad vastavad vähemalt kaitseklassile RC2 standardi EVS-EN 1627 järgi.

b. Andmekeskuse olemasolul vastavad selle uksed ja nende paigaldus vähemalt kaitseklassile RC3.

c. Ruumi akende, uste ja seinte sissetungi-, tule- ja suitsukindlus on vähemalt teiste osistega samaväärne.

d. Turvauste ja -akende seisundit kontrollitakse regulaarselt.

INF.1.M23 Turvatsoonid [arhitekt] (C)

a. Ruumid ja piirkonnad on sarnase kaitsetarbe järgi rühmitatud kaheks, kolmeks või neljaks turvatsooniks (nt. välispiirkond, kontrollitav sisepiirkond, sisepiirkond, suure kaitsetarbega piirkond).

b. Posti-, tarne- ja laadimistsoonid peavad paiknema nii, et kaubasaadetisi saaks vastu võtta ilma et tarnija peaks sisenema hoone muudesse piirkondadesse.

c. Suure kaitsetarbega turvatsooni sisenemisel rakendatakse täiendavaid pääsukontrolle (nt turvavärav). Suure kaitsetarbega tsooni sissepääsu õigust omavate isikute ring on väga väike.

d. Hoonete ja territooriumi turvatsoonid ja nende kaitsetarve on dokumenteeritud.

INF.1.M24 Automaatne vee-eemaldus (A)

a. Veeohuga piirkonnad on varustatud lekkeandurite ja vee-eemaldussüsteemidega.

b. Passiivsed vee-eemaldussüsteemid (põrandatrappide kaudu otse kanalisatsioonisüsteemi) on varustatud tagasivooluklappidega.

c. Passiivse vee-eemaldussüsteemi puudumisel kasutatakse vee juhtimiseks piisava jõudluse ja töökindlusega veepumpasid (aktiivne vee-eemaldus).

d. Vee-eemaldussüsteemide töökorras olekut kontrollitakse regulaarselt.

INF.1.M25 Sobiva asukoha valimine [organisatsiooni juhtkond] (A)

a. Hoone asukoha valimisel on arvestatud järgmiste keskkonnaohtudega:

- liiklusest (maantee, raudtee) tekkiv vibratsioon;
- liiklustrasside lähedusest tulenev õnnetusrisk;
- kõrgepingeliinide või raadiosidemastide tekitatavad häiringud;
- üleujutuse võimalikkus;
- tehnilised õnnetused naaberrajatistes;
- ümbruskonna kriminogeensus.

INF.1.M26 Valve- ja turvateenistus [haldusosakond] (C-I-A)

a. Valve- ja turvateenistuse ülesanded on selgelt dokumenteeritud.

b. Valve- ja turvateenistuse töötajad registreerivad isikute liikumise läbi peasissepääsu (-värava) ja jälgivad videovalve abil ka teisi sissepääse. Valve- ja turvateenistuse ülesannete hulka kuuluvad ka pärast tööpäeva lõppu tehtavad turvakontrollid (hoonete välisuste lukustamise ja akende sulgemise kontroll, signalisatsiooni sisselülitamine jms).

c. Töötajad ja külastajad esitavad valveteenistuse töötaja nõudmisel pildiga pääsukaardi (kui selline on rakendatud) või isikut tõendava dokumendi.

d. Külastajale väljastatakse pärast tema isiku kontrollimist külastajakaart ja juhendatakse, kuidas seda kasutada. Külastaja lahkumisel külastajakaart tagastatakse.

e. Valve- ja turvateenistusega teabevahetuseks on määratud kontaktisik. Valve- ja turvateenistuste töötajaid teavitatakse pääsuõiguste muudatustest õigeaegselt.

INF.1.M30 Sobiva hoone valimine [infoturbejuht] (C-I-A)

a. Hoonete sobivuse hindamiseks on koostatud funktsionaalsete ja turvanõuete spetsifikatsioon.
b. Infoturbe seisukohast arvestatakse hoone sobivuse hindamisel järgmisi aspekte:
   - milline on hoone perimeetri ulatus;
   - kas hoone tarindid on piisavalt tugevad serveriruumide, puhvertoiteallikate ja IT-seadmete paigutamiseks selleks kõige paremini sobivatesse asukohtadesse hoones.
   - kas saab turvatsoone üksteisest eraldada, luua turvaväravad ning juurdepääsuteed.
   - kas juurdepääsuteed sobivad suuremõõduliste IT-komponentide transpordiks.
   - kas rendihoonet kasutavad samal ajal ka teised.
c. Hoone väljavalimise käigus on veendutud, et hoones saab vajalikke turvameetmeid rakendada, seda eriti rendiobjektide korral.

INF.1.M31 Turvaline väljakolimine [haldusosakond] (C)

a. Enne väljakolimist on koostatud infoturbe vaatest oluliste varade loend (nt riistvara, tarkvara, andmekandjad, kaustad ja dokumendid).
b. Igale töötajale on teatatud, milliste asjade kolimise eest tema vastutab.
c. Tarbetud seadmed, andmekandjad jms on enne kolimist kasutusest kõrvaldatud.
d. Pärast väljakolimist kontrollitakse kõiki ruume mahajäänud varade leidmiseks.

INF.1.M34 Häire- ja hoiatussüsteem (A)

a. Kasutatakse ruumidele ja riskidele vastavat häire- ja hoiatussüsteemi.
b. Häire- ja hoiatussüsteem vastab standardile EVS-EN 50518.
c. Keskse häire- ja hoiatussüsteemi puudumisel kasutatakse kõrge kaitsetarbega ruumides autonoomseid valvesüsteeme.
d. Häire- ja hoiatussüsteemi kontrollitakse ja hooldatakse regulaarselt.
e. Häirele reageerimiseks on kehtestatud protseduur.
f. Häirele reageerimist analüüsitakse, vajadusel korrigeeritakse protseduuri.

INF.1.M35 Välisperimeetri kaitsmine [arhitekt] (C-A)

a. On kasutusele võetud meetmed hoone välisperimeetri kaitsmiseks.
b. Perimeetri käitamiseks on kaalutud järgmiste kaitsemeetmete rakendamist:
   - hoonete ümbritsemine aiaga;
   - meetmed territooriumile kogemata sattumise ärahoidmiseks;
   - meetmed territooriumile tahtliku sissetungi raskendamiseks:
   - välikaamerad ja videosalvestusseadmed;
   - inimeste ja sõidukite liikumise automaatne tuvastamine;
   - automaatne häire- ja hoiatussüsteem.

4. Lisateave

Lühend	Publikatsioon
[RT]	Määrus „Ehitisele esitatavad tuleohutusnõuded ja nõuded tuletõrje veevarustusele“, vastu võetud 30.03.2017
[ISO1627]	EVS-EN 1627:2021 „Uksed, aknad, rippfassaadid, võred ja luugid. Sissemurdmiskindlus. Nõuded ja klassifikatsioon“
[ISO62305]	EVS-EN 62305-1:2011 „Piksekaitse. Osa 1: Üldpõhimõtted“
[ISO50518]	EVS-EN 50518:2019 „Monitoring and alarm receiving centre“

INF.2 Serveriruum ja andmekeskus

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed serveriruumis ja andmekeskuses turvaliste ning jätkusuutlike käidutingimuste loomiseks ja säilitamiseks. Mooduli meetmeid rakendatakse iga andmekeskuse ja serveriruumi korral.

1.2 Vastutus

Serveriruumi ja andmekeskusega seonduvate meetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Andmekaitsespetsialist, tehnikatalitus, töötaja, arhitekt, hooldepersonal, tuleohutusspetsialist.

1.3 Piirangud

Kõikidel organisatsioonidel ei pruugi andmekeskust olla, selle asemel on üks või mitu serveriruumi. Serveriruumi turvalisuse tagamiseks rakendatakse põhimeetmed ja ülejäänud meetmed vastavuses kaitsetarbega (C-I-A hinnangu alusel).

Mooduli meetmeid ei kohandata väikesele organisatsioonile, millel on mõned IT-töökohad ja eraldi ruumis paiknev server. Siis piisab ka mooduli INF.5 *Tehnilise taristu ruum või kapp* rakendamisest seadmeruumile ja tehnilise taristu seadmekapile. Täiendavalt rakendatakse meetmeid hoone (INF.1 *Hoone üldiselt*) ja kaabelduse (INF.12 *Kaabeldus*) kaitseks.

2 Ohud

2.1 Andmekeskuse kavandamisvead

Andmekeskuse asukohast tulenevad ohud (nt tööstusõnnetused, maavärinad või üleujutused) võivad mõjutada IT-süsteemide töökindlust ja käideldavust. Andmekeskuse tööd mõjutab piisava energiavarustuse või andmesideühenduse puudumine märkimisväärselt.

2.2 Lubamatu sissepääs

Puuduliku pääsukontrolli korral saavad volitamata isikud andmekeskusesse siseneda ning hooletusest (nt puudulike valdkonnateadmiste tõttu) või tahtlikult kahju tekitada. Tahtlik kahju seisneb eelkõige seadmete varguses või nende rikkumises.

2.3 Puudulik seire

Kui andmekeskuse taristu seire ja haldus on puudulik, märgatakse tehniliste komponentide rivist välja langemist liiga hilja ja tõrkele ei reageerita õigeaegselt. Tehnilised tõrked mõjutavad otseselt serverite käideldavust.

2.4 Andmekeskuse ebasobiv mikrokliima

Kui andmekeskuse temperatuuri, õhuniiskust või peenosakeste sisaldust õhus ei hoita seadmetootjate poolt ettenähtud tasemel, põhjustab see tehniliste komponentide väärtalitust või tõrkeid. Õhukonditsioneeri tõrge põhjustab serveriruumi temperatuuri kiiret tõusu, mis võib tekitada tehniliste komponentide ülekuumenemist ja tõrkeid. Samuti võivad kõrge temperatuuri või niiskuse tõttu kahjustuda andmekandjad.

2.5 Tuli

Tuli ja suits võivad põhjustada suurt kahju. Serveriruumis on tulekahju pigem harvaesinev, kuid väga raskete tagajärgedega sündmus. Kõige tavalisem tulekahju põhjus on rikkis elektriseadmetes (nt häired andmekeskuse tugifunktsioonidega seotud seadmetes nagu avariitoitegeneraator, puhvertoiteallikas, kliimaseade). Kui andmekeskusel puudub sisemine tuletõkkesüsteem, saab tulekahju kiiresti levida. Samuti võib väljaspool hoonet tekkinud tulekahju levida andmekeskusesse. Tuli ja suits kujutavad ohtu inimest elule ja tervisele.

2.6 Vesi

Vesi satub andmekeskusesse nt lekkiva veetorustiku, üleujutuse, katkiste torude, defektsete sprinkler- või kliimaseadmete tõttu. Veeõnnetus põhjustab seadmete seiskumist ja kahjustumist. Seadmekahjustus võib ilmneda ka alles teatud aja möödudes. Veeõnnetus võib tekitada lühise, mis võib põhjustada tulekahju või kaasa tuua laiaulatuslikke tõrkeid.

2.7 Puuduv või puudulik sissemurdmistõrje

Ka hästi toimiva pääsukontrolli puhul võib eesmärgipäraselt tegutsev ründaja andmekeskusesse sisse pääseda kui pole rakendatud sissemurdmistõrje meetmeid. Ründaja saab lekitada tundlikke andmeid, varastada või manipuleerida IT-komponente. Samuti võib ta seadmeid hävitada või andmekeskust kahjustada.

2.8 Elektrikatkestus

Elektrikatkestus häirib märkimisväärselt andmekeskuse tööd ja seeläbi terve organisatsiooni äriprotsesside toimimist. Andmekeskuse võimaldatavad IT-teenused ei ole ootamatult enam kasutatavad. Elektrikatkestus võib põhjustada andmekadu, kahjustada IT-süsteeme, teha kahju sidesüsteemidele või valveseadmetele.

2.9 Ebapuhas keskkond

Tolm andmekeskuses põhjustab aja jooksul tehniliste komponentide seiskumise. Seadmed, milles on kiiresti liikuvaid osi (nt ventilaatorid), kuluvad tolmuses keskkonnas kiiremini ja neil on rohkem tõrkeid.

3 Meetmed

3.1 Elutsükkel

Kavandamine

INF.2.M1 Andmekeskuse turvanõuete kehtestamine
INF.2.M12 Andmekeskuse perimeetri turve
INF.2.M13 Andmekeskuse valvesüsteem

Evitus

INF.2.M2 Tuletõkkesektsioonid
INF.2.M3 Puhvertoiteallikas (UPS)
INF.2.M4 Toite avariilüliti
INF.2.M9 Tulekustutussüsteem ja kustutusvahendid
INF.2.M15 Liigvoolukaitse
INF.2.M17 Tulekahju varajane tuvastamine
INF.2.M29 Juhtistiku kontroll

Käitus

INF.2.M5 Õhutemperatuuri ja -niiskuse reguleerimine
INF.2.M6 Pääsu reguleerimine
INF.2.M7 Uste ja akende lukustus ja turve
INF.2.M8 Tulekahjusignalisatsioon
INF.2.M10 Taristu ülevaatus ja hooldus
INF.2.M11 Taristu seire
INF.2.M14 Avariitoitegeneraator
INF.2.M16 Andmekeskuse keskkonnatingimused
INF.2.M19 Tehnilise taristu testimine

Lisanduvad kõrgmeetmed

INF.2.M21 Varuandmekeskus
INF.2.M22 Tolmutõrje
INF.2.M23 Andmekeskuse turvaline kaabeldus
INF.2.M24 Videovalvesüsteem
INF.2.M25 Puhvertoiteallikate dubleerimine
INF.2.M26 Avariitoitegeneraatori dubleerimine
INF.2.M28 Kõrgendatud nõuetele vastav valvesüsteem

3.2 Põhimeetmed

INF.2.M1 Andmekeskuse turvanõuete kehtestamine [tehnikatalitus, arhitekt]

a. Andmekeskuse või serveriruumi tarbeks on kehtestatud tehnilised ja korralduslikud nõuded.

b. Andmekeskuse kavandamisel või sobivate ruumide valimisel on arvestatud seal asuvate IT-komponentide kaitsetarvet (eelkõige käideldavuse osas) ja vajalike turvameetmete rakendamise võimalikkust.

c. Andmekeskus on kavandatud suletud turvaalana, mis on jaotatud kaitsetarbe kohaselt turvatsoonideks. Ka serveriruumi korral otsustatakse, kas eri turvatsoonide rajamine serveriruumis on otstarbekas.

d. Andmekeskuse halduse, logistika, tugitehnika ja IT-seadmete tsoonid on üksteisest selgesti eraldatud.

INF.2.M2 Tuletõkkesektsioonid [arhitekt]

a. Tule ja suitsu leviku piiramiseks on andmekeskus ja võimalusel ka serveriruum jaotatud tule- ja suitsutõkkesektsioonideks.

b. Tsoonide eraldamine vastab kehtivatele ehitus- ja tuleohutuseeskirjadele.

INF.2.M3 Puhvertoiteallikas (UPS) [tehnikatalitus]

a. Andmekeskuse tööks olulised elektri- ja IT-seadmed, välja arvatud suure energiatarbega seadmed (nt kliimaseadmed), on katkematu toite tagamiseks ühendatud puhvertoiteallikaga (ingl *uninterruptable power supply*, UPS).

b. Puhvertoiteallika võimsus on piisav ja selle piisavust kontrollitakse pärast igat elektritarvititega seotud olulist muudatust.

c. Andmekeskuse UPS-süsteemis hoitakse energiat salvestavaid akusid tootja ettenähtud temperatuuri- ja niiskusvahemikus, selleks on soovitav akud paigutada elektritarvititest eraldi asukohta.

d. Puhvertoiteallikaid hooldatakse ja nende töövõimelisust kontrollitakse perioodiliselt, tootja ettenähtud sagedusega (vt INF.2.M10 *Taristu ülevaatus ja hooldus*).

INF.2.M4 Toite avariilüliti [tehnikatalitus]

a. Avarii korral saab andmekeskuse elektriga varustamist välja lülitada üksikute elektritarvitite rühmade haaval.

b. Avarii korral lülitatakse toide välja läbimõeldud kava alusel, kogu andmekeskuse toidet võimalusel välja ei lülitata. Sealhulgas arvestatakse, kuidas on elektrivõrguga ühendatud puhvertoiteallikad ja millised elektritarvitid nendega on seotud.

c. Avariilülitid on kaitstud tahtmatu või lubamatu väljalülitamise eest.

INF.2.M5 Õhutemperatuuri ja -niiskuse reguleerimine [tehnikatalitus]

a. IT-seadmete asukohtade õhutemperatuur ja -niiskus on lubatavates piirides.

b. Pärast igat muudatust elektriseadmete koosseisus ja paigutuses kontrollitakse jahutatavate alade soojuskoormuse muutumist.

c. Õhukonditsioneerid on võimalusel paigutatud eraldi, vee äravoolu võimalusega ruumi.

d. Õhukonditsioneere hooldatakse regulaarselt.

e. Temperatuurile ja niiskusele seatud piiväärtuste ületamist saab tagantjärele tuvastada.

INF.2.M6 Pääsu reguleerimine [tehnikatalitus]

a. Andmekeskuse ja serveriruumi pääsuõiguste haldus on kooskõlas mooduliga ORP.4 *Identiteedi ja õiguste haldus*.

b. On määratud, millistel organisatsioonisisestel ja -välistel isikutel, millises ajavahemikus, millistesse ruumidesse ja missugusel eesmärgil on andmekeskusse sissepääsu õigus.
c. Kõik sisenemised andmekeskusesse registreeritakse.
d. Andmekeskusesse ei ole muid sissepääse peale nende, mille läbimine registreeritakse.
e. Serveriruumi puhul on hinnatud, kas eraldi pääsukontrollisüsteemi kasutuselevõtt on vajalik.
f. Pääsusüsteemide toimimist ja sisenejate registreerimist kontrollitakse regulaarselt.

INF.2.M7 Uste ja akende lukustus ja turve [töötaja, tehnikatalitus]

a. Andmekeskuse kõik uksed on alati lukustatud.
b. Andmekeskus on projekteeritud ilma akendeta. Akende olemasolul on need sarnaselt ustega alati lukustatud.
c. Uksed ja aknad tagavad kaitse rünnete ja keskkonnamõjude eest.
d. Andmekeskuse või serveriruumi kõik piirdekonstruktsioonid on samaväärse kaitsetoimega.

INF.2.M8 Tulekahjusignalisatsioon [arhitekt, tuleohutusspetsialist]

a. Andmekeskuses on paigaldatud kõiki ruume kattev tulekahjusignalisatsioon.
b. Tulekahjusignalisatsiooni häiresõnumid edastatakse ettenähtud korras (vt INF.2.M13 *Valvesüsteem*).
c. Tulekahjusignalisatsiooni hooldatakse regulaarselt.
d. Andmekeskuses ei ole liigseid tuletundlikke materjale.

INF.2.M9 Tulekustutussüsteem ja kustutusvahendid [tehnikatalitus, tuleohutusspetsialist]

a. Andmekeskusesse on paigaldatud ajakohane automaatselt käivituv tulekustutussüsteem. Ilma automaatse tulekustutussüsteemita serveriruumidesse on paigaldatud tulekahju varaseks tuvastamiseks tule- ja suitsuandurid (vt INF.2.M17 *Tulekahju varajane tuvastamine*).
b. Töötajaid on teavitatud, kuidas tulekustutussüsteemi käivitumise puhul tegutseda.
c. Serveriruumi on paigaldatud vajaliku suurusega ning ettenähtud kustutusainega käsikustutid.
d. Tulekustuteid on piisav arv ning need on paigutatud kergesti juurdepääsetavatesse kohtadesse Tulekustutini on võimalik jõuda vähem kui kolme minutiga.
e. Andmekeskusesse või serveriruumi pääsuõigust omavad töötajad oskavad käsikustuteid ja tulekustutussüsteemi ohutult kasutada.
f. Tulekustuteid kontrollitakse ja hooldatakse regulaarselt.

INF.2.M10 Taristu ülevaatus ja hooldus [tehnikatalitus, hooldepersonal]

a. Ehitusliku ja tehnilise taristu komponentide hooldusel järgitakse tootja soovitatud või nõuetes määratud hooldusintervalle.
b. Taristu ülevaatused ja hooldetööd dokumenteeritakse.
c. Tule- ja suitsutõkkesektsioonide vaheliste kaabli- ja toruläbiviikude tuletõkestust kontrollitakse regulaarselt.

INF.2.M11 Taristu seire [tehnikatalitus]

a. Taristuautomaatika (nt lekketuvastus-, kliima-, elektrivarustus- ja UPS-süsteemide) tõrke- ja muid teateid seiratakse, võimalusel toimub seire automaatselt.

b. Teateid edastatakse ettenähtud viisil ja neile reageeritakse nii kiiresti kui võimalik.

c. Harva kasutatavatel serveriruumi IT- ja tugiseadmetel on olemas kaugseire võimalus.

INF.2.M17 Tulekahju varajane tuvastamine [arhitekt, tehnikatalitus]

a. Suitsu või vingugaasi varajaseks tuvastamiseks on andmekeskusesse ja serveriruumi paigaldatud tule -ja suitsuandurid.

b. Andurisignaalid edastatakse automaatselt häirekeskusesse, kus häirele reageeritakse maksimaalselt viie minuti jooksul.

c. IT-seadmete dubleerimisel on vastavad seadmed paigutatud erinevatesse elektritoite väljalülitustsoonidesse.

INF.2.M29 Juhistiku kontroll [arhitekt, tehnikatalitus]

a. Andmekeskusesse on paigaldatud üksnes andmekeskuse seadmete toiteks vajalikud elektrikaablid.

b. Juhistik on andmekeskuses või serveriruumis paigaldatud nõuetekohaselt, juhtmete kulgemistee on jälgitav.

c. Kui andmekeskust või serveriruumi läbib muid juhtmeid, on nende kasutamise põhjus dokumenteeritud. Ka neid juhtmeid käsitletakse ja kaitstakse andmekeskuses kehtivate nõuete kohaselt.

d. Juhtmete seisundit kontrollitakse regulaarselt.

3.3 Standardmeetmed

INF.2.M12 Andmekeskuse perimeetri turve [arhitekt, tehnikatalitus]

a. Andmekeskuse perimeetri turvameetmed vastavad turbe programmile ja hoone kaitsetarbele.

b. Andmekeskuse perimeetri turve hõlmab järgmisi meetmeid:
   - turvalised välispiirded;
   - andmekeskuse ümbritsemine aiaga;
   - meetmed piiratud territooriumile kogemata sattumise ärahoidmiseks;
   - meetmed andmekeskusesse sissetungi raskendamiseks:
   - välikaamerad ja videosalvestusseadmed;
   - inimeste ja sõidukite liikumise automaatne tuvastamine;
   - automaatne häire- ja hoiatussüsteem.

INF.2.M13 Andmekeskuse valvesüsteem [tehnikatalitus]

a. Valvesüsteemi kavandamisel on lähtutud andmekeskuse turvanõuetest ning arvestatud andmekeskuse hooneosade erineva kaitsetarbe ja võimaliku kasutusotstarbe muutusega.

b. Valvesüsteemi seadmed sobivad paigalduskoha keskkonnatingimustega.

c. Hooneosade kasutuse muudatuste korral kohandatakse valvesüsteemi konfiguratsiooni.

d. Valvesüsteemi teated ja alarmid on suunatud reageerimise eest vastutajatele, kellel on 24/7 võimekus häirele reageerimiseks.
e. Alarmiedastusteid testitakse regulaarselt.

INF.2.M14 Avariitoitegeneraator [arhitekt, tehnikatalitus]

a. Voolukatkestuse korral kasutatakse andmekeskuse toite tagamiseks lisaks UPS-idele avariitoitegeneraatorit.
b. Generaatorit hooldatakse regulaarselt, hoolduse kuupäev ja tehtud tööd dokumenteeritakse. Hoolduse käigus tehakse generaatori kontrollkäivitus.
c. Avariitoitegeneraatori kütus peab olema hoitud turvaliselt, vastavalt kütuse hoidmise nõuetele.
d. Avariitoitegeneraatori kütusevaru kontrollitakse regulaarselt. Kütuse kogus peab püsima lubatud piirides, kuid võimaldama toimepidevuse tagamist.
e. Generaatori kütusemahuti tankimised dokumenteeritakse.

INF.2.M15 Liigvoolukaitse [arhitekt, tehnikatalitus]

a. Liigvoolukaitsed ja nende paigaldus vastab standardile EVS-EN 62305-4 ja seadmete spetsifikatsioonidele.
b. Liigvoolukaitseid testitakse vähemalt üks kord aastas.

INF.2.M16 Andmekeskuse keskkonnatingimused [arhitekt, tehnikatalitus]

a. Andmekeskuses on loodud sobivad keskkonnatingimused.
b. Andmekeskuse õhutemperatuur ja -niiskus vastavad normtingimustele ja seadmete spetsifikatsioonidele.
c. Õhukonditsioneerid on valitud andmekeskuse tarbeks piisava võimsuse ja tõrkekindlusega.
d. Õhu parameetreid seiratakse regulaarselt, kõrvalekalletest teavitatakse vastutajat automaatselt.

INF.2.M19 Tehnilise taristu testimine [tehnikatalitus]

a. Andmekeskuse tehnilise taristu toimimist testitakse vähemalt üks kord aastas. Lisaks testitakse taristut pärast intsidente, olulisi süsteemimuudatusi või ulatuslikku remonti.
b. Taristu testimise tulemused dokumenteeritakse.

3.4 Kõrgmeetmed

INF.2.M21 Varuandmekeskus (A)

a. Avariiolukordade tarbeks on kasutusvalmis teises geograafilises asukohas paiknev varuandmekeskus.
b. Varuandmekeskus on suuteline jätkama kõiki andmekeskuses tehtavaid protsesse.
c. Operatiivandmed kas peegeldatakse või regulaarselt kopeeritakse põhiandmekeskusest.
d. Üleminekut varuandmekeskusele testitakse ja harjutatakse regulaarselt.
e. Varuandmekeskuse andmekanalid on turvalised ja dubleeritud.

INF.2.M22 Tolmutõrje [tehnikatalitus] (I-A)

a. Andmekeskuse ehitustöödel ja laiendamisel kavandatakse ja rakendatakse kaitset tolmu ja õhureostuse eest.

b. Tolmutõrje meetmete tõhusust kontrollitakse ehitustööde käigus regulaarselt. Kontrolle viivad läbi ehitustööde läbiviimisega otseselt mitteseotud isikud.

INF.2.M23 Andmekeskuse turvaline kaabeldus [tehnikatalitus] (A)

a. Andmekeskuse kaablid on kaitstud soovimatu mehaanilise koormuse, manipuleerimise, pealtkuulamise ja tulekahjustuse eest.

b. Kaablid ja kandesüsteemid vastavad andmekeskuse kaitsetarbest tulenevatele nõuetele.

c. Mitme toiteallikaga IT-seadmete kaablid ja muud üksteist dubleerivad kaablid on paigutatud eraldi kaablirennidesse ja lähevad ruumist välja erinevate läbiviikude kaudu.

INF.2.M24 Videovalvesüsteem [arhitekt, tehnikatalitus, andmekaitsespetsialist] (I-A)

a. Pääsu reguleerimise süsteeme ja sissemurdmise vastast valvesüsteemi on tundlikes asukohtades täiendatud videovalvesüsteemiga.

b. Videovalvesüsteemi kasutamine on vastavuses üldise turbekontseptsiooniga.

c. Videovalvesüsteemi kavandamisse on kaasatud ja videovalvesüsteemi kasutuselevõtu on kooskõlastanud andmekaitsespetsialist.

d. Videovalvesüsteemi keskseadmed asuvad turvalises keskkonnas ja on kaitstud volitamata juurdepääsu eest.

e. Videovalvesüsteemi toimimist kontrollitakse regulaarselt.

INF.2.M25 Puhvertoiteallikate dubleerimine [arhitekt] (A)

a. Andmekeskuse UPS-süsteemid on piisava liiasusega.

b. Kui andmekeskus on ühendatud mitme toiteliiniga, on iga toiteliin varustatud sõltumatu UPS-süsteemiga.

c. UPS-süsteemid tagavad andmekeskuse oluliste komponentide toite kuni alternatiivsele toiteallikale siirdumiseni.

INF.2.M26 Avariitoitegeneraatori dubleerimine [arhitekt] (A)

a. Suure käideldavustarbe korral on avariitoitegeneraator dubleeritud.

b. Avariitoitegeneraatorite süsteemi hooldatakse regulaarselt.

INF.2.M28 Kõrgendatud nõuetele vastav valvesüsteem [arhitekt] (I-A)

a. Andmekeskuse suure kaitsetarbega asukohtade valvesüsteem vastab standardi EVS-EN 50131-1 kategooriale (*Grade*) 3 või 4.

4 Lisateave

Lühend	**Publikatsioon**
[ISO62305]	EVS-EN 62305-4:2011 “Piksekaitse. Osa 4: Ehitiste elektri- ja elektroonikasüsteemid”

[ISO50131]	EVS-EN 50131-1:2006/A3:2020 “Häiresüsteemid. Sissetungi- ja paanikahäire süsteemid. Osa 1: Üldnõuded”

c.

INF.5 Tehnilise taristu ruum või kapp

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed tehnilise taristu ruumi või tehnilise taristu kapi turvalisuse tagamiseks. Tehnilise taristu ruumis võivad paikneda näiteks energiavarustuse- ja ventilatsiooniseadmed, sidesüsteemi komponendid, kaablipaneelid, kommutaatorid või ruuterid.

1.2 Vastutus

„Tehnilise taristu ruum või kapp“ turvameetmete täitmise eest vastutab infoturbejuht.

Lisavastutajad

Tehnikatalitus, IT-talitus, töötaja, arhitekt, hooldepersonal.

1.3 Piirangud

Serverite majutamisel rakendatakse täiendavalt meetmeid moodulist INF.2 Andmekeskus ja serveriruum. Kui kaitstavat tehnilist taristut ei saa eraldi ruumi paigutada, saab tehnilise taristu paigutada ka spetsiaalse varustusega kappi.

Tehnilise taristu ruumi side- ja elektrikaabeldust käsitletakse moodulis INF.12 Kaabeldus.

Väikses organisatsioonis, kus on ainult mõned kesksed IT-seadmed, rakendatakse antud moodulit mooduli INF.2 Andmekeskus ja serveriruum asemel.

2 Ohud

2.1 Halb planeering

Tehnilise taristu ruumi (tehnoruumi) ebasobiva asukoha korral võib ruumi tungida vesi. Otsese päikesepaiste tõttu võivad IT-komponendid üle kuumeneda. Ruumi ebasobiv asukoht suurendab oluliselt sissemurdmise võimalikkust.

Probleemid võivad tekkida ka juhul, kui ruumi ehitamisel on kasutatud madalakvaliteedilisi ehitusmaterjale, pole tagatud häireteta elektrivarustus või kui kaabeldus on ebakvaliteetne. Turvanõuetega mittearvestamine tehnilise taristu ruumi kavandamisel toob kaasa põhjendamatult suuri kulusid hilisemal planeeringuvigade parandamisel.

2.2 Lubamatu juurdepääs

Kui pääsukontroll pole piisav või sissemurdmist takistavad meetmed pole tõhusad, võivad volitamata isikud tehnilise taristu ruumi sisse pääseda ning seal tahtmatult (nt puudulike valdkonnateadmiste tõttu) või tahtlikult kahju põhjustada. Lisaks seadmevargusele saab ruumi pääsenud ründaja ruumis olevaid seadmeid asendada, manipuleerida või hävitada.

2.3 Ebapiisav ventilatsioon

Tehniliste seadmete ebapiisava ventilatsiooni tõttu tõuseb kinnises ruumis või kapis temperatuur üle seadmete normaalse töö piirnormi. Selle tagajärjel võivad seadmetes tekkida tõrked. Kõrge temperatuuri mõjul võivad tundlikud seadmed saada püsivaid kahjustusi.

2.4 Tuli

Tulekahjus võib tehnilise taristu ruum saada märkimisväärseid kahjustusi või hävida täielikult. Selle tulemusena katkevad äriprotsessid, mis ruumis asuvatest seadmest sõltuvad.

Levinud tulekahju põhjused on hooletus (nt kui ruumis suitsetamise tõttu süttivad tuleohtlikust materjalist kaablid ja seadmed) või seadmerike (nt kui kaitselülitid või seadmekaitsmed ülepinge korral ei rakendu). Tehnilise taristu ruumis tekkinud tulekahju võib levida teistesse hooneosadesse ja vastupidi, hoones puhkenud tulekahju võib levida ka tehnilise taristu ruumi.

2.5 Vesi

Tehnilise taristu ruumi üleujutus põhjustab veekahjustusi nii selles asuvatele seadmetele kui ruumile endale. Ruumi üleujutust tekitab lähedalasuvate veetorude leke, ummistus kanalisatsioonitorudes või tugeva saju tagajärjel ruumi tunginud vihmavesi. Veekahjustused võivad põhjustada lühiseid elektriseadmetes. Veega kokku puutumisel tekib seadmetes hallitus ja korrosioon.

2.6 Elektrikatkestus

Elektrikatkestuse tagajärjel ja varutoiteallika puudumisel seadmed seiskuvad, mis toob kaasa häireid organisatsiooni äriprotsessides. Elektritoite ootamatu ja kontrollimatu katkestus tekitab seadmetele kahjustusi, mille tegelik mõju selgub alles pärast elektrivarustuse taastumist. Seadme väljalangemine elektrikatkestuse tõttu võib tekitada ka kaudset kahju (nt kui pärast elektrikatkestust ei rakendu automaatselt tööle ventilatsiooniseade, võib temperatuur ruumis kiiresti tõusta ja teised seadmed võivad selle tõttu töötamast lakata).

2.7 Äike ja liigpinge

Välgutabamuse mõju võib kaasneva induktsiooniefekti tõttu olla ohtlik ka elektriseadmetele, mis asuvad välgutabamuse saanud punktist mõnesaja meetri kaugusel. Hetkeline ülepinge kaablites ja tehnilise taristu ruumi elektriseadmetes võib põhjustada häireid seadmete töös või isegi seadmete täieliku hävimise.

2.8 Elektromagnetilised häiringud

Tehnilise taristu ruumi või kapi lähedal asuvad elektromagnetilise välja allikad (nt liftimootor, saateantenn või piksekaitsesüsteemi maandus) võivad häirida automaatika- ja IT-seadme toimimist. Elektromagnetilised häiringud võivad põhjustada elektrit tarbivate tundlike komponentide tõrkeid ja kahjustusi. Ka tehnilise taristu ruumi seadmed ise võivad üksteise tööd häirida.

2.9 Elektrostaatilised häiringud

Elektrostaatilise laengu kogunemine ja ootamatu vallandumine näiteks seadme puudutamisel võib kahjustada tehnilise taristu ruumis asuvaid tundlike elektrooniliste komponentidega seadmeid. Raskemal juhul võib elektrostaatiline laeng seadme täielikult rikkuda.

3 Meetmed

3.1 Elutsükkel

Kavandamine

INF.5.M1 Tehnilise taristu ruumi turbe kavandamine
INF.5.M2 Tehnilise taristu ruumi sobiv asukoht ja suurus
INF.5.M4 Sissemurdmiskaitse
INF.5.M5 Elektromagnetiliste häireväljade vältimine ja kaitse nende eest
INF.5.M6 Tuletundlikkuse vähendamine
INF.5.M8 Kontrollimatu elektrostaatilise laengu vältimine
INF.5.M9 Sobiv elektrivarustussüsteem
INF.5.M10 Sobiv õhutemperatuur ja -niiskus
INF.5.M11 Kommunaal- ja gaasitorustike vältimine
INF.5.M12 Ühenduskanalite kaitse juhuslike kahjustuste eest
INF.5.M13 Kaitse tule- ja suitsukahjustuste eest
INF.5.M14 Naaberalade tuleohu minimeerimine
INF.5.M15 Pikse- ja liigpingekaitse
INF.5.M18 Tehnilise taristu ruumi asukoht

Käitus

INF.5.M3 Sissepääsu reguleerimine ja -kontroll
INF.5.M7 Ruumi otstarbekohane kasutamine
INF.5.M16 Puhvertoiteallika kasutamine
INF.5.M17 Taristu ülevaatus ja hooldus

Lisanduvad kõrgmeetmed

INF.5.M19 Tehnilise taristu varuasukoht
INF.5.M20 Laiendatud sissemurdmiskaitse
INF.5.M22 Varutoide
INF.5.M23 Avariitoitegeneraator
INF.5.M24 Ventilatsioon ja jahutus
INF.5.M25 Tugevam kaitse tule- ja suitsukahjustuste eest
INF.5.M26 Elektrivarustuse seire

3.2 Põhimeetmed

INF.5.M1 Tehnilise taristu ruumi turbe kavandamine [arhitekt]

a. Tehnilise taristu ruumides on kaitsetarbest, õigusaktidest ja eeskirjadest lähtuvalt rakendatud sobivad tehnilised ja korralduslikud turvameetmed.
b. Turbe kavandamisel on arvestatud ruumi asukohast tingitud keskkonna- ja sissetungiohtudega.

INF.5.M2 Tehnilise taristu ruumi sobiv asukoht ja suurus [arhitekt]

a. Tehnilise taristu ruum ei ole läbikäidav. Tehnilise taristu kapp ei asu läbikäidavas kohas.

b. Töötamiseks ja vajadusel evakueerumiseks on piisavalt ruumi.

INF.5.M3 Pääsu reguleerimine ja kontroll [tehnikatalitus, IT-talitus]

a. On määratud, kellel, millises ajavahemikus ja missugusel eesmärgil on tehnilise taristu ruumide pääsuõigus.

b. Välditakse põhjendamatult ulatuslike pääsuõiguste andmist.

c. Kõik tehnilise taristu ruumis viibimised registreeritakse.

INF.5.M4 Sissemurdmiskaitse [arhitekt, tehnikatalitus]

a. Tehnilise taristu ruum on kaitstud lubamatu sissepääsu eest.

b. Tehnilise taristu ruumi seinad, laed, põrandad, aknad ja uksed vastavad ruumi kaitsetarbele.

c. Piirete sissemurdmiskindlus vastab standardi EVS-EN 1627 nõuetele. Ruumi uksel on sobiv kaitseklass.

INF.5.M5 Kaitse elektromagnetiliste häiringute eest [arhitekt]

a. On testitud, et tehnilise taristu ruumi vahetus läheduses puudub häiriv elektromagnetkiirgus.

b. Tehnilise taristu ruum või kapp ei asu suurte elektrimootorite (nt liftimootorid) vahetus läheduses.

INF.5.M6 Tuletundlikkuse vähendamine [töötaja, arhitekt]

a. Tehnilise taristu ruumis ja selle vahetus läheduses ei hoiustata tuleohtlikke materjale.

b. Ruumi piirdekonstruktsioon ja ruumi sisustuselemendid ei sisalda tuletundlikke materjale.

INF.5.M7 Ruumi otstarbekohane kasutamine [töötaja, arhitekt]

a. Tehnilise taristu ruumi ei kasutata ettenähtust erinevaks otstarbeks.

INF.5.M9 Sobiv elektrivarustussüsteem [tehnikatalitus]

a. Tehnilise taristu ruumi madalpingevõrk on koostatud TN-S (eraldatud neutraal- ja kaitsejuhiga) juhistikusüsteemis.

INF.5.M16 Puhvertoiteallikas (UPS) [tehnikatalitus]

a. On määratud, millised seadmed peavad olema puhvertoiteallikaga ühendatud ning milliseid seadmeid UPS-iga ühendada ei tohi.

b. Puhvertoiteallika pinge ja voolutugevus on kalkuleeritud vastavalt ühendatud elektritarvititele. Oluliste elektritarbimist mõjutavate muudatuste järgselt kontrollitakse UPS-süsteemide võimekuse piisavust.

c. Puhvertoiteallika akude eluea pikendamiseks hoitakse akusid optimaalses temperatuurivahemikus.

d. UPS-i varutoite ajaline kestvus on piisav kõigi temaga ühendatud elektritarvitite turvaliseks väljalülitamiseks.

e. Puhvertoiteallikat hooldatakse ja selle töövõimet kontrollitakse vähemalt tootja soovitatud regulaarsusega.

3.3 Standardmeetmed

INF.5.M8 Kontrollimatu elektrostaatilise laengu vältimine [arhitekt]

a. Tehnilise taristu ruumi on paigaldatud elektrostaatilisi laenguid mittekoguv põrandakate, mis vastab standardile EVS-EN 14041.

INF.5.M10 Sobiv õhutemperatuur ja -niiskus [tehnikatalitus]

a. Tehnilise taristu ruumi õhutemperatuur ja -niiskus jäävad käitatavate seadmete spetsifikatsioonides ettenähtud väärtuste piiresse.

b. Ventilatsioonisüsteem on piisava võimsusvaruga.

INF.5.M11 Kommunaal- ja gaasitorustike vältimine [arhitekt, tehnikatalitus]

a. Tehnilise taristu ruumis paikneb ainult ruumis asuva tehnoloogia käitamiseks vajalik torustik.

b. Tehnilise taristu ruumi ei läbi vee-, gaasi-, kütuse-, kütte-, kanalisatsiooni- vms torud.

INF.5.M12 Ühenduskanalite kaitse juhuslike kahjustuste eest [arhitekt]

a. Väljaspool tehnilise taristu ruumi asuvad ühenduskanalid (nt kaitsetorud ja kaablikanalid) on kaitstud juhuslike kahjustuste eest.

INF.5.M13 Kaitse tule- ja suitsukahjustuste eest [arhitekt, tehnikatalitus]

a. Kõikidel konstruktsioonielementidel (sh ustel ja akendel) on sarnased suitsu levikut takistavad omadused.

b. Tehnilise taristu ruumi piirdekonstruktsioon peab tulele ja suitsule vastu vähemalt 30 minutit.

c. Kaablitrasside ligiduses ei ole tuleohtlikke materjale.

INF.5.M14 Naaberalade tuleohu minimeerimine [arhitekt, tehnikatalitus]

a. Tehnilise taristu ruumi vahetus läheduses ei asu tuleohtlikke materjale sisaldavaid tehnoruume.

INF.5.M15 Pikse- ja liigpingekaitse [arhitekt, tehnikatalitus]

a. Hoone elektrisüsteem on kaitstud liigpinge eest.

b. Tehnilise taristu ruum vastab vähemalt standardi EVS-EN 62305 piksekaitsetsoonile 2 (LPZ 2).

c. Liigpingekaitseseadmeid kontrollitakse regulaarselt, vajadusel seadmed asendatakse.

INF.5.M17 Taristu ülevaatus ja hooldus [tehnikatalitus, IT-talitus, hooldepersonal]

a. Ehitusliku ja tehnilise taristu komponentide hooldusel järgitakse tootja soovitatud või normdokumentides määratud hooldusintervalle.

b. Tule- ja suitsutõkkesektsioonide vaheliste kaabli- ja toruläbiviikude tuletõkestust kontrollitakse regulaarselt.

c. Taristu ülevaatused ja hooldetööd dokumenteeritakse.

3.4 Kõrgmeetmed

INF.5.M18 Tehnilise taristu ruumi asukoht [arhitekt] (C-A)

a. Tehnilise taristu ruumi kavandamisel on arvestatud siseste ja väliste ohtudega.

b. Tehnilise taristu ruum on kaitstud veega (nt vihm, vesi, heitvesi) seotud ohtude eest. Ruumi paiknemisel hoone ülemisel korrusel on tagatud, et vesi ei pääseks hoonesse katuselt.

c. Tehnilise taristu ruumid on kaitstud päiksekiirgusest tingitud soojenemise eest.

INF.5.M19 Tehnilise taristu varuasukoht [arhitekt] (A)

a. Avariiolukorra puhul saab tehnilise taristu ümber kolida teise selleks otstarbeks ettevalmistatud asukohta.

b. Tehnilise taristu pea- ja varuruumi toide on võetud mitmest elektrijaotusseadmest.

c. Ruumid paiknevad eraldi tuletõkkesektsioonides ning neil on üksteisest sõltumatud õhukonditsioneerimissüsteemid.

INF.5.M20 Laiendatud sissemurdmiskaitse [arhitekt] (C-I-A)

a. Tehnilise taristu ruum on ilma akendeta. Akende olemasolul on need alati suletud ja akende kaitseks on rakendatud korruse kõrgusest tulenevaid kaitsemeetmeid.

b. Ruumi muud pääsuavad peale akende ja uste (nt ventilatsioonikanalid) on kaitstud teiste piirdekonstruktsioonidega samaväärselt.

c. Tehnilise taristu ruumis olev valvesignalisatsioon katab kõiki aknaid, uksi ja muid pääsuavasid.

d. Side- ja elektrikaablid on volitamata juurdepääsu eest kaitstud täies ulatuses.

e. Piirdekonstruktsioonide, sh akende ja uste, murdmiskindlus vastab ruumi kaitsetarbele.

f. Lukkude, lukusüdamike ja turvaliistude kvaliteet vastab ukse kaitseklassile.

INF.5.M22 Varutoide [arhitekt] (A)

a. Elektrivarustus on peajaotuskilbist kuni tehnilise taristu ruumi elektritarvititeni dubleeritud eraldi tuletõkkesektsioonis asuvate toiteliinidega.

b. Madalpinge jaotussüsteemis on varuliinide lisamise võimalus.

INF.5.M23 Avariitoitegeneraator [arhitekt, tehnikatalitus, hooldepersonal] (A)

a. Energiavarustusettevõtte võrgutoidet täiendab avariitoitegeneraator.

b. Avariitoitegeneraatori kütus peab olema hoitud turvaliselt, vastavalt kütuse hoidmise nõuetele.

c. Avariitoitegeneraatori kütusevaru kontrollitakse regulaarselt. Kütuse kogus peab püsima lubatud piirides, kuid võimaldama toimepidevuse tagamist.

d. Avariitoitegeneraatoreid hooldatakse regulaarselt.

e. Avariitoitegeneraatori hoolduse käigus tehakse generaatori kontrollkäivitusi ja koormustestimist.

INF.5.M24 Ventilatsioon ja jahutus [arhitekt, tehnikatalitus, hooldepersonal] (A)

a. Tehnilise taristu ruumide ventilatsiooni- ja jahutusseadmed on dubleeritud.

b. Ventilatsiooni- ja jahutussüsteeme hooldatakse regulaarselt.

c. Väga suure kaitsetarbe korral on ventilatsiooni- ja jahutusseadmete hooldus dubleeritud.

INF.5.M25 Tugevam kaitse tule- ja suitsukahjustuste eest [arhitekt] (A)

a. Tehnilise taristu ruumi piirdekonstruktsioon, õhuklapid ja toiteliinid peavad tulele ja suitsule vastu vähemalt 90 minutit.
b. Väga suure kaitsetarbe korral käsitletakse üksikuid ruume iseseisvate tuletõkkesektsioonidena.
c. Kaablitrassid väljapool tehnilise taristu ruumi paiknevad eraldi tuletõkkesektsioonides.
d. Tehnilise taristu ruumidesse on paigutatud tsentraalse tulekahjusignalisatsiooniga ühendatud tule- ja suitsuandurid.
e. Ventilatsioonikanalitesse on paigutatud suitsuanduritele reageerivad tuletõkkeklapid.
f. Väga suure kaitsetarbe korral on tehnilise taristu ruumi paigaldatud automaatne tulekustutussüsteem.
g. Tulekahjusignalisatsioon, suitsuandurid ja automaatne kustutussüsteem on ühendatud puhvertoiteallika ja avariitoitegeneraatoriga.

INF.5.M26 Elektrivarustuse seire [arhitekt, tehnikatalitus] (A)

a. On paigaldatud seireseadmed elektrivarustuse tõrgete avastamiseks ja tõrgetest teavitamiseks.
b. Lekke- ja tasandusvoolude testmõõtmisi tehakse regulaarselt.

4 Lisateave

Lühend	**Publikatsioon**
[ISO1627]	EVS-EN 1627:2021 “Uksed, aknad, rippfassaadid, võred ja luugid. Sissemurdmiskindlus. Nõuded ja klassifikatsioon”
[ISO14041]	EVS-EN 14041:2018 “Elastsed, tekstiil-, laminaat ja mitmekihilised põrandakatted. Põhiomadused”
[ISO62305]	EVS-EN 62305-4:2011 “Piksekaitse. Osa 4: Ehitiste elektri- ja elektroonikasüsteemid”

d.

INF.6 Andmekandjate arhiiv

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed andmekandjate arhiivi ja arhiveeritavatel andmekandjatel oleva teabe kaitseks. Moodulit rakendatakse kõikidele ruumidele, mida kasutatakse andmekandjate arhiivina.

1.2 Vastutus

Andmekandjate arhiivi meetmete täitmise eest vastutab infoturbejuht.

Lisavastutajad

Tuleohutusspetsialist, tehnikatalitus, töötaja, arhitekt.

1.3 Piirangud

Moodulis käsitletakse andmekandjate arhiivi turvameetmeid. Arhiveerimist käsitlevad meetmed esitatakse moodulis OPS.1.2.2 *Arhiveerimine*.

2 Ohud

2.1 Lubamatu temperatuur ja õhuniiskus

Pikaajaliselt säilitatavate andmekandjate hoidmisel võivad temperatuurimuutused ja liigne õhuniiskus põhjustada vigu andmetes ja lühendada andmekandjate säilimisaega.

2.2 Eeskirjade puudumine või puudulikkus

Kui tööks arhiiviruumis pole kehtestatud korda, võivad töötajad tahtmatult põhjustada ohtlikke olukordi. Näiteks kui töötajad pärast andmekandjate arhiivist lahkumist aknaid ja uksi ei sulge ega lukusta, saab andmekandjad arhiivist varastada. Volitamata isikud pääsevad ligi tundlikele andmetele, saavad neid vaadata, salvestada või edastada. Probleemid tekivad ka siis, kui tegevuskord on olemas, kuid seda ei järgita.

2.3 Lubamatu sissepääs kaitset vajavatesse ruumidesse

Puuduliku või olematu pääsukontrolli puhul saavad volitamata isikud siseneda andmekandjate arhiivi ja tundlikku teavet vaadata, varastada või manipuleerida. Sõltumata esialgselt tekitatud kahju suurusest võivad manipuleeritud andmed oluliselt tööprotsesse mõjutada.

2.4 Vargus

Andmekandjate väiksuse tõttu on neid lihtne märkamatult taskusse või riiete alla peita ja endaga kaasa võtta. Kui andmetest varukoopiat ei ole, jääb organisatsioon nendest andmetest ilma. Andmekandja varastanud isikutel on võimalus konfidentsiaalseid andmeid vaadata ja need avalikustada. Vargusest tekkiv kahju on märkimisväärselt suurem kui andmekandja asendamise kulu.

3 Meetmed

3.1 Elutsükkel

Kavandamine

INF.6.M1 Käsikustutid

INF.6.M3 Kaitse tolmu ja määrdumise eest

INF.6.M6 Veetorude vältimine

INF.6.M7 Sobiv sisekliima

Evitus

INF.6.M8 Turvalised uksed ja aknad

Käitus

INF.6.M2 Sissepääsu reguleerimine ja kontroll

INF.6.M4 Akende ja uste sulgemine ja lukustamine

INF.6.M5 Kaitsekapid

Lisanduvad kõrgmeetmed

INF.6.M9 Valvesüsteem

3.2 Põhimeetmed

INF.6.M1 Käsikustutid [tuleohutusspetsialist]

a. Andmekandjate arhiivi on paigaldatud gaasiga käsikustutid (kaaluga kuni 20 kg).
b. Tulekahju korral on käsikustutid kergesti juurdepääsetavad.
c. Käsikustuteid kontrollitakse ja hooldatakse regulaarselt.
d. Töötajad teavad käsikustutite asukohti ja oskavad käsikustuteid kasutada.

INF.6.M2 Sissepääsu reguleerimine ja kontroll [tehnikatalitus]

a. Sissepääs andmekandjate arhiivi on ametipõhiselt piiratud.
b. Pääsusüsteem võimaldab juurdepääsu ainult volitatud isikutele.
c. Väljastatud pääsuõigused dokumenteeritakse, töötajad on võimelised tuvastava volitamata isikud.
d. Pääsukontrolli meetmete tõhusust kontrollitakse regulaarselt.
e. Arhiiviruumi sissetungikindlus on vähemalt RC2 standardi EVS-EN 1627 järgi.

INF.6.M3 Kaitse tolmu ja määrdumise eest [töötaja]

a. Tolmu ja määrdumise eest kaitsmise vajadusega on arvestatud juba arhiiviruumi rajamisel.
b. Andmekandjad on pakendatud ja ladustatud viisil, et tolm neid isegi pikaajalisel hoidmisel ei kahjustaks.
c. Suitsetamine andmekandjate arhiivis on rangelt keelatud.

INF.6.M4 Akende ja uste sulgemine ja lukustamine [töötaja]

a. Andmekandjate arhiiv on võimalusel ilma akendeta. Akende olemasolul suletakse need enne arhiivist lahkumist.
b. Ajal, mil andmekandjate arhiivis kedagi ei viibi, on kõik arhiivi aknad suletud ja uksed lukustatud.
c. Akende sulgemise ja uste lukustamise nõue on sätestatud arhiiviruumi kasutamise eeskirjas.
d. Töötajad on tutvunud arhiiviruumi kasutamise eeskirjaga ja järgivad seda.
e. Akende ja uste sulgemist ja lukustatust kontrollitakse regulaarselt.

3.3 Standardmeetmed

INF.6.M5 Kaitsekapid [töötaja]

a. Andmekandjate kaitsmiseks tule ja volitamata kasutamise eest hoitakse arhiivis andmekandjaid sobivates kaitsekappides.

INF.6.M6 Veetorude vältimine [tehnikatalitus]

a. Andmekandjate arhiivis asuvad ainult veetorud, mis on vältimatult vajalikud.

b. Andmekandjate arhiivi läbivate veetorude lekkekindlust kontrollitakse regulaarselt.

c. On rakendatud meetmed lekete varajaseks tuvastamiseks (lekkeandurid) ja kahjude vähendamiseks (vee äravoolukanalid).

d. Suure kaitsetarbega arhiivi tarbeks on koostatud intsidendihalduse kava, mis määratleb, keda lekke korral teavitatakse ja kuidas lekke peatamisel toimitakse.

INF.6.M7 Sobiv sisekliima [tehnikatalitus]

a. Andmekandjate arhiivi õhutemperatuur, -niiskus ning tahkete osakeste sisaldus õhus on andmekandjate tootjate sätestatud piirides.

b. Arhiivi ventilatsiooni- ja kliimaseadmeid kontrollitakse ja hooldatakse regulaarselt.

c. Õhutemperatuuri ja -niiskuse näidud registreeritakse. Kõrvalekalletele reageeritakse koheselt.

INF.6.M8 Turvalised uksed ja aknad [arhitekt]

a. Arhiivi piirdekonstruktsioonide murdmiskindlus on vähemalt RC3 standardi EVS-EN 1627 järgi.

b. Uste ja akende tule- ja suitsukindlus on piisav.

c. Arhiiviruumi piirdekonstruktsioonide sissetungi-, tule- ja suitsukindlus on samaväärne.

d. Uste ja akende turvalisust kontrollitakse regulaarselt.

3.4 Kõrgmeetmed

INF.6.M9 Valvesüsteem [tehnikatalitus] (C-I-A)

a. Andmekandjate arhiivi on paigaldatud kaitsetarbele vastav (tsentraalne või lokaalne) valvesüsteem.

b. Valvesüsteemi teated ja alarmid on suunatud reageerimise eest vastutajatele, kellel on 24/7 võimekus häirele reageerimiseks.

c. Valvesüsteemi kontrollitakse ja hooldatakse regulaarselt.

4 Lisateave

Lühend	Publikatsioon
[ISO1627]	EVS-EN 1627:2021 “Uksed, aknad, rippfassaadid, võred ja luugid. Sissemurdmiskindlus. Nõuded ja klassifikatsioon”

INF.7 Bürootöökoht

1 Kirjeldus

1.1 Eesmärk

Esitada bürooruumidele ja bürootöökohtadele kohandatavad infoturbemeetmed. Bürootöökoht on organisatsioonisisene ala, mida üks või mitu töötajat kasutavad oma tööülesannete täitmiseks.

1.2 Vastutus

Bürootöökoha meetmete täitmise eest vastutab infoturbejuht.

Lisavastutajad

Tehnikatalitus, töötaja, ülemus, haldusosakond.

1.3 Piirangud

Moodulis ei käsitleta IT-süsteemide konfigureerimise ja turbega seotud soovitusi, need meetmed on esitatud SYS mooduligrupis. Bürooruumide kaabeldusega seotud meetmed esitatakse moodulis INF.12 Kaabeldus. Hoonete tuleohutuse ja pääsu reguleerimise meetmed on esitatud moodulis INF.1 Hoone üldiselt.

2 Ohud

2.1 Lubamatu sissepääs

Puuduliku või olematu pääsukontrolli puhul saavad volitamata isikud siseneda bürooruumidesse ja tundlikku teavet vaadata, varastada või manipuleerida. Sõltumata esialgselt tekitatud kahju suurusest võivad manipuleeritud andmed oluliselt tööprotsesse mõjutada.

2.2 Ebasobivad töötingimused

Mitteergonoomiline töökoht, ebaefektiivne ruumikasutus või ebasobiv töökeskkond võivad tähendada ohtu ruumis töötavate inimeste tervisele ja töövõimele. Bürooruumide müratase, klientide sage liikumine, halb valgustus või puudulik ventilatsioon põhjustavad töötaja töövõime langust. Kui töötajad ei saa häirimatult keskenduda, suureneb inimlike vigade arv ja tekib oht andmete terviklusele.

2.3 Külastajate ja välispersonaliga seotud ohud

Ka isikud, kes viibivad bürooruumides külastajana või on täitmas ajutist tööülesannet, võivad olla ohuks organisatsiooni turvalisusele. Külalisena ruumides viibijale paljastatakse tahtmatult organisatsiooni siseteavet. Välise teenuseandja töötaja saab lugeda laokile jäetud dokumente või pääseda läbi lahti jäetud arvuti ligi organisatsiooni IT-süsteemidele.

Koristusettevõtte töötaja võib asjatundmatusest rikkuda mõne olulise tehnilise seadme või kogemata visata olulised dokumendid prügikasti. Koristuse käigus võib IT-seadmetesse sattuda vett, mistõttu seade kas kohe või mõne aja möödudes lakkab töötamast.

2.4 IT varade manipuleerimine või hävitamine

Ründaja võib võtta organisatsiooni IT-süsteemide ja varade hävitamise omaette eesmärgiks. Andmekandja hävitamine või manipuleerimine võib kaasa tuua märkimisväärseid seisakuid

tööprotsessides. Ründe mõju on seda laiaulatuslikum, mida hiljem see avastatakse ja mida laiemad on toimepanija teadmised.

2.5 Vargus

Kui büroouume ei lukustata või kui IT-seadmeid piisavalt ei turvata, on andmekandjat või nutiseadet väga lihtne kiiresti ja märkamatult taskusse pista ja endaga kaasa võtta. Vargusest tekkiv kaudne kahju on märkimisväärselt suurem kui andmekandja asendamise kulu.

IT-seadme või andmekandja varastanud isik võib ligi pääseda konfidentsiaalsetele andmetele, neid oma huvides ära kasutada või avalikustada.

2.6 Kaabelduse korraldamatus

Olenevalt sellest, kui läbimõeldult on büroouumides lahendatud kaabliühenduste ja pistikute paigutus, kasutavad töötajad kas vajaduse või mugavuse tõttu pikendusjuhtmeid või kaablipikendusi. Tihti on pikendusjuhtmed veetud üle põranda ja käiguteede. Sellise vaba kaabelduse tulemusena võivad inimesed komistada ja ennast vigastada. Samuti võivad töötajad kaabli taha takerdudes tõmmata laualt maha või muud moodi rikkuda mõne IT-seadme.

3 Meetmed

3.1 Elutsükkel

Kavandamine

INF.7.M1 Sobiva büroouumi valimine

INF.7.M3 Toite- ja sidekaablite turvaline paigutus

INF.7.M5 Ergonoomiline töökoht

Käitus

INF.7.M2 Akende sulgemine ja uste lukustamine

INF.7.M6 Korras töökoht

INF.7.M7 Dokumentide ja andmekandjate hoiustamise kord

Lisanduvad kõrgmeetmed

INF.7.M8 Vargusvastased vahendid

3.2 Põhimeetmed

INF.7.M1 Sobiva büroouumi valimine [ülemus]

a. Büroouumidena kasutatakse ainult selleks kasutusotstarbeks ettenähtud ja vastavalt sisustatud ruume.

b. Ruumi turve ja pääsukontrollisüsteemid vastavad ruumis käideldava teabe kaitsetarbele.

c. Üldkasutatavad büroouumid on eraldatud kõrge kaitsetarbega aladest.

INF.7.M2 Akende sulgemine ja uste lukustamine [töötaja, haldusosakond]

a. Töövälisel ajal on büroouumi aknad suletud.

b. Juhul, kui büroouumis hoitakse konfidentsiaalset teavet, lukustavad töötajad ruumist lahkudes ukse.

c. Tule- ja suitsutõkkeuksed on alati suletud.

d. Akende ja uste sulgemise ja lukustamise kohustus on sätestatud eeskirjaga, töötajad on eeskirjaga tutvunud ja järgivad seda.

e. Eeskirja järgimist akende sulgemisel ja uste lukustamisel kontrollitakse regulaarselt.

INF.7.M6 Korras töökoht [töötaja]

a. Töötaja on kohustatud oma töökoha korras hoidma. Töökohal ei ole liigseid dokumente, andmekandjaid ega muid esemeid.

b. Töötaja kaitseb IT-rakendusi ja tundlikku teavet lubamatu juurdepääsu eest.

c. Kuvariekraan ei asu kõrvaliste isikute nägemisväljas, vajadusel kasutatakse ekraanifiltrit.

d. Töötaja eemalolekul tema töökohast on ekraan lukus ning andmekandjad ja dokumendid laualt ära pandud (tühja laua poliitika).

e. Töökoha korrasolekut kontrollitakse pisteliselt.

3.3 Standardmeetmed

INF.7.M3 Toite- ja sidekaablite turvaline paigutus

a. Toite- ja võrgupesade arv bürooruumis on piisav ja nende asukoht on IT-seadmete läheduses.

b. Kui lahtiste toite- või sidekaablite asetamine põrandale on vältimatu, kaetakse kaablid kaablikaitselindiga.

INF.7.M5 Ergonoomiline töökoht [haldusosakond, ülemus]

a. Töötajate töökohad on ergonoomilised ja vastavad töökaitsenõuetele.

b. Arvutitöökoha laud ja tool on töötaja individuaalsete vajaduste kohaselt reguleeritavad.

c. Kuvar, klaviatuur ja hiir on ergonoomilised, võimaluste piires on nende valikul arvestatud töötaja harjumusi.

d. Arvutiga töötajatele on kehtestatud kuvariga töötamise kord, mis sätestab regulaarsete puhkepauside tegemise.

INF.7.M7 Dokumentide ja andmekandjate hoiustamise kord [töötaja, tehnikatalitus]

a. Bürooruumides või nende läheduses on piisava hoiustusmahuga hoidlad tundlikku teavet sisaldavate dokumentide ja andmekandjate hoidmiseks.

b. Tundlikku teavet sisaldavad dokumendid ja andmekandjad, mida hetkel ei kasutata, on paigutatud igale töötajale eraldatud lukustatavasse sahtliboksi või kappi.

c. Tundliku materjali hoiukoha ja luku murdmiskindlus vastab teabe kaitsetarbele.

3.4 Kõrgmeetmed

INF.7.M8 Vargusvastased vahendid [töötaja] (C-I-A)

a. Pääsukontrollisüsteemi puudumisel on IT-seadmed turvatud kas mehhaaniliste (nt trosslukk, *Kensington Lock* lukk) või elektrooniliste vargusvastaste vahenditega.

b. IT-seadmete kasutamisel üldkasutatavates ruumides on vargusvastaste kaitsevahendite kasutamine kohustuslik.

INF.8 Kodutöökoht

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed organisatsiooni teabe kaitseks ja turvalise taristu rajamiseks kodutöökohas. Üldjuhul on kodutöökoht juurdepääsetav ka pereliikmetele, külalistele ja lemmikloomadele.

1.2 Vastutus

Kodutöökoha meetmete täitmise eest vastutab töötaja.

1.3 Piirangud

Moodulit INF.8 Kodutöökoht rakendatakse ruumide korral, mida kasutatakse kaugtöökohana. IT-süsteemide turvameetmeid käsitletakse moodulis OPS.1.2.4 Kaugtöö ja vastavates süsteemikohastes moodulites. Moodulit täiendavad meetmed moodulitest NET.3.3 Virtuaalne privaatvõrk (VPN) ja SYS.2.1 Klientarvuti üldiselt.

2 Ohud

2.1 Kodus töötamise eeskirja puudumine või puudulikkus

Kui kodus töötamiseks puuduvad konkreetsed tegevusjuhised, võib IT-süsteemide kasutamine ebaõnnestuda ja seeläbi tekkida pikemaid tööseisakuid. Kui IT-probleeme ei õnnestu kaughalduse kaudu lahendada, on erakorralistel juhtudel vajalik IT-töötaja kohalesõit, mis tekkinud seisakuaega veelgi pikendab.

Kui kodus töötamise eeskirjaga ei ole sätestatud siseteabe töötlemise korda, võib töötaja talletada tundlikke andmeid ebaturvalisse asukohta, näiteks koduarvutisse, millele võivad pääseda ligi ka teised pereliikmed. Tekib oht andmete konfidentsiaalsusele ja terviklusele.

2.2 Lubamatu sissepääs kodutöökohta

Kodutöökoha ruumidele, kus töödeldakse kaitset vajavaid andmeid või hoitakse kaitset vajavaid seadmeid, pääsevad juurde volitamata isikud. Järelevalveta jäetud arvuti varastatakse või nakatatakse kahjurvaraga. Koos varastatud IT-seadmega kaotatakse ka olulised andmed. Ka tundlikke dokumente ei saa koduses töökohas piisavalt turvata ja lubamatu juurdepääsu eest kaitsta.

2.3 Ebasobivad töötingimused

Kodutöökohas ei saa alati tagada tööks sobivat töökeskkonda. Arvuti kasutamine pole ergonoomiline, mistõttu pikaajaline järjest töötamine vähendab tootlikust ja mõjub halvasti töötaja tervisele. Ümbritsev müra, pereliikmete ja koduloomade põhjustatud häiringud mõjuvad ebasoodsalt ja võivad tekitada andmete sisestusvigu. Tihti on probleemiks ka ebapiisav valgustus või halb ventilatsioon.

2.4 Andmekandjate ja dokumentide ebaturvaline transport

Organisatsiooni ja kodutöökoha vahelise transportimise käigus võivad dokumendid või andmekandjad sattuda varguse objektiks ja kaotsi minna. Volitamata isikud võivad saada juurdepääsu tundlikele andmetele, neid lugeda või manipuleerida. Krüpteerimata andmekandjate sattumisel valedesse kätesse võib tekkida märkimisväärne konfidentsiaalsuse kadu.

Kui transportimise käigus läheb kaduma andmekandja, millel puudub varukoopia, siis võib see organisatsiooni eesmärkide täitmist olulisel määral mõjutada.

2.5 Andmekandjate ja dokumentide ebaturvaline kõrvaldamine

Kui kodutöökohas pole loodud tingimusi andmekandjate ja dokumentide turvaliseks kõrvaldamiseks, võivad need sattuda olmeprügi hulka. Ründaja võib seeläbi saada väärtuslikku teavet, mida saab sihipäraselt ära kasutada organisatsioonivastaste küberkuritegude (nt petukirja koostamine) või väljapressimiskatsete läbiviimiseks. Tagajärjed võivad raskemal juhul ohustada terve organisatsiooni tegevust, näiteks kui ründe tulemuseks on oluliste tellimuste nurjumine või partnerlussuhete katkemine.

2.6 IT-seadmete, andmete või tarkvara manipuleerimine või rikkumine

IT-seadmete rikkumine kodutöökohas on palju tõenäolisem kui organisatsiooni ruumides. Ka andmete manipuleerimine on töökohast eemal olevas asukohas lihtsam, sest puuduvad bürooruumides rakendatud turvameetmed ning pole ka kaastöötajaid, kes andmete manipuleerimist või seadmete rikkumist võiksid märgata ja takistada.

Kui IT-seade läheb kodutöökohas katki, ei saa töötaja tihti tööd jätkata või saab seda ainult piiratud mahus. Hävitatud IT-komponentide asendamine kodutöökohas nõuab aega ja IT-töötajate ressurssi, mistõttu töökatkestus võib venida väga pikaks.

2.7 Vargusoht kodutöökohas

Kodutöökoht ei ole enamasti nii hästi kaitstud kui organisatsiooni ruumid. Eramus võivad puududa bürooruumidele omased turvameetmed nagu turvauksed, turvateenus või valvekaamerad. Seetõttu on kodus oht, et keegi pääseb lubamatult hoonesse, palju suurem kui bürooruumide puhul. Sissetungijad varastavad enamasti esmalt kallihinnalisi ja kiiresti ning lihtsalt müüdavaid esemeid. Sellesse kategooriasse kuuluvad ka IT-seadmed. Kuna organisatsioonile tekib sellest rohkem kahju kui seda on seadme turuväärtus, siis teadlikum sissetungija proovib saada suuremat kasu väljapressimise või andmete edasimüümise teel.

3 Meetmed

3.1 Elutsükkel

Kavandamine

INF.8.M4 Kodutöökoha õige korraldus

Käitus

INF.8.M1 Dokumentide ja andmekandjate turve kodutöökohas

INF.8.M2 Dokumentide ja andmekandjate turvaline transportimine kodutöökohta

INF.8.M3 Kaitse lubamatu sissepääsu eest kodutöökohta

Väljavahetamine

INF.8.M5 Konfidentsiaalsete andmete turvaline kõrvaldamine

Lisanduvad kõrgmeetmed

INF.8.M6 Suure kaitsetarbega töödokumentide turvalisem käsitlemine kodutöökohas

3.2 Põhimeetmed

INF.8.M1 Dokumentide ja andmekandjate turve kodutöökohas

a. Tööalased dokumendid ja andmekandjad on kodutöökohas kaitstud volitamata juurdepääsu eest.
b. Tundlikke andmeid sisaldavad andmekandjad on krüpteeritud.
c. Töökohast eemal viibimise ajal on tööruum lukus. Kui ruumi ei saa lukustada, asuvad dokumendid ja andmekandjad lukustatud kapis või laualaekas.
d. Töötaja lühiajalisel eemalviibimisel töökohast lukustatakse kuvari ekraan, töötaja pikaajalisel eemalviibimisel on arvuti suletud.
e. Töötaja hoiab kodutöökoha korras ja töölaua liigsetest tööpaberitest ja dokumentidest puhtana.

INF.8.M2 Dokumentide ja andmekandjate turvaline transportimine kodutöökohta

a. On kehtestatud organisatsiooni dokumentide ja andmekandjate käitlemise kord, mis määrab:
   - milliseid materjale ja millisel viisil on lubatud transportida (post, kuller vm);
   - milliseid turvameetmeid rakendatakse transpordil (sobiv pakend, märgistus vm);
   - milliseid materjale on lubatud transportida ainult personaalselt;
   - milliseid andmeid enne transportimist varundatakse.
b. Digitaalsetel andmekandjatel olevad andmed krüpteeritakse enne transportimist.
c. Võimalusel välditakse dokumentide ainueksemplaride väljaviimist organisatsiooni ruumidest.
d. Dokumentide ja andmekandjate käitlemise kord on töötajatele teatavaks tehtud. Töötajad järgivad kehtestatud korda.

INF.8.M3 Kaitse lubamatu sissepääsu eest kodutöökohta

a. Töötajaid on teavitatud, milliste sissetungi- ja pääsukaitse meetmete rakendamine kodutöökohas on kohustuslik ja milline töötaja vastutus sellega kaasneb.
b. Kodutöökohas on rakendatud sobivaid sissemurdmiskaitse meetmeid (nt turvauksed ja -aknad, turvalised ukselukud).
c. Kui töötaja kodutöökohal ei viibi, on tööruumi aknad suletud ja uksed lukustatud.

3.3 Standardmeetmed

INF.8.M4 Kodutöökoha õige korraldus

a. Kodutöökoht asub võimaluse korral eluruumidest eraldi paiknevas, lukustatava uksega ruumis.
b. Kodutöökoha sisustus on valitud ergonoomika, tööohutuse ja tervisekaitse tingimusi arvestades.
c. Kodutöökohas on järgitud organisatsioonis üldkehtivaid nõudeid töökohale ja töökeskkonnale.
d. Arvutiekraan on paigutatud nii, et valgus ekraanilt otse ei peegelduks ja kõrvalised isikud töötaja selja tagant ekraani ei näe.

e. Kodutöökoht on konkreetsete tööülesannete täitmiseks piisavalt varustatud, selleks vajalikud töövahendid annab tööandja.

3.4 Kõrgmeetmed

INF.8.M5 Konfidentsiaalsete andmete turvaline kõrvaldamine (C)

a. Konfidentsiaalsete andmete kõrvaldamiseks on kehtestatud kord. Andmete kõrvaldamisel kodutöökohal järgitakse organisatsioonis selleks kehtestatud korda.
b. Korduvkasutatavatelt andmekandjatelt kustutatakse andmed turvaliselt. Ühekordselt kirjutatavad andmekandjad purustatakse kõrvaldamisel mehhaaniliselt (vt CON.6 *Andmete kustutus ja hävitamine*).
c. Kodutöökohas on tagatud turvaliseks materjalide kõrvaldamiseks vajalike vahendite olemasolu.
d. Tundlikke dokumente ja tundlikke andmeid sisaldavaid andmekandjaid hoitakse enne kõrvaldamist lukustatud hoiukohas, kaitstuna lubamatu juurdepääsu eest.

INF.8.M6 Suure kaitsetarbega töödokumentide turvaline käitus (C-I-A)

a. Suure kaitsetarbega töödokumentide käitlemine toimub üldjuhul põhitöökohas, materjalide väljastamist kodus töötamiseks välditakse.
b. Kui töötaja erandkorras kasutab suure kaitsetarbega töödokumente kodutöökohas, rakendatakse kodutöökohale tavapärasest rangemaid turvameetmeid.
c. Kodutöökoha lukustatavad kapid ja sahtliboksid vastavad dokumentide ja andmekandjate kaitsetarbele.

INF.9 Mobiiltöökoht

1 Kirjeldus

1.1 Eesmärk

Esitada mobiiltöökohale kohaldatavad korralduslikud, tehnilised ja personali käsitlevad meetmed, mida arvestatakse ja täidetakse siis kui töötajad töötavad organisatsiooni ruumide asemel organisatsioonivälistes töökohtades.

1.2 Vastutus

Mobiiltöökoha meetmete täitmise eest vastutab infoturbejuht.

Lisavastutajad

IT-talitus, töötaja, personaliosakond, haldusosakond.

1.3 Piirangud

Mobiiltöö IT-süsteemide, andmekandjate ja dokumentide turbe korral arvestatakse süsteemispetsiifilisi mooduleid SYS.3.1 *Sülearvuti*, SYS.3.2 *Nutitelefon ja tahvelarvuti üldiselt*, SYS.4.5 *Irdandmekandjad*, NET.3.3 *Virtuaalne privaatvõrk* (VPN) ja SYS.2.1 *Klientarvuti üldiselt*.

Moodulit täiendavad püsivaks kasutuseks rajatud kaugtöökoha meetmed moodulist OPS.1.2.4 *Kaugtöö*. Kodutöökoha taristu turvameetmeid käsitletakse moodulis INF.8 *Kodutöökoht*.

2 Ohud

2.1 Eeskirjade puudumine või puudulikkus

Kui mobiiltöö organisatsioonis pole eeskirjadega reguleeritud, võivad töötajad tahtmatult lekitada konfidentsiaalset teavet, kuna nad ei ole teadlikud turvameetmete kasutamise kohustusest. Näiteks võib teave sattuda valedesse kätesse ebaturvaliselt korraldatud teabevahetuse käigus. Ründaja saab lekkinud siseteavet kasutada organisatsiooni vastu rünnete algatamiseks.

2.2 Keskkonnast tingitud kahjulikud mõjud

Mobiilseadmeid ja andmekandjaid kasutatakse väga mitmesugustes keskkonnatingimustes. IT-seadmeid võivad kahjustada liiga kõrged või madalad temperatuurid, tolm või niiskus. Mobiilseade võib maha kukkuda ja puruneda.

Lisaks füüsilisele keskkonnale esinevad ka tehnoloogilisest keskkonnast ja seonduvast IT-infrastruktuurist tulenevad ohud. Mobiilseadmed võivad ühenduda ebausaldusväärse turvalisusega võrkudesse. Mobiilseadmetega saab ühendada lisaseadmeid, millest kõik ei pruugi olla turvalised. Nii saab mobiilseadmesse edastada kahjurvara või kopeerida seadmest tundlikke andmeid.

2.3 IT-seadmete, -tarvikute ja -süsteemide manipuleerimine või hävitamine mobiiltöökohal

Kaasaskantavaid IT-seadmeid, IT-tarvikuid ja IT-süsteeme saab üldjuhul lihtsamalt manipuleerida või hävitada kui seda saaks organisatsiooni ruumides. Mobiiltöökoht on juurdepääsetav kõrvalistele isikutele ning seal ei saa rakendada keskselt kontrollitavaid turvameetmeid (nt valveteenust). Mobiilseadme hävimine või kaotus tekitab töötajale töökatkestuse, sest juurdepääs organisatsiooni IT-süsteemidele ajutiselt puudub. Ka mobiilseadmete asendamine on juhul, kui mobiiltöökohti on palju, organisatsioonile märkimisväärne kulu.

2.4 Töötaja kättesaadavuse piiratus

Enamasti ei ole mobiilseade organisatsiooni sisevõrguga pidevalt ühendatud. Organisatsioonist väljaspool asudes on seda ka raske saavutada. Teabe liikumine aeglustub. Isegi siis, kui teave edastatakse e-posti teel, ei ole kindel, et mobiilne töötaja lähiajal e-posti loeb. Kättesaadavuse piiratusel võib olenevalt olukorrast ja organisatsioonist olla suur mõju.

2.5 Andmekandjate ja dokumentide ebaturvaline transport

Organisatsiooni ja mobiiltöökoha vahelise transportimise käigus võivad dokumendid või andmekandjad sattuda varguse objektiks ja kaotsi minna. Volitamata isikud võivad saada juurdepääsu tundlikele andmetele, neid lugeda või manipuleerida. Krüpteerimata andmekandjate sattumisel valedesse kätesse võib tekkida märkimisväärne konfidentsiaalsuse kadu.

Kui transportimise käigus läheb kaduma varundamata andmetega andmekandja, võib see organisatsiooni eesmärkide täitmist olulisel määral mõjutada.

2.6 Andmekandjate ja dokumentide ebaturvaline kõrvaldamine

Kui mobiiltöökohal pole loodud tingimusi andmekandjate ja dokumentide turvaliseks kõrvaldamiseks, võivad need sattuda olmeprügi hulka. Ründaja saab seeläbi väärtuslikku teavet, mida sihipäraselt ära kasutada organisatsioonivastaste küberkuritegude (nt petukirja koostamine või väljapressimiskatse) läbiviimiseks. Tagajärjed võivad raskemal juhul ohustada terve organisatsiooni tegevust (nt kui ründe tulemuseks on oluliste tellimuste nurjumine või partnerlussuhete katkemine).

2.7 Andmete konfidentsiaalsuse kadu

Ründajatel on mobiiltöökohal võrdluses bürooruumidega oluliselt lihtsam juurde pääseda kõvakettal, ird- või paberkandjal olevatele andmetele. Samuti on võimalik pealt kuulata sideühendusi. Selliste andmete avalikustamisel või ründeks kasutamisel võivad olla organisatsioonile märkimisväärsed tagajärjed. Andmeleke võib kaasa tuua seaduserikkumise (näiteks isikuandmete paljastumise tõttu) või ebasoodsa konkurentsiolukorra.

2.8 Andmekandjate ja dokumentide vargus või kaotamine

Mobiiltöökoht ei ole nii hästi kaitstud kui organisatsiooni ruumides asuv töökoht. IT-seadmete või dokumentide vargus rongis, hotellitoast või organisatsioonivälisest konverentsiruumist on palju tõenäolisem kui pääsukontrollisüsteemiga ja kaastöötajatega bürooruumist. Töötaja võib mobiilseadme ära kaotada (nt taksosse unustada).

Peale otsese varalise kahju lisanduvad mobiilseadme varguse või kaotamise korral tundlike andmete (nt e-post, nõupidamiste märkmed, aadressid vm dokumendid) paljastamisega seotud kahjud. Kahjustuda võib ka organisatsiooni maine.

3 Meetmed

3.1 Elutsükkel

Kavandamine

INF.9.M1 Mobiiltöökoha sobivuse kriteeriumid

INF.9.M2 Mobiilseadmete kasutamise eeskiri

INF.9.M7 Mobiiltöö õiguslikud raamtingimused

INF.9.M8 Mobiiltöökoha turvanõuete kehtestamine

Evitus

INF.9.M9 Mobiilseadmete ja andmekandjate krüpteerimine

Käitus

INF.9.M3 Kaitse lubamatu juurdepääsu eest

INF.9.M4 Organisatsioonivälise IT-süsteemiga töötamise kord

INF.9.M5 Mobiilseadme kaotusest teatamine

INF.9.M12 Ekraanifiltri kasutamine

Kõrvaldamine

INF.9.M6 Konfidentsiaalse teabe turvaline kõrvaldamine

Lisanduvad kõrgmeetmed

INF.9.M10 Vargusvastaste vahendite rakendamine

INF.9.M11 Mobiiltöö keeld ebaturvalistes oludes

3.2 Põhimeetmed

INF.9.M1 Mobiiltöökoha sobivuse kriteeriumid [IT-talitus]

a. Organisatsioon on kehtestanud nõuded, millele mobiiltöökoht peab vastama.

b. Töötaja järgib organisatsioonis kehtestatud nõudeid.

c. Töötaja on teadlik, millistes tingimustes on mobiiltöö täielikult keelatud.

INF.9.M2 Mobiilseadmete kasutamise eeskiri [personaliosakond]

a. On kehtestatud mobiilseadmete kasutamise eeskiri, mis sätestab:
   - milliseid andmeid ei ole lubatud väljaspool organisatsiooni käidelda;
   - mis tingimustel saab mobiiltöötaja ligipääsu organisatsiooni ressurssidele;
   - mobiilseadmes rakendatavad turvameetmed (sh lubatavad autentimismeetodid);
   - millised andmed krüpteeritakse ja kuidas;
   - isiklike mobiilseadmete tööalase kasutamise korra;
   - nõuded mobiilseadmete turvaliseks ja heaperemehelikuks kasutamiseks;
   - kuidas vältida mobiilseadmete kaotamist või vargust;
   - mobiilseadmete soetamise ja kuluarvestuse protseduurid;
   - kuidas on korraldatud mobiilseadmete ja nende rakenduste hooldamine ja haldus;
   - kuidas mobiilseadmeid turvaliselt kõrvaldada.

b. Kõik mobiilseadmete kasutajad on mobiilseadmete kasutamise eeskirjaga tutvunud ja järgivad seda.

INF.9.M3 Kaitse lubamatu juurdepääsu eest [haldusosakond, töötaja]

a. Mobiiltöökoha kasutajad teavad varguse ja lubamatu juurdepääsu ohte ja oskavad turvameetmeid mobiiltöökohal rakendada.

b. Mobiilseadmeid ei jäeta järelevalveta.

c. Kui mobiiltöökohalt hetkeks lahkutakse, suletakse aknad ja lukustatakse uks (nt hotellitoas). Kui ust ei saa lukustada (nt rongis), hoitakse dokumente ja mobiilseadmeid turvalises kohas.

d. Lühiajalisel lahkumisel ruumist lukustatakse IT-seadme ekraan, et pooleliolevat tööd jätkata saaks ainult pärast tulemuslikku autentimist.

INF.9.M4 Organisatsioonivälise IT-süsteemiga töötamise kord [IT-haldus, töötaja]

a. On kehtestatud kord organisatsioonivälise IT-süsteemide (internetikohvik, külastatava ettevõtte kontoriarvuti vms) tööalaseks kasutamiseks.

b. Kõik mobiilsed töötajad teavad organisatsioonivälise IT-süsteemi kasutamise ohte.

c. On selgelt määratletud, milliseid andmeid on lubatud organisatsioonivälistes IT-süsteemides töödelda ja milliseid mitte.

d. Organisatsioonivälises IT-süsteemis töö lõpetamisel kustutatakse arvutist töö käigus loodud ajutised andmed (nt kasutajanimede ja paroolide automaatsalvestused brauseris).

3.3 Standardmeetmed

INF.9.M5 Mobiilseadme kaotusest teatamine [töötaja]

a. Töötajad on kohustatud dokumentide, mobiilseadme või andmekandja kaotusest või vargusest teavitama organisatsiooni esimesel võimalusel.

b. Kaotusest teavitamiseks on organisatsioonis määratud konkreetsed teatamisteed ja kontaktisikud.

c. Võimalusel kasutatakse mobiilseadme kaotsimineku järgselt seadme kauglukustuse, kaugkustutuse või seadme asukoha määramise funktsioone.

d. Kadunud mobiilseadme leidmisel kontrollitakse, kas seadet pole vahepeal manipuleeritud. Kahtluste korral seade kõrvaldatakse kasutusest või laaditakse seadmele uuesti algne operatsioonisüsteem koos kõigi vajalike rakendustega.

INF.9.M6 Konfidentsiaalse teabe turvaline kõrvaldamine [töötaja]

a. Väljaspool organisatsiooni või reisil olles järgitakse organisatsioonis kehtivat andmekandjate turvalise kõrvaldamise korda.

b. Enne kasutatud andmekandjate ja dokumentide kõrvaldamist kontrollitakse, kas neil leidub tundlikke andmeid.

c. Reisil olles konfidentsiaalsete andmetega andmekandjaid võimaluse korral ei hävitata, vaid tuuakse need tagasi organisatsiooni, kus on olemas vahendid andmekandjate turvaliseks kõrvaldamiseks (vt CON.6 *Andmete kustutus ja hävitamine*).

INF.9.M7 Mobiiltöö õiguslikud raamtingimused [personaliosakond]

a. Mobiiltöö korraldus vastab tööõiguslikele ja teistele kohaldatavatele õigusaktidele.

b. Muud olulised mobiiltöö aspektid (töötaja vastutus, kulude hüvitamine jne) on reguleeritud töötaja ja tööandja vahelise töölepingu ja mobiiltööd puudutavate lisakokkulepetega.

INF.9.M8 Mobiiltöökoha turvanõuete kehtestamine [IT-haldus]

a. Üldise turvapoliitika alusel on kehtestatud mobiiltöökoha turvaeeskiri või täiendatud mobiiltöökoha turvanõuetega mobiilseadme kasutamise eeskirja (vt INF.9.M1 *Mobiilseadmete kasutamise eeskiri*).

b. Mobiiltöökoha turvanõuetega on määratletud:

- kokkulepitud andmevahetusajad, reageerimisaeg;
- konfidentsiaalse teabe käitluse kord;
- turvaintsidentidest teatamise kord;
- lubatud ja keelatud töövahendid;
- mobiilseadmete ekraanifiltrite kasutamine;
- dokumentide ja andmekandjate transport;
- andmevarundus;
- andmekaitse nõuded;
- dokumentide ja andmekandjate kõrvaldamise protseduurid.

c. Mobiiltöökoha turvanõuded on kooskõlastatud asjaomaste allüksustega, töötajad on eeskirjast teadlikud ja see on mobiiltöötajaile siduv.

d. Mobiiltöökoha turvaeeskirja ajakohastatakse regulaarselt.

INF.9.M9 Mobiilseadmete ja andmekandjate krüpteerimine [IT-haldus, kasutaja]

a. Mobiilseadmed ja andmekandjad on krüpteeritud organisatsioonis kehtiva korra kohaselt (vt CON.1 *Krüptokontseptsioon*).

b. Krüptovõtme kasutamisel hoitakse seda krüpteeritud seadmest või andmekandjast lahus.

INF.9.M12 Ekraanifiltri kasutamine [töötaja]

a. Mobiiltöökohas kasutatava IT-seadme ekraanil kuvatava teabe kaitseks kasutatakse ekraani katvat ekraanifiltrit.

3.4 Kõrgmeetmed

INF.9.M10 Vargusvastaste vahendite rakendamine [töötaja] (C-I-A)

a. Kui IT-seade omab vargust takistavat või seadme kaotamisel seadme leidmist hõlbustavat funktsionaalsust, on see funktsionaalsus aktiveeritud.

b. Rahvarohkes ruumis kasutatakse võimalusel vargusvastaseid vahendeid (nt trosslukk sülearvuti kasutamisel).

c. Vargusvastased vahendid vastavad andmete kaitsetarbele.

INF.9.M11 Mobiiltöö keeld ebaturvalistes oludes [IT-haldus] (C-I-A)

a. On kehtestatud kriteeriumid mobiiltöö keelamiseks ebaturvalises oludes.

b. Mobiiltöö on keelatud juhul kui mobiilseadme ekraani ei saa kõrvaliste isikute eest varjata.

c. Mobiiltöö on keelatud avalikus ja ilma paroolita WiFi võrgus.

INF.10 Koosoleku-, ürituse- ja koolitusruum

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed koosoleku-, ürituse- ja koolitusruumides töödeldava teabe ja neis ruumides olevate IT-seadmete kaitseks.

Koosoleku-, ürituse- ja koolitusruume iseloomustab asjaolu, et enamasti kasutavad neid nii töötajad kui külastajad ja lisaks organisatsiooni seadmetele on kasutusel ka võõrad IT-seadmed.

1.2 Vastutus

Koosoleku-, ürituse- ja koolitusruumi meetmete täitmise eest vastutab haldusosakond.

Lisavastutajad

Tehnikatalitus, IT-talitus, töötaja.

1.3 Piirangud

Koosolekuruumis olulisi andmesideaspekte käsitletakse moodulites NET.2 *Traadita võrgud* ja NET.4 *Side*. Ruumides asuva kaabelduse puhul järgitakse moodulit INF.12 *Kaabeldus*. Tuleohutust käsitlevad meetmed on esitatud moodulis INF.1 *Hoone üldiselt.* Külastajatega seotud turvameetmeid käsitletakse moodulis ORP.1 *Infoturbe korraldus.*

2 Ohud

2.1 Eeskirjade puudumine või puudulikkus

Paljud turvaprobleemid ilmnevad siis, kui töötajad ei järgi ruumide kasutamise korda või pole sellest teadlikud. Kui töötajad ei sulge pärast koolitusruumist lahkumist aknaid ja uksi, saab volitamata isik ruumi sisse pääseda, rikkuda vara või varastada seal olevaid seadmeid. Kui konfidentsiaalne teave jääb pärast koosolekut marker- või pabertahvlilt eemaldamata, on see volitamata isikutele vabalt kättesaadav.

2.2 IT-seadmete ühildumatus

Erinevate tootjate IT-seadmed võivad kasutada elektritoiteks või video- või audiosignaali edastamiseks erinevaid kaabli- ja ühendusstandardeid. Ka võivad vanematel seadmetel puududa samad ühendusvõimalused kui on uuematel seadmetel. Nii juhtub, et koosolekuruumis ei saa IT-seadmeid soovipäraselt kasutada. Probleem tekib eelkõige organisatsioonivälistе seadmete kasutamisega, nt külalise sülearvuti ühendamisel koosolekuruumi statsionaarse projektoriga.

Kaablite või andmekandjate ühendamise katsed valesse ühendusliidesesse võivad seadmeid või andmekandjaid kahjustada.

2.3 Külastajatest tulenevad ohud

Kuna külastajad organisatsiooni nõudeid ei tea, ei saa olla kindel, et külastajad neile kättesaadavaks tehtud andmeid ja IT-seadmeid turvaliselt kasutavad. Külastajad võivad konfidentsiaalsele teabele juurdepääsu saada ka töötajate tähelepanematuse tõttu. Külastaja võib näiteks tualettruumi otsides eksida uksega ja siseneda bürooruumi, milles asuval markertahvlil on konfidentsiaalset teavet.

2.4 Lahtised kaablid

Koosoleku-, ürituse- ja koolitusruumide kasutajad, laudade asetus ja ruumide kasutusviisid võivad muutuda. Seetõttu on vaja muuta ka ruumidesse paigaldatud IT-seadmete ja nendega ühendatud kaablite asetust. Olenevalt ruumis asuvate ühenduspunktide (elektrivarustuse ja andmesidevõrgu pistikupesad) asukohast juhitakse kaableid läbi ruumi, isegi üle käiguteede. See tekitab komistusohu, mis võib kahjustada inimest tervist ja rikkuda IT-seadmeid, kui komistades tõmmatakse koos kaabliga kaasa ka IT-seade.

2.5 Vargus

Koosolekuruumis asuvate andmekandjate, IT-seadmete ja muu vara vargus toob kaasa kulutused varade asendamiseks. Ühtlasi tähendab see seda, et ajutiselt ei saa neid ruume täies mahus kasutada. Varguse tõttu kaotab organisatsioon konfidentsiaalseid andmeid, mida varas saab organisatsooni vastu ära kasutada ja seeläbi täiendavat kahju tekitada.

Kui koosoleku-, ürituse- ja koolitusruume ei lukustata (nt lõunapausi ajal), kui puudub ruumi järelevalve või kui IT-süsteemidel puudub piisav turve, saab ruumi jäetud mobiilseadmeid kiiresti ja märkamatult varastada.

2.6 Teabe konfidentsiaalsuse kadu

Tehniliste tõrgete, töötajate tähelepanematuse või teadmatuse tõttu on võimalik IT-seadme salvestuskandjal (nt kõvaketas), irdkandjal (nt mälupulk või DVD), paberkandjal või joonistustahvlil oleva konfidentsiaalse teabe paljastumine. Ka ründaja otsib võimalusi tundlikule teabele ligipääsemiseks. Konfidentsiaalsete andmete lekkimisel on organisatsioonile märkimisväärsed tagajärjed (nt õigusrikkumine, ebasoodne konkurentsiolukord või rahaline mõju).

3 Meetmed

3.1 Elutsükkel

Kavandamine

INF.10.M1 Koosoleku-, ürituse- ja koolitusruumi turvaline kasutamine

INF.10.M4 Koosoleku-, ürituse- ja koolitusruumide turvaline asukoht

INF.10.M6 Turvalise võrkupääsu korraldus

Evitus

INF.10.M7 Koolitus- ja esitlusarvutite turvaline konfiguratsioon

INF.10.M8 Ruumikasutuse registreerimise kord

Käitus

INF.10.M3 Akende ja uste sulgemine

INF.10.M5 Toite- ja sidekaablite turvaline paigutus

Lisanduvad kõrgmeetmed

INF.10.M9 Koolitus- ja esitlusarvutite algseadistamine

3.2 Põhimeetmed

INF.10.M1 Koosoleku-, ürituse- ja koolitusruumi turvaline kasutamine [tehnikatalitus, IT-haldus]

a. On kehtestatud ja dokumenteeritud ruumi kasutamise kord, mis määrab:
   - kes haldab ruumis asuvaid IT- ja muid süsteeme;
   - millistel tingimustel tohivad külastajad kasutada kaasatoodud IT-vahendeid;
   - milliseid võrguühendusi ja -liideseid tohivad külastajad kasutada.

b. Koosoleku-, ürituse-, ja koolitusruumides on saadaval tehniliste probleemide lahendaja kontaktandmed.

c. Ruumis asuvad seadmed on kindlustatud ja/või on varguse eest kaitstud sobivate pääsukontrollisüsteemide ja vargusvastaste vahenditega.

d. Esitluse eel suletakse võimaliku juhusliku andmelekke vältimiseks esitlusarvutis kõik mittevajalikud rakendused ja andmesideühendused.

e. Pärast koosoleku või ürituse lõppu võetakse kaasa või kõrvaldatakse turvaliselt kõik tundlikku teavet sisaldada võivad materjalid.

f. Ürituse- või koolitusruumist ajutisel lahkumisel ja järelevalve puudumisel ruumi uksed lukustatakse.

g. Ruumides on nähtaval kohal juhised tulekahju korral tegutsemise ja evakuatsiooniteede kohta.

INF.10.M3 Akende ja uste sulgemine [töötaja]

a. Koosoleku-, ürituse- ja koolitusruumide aknad on väljaspool ürituste toimumise aega suletud, väljaspool organisatsiooni turvaperimeetrit asuvate ruumide uksed lisaks ka lukustatud.

b. Ajutisel lahkumisel otsese järelevalveta koosoleku-, ürituse- ja koolitusruumidest lukustatakse uksed ja suletakse aknad, kust on võimalik ruumi siseneda.

c. Akende ja uste suletust ja lukustatust kontrollitakse regulaarselt.

3.3 Standardmeetmed

INF.10.M4 Koosoleku-, ürituse- ja koolitusruumide turvaline asukoht

a. Koosoleku-, ürituse- ja koolitusruumide kavandamisel on arvestatud ruumide asukohast ja kasutusviisist tingitud ohtudega.

b. Külastajatele mõeldud ruumid ei asu hooneosas, kus regulaarselt töödeldakse konfidentsiaalset teavet.

c. Koosoleku-, ürituse- ja koolitusruumid ja nendesse viivad käiguteed on valitud nii, et külaliste liikumine ja ruumides toimuvad üritused tavapärast tööd ei segaks.

d. Konfidentsiaalset teavet käsitlevad koosolekud peetakse selleks sobivaks tunnistatud ja vastavat märget omavates koosolekuruumides, kus on rakendatud meetmeid pealtkuulamise piiramiseks (nt seina ja uste läbikostvuse vähendamiseks).

INF.10.M5 Toite- ja sidekaablite turvaline paigutus

a. Koosoleku-, ürituse- ja koolitusruumides on külaliste seadmete tarbeks piisavalt toite- ja võrgupesasid.

b. Kui lahtiste toite- või sidekaablite asetamine põrandale on vältimatu, kaetakse kaablid kaablikaitselindiga.

INF.10.M6 Turvalise võrkupääsu korraldus [IT-haldus]

a. Ruumis asuvaid IT-süsteeme ei saa korraga ühendada sisevõrgu ja Internetiga.

b. Külastajate andmesidevõrk on organisatsiooni kohtvõrgust eraldatud. Külastajate IT-süsteeme ei saa ühendada organisatsiooni kohtvõrguga.

c. Kõrvalised isikud ei saa koosolekuruumist töötajate kohtvõrgu kasutamist ja andmeliiklust jälgida ega pealt kuulata.

d. Koosoleku-, ürituse- ja koolitusruumide elektrivarustus on jaotuskilbist alates organisatsiooni muude ruumide elektrivarustusest eraldatud.

INF.10.M7 Koolitus- ja esitlusarvutite turvaline konfiguratsioon [IT-haldus]

a. Koolitus- ja esitlusarvutitele on kehtestatud tüüpkonfiguratsioonid, mis on minimaalsed ja ei sisalda liigseid rakendusi.

b. Koolituse eel kontrollitakse, kas IT-süsteemid on koolituse tarbeks sobivalt seadistatud.

c. Koolitus- ja esitlusarvutid on organisatsiooni kohtvõrgust eraldatud.

d. Kasutajate õigusi on vajadusepõhiselt piiratud. Kasutajad ei saa arvutitesse tarkvara installida ega arvutitest andmeid kopeerida.

INF.10.M8 Ruumikasutuse registreerimise kord

a. Olenemata koosoleku-, ürituse- ja koolitusruumi kasutusviisist saab järele vaadata, kes ja millisel ajavahemikul ruume kasutas.

b. Organisatsioonis on rakendatud kord ja protseduurid koosoleku-, ürituse- ja koolitusruumide eelnevaks reserveerimiseks.

3.4 Kõrgmeetmed

INF.10.M9 Koolitus- ja esitlusarvutite algseadistamine [IT-haldus] (C-A)

a. Pärast ruumi kasutamise lõpetamist on arvutitest kõrvaldatud kõik üritusega seotud andmed ja arvuti on viidud tüüpkonfiguratsiooniga määratud algseisu. (vt INF.10.M7 *Koolitus- ja esitlusarvutite turvaline konfiguratsioon*).

c.

INF.11 Sõidukite IT-komponendid

1 Kirjeldus

1.1 Eesmärk

Esitada organisatsiooni sõidukite turvameetmed juhul, kui sõiduk (sõiduauto, veoauto, kaater, laev, helikopter, lennuk vms) on varustatud tänapäevaste infotehnoloogiliste komponentidega.

1.2 Vastutus

„Sõidukite IT-komponendid“ meetmete täitmise eest vastutab infoturbejuht.

Lisavastutajad

Kasutaja, hankeosakond, andmekaitsespetsialist, vastutav spetsialist, IT-talitus, töötaja.

1.3 Piirangud

Moodul käsitleb sõidukeid üldiselt. Eriotstarbeliste sõidukitele (nt kiirabiauto, päästekopter, militaarsõidukid) rakendatakse täiendavaid vajaduspõhiseid turvameetmeid.

Täiendavalt võivad sõidukile kohalduda meetmed moodulist SYS.3.1 *Sülearvutid* ja mooduligruppidest SYS.3.2 *Nutitelefon ja tahvelarvuti* ning NET.2 *Raadiovõrgud*.

Sõiduki IT-seadmetes olevate andmete kustutamist enne sõiduki teisele kasutajale andmist või maha kandmist käsitletakse moodulis CON.6 *Andmete kustutus ja hävitamine*.

2 Ohud

2.1 Puuduv või puudulik sõiduki kasutamise kord

Kui kasutajaid ei ole juhendatud, mis andmeid on lubatud sõiduki IT-süsteemis hoida ning mis seadmeid ja kuidas (USB või *Bluetooth*'i kaudu) sellega ühendada, võib sõiduki IT-süsteemi jääda tundlikku teavet. See teave võib olla nähtav järgmisele sõidukikasutajale või teistele volitamata isikutele (nt sõiduki varguse korral).

Sõiduki kasutamise korra puudumisel ei pruugi kasutaja mõista IT-komponentide funktsionaalsust ja eesmärke. Lennuki IT-süsteemi seadistamisel tehtav muudatus, mis puudutab lennueelsete automaattestide ärajätmist, ohustab lennuki turvalisust õhus. Auto telefonisüsteemi kontaktiloendit võidakse automaatselt sünkroonida kasutaja telefonis oleva kontaktiloendiga, mistõttu kõik nimed ja telefoninumbrid muutuvad kättesaadavaks ka kõrvalistele isikutele.

Vääralt välja lülitatud IT-komponendid võivad jääda sõiduki akut koormama ka pärast sõiduki seisma jätmist. Kiirabiauto mittekäivitumine tühjenenud aku tõttu võib kaasa tuua raskeid tagajärgi. Samuti võib pikaajaline elektrikatkestus kahjustada autos olevaid keerulisi meditsiiniseadmeid.

2.2 Ohutusnõuete eiramine

Kui kasutajad pole teadlikud sõidukil olevate juhtimisseadmete väära kasutamise võimalikest tagajärgedest, võib kasutaja hooletuse või teadmatuse tagajärjel tekkida oht inimeste füüsilisele turvalisusele. Kui keegi teeb muudatuse laeva navigatsiooni- ja juhtimissüsteemi seadetes ilma vastava loata või teisi sellest teavitamata, võib tagajärjeks olla laevaõnnetus. Hooletusest lukustamata jäetud sõiduki (nt autokraana) kabiini sisenenud volitamata isik võib rikkuda seadmeid, muuta seadistusi või käivitada sõiduki.

2.3 Ebaturvaline andmevahetus

Paljudel kaasaegsetel sõidukitel on lisaks *Bluetooth*'i ja traadita andmeside liidestele integreeritud täiendavaid, kasutaja eest varjatud andmesideliideseid. Sõiduki IT-komponendid võivad integreeritud raadioliideste kaudu infot vahetada väliste osapooltega, ilma et kasutaja saaks seda andmevahetust mõjutada (nt uutesse sõiduautodesse paigaldatud eCall süsteem). Kuid auto võib ka autotootjale saata üksikasjalikke andmeid auto asukoha, sõidetud kilomeetrite arvu või sõidukijuhi juhtimisharjumuste kohta. See tähendab, et sõiduki kasutajate kohta on võimalik koguda ulatuslikke isikuandmeid ilma, et nad oleksid sellest teadlikud või annaksid selgesõnalise nõusoleku selliseks andmete kogumiseks ja töötlemiseks. Ebaturvalised andmevahetusliidesed võimaldavad andmete pealtkuulamist ja manipuleerimist.

Ründaja võib ebaturvalist andmevahetusliidest kasutada kasutaja kohta teabe hankimiseks. Kui sõiduki info- ja meelelahutussüsteem lubab *Bluetooth* ühenduse luua ilma turvakoodi sisestamata, võib ründaja oma seadme märkamatult sõiduki IT-süsteemiga ühendada ning sünkroonida autokasutaja kontaktiloendi.

2.4 Sõiduki lubamatu või ebaturvaline ümberseadistus

Sõiduautot tavaliselt keegi ümber ei ehita, kuid eriotstarbeliste sõidukite ja ka veesõidukite puhul on see levinud praktika. Kui ümberseadistust tehakse vääralt (nt eriotstarbeliste sõidukite puhul ei kaasata selleks spetsialiseerunud ettevõtet), võib isegi lisakaabli vale paigutus kaasa tuua märkimisväärse kahju.

Kasutaja võib manipuleerida sõiduki elektroonikasüsteemi, et avada täiendav funktsionaalsus, parendada sõiduki võimekust või blokeerida mõni hoiatussüsteem. Sellised illegaalsed tarkvaramuudatused tähendavad muuhulgas ka seda, et sõiduki IT-komponendid ei saa enam tootja välja antud tarkvarauuendusi ja olemasolevad turvanõrkused jäävad parandamata.

2.5 Sõiduki vargus ja volitamata juurdepääs

Sõidukite kaugjuurdepääsusüsteemid võivad sisaldada turvanõrkusi. Ründaja võib avada kauglukustusega auto uksed ja auto käivitada ilma autentset autovõtit omamata.

Sissemurdmise ja ärandamise oht on suurem selliste sõidukute puhul, mida sageli jäetakse valveta parklatesse (veesõidukite puhul valveta paadisadamatesse).

Ründajal on sõidukisse sisse saades võimalik hävitada või manipuleerida sõiduki IT-süsteeme ning võtta kaasa IT-süsteemides sisalduvad andmed. Samuti on ohus sõidukisse jäetud nutiseadmed ja muud väärtuslikud esemed.

2.6 Sõiduki hoolduse ja IT-komponentide uuenditega seotud ohud

Kui sõidukite IT-komponentide toimimist piisava regulaarsusega ei kontrollita, võivad mõned neist aja jooksul lakata töötamast või töötada ainult osalise funktsionaalsusega. See võib põhjustada rikkeid sõiduki kasutamisel ja halvimal juhul kaasa tuua õnnetusjuhtumi.

Kui sõidukit hooldatakse mujal kui ametlikus esinduses, siis võidakse hoolduses IT-komponentidega seotud probleeme mitte tuvastada, kuna puuduvad vastavad diagnostikavahendid.

Sõiduki IT-komponentide tarkvarauuendite paigaldamine sageli viibib, kuna sõiduki korralist hooldust tehakse üldjuhul ainult kord aastas. Lisaks ei takista vananenud tarkvara kasutamine kuidagi sõiduki kasutamist, mistõttu jäetakse turvauuendite paigaldamine tegemata. Väga paljude sõidukite IT-komponendid on turvanõrkustega, mida teadlikul ründajal on võimalik andmevarguseks või sõiduki manipuleerimiseks ära kasutada.

2.7 Kasutaja andmete kõrvaldamata jätmine

Sõiduki võõrandamisel või kasutaja vahetamisel on oht, et eelmine kasutaja jätab sõiduki IT-süsteemidest kustutamata endaga seotud andmed. Selle tulemusena on järgmisel kasutajal teada eelmise kasutaja telefoniraamat, helistatud numbrid, navigatsioonirakendusse salvestatud elu- ja töökoht, sisestatud aadressid ja muud personaalsed andmed.

Sõidukisse unustanud mobiilandmeside tarbeks mõeldud SIM-kaarti on võimalik kasutada pettuste või illegaalsete tehingute sooritamiseks.

2.8 Sobimatud keskkonnatingimused

Ekstreemne kuumus või sobimatud niiskustingimused võivad sõidukite IT-komponentidele mõjuda hävitavalt. IT-süsteemid võivad lakata töötamast ja muuta sõiduki kasutuskõlbmatuks.

Päikse käes võib salongi sisetemperatuur tõusta üle 70 kraadi, mis oluliselt ületab liitiumioonakude soovituslikku töötemperatuuri.

3 Meetmed

3.1 Elutsükkel

Kavandamine

INF.11.M1 Sõiduki hanke kavandamine

Evitus

INF.11.M3 Sõiduki infoturbe juhendid

INF.11.M4 Sõidukite infoturbe eeskirja jõustamine

INF.11.M9 Sõiduki kasutusvalmiduse tagamine

Käitus

INF.11.M2 Korrakohane hooldus ja IT-komponentide uuendamine

INF.11.M5 Sõidukite inventariloend

INF.11.M7 Sõiduki turvaline kasutamine
INF.11.M8 Sõiduki kaitse ilmastikumõjude eest
INF.11.M12 Vargusvastase kaitse vahendid

Avariivalmendus

INF.11.M6 Detailsed tegevusjuhised

Kõrvaldamine
INF.11.M10 Sõidukite kasutusest kõrvaldamise kord

Lisanduvad kõrgmeetmed

INF.11.M11 Asendamise kord
INF.11.M13 Sõiduki kaitse kahjulike välismõjude eest
INF.11.M14 Konfidentsiaalse teabe kaitse
INF.11.M15 Sõiduki liideste kaitse
INF.11.M16 Tulekustutussüsteem
INF.11.M17 Sõidukisisese võrgu eraldamine

3.2 Põhimeetmed

INF.11.M1 Sõiduki hanke kavandamine [vastutav isik, hankeosakond, andmekaitsespetsialist]

a. Sõiduki hankimisel lähtutakse kasutusotstarbe, funktsionaalsetele nõuete ja tasuvuse kõrval ka infoturbe ja andmekaitse aspektidest.
b. Infoturbe nõuded peavad olema täidetud sõiduki kogu elutsükli vältel.
c. Sõiduki lukustussüsteem on piisavalt turvaline (või tagatakse sõiduki füüsiline turve muude meetmetega).
d. Sõiduki hankimisel arvestatakse, et paljud sõidukid edastavad käiduandmeid sõiduki tootjale või teistele kolmandatele osapooltele.

INF.11.M2 Korrakohane hooldus ja IT-komponentide uuendamine [vastutav isik, IT-talitus]

a. Sõidukeid ja integreeritud IT-komponente hooldatakse lähtudes tootja antud spetsifikatsioonidest ja hooldusintervallidest.
b. IT-komponentide uuendite paigaldamine võib toimuda ka tavahoolduste vahelisel ajal.
c. Traadita andmeside kaudu tehtavad (ingl *over-the-air*, OTA) tarkvarauuendused viiakse läbi turvaliselt ja kontrollitult.
d. Sõidukite hooldus- ja remonditöid viivad läbi volitatud ettevõtted ja kvalifitseeritud hooldustöötajad.
e. Väljaspool organisatsiooni toimuva sõiduki hooldus- või remonditöö ajaks eemaldatakse sõidukilt tundliku teavet sisaldavad IT-komponendid.
f. Pärast sõiduki hooldust ja/või tarkvarauuendite paigaldamist kontrollitakse IT-komponentide nõuetekohast funktsioneerimist.

INF.11.M3 Sõiduki infoturbe juhendid [IT-talitus, vastutav isik, kasutaja, andmekaitsespetsialist]

a. Sõidukis töödeldavad andmed (sh isikuandmed) on kaardistatud ja dokumenteeritud.

b. Sõidukis töödeldavat andmeid (sh sõidukis peetud vestluste salvestisi) kaitstakse lähtudes andmete kaitsetarbest. On määratud, kellel ja mis tingimustel on nendele andmete juurdepääs.

c. On määratud, milliseid andmeid on lubatud sõiduki info- ja meelelahutussüsteemiga (ingl *infotainment system*) sünkroonida või sinna käsitsi sisestada.

d. On määratud, milliseid turvameetmeid kasutatakse sõiduki andmesideliideste kaitseks.

e. On koostatud juhendid sõiduki IT-süsteemide turvaliseks kasutamiseks ja haldamiseks.

INF.11.M12 Vargusvastase kaitse vahendid [vastutav spetsialist, töötaja]

a. Organisatsiooni sõidukid on varustatud vargusvastase alarmsüsteemi ja mootori käivitamist blokeeriva immobilaiseriga.

b. Sõiduki jätmisel ilma järelevalveta on vargusvastase kaitse vahendid alati aktiveeritud.

3.3 Standardmeetmed

INF.11.M4 Sõidukite infoturbe eeskirja jõustamine [vastutav spetsialist, IT-talitus]

a. Organisatsioonile kuuluvate sõidukite kasutamisel on sobivate turvameetmete rakendamine tehtud kõigile töötajatele ja sõiduki kasutajatele kohustuslikuks.

b. Sõidukite infoturbe eeskiri on dokumenteeritud, asjaomastele töötajad järgivad kinnitatud sõidukite infoturbe eeskirja.

c. Sõidukite infoturbe eeskirja vaadatakse üle perioodiliselt, vajadusel uuendatakse eeskirja.

INF.11.M5 Sõidukite inventariloend

a. Sõiduki kohta on koostatud loend sõidukisse sisse ehitatud IT-komponentidest (nt navigatsioonisüsteem) ning sõidukile hiljem lisatud seadmetest (nt käsiraadiojaam).

b. Sõidukite inventariloend sisaldab teavet sõidukite IT-süsteemidega *Bluetooth*'i kaudu seotud nutiseadme(te) kohta.

c. Inventariloendisse kantud IT-komponentide kohta on olemas tehnilised juhendid ning kasutajat IT-süsteemidega töötamisel abistavad kasutusjuhendid.

d. Inventariloendit uuendatakse vastavalt vajadusele.

e. Perioodiliselt kontrollitakse sõidukite inventariloendi vastavust tegelikule olukorrale. Ülevaatuse käigus kontrollitakse, kas sõiduki info- ja meelelahutussüsteem pole seotud volitamata nutiseadmetega.

INF.11.M6 Detailsed tegevusjuhised [vastutav isik, kasutaja]

a. On koostatud detailsed tegevusjuhised tegutsemiseks sõiduki avariiolukorra ja IT-komponentide rikke korral.

b. Juhised avariiolukorra ja IT-komponendi rikke korral tegutsemiseks asuvad sõidukis kättesaadavas asukohas.

c. On koostatud tegevusjuhend tegutsemiseks sõiduki ärandamise või volitamata sissetungi puhuks.

INF.11.M7 Sõiduki turvaline kasutamine [vastutav isik, kasutaja]

a. Organisatsioon on kehtestanud sõidukite kasutamise korra, mis määratleb:
   - kes ja mis otstarbel võivad sõidukit kasutada;
   - kuidas on korraldatud sõiduki parkimine;
   - vargusvastased vahendid, mis tuleb sõiduki parkimisel (või veesõiduki dokkimisel) aktiveerida;
   - sõidukis viibivate inimeste ja veose kaitsemeetmed.

b. Sõidukit juhtima volitatud isikud:
   - omavad kehtivat juhiluba;
   - oskavad sõidukit ja selle IT-süsteeme käsitseda;
   - teavad kaasnevaid turvariske.

INF.11.M8 Sõiduki kaitse ilmastikumõjude eest [kasutaja, vastutav spetsialist]

a. Sõidukid ja nendesse paigaldatud IT-komponendid on piisavalt kaitstud ilmastikumõjude eest.

b. Ekstreemsete ilmastikuolude puhul ning sõltuvalt sõiduki tüübist, asukohast ja keskkonnatingimustest on sõiduki volitatud kasutaja kohustatud rakendama täiendavaid kaitsemeetmeid.

INF.11.M9 Sõiduki kasutusvalmiduse tagamine [vastutav spetsialist]

a. Enne sõiduki kasutuselevõttu on teada, kus tehakse sõiduki hooldust ja kust hangitakse sõidukile vajalikke varuosasid ja kulumaterjale.

b. Sõiduki varuosadest ja kulumaterjalidest on piisav kohapealne varu. Kulumaterjalide kättesaadavus on tagatud sõiduki kasutusaja jooksul.

INF.11.M10 Sõidukite kasutusest kõrvaldamise kord [IT-talitus, vastutav spetsialist]

a. Enne sõiduki kasutusest kõrvaldamist kustutatakse turvaliselt kõik sõiduki IT-komponentidesse talletatud tundlikud andmed.

b. Sõidukis oleva andmestiku kustutamisel kasutatakse eelnevalt kaardistatud IT-komponentide loendit (vt INF.11.M5 *Sõidukite inventariloend*).

3.4 Kõrgmeetmed

INF.11.M11 Asendamise kord [vastutav spetsialist] (A)

a. Organisatsioon on koostanud tegevuskava juhuks kui sõidukit tabab ootamatu tehniline rike või muu asjaolu, miks sõidukit antud hetkel pole võimalik kasutada.

b. Ärikriitilist funktsiooni omavatele sõidukitele on võimalik mõistliku aja jooksul leida samaväärne asendussõiduk.

c. Igale sõidukijuhile on määratud teda vajadusel asendav töötaja.

INF.11.M13 Sõiduki kaitse kahjulike välismõjude eest [vastutav spetsialist] (A)

a. Sõltuvalt sõiduki tüübist välditakse sõiduki pikaajalist viibimist kahjulike välismõjudega (nt segavate raadiolainetega) asukohas.

b. Kahjulike välismõjude vastu rakendatakse sobivaid kaitsemeetmeid.

INF.11.M14 Konfidentsiaalse teabe kaitse [IT-talitus, vastutav spetsialist] (C-I-A)

a. Sõidukid ja sõiduki IT-komponendid on kaitstud andmevarguse, andmete manipuleerimise ja volitamata kasutamise eest.

b. Sõidukitootja kavandatud andmekaitse meetmed on rakendatud ning nende toimet on kontrollitud.

c. Vajadusel täiendatakse olemasolevaid turvameetmeid (nt paigaldatakse täiendav vargusvastane alarmsüsteem).

INF.11.M15 Sõiduki liideste kaitse [IT-talitus, vastutav spetsialist] (C-I-A)

a. Kõik sõiduki füüsilised välisliidesed ja andmesideliidesed on kaitstud volitamata juurdepääsu ja volitamata kasutamise eest.

INF.11.M16 Tulekustutussüsteem [vastutav spetsialist] (A)

a. Sõiduk on lisaks kohustuslikule käsikustutile varustatud autonoomse tulekustutussüsteemiga.

INF.11.M17 Sõidukisisese võrgu eraldamine (C)

a. Sõidukisisene andmesidevõrk (ingl *In-Vehicle Network*, IVN) on kasutajaandmeid sisaldavate IT-komponentide võrgust eraldatud turvalüüsiga (ingl *security gateway*).

INF.12 Kaabeldus

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed elektri- ja sidekaabelduse kaitseks rikete, häirete ja manipuleerimise eest.

1.2 Vastutus

Kaabelduse meetmete täitmise eest vastutab vastutav spetsialist.

Lisavastutajad

Tehnikatalitus, IT-talitus.

1.3 Piirangud

Moodul käsitleb kaabeldust üldiselt, mooduli meetmed kehtivad nii elektrikaabeldusele kui IT- ja sideteenuse kaabeldusele.

Hoonete ja ruumide kaabelduse paigutuse ja tuleohutuse osas esitatakse täiendavad meetmed moodulis INF.1 Hoone üldiselt.

Moodul ei käsitle aktiivsete võrgukomponentide (ruuterid, kommutaatorid jms) ega traadita võrgu turvet. Vastavaid teemasid käsitletakse NET mooduligrupis.

2 Ohud

2.1 Kaabli süttimine

Kaabli süttimine tekitab tulekahjuks arenedes märkimisväärset kahju. Lisanduvateks tagajärgedeks on elektrilühised ja elektriseadmete rikked. Kaabli süttimisega kaasneb agressiivse toimega gaasiühendite eraldumine, hõõguv põlemine või lahtine tuli. Kaabli süttimise korral ei tõuse ümbritseva keskkonna temperatuur enamasti järsult, mistõttu suitsuvingu oht tekib enne kui lakke paigaldatud suitsuandurid jõuavad rakenduda.

2.2 Kaabelduse aladimensioneerimine

Töökohtade, serveriruumide ja andmekeskuste kaabeldus kavandatakse sageli vaid hetkevajadusele tuginedes. Kuna sageli pole võimalik kaableid vahetada või neid juurde lisada, määravad elektrivõrgu voolutaluvuse (nt täiendavate serverite kasutuselevõtuks) olemasolevad kaablid. Aladimensioneeritud kaablite puhul tekib kaablite ülekuumenemise ja süttimise oht.

Sidevõrgu aladimensioneerimisel võib kannatada selle käideldavus. Seejuures jääb sageli tähelepanuta, et uute IT-süsteemide lisandumisel, andmemahtude suurenemisel või tehniliste standardite muutumisel on vaja võrgu läbilaskevõimet suurendada. Seda saab teha määral, kuivõrd olemasolevad kaablid ja võrguseadmed seda võimaldavad või on jäetud ruumi täiendavate kaablite paigaldamiseks.

2.3 Kaabelduse puudulik dokumenteerimine

Kui puuduliku dokumentatsiooni tõttu pole teada kaablite täpset asukohta, võivad kaablid saada väljaspool hoonet või hoone sees tehtavate ehitustööde tõttu kahjustada. Samuti takistab puudulik dokumentatsioon kaablite kontrolli, hooldust ja parandust.

2.4 Jaotusseadmete puudulik turve

Sageli on toitevõrgu jaotuskilbid ja võrguseadmekapid lukutamata ja asuvad vabalt juurdepääsetavates ruumides. Ebapiisav füüsiline turve võimaldab igaühel jaotuskappe avada, sidekaableid manipuleerida või elektrikatkestusi põhjustada.

Kui pingestatud komponente saab vahetult puudutada, kaasneb sellega otsene oht inimeste elule ja tervisele.

2.5 Kaablikahjustused

Kaablite juurdepääsetavuse ja ebaturvalise paigutuse puhul on oht, et keegi võib kaableid tahtmatult või tahtlikult kahjustada. Kaabli kahjustumine võib tekitada tõrkeid andmesides või põhjustada kaablis lühise, mis omakorda kahjustab ühendatud elektritarviteid. Kahjustus ei pruugi mõjuda koheselt, katkestuse mõju võib avalduda aja jooksul.

Sidekaablite tahtlik hävitamine häirib IT-seadmete toimimist ja põhjustab organisatsioonile rahalist kahju.

2.6 Pinge võnkumine, liig- ja alapinge

Pinge võnkumisel võivad tekkida IT-süsteemide tõrked ja kahjustused. Võnkumised ulatuvad väga lühiajalistest ja väikestest sündmustest, millel on IT-süsteemidele vähene või puuduv mõju, kuni täieliku katkestuse või seadmeid hävitava liigpingeni. Pinge võnkumist võib esineda kõikjal elektrivõrgustikus, alates energiavarustusettevõtte põhivõrgust kuni elektriahelani, millega on ühendatud lokaalsed seadmed.

2.7 Liigne pikendusjuhtmete kasutamine

Sobivas asukohas püsivalt paigaldatud pistikupesade arv ei ole tihti paljude seadmete ühendamiseks piisav. Selle kompenseerimiseks kasutatakse pikendusjuhtmeid. Kui pikendusjuhtmed ei ole kvaliteetsed ja ei vasta nõuetele, võivad nad põhjustada tulekahju. Kui seadmetele piisava arvu pistikupesade tagamiseks on järjestikku ühendatud mitu pikendusjuhet, suureneb ühenduste liigkoormuse tõttu tulekahju oht veelgi.

2.8 Lubamatud ühendused

IT-süsteemide või muude tehniliste komponentide vahele rajatud lubamatud ja dokumenteerimata kaabliühendused ning lubamatute seadmete kasutamine võivad põhjustada turvaprobleeme ja töötõrkeid. Selliste lubamatute ühenduste kaudu on võimalik saada võrkudele, süsteemidele, teabele või rakendustele volitamata juurdepääs.

2.9 Liinihäiringud

Elektriliste signaalide edastust võivad kahjustada keskkonna elektri- ja magnetväljad. Liinihäiringu erivorm on läbikoste (ingl *crosstalk*). Häiringuid ei põhjusta seejuures enamasti keskkond, vaid külgnevatest liinidest edastatavate signaalide elektrivool.

2.10 Pealtkuulamine ja manipuleerimine

Liinide pealtkuulamisründed on ohuks teabe turvalisusele. Sidekaablid ei ole kunagi täiesti pealtkuulamiskindlad. Seda, kas liini tegelikult pealt kuulatakse, saab kindlaks teha üksnes keeruka mõõtmise teel. Oht on suurem, kui sidekaabeldus asub osaliselt väljaspool kaitstavat turvaperimeetrit. Sideliinide manipuleerimise eesmärk on häirida infotehnoloogia toimimist ning põhjustada organisatsioonile rahalist kahju.

3 Meetmed

3.1 Elutsükkel

Kavandamine

INF.12.M1 Sobiva kaablitüübi valimine

INF.12.M2 Kaabelduse kavandamine

INF.12.M4 Tasandusvoolude vältimine varjetes

INF.12.M5 Kaabelduse nõuete analüüs

INF.12.M7 Liigvoolukaitse

Evitus

INF.12.M3 Asjatundlik kaablipaigaldus

INF.12.M6 Kaabelduse vastuvõtmine

INF.12.M10 Kaabelduse dokumenteerimine ja märgistus

INF.12.M11 Jaotusseadmete dokumentatsioon

INF.12.M16 Turvalised jaotuskapid

Käitus

INF.12.M9 Kaablite tuleohutus

INF.12.M12 Paigaldiste ja ühenduste ülevaatus

INF.12.M13 Elektritarvitite süttimise vältimine

Kõrvaldamine

INF.12.M8 Liigsete kaablite kõrvaldamine

Lisanduvad kõrgmeetmed

INF.12.M14 Dubleeritud toide

INF.12.M15 Kaabelduse füüsiline turve

INF.12.M17 Sidekaablite dubleerimine

3.2 Põhimeetmed

INF.12.M1 Sobiva kaablitüübi valimine [IT-talitus, tehnikatalitus]

a. Elektrikaablite voolutaluvus on piisav ja on valitud varuga.
b. Kaablitüübi valimisel arvestatakse järgmisi tegureid:
   - ümbritsev keskkond (vesi, pinnas, gaas, valgus jne) ja selle temperatuur;
   - kaitse näriliste ja kaabli läbilõikamise eest;
   - kaabli tõmbetugevus (nt õhuliinina kasutamisel) ja painderaadius;
   - kaablivarjestus ja elektromagnetilised häiringud;
   - paigaldusviis, paigaldustrassi või kaablirenni iseärasused;
   - edastusseadmete vaheline kaugus;
   - ründekindlus;
   - elektritarvitite iseärasused.
c. Elektrikaablite valimisel järgitakse kohalduvaid standardeid, nõudeid ja eeskirju.
d. Sidekaablid on valitud piisava läbilaskevõime ja edastuskiiruse varuga.
e. Sidekaabli liigi (koaksiaal-, keerdpaar-, valguskaabel) ja kaablitüübi valiku põhjendused on dokumenteeritud.

INF.12.M2 Kaabelduse kavandamine [IT-talitus, tehnikatalitus]

a. Enne kaablite valimist ja paigaldust on koostatud elektri- ja sidekaabelduse kava, millega on määratud kaablite turvaline paigutus, jaotuspunktid, läbiviigud ja reservivajadus.
b. Kaablid, kaablikanalid ja -rennid võimaldavad rahuldada ka tulevikuvajadusi, st olemasolevad kaablid sobivad ka tarbimisvõimsuse kasvu korral ning kaablikanalitesse saab vajadusel paigaldada lisakaableid.
c. Kui täismõõdus kaablirenne kohe ei paigaldata, tuleks seina- ja laeläbiviikude läbimõõdud projekteerida piisava varuga ja täita pehme tuletõkkematerjaliga.
d. Võimalusel paigaldatakse kaablid asukohtadesse, mis on juurdepääsetavad ainult organisatsioonile kuuluvatest ruumidest.
e. Võimalusel välditakse kaablite paigaldamist käiguteedele ja suure tuleohtlikkusega piirkondadesse.
f. Samas kaablirennis asuvad side- ja elektrikaablid on paigaldatud erinevatesse kaablirenni sektsioonidesse.

INF.12.M3 Asjatundlik kaablipaigaldus [IT-talitus, tehnikatalitus]

a. Elektrikaabelduse paigaldavad nõutava kvalifikatsiooniga töötajad.

b. Kaabelduse paigaldaja jälgib, et tarnitud kaablid ning vajaminevad materjalid ning ühendusdetailid vastaksid spetsifikatsioonile ega saaks paigaldamise käigus kahjustada.

c. Kõikides tööetappides kontrollib tellija kaabelduse teostusele esitatud nõuete täitmist.

INF.12.M10 Kaabelduse dokumenteerimine ja märgistus [IT-talitus, tehnikatalitus]

a. Kaabelduse dokumentatsioon sisaldab kaabliskeeme, hooneplaane, rennide asendiplaane, pistikupesade asukohti ja jaotuskappide kaabliühendusjooniseid.

b. Sisedokumentatsioon hõlmab lisaks kaablite paigalduse dokumentatsioonile ka tehtud hoolduste ning muudatuste andmeid.

c. Kaablite märgistus dokumentatsioonis on läbivalt ühtne ja ühetähenduslik.

d. Sisedokumentatsiooni kasutajaskond on piiratud tööpõhise vajadusega.

e. Väljapoole jagatav kaabelduse dokumentatsioon ei sisalda tundlikku ega liigset teavet.

f. Kaabelduses tehtud muudatused dokumenteeritakse esimesel võimalusel.

g. Kaabelduse ja seotud võrguseadmete dokumentatsioon vaadatakse üle vähemalt üks kord kolme aasta jooksul.

INF.12.M11 Jaotusseadmete dokumentatsioon [IT-talitus, tehnikatalitus]

a. Iga jaotusseadme (jaotuskilbi) juures asub selle seadme kaablite paigutusskeem.

b. Paigutusskeem on üheselt mõistetav, et tagada hooldustööde ohutus.

c. Jaotusseadme dokumentatsioon on objektiivne, ei näita liinide otstarvet ega esita muud tundlikku teavet. Erandina on otstarve märgitud avariielektritoite liinil.

INF.12.M13 Elektritarvitite süttimise vältimine [tehnikatalitus]

a. Elektriseadmeid on enne kasutuselevõttu kontrollinud kvalifitseeritud elektrik.

b. Isiklike elektriseadmete kasutamine on reguleeritud ja toimub selleks kehtestatud korra alusel.

c. Kodumasinaid kasutatakse ainult selleks ette nähtud ruumides.

d. Pistikupesad paigaldatakse olemasolevatele kaablikanalitele või fikseeritakse seinale.

e. Kui pikendusjuhtmete kasutamine on vältimatu, siis arvestatakse järgmist:
   - kasutatakse ainult kvaliteetseid ja kontrollitud pikendusjuhtmeid;
   - tarbitav võimsus vastab pikendusjuhtme spetsifikatsioonile ega ületa 3500 W;
   - pikendusjuhtmed ei ole üksteise külge ühendatud;
   - pikendusjuhtmed ei jää töötamiskohal inimestele jalgu ega asu käiguteedel.

f. Ventilaatoreid puhastatakse kogunenud tolmust vähemalt kord aastas ja vajadusel sagedamini.

3.3 Standardmeetmed

INF.12.M4 Tasandusvoolude vältimine varjetes [tehnikatalitus]

a. IT-komponentide toitekaablid on valitud sellised, et tasandusvoolud ei häiriks sidekaablite varjestust.

b. IT-seadmete madalpingevõrk on paigaldatud TN-S (neutraal- ja kaitsejuhe on teineteisest eraldatud) juhistikusüsteemis.
c. Kaablite omavahelise kauguse, varjestuse ja maanduse osas järgitakse kohalduvaid standardeid, nõudeid ja eeskirju.
d. Regulaarselt tehakse tasandusvoolude testmõõtmist.

INF.12.M5 Kaabelduse nõuete analüüs [IT-talitus, tehnikatalitus]

a. Kaabelduse tulevikukindluse, vajaduspõhisuse ja ökonoomsuse tagamiseks hinnatakse organisatsiooni hetkevajadust ja pikaajalisi arenguvajadusi.
b. Sidekaabelduse kavandamisel on kaablite liigi ja konstruktsiooni valimiseks tehtud nõuete analüüs, milles on võetud arvesse:
    - lähiperspektiivis vajalik läbilaskevõime;
    - läbilaskevõime vajaduse kasv tulevaste teenuste ja rakenduste lisandumise tõttu;
    - andmeedastuse käideldavus, terviklus ja konfidentsiaalsus;
    - erinevad kaablid teatud rakendustele (nt valvesüsteem, protsessijuhtimine);
    - eraldi kaablid teiste vajadustega või erineva kaitsetarbega aladele;
    - aktiivkomponentide toitevajadus sidekaablist;
    - lahenduse maksumus.
c. Nõuete analüüsi tulemuste alusel korrigeeritakse elektri- ja sidekaabelduse kava (vt INF.12.M2 *Kaabelduse kavandamine*).

INF.12.M6 Kaabelduse vastuvõtmine [IT-talitus, tehnikatalitus]

a. Kaabelduse vastuvõtmiseks on kehtestatud ja dokumenteeritud protseduur ja kontroll-loend.
b. Vastuvõtuprotseduur algatatakse ainult siis, kui kaabelduse paigaldaja on teatanud kõigi tööde lõpetamisest.
c. Vastuvõtmisel kontrollib tellija
    - vastavust kaabelduse kavale;
    - defektide puudumist;
    - vastavust standarditele ja eeskirjadele;
    - paigaldustööde tegelikku mahtu ja arvete õigsust.
d. Vastuvõtu kontroll-loend ja kõikide osapoolte siduvalt allkirjastatud üleandmis-vastuvõtuakt säilitatakse osana kaabelduse sisedokumentatsioonist.

INF.12.M7 Liigvoolukaitse [tehnikatalitus]

a. On kavandatud ja rakendatud meetmed elektritarvitite kaitsmiseks liigvoolu eest.
b. Iga kaitseelemendi (liigvoolukaitselüliti) järel tohib mõjuda maksimaalselt nii palju liigvoolust põhjustatud energiat, kui selle järel paiknevad elektritarvitid (sh järgmised liigvoolukaitselülitid) suudavad taluda.
c. Elektrisüsteemide liigvoolukaitse vastab kohalduvatele standarditele ja eeskirjadele.
d. Liigvoolukaitse kava hõlmab ka avariitoitegeneraatoreid ja puhvertoiteallikaid.

e. Liigvoolukaitselülitite toimimist kontrollitakse perioodiliselt ja lisaks ka kaitse puudulikkusele viitavate sündmuste ilmnemisel. Vajadusel asendatatakse liigvoolukaitselülitid uutega.

INF.12.M8 Liigsete kaablite kõrvaldamine [IT-talitus, tehnikatalitus]

a. Hoone kasutusotstarbe muutumise tõttu või muul põhjusel tarbetuks osutunud kaablid eemaldatakse täielikult.

b. Pärast liigsete kaablite eemaldamist paigaldatakse läbiviikudesse uuesti tuletõkked.

c. Liigsed kaablid, mida saab kasutada varuühenduse tarbeks, hoitakse töökorras ja need on vastavalt märgistatud.

d. On olemas ajakohane ülevaade, millised kaablid seisavad kasutuseta, on lahti ühendatud või eemaldatud. Muudatused kaabelduses dokumenteeritakse.

INF.12.M9 Kaablite tuleohutus [tehnikatalitus]

a. Kaablite süttimise vältimiseks on valitud õiget tüüpi elektrikaablid (vt INF.12.M1 *Sobivad kaablitüübid)* ja piisavate mõõtmetega kaablirennid.

b. Kaablitrassid on kooskõlastatud tuleohutuse eest vastutajaga.

c. Kaablid ei ole paigutatud liiga tihedalt, vajadusel on paigutatud kaableid eraldavad tuletõkked.

d. Kaablirennides on tagatud piisav õhuvahetus.

INF.12.M12 Elektripaigaldiste ja ühenduste ülevaatus [IT-talitus, tehnikatalitus]

a. Pärast paigaldamist ja perioodiliselt ka hiljem kontrollib elektripaigaldisi, jaotusseadmeid ja ühenduskarpe atesteeritud spetsialist.

b. Ülevaatuse tegemisel järgitakse valdkonnapõhiseid standardeid ja õigusakte.

c. Ülevaatuse käigus veendutakse, kas:

- elektripaigaldised on paigaldatud tootja spetsifikatsiooni kohaselt;
- läbiviikude tuletõkked on tehtud õigesti;
- kaablid on valitud vastavalt lubatavale voolutugevusele, kaitseseadmete valikule ja seadistusele;
- ühendusskeemid on täielikud ja õiged;
- hoiatussildid on paigaldatud;
- automaatkaitselüliti automaatne väljalülitus töötab.

d. Testimise ja visuaalse ülevaatuse käigus avastatud puudused dokumenteeritakse ja edastatakse vastutajatele puuduste kõrvaldamiseks ja põhjuste väljaselgitamiseks.

INF.12.M16 Turvalised kaitsekapid [tehnikatalitus]

a. Elektriühenduste ja jaotusseadmete tööohutuse tagamiseks on elektri- ja IT-seadmed paigutatud turvalistesse ja lukustatud kaitsekappidesse.

b. Kaitsekapid on paigutatud vastavalt kaitsetarbele ning varustatud sobivate uste, külgseinte ja lukustusega.

c. Võrguseadmed on paigutatud seadmepüstikutesse (ingl *rack*) või kaitsekappidesse.

d. Juurdepääs kaitsekappides asuvatele seadmetele on ametipõhiselt piiratud.

e. Kaitsekappi paigutatud seadmete summaarne soojuseraldus ei ületa lubatavat piirmäära.

f. Kappidesse on jäetud piisav laiendusvaru.

3.4 Kõrgmeetmed

INF.12.M14 Dubleeritud toide [tehnikatalitus] (A)

a. Suure käideldavustarbega oluliste IT-komponentide toiteks on kasutusel kaks eraldi liini, mis tulevad erinevatest jaotusseadmetest.

b. Võimalusel paigaldatakse dubleerivad toitekaablid eraldi asukohtadesse.

c. Mõlemal toiteliinil on rakendatud automaatseire, tõrgetest alarmeeritakse viivitamata.

INF.12.M15 Kaabelduse füüsiline turve [IT-talitus, tehnikatalitus] (I-A)

a. Üldkasutatavates ruumides ja hoone mittejälgitavates asukohtades on kaablid ja jaotusseadmed kaitstud volitamata juurdepääsu eest.

b. Kaabeldus on peidetud ja kaitstud kaablikanalitega või tugevdatud paigaldustorudega.

c. Jaotusseadmed on lukustatud ja nende pääsuõigused on ametipõhiselt piiratud. On kehtestatud kord juurdepääsu reguleerimiseks ja võtmete haldamiseks.

INF.12.M17 Sidekaablite dubleerimine [IT-talitus] (A)

a. Kõrge käideldavusnõudega süsteemide tarbeks on paigaldatud esmast sidekaablit dubleeriv sidekaabel.

b. Dubleeritud kaablid on paigaldatud erinevatesse püstikutesse ja kaablirennidesse, mis võimalusel asuvad ka hoone erinevates tuletõkkesektsioonides.

c. Kõrge käideldavusnõudega süsteemide puhul on kaalutud samaaegseid välisühendusi mitmete IT- või sideteenuse tarnijatega.

d. Kui kaablite paralleelkasutust ei rakendata, kontrollitakse dubleeritud kaablite korrasolekut regulaarselt.

4 Lisateave

Lühend	**Publikatsioon**
[ISO60364]	EVS-HD 60364 “Madalpingelised elektripaigaldised”
[ISO50173]	EVS-EN 50173 “Information technology - Generic cabling systems”
[ISO50174]	EVS-EN 50174 “Information technology – Cabling installation”
[ISO50310]	EVS-EN 50310 “Telecommunications bonding networks for buildings and other structures”

INF.13 Hoonete tehniline haldus

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed hoone või hoonete kogumi tehnoseadmete ja -süsteemide (kütte-, jahutus-, ventilatsiooni-, konditsioneerimis-, vee-, valgustus-, tulekaitse- ja nõrkvoolusüsteemid) turvaliseks kavandamiseks, evitamiseks, käitamiseks ja arendamiseks. Protsessi nimetatakse lühendatult TBM (*Technical Building Management*).

1.2 Vastutus

Hoonete tehnilise halduse meetmete rakendamise eest vastutab tehnikatalitus.

Lisavastutajad

Arhitekt, IT-talitus, organisatsiooni juhtkond.

1.3 Piirangud

Moodulis esitatud meetmed kohalduvad kõigile tehnosüsteeme sisaldavatele hoonetele. Hooneautomaatika süsteemide (ingl Building Automation and Control System, BACM) turvameetmeid käsitletakse detailsemalt moodulis INF.14 Hooneautomaatikasüsteemid. Automaatjuhtimisega tehnosüsteemide puhul rakendatakse meetmeid mõlemast moodulist.

Sõltuvalt tehnilise halduse süsteemi taristust ja automaatjuhtimissüsteemide arhitektuurist rakendatakse täiendavalt meetmeid gruppidest IND ja SYS, nt IND.2.1 „Tööstusautomaatika komponendid üldiselt“ või SYS.4.4 Esemevõrgu (IoT) seade üldiselt.

Hoonete tehnilise halduse protsessile tervikuna rakenduvad meetmed mooduligruppidest OPS.1 Oma käidutööd ja OPS.2 Käidutööd teenusena. Haldusega seotud isikutele kehtivad turvameetmed on esitatud moodulites ORP.2 Personal ja ORP.4 Identiteedi ja õiguste haldus.

Hoone tehnilise halduse süsteemi komponentide turvalise kaughoolduse meetmeid kirjeldatakse moodulites OPS.1.2.5 Kaughooldus ja IND.3.2 Tööstusautomaatika komponentide kaughooldus. Kui TBM protsessis kasutatakse pilvteenuseid, lisanduvad meetmed moodulist OPS.2.2 Pilvteenuste kasutamine.

Hoonete füüsilist turvalisust käsitletakse moodulis INF.1 Hoone üldiselt.

2 Ohud

2.1 Tehnosüsteemidele esitavate nõuete puudumine kavandamisetapis

Kui hoone kavandamise ja ehituse planeerimise etapis pole määratud vastutajaid ning tehnosüsteemide täpne vajadus ja paigutus on jäänud ebaselgeks, on tellija vajadustele vastavate ja turvaliste tehnosüsteemide ehitamine raskendatud. Hoone ei vasta tegelikule kasutusvajadusele.

Kui tehnosüsteemide kavandamisel pole arvestatud kõiki kehtivaid regulatsioone ja nendest tulenevaid ehitus-, ekspluatatsiooni- ja turvanõudeid, võib juhtuda, et valmiv hoone ei vasta tehnilistele nõuetele.

2.2 Hoone tehnilise halduse dokumentatsiooni puudumine või puudulikkus

Sageli tegelevad hoonete tehnilise haldusega erinevad välised teenuseandjad. Kui konkreetsed kontaktisikud on määramata ja teenusega seotud dokumentatsioon ning kohustusi sisaldavad teenusetaseme lepped (ingl *Service Level Agreement,* SLA) on puudulikud või vajalikul hetkel juurdepääsematud, tekivad avariiolukorras tarbetud viivitused. Olulise tehnosüsteemi rike või tehnosüsteemi toimimise katkestus võib raskemal juhul ohustada hoones viibijate elu ja tervist.

Kui tehnosüsteeme järjepidevalt ei hooldata, tehnosüsteemidel puuduvad vajalikud ohutussertifikaadid või korraliste hoolduste tegemine pole dokumenteeritud, on tegemist ehitusseadustikus esitatud nõuete rikkumisega. Olenevalt tehnosüsteemist võib korralise hoolduse tegemata jätmine olla ohtlik inimeste hoones viibijate tervisele.

Kui tehnosüsteemide korralised hooldused on tegemata, ei pruugi olla võimalik kindlustuslepingu alusel korvata intsidentidest tekkivat kahju.

2.3 Tehnosüsteemide liidestamisel tehtud vead

Tehnosüsteemide poolt genereeritud alarmid või automaatsed teavitused võivad käivitada teatud tegevusi teistes tehnosüsteemides. Kui kriitiliste tehnosüsteemide (nt ohutusautomaatika süsteemid, automaatsed tulekahjusignalisatsioonisüsteemid) liidestamisel teiste süsteemidega on tehtud vigu või liidestes esinevad tõrked, võib see kaasa tuua seaduserikkumise ning ohustada hoones viibijate elu ja tervist.

Näiteks kui andmekeskuse tulekahjusignalisatsiooni käivitumisel ei rakendu akustilised ja/või optilised häiresüsteemid, ei pruugi andmekeskuses viibivad inimesed ruumist välja saada enne kui ruum on täidetud kustutusgaasiga. Tehnosüsteemide põhjustatud võltsalarmid võivad nõrgendada inimeste valvsust, võimaldada volitamata ruumidesse sisenemist või vastupidi - põhjustada inimeste tarbetu ruumidesse kinnijäämise.

2.4 Tehnosüsteemide toimimise ebapiisav seire

Kui hoone tehnosüsteemide toimimise seire on ebapiisav, võivad turvalisuse seisukohast olulised sündmused (nt. veetorustiku lekked) jääda õigeaegselt avastamata. Olenevalt sündmusest võib see kaasa tuua arvestatavaid hoonekahjustusi või ohustada inimeste elu ja tervist.

Kui talvel toimuvast küttesüsteemi rikkest ei saada õigeaegselt teada, võib ruumide temperatuuri järsk langus tekitada veetorustiku külmumise ning kahjustusi hoone sisustuses. Kui kindlat temperatuuri või õhuniiskust vajavate kaupade hoiuruumide tehnosüsteemide seadistamisel on tehtud vigu ja seire ei toimi, võib kaupade riknemisest tingitud kahju olla märkimisväärne.

Rike tulekaitsesüsteemis ei võimalda tekkinud tulekahju õigeaegselt avastada, viivituse tõttu suurenevad tule poolt tekitatud kahjustused oluliselt.

2.5 Puudulik pääsuõiguste haldus

Kui hoone tehnosüsteemid on organisatsiooni IT-süsteemidest füüsiliselt eraldatud, käsitletakse tehnosüsteemide pääsuõiguste haldust sageli eraldiseiseva protsessina.

Hoone tehnilise haldusega seotud pääsuõiguste puudulikul rakendamisel võib juhtuda, et sama kasutajakontot kasutavad mitmed töötajad. Ei ole tagatud, et organisatsiooniga lepingu lõpetanud töötajate või või teenuseandja töötajate pääsuõigused süsteemist õigeaegselt eemaldatakse. Volitamata juurdepääs hoone tehnosüsteemidele võib kaasa aidata rünnetele organisatsioonile kahju tekitamiseks.

3 Meetmed

3.1 Elutsükkel

Kavandamine

INF.13.M1 Tehnosüsteemide seisukorra hindamine hoone vastuvõtmisel
INF.13.M2 Vajalike pädevuste ja vastutajate määramine
INF.13.M4 Hoonete tehnilise halduse turvaeeskiri
INF.13.M5 Hoone tehnilise halduse kavandamine
INF.13.M6 Hoonete tehnilise halduse kontseptsioon
INF.13.M9 CAFM tarkvara kasutamise kord
INF.13.M10 Hooneteabe digitaalse modelleerimise tarkvara (BIM) turvaline haldus
INF.13.M14 Hoonete tehnilise halduse erirollide ja -volituste haldus

Evitus

INF.13.M3 Piisav hoone tehniline dokumentatsioon
INF.13.M7 Kasutatavate raadiosageduste loend
INF.13.M8 Hoone tehnilise halduse objektide loend
INF.13.M12 Hoonete tehnilise halduse rakenduse turvaline konfigureerimine
INF.13.M13 Hoonete tehnilise halduse süsteemi turvaline liidestamine

Käitus

INF.13.M11 Hoonete tehnilise halduse protsessi turbe tugevdamine
INF.13.M15 Hoonete tehnilise halduse süsteemi kaitse kahjurvara eest
INF.13.M16 Hoonete tehnilise halduse süsteemi muudatuste haldus
INF.13.M17 Hoonete turvalised hooldus- ja remonditööd
INF.13.M18 Ennetavad hooldustööd hoonete tehnilises halduses
INF.13.M19 Hoonete tehnilise halduse süsteemi seire
INF.13.M20 Hoonete tehnilise halduse süsteemi sündmuste käsitlemine
INF.13.M21 Hoonete tehnilise halduse süsteemi logimine
INF.13.M22 Hoonete tehnilise halduse süsteemi testimine
INF.13.M23 Hoonete tehnilise halduse süsteemi turvanõrkuste ja -uuendite teabe seire
INF.13.M24 Hoonete tehnilise halduse süsteemi andmete turvaline pilvtöötlus

Lisanduvad kõrgmeetmed

INF.13.M25 Hoonete tehnilise halduse süsteemi testkeskkond
INF.13.M26 Hooneteabe digitaalse modelleerimise tarkvara (BIM) valideerimine
INF.13.M27 Privaatpilve kasutamine hoonete tehnilise halduse süsteemis
INF.13.M28 Intellektitehnika turvaline kasutamine hoonete tehnilises halduses
INF.13.M29 Hoonete tehnilise halduse süsteemi integreerimine SIEM lahendusega
INF.13.M30 Hoonete tehnilise halduse süsteemi läbistustestimine

3.2 Põhimeetmed

INF.13.M1 Tehnosüsteemide seisukorra hindamine hoone vastuvõtmisel

a. Uue või eksisteeriva hoone vastuvõtmisel hinnatakse hoonesse paigaldatud tehnosüsteemide seisukorda, turvalisust ja jätkusuutlikkust.

b. Tehnosüsteemide hindamise käigus kontrollitakse tehnosüsteemide dokumentatsiooni täielikkust, piisavust ja täpsust (nt tootja dokumentatsiooni vastavust kasutusel olevate toodete ja tooteversioonidega).

c. Kaardistatakse tehnosüsteemide ja süsteemidokumentatsiooni seisukord, tuvastatud puudused likvideeritakse esimesel võimalusel. Suuremahuliste muudatuste (nt tehnosüsteemide väljavahetamise) teostamiseks koostatakse tegevuskava.

INF.13.M2 Vajalike pädevuste ja vastutajate määramine [organisatsiooni juhtkond, arhitekt]

a. Kuna erinevad hoone tehnilise halduse valdkonnad vajavad erinevaid oskusi, on määratletud ja dokumenteeritud iga valdkonna protsessidega seotud õigused, kohustused ja tööülesanded.

b. On määratud hoone tehnilise halduse (ingl *Technical Building Management,* TBM) protsessis osalejad ja vastutajad.

c. Kui hoone tehnilise halduse protsessi on kaasatud väline partner (nt büroohoone omanik), on kõik partneri õigused, kohustused, ülesanded ja pädevused fikseeritud hanke- või rendilepingus (vt OPS 2.3 *Väljasttellimine*).

d. Kõigi hoone tehnilises halduses osalejate vahel on kokku lepitud ja dokumenteeritud andmevahetus-, aruandlus- ja suhtluskanalid.

INF.13.M3 Piisav hoone tehniline dokumentatsioon

a. Kõigi hoonete kohta on olemas kehtivale regulatsioonile vastav ehituslik dokumentatsioon. Hoonetele on väljastatud kasutusluba.

b. Hoone dokumentatsiooni on täiendatud tehnilise dokumentatsiooniga. Hoone tehniline dokumentatsioon sisaldab muuhulgas teavet järgmiste objektide kohta:

- elektrikaabeldus, sh UPSid ja avariitoitegeneraatorid;
- sidekaabeldus;
- piksekaitsesüsteem;
- kanalisatsioonisüsteem;
- küttesüsteem;
- ventilatsiooni- ja konditsioneerimissüsteemid;
- tulekahjusignalisatsioon;
- läbipääsusüsteemid;
- liftisüsteemid;
- valve- ja kaamerasüsteemid;
- hooneautomaatika juhtsüsteemid.

c. Iga tehnosüsteemi kohta on dokumenteeritud vähemalt järgmine teave:

- tootja;

- riistvara ja tarkvara teave (sh mudeli- ja versiooninumber);
- seadmete soetamisaeg;
- liidestused teiste tehno- või IT-süsteemidega;
- juurdepääsu reeglid;
- kontaktisikute andmed;
- erinõuded (nt. käideldavusnõue 24X7).

d. Hoonete, hoonete tehnilise halduse ja konkreetsete tehnosüsteemide dokumentatsioon on ajakohane ja volitatud isikutele vajadusel kättesaadav.

3.3 Standardmeetmed

INF.13.M4 Hoonete tehnilise halduse turvaeeskiri

a. Organisatsioon on kehtestanud üldise turvapoliitikaga kooskõlas oleva hoonete tehnilise halduse turvaeeskirja.

b. Turvaeeskiri on aluseks valdkonnapõhiste turvajuhendite koostamisel. Hoonete tehnilise halduse turvaeeskiri käsitleb järgmisi valdkondi:

- tehnilise halduse kesksete tööriistade rakendamine;
- protsesside automatiseerimine (sh testimise ja konfiguratsioonihalduse nõuded);
- lubatavad tööriistad ja automatiseerimisvahendid;
- pääsuhaldus;
- andmeside turve;
- eeliskontode ja –õiguste kasutamine;
- logimine ja seire.

c. Hoonete tehnilise halduse turvaeeskirja vaadatakse regulaarselt üle, vajadusel eeskiri ajakohastatakse.

d. Kõik hoone tehnilise halduse eest vastutajad tunnevad ja järgivad turvaeeskirja.

INF.13.M5 Hoone tehnilise halduse kavandamine

a. Hoonete tehnilises halduse kavandamisel on arvestatud hoone olemasolevat ja kavandatavat taristut ja sellega seotud protsesse.

b. Kavandamisel on dokumenteeritud vähemalt järgmine:

- vajaduste analüüs (funktsionaalsus, liidestamine teiste süsteemidega);
- detailne nõuete spetsifikatsioon (sh tehnilise turbe ja käideldavuse nõuded);
- rakenduskava (vajalikud seadmed ja tööriistad, konfiguratsioon, kasutajad);

c. Detailsete nõuete puudumisel koostatakse tänapäevast tehnoloogiat arvestavad põhinõuded, millele on seadmete ja tööriistade valikul võimalik tugineda.

d. Rakenduskava sisaldab tehnosüsteemide sobivus- ja süsteemitestide läbiviimist enne väliste teenuste kasutuselevõttu või riist- või tarkvara soetamist (vt INF.13.A22 *Tehnosüsteemide testimine*).

e. Enne intellektitehnika (ingl *artificial intelligence*, AI) kasutuselevõttu hoonete tehnilises halduses on veendutud lahenduse turvalisuses (nt on konsulteeritud tootjaga ja tutvututud reaalsete kasutuslugudega).

f. Kavandamisel on arvestatud kõiki hoonete tehnilise halduse turvaeeskirjas (vt INF.13.M4 *Hoonete tehnilise halduse turvaeeskiri*) esitatud nõudeid.

INF.13.M6 Hoonete tehnilise halduse kontseptsioon [arhitekt]

a. Hoone tehnilise halduse kavandamine ja turvanõuded on koondatud hoonete tehnilise halduse kontseptsiooni.

b. Hoonete tehnilise halduse kontseptsioon sisaldab vähemalt järgmist:
   - hoonete tehnilise halduse protsesside kirjeldus;
   - hoonete tehnilise halduse meetodid ja vahendid;
   - pääsuõiguste halduse ja andmevahetuse reeglid;
   - võrgu segmentimine ja andmevahetuse turve võrgus;
   - toimingute seire, sündmuste logimine ja automaatselt saadetavad teavitused;
   - halduri juurdepääs ja selle turve;
   - teavitusahelad rikete ja turvaintsidentide korral (sh e-posti ja SMS teavitused);
   - teabevahetus muu tegevusvaldkonna protsesside ja IT-süsteemidega;
   - hoonete tehnilise halduse protsessi integreerimine organisatsiooni üldise avariihaldusega.

c. Hoonete tehnilise halduse kontseptsiooni valideeritakse ja vajadusel uuendatakse regulaarselt.

d. Hoonete tehnilise halduse kontseptsiooni järgimist kontrollitakse regulaarselt. Ülevaatuste käigus veendutakse, kas tehnosüsteemid on konfigureeritud vastavalt spetsifikatsioonidele ning on halduse põhimõtetega kooskõlas.

e. Ülevaatuste tulemused dokumenteeritakse, võimalike kõrvalekalletega tegeletakse esimesel võimalusel.

INF.13.M7 Kasutatavate raadiosageduste loend

a. Kõik traadita andmesidet (sh WLAN, Bluetooth ja mobiilne andmeside) kasutavad tehnosüsteemid on organisatsiooni erinevate asukohtade lõikes kaardistatud. Erinevad sagedusalad ja nende kasutajad on lisatud raadiosageduste loendisse.

b. Traadita andmeside kasutamine on IT-talituse ja käidutehnoloogia talitusega kooskõlastatud. Kasutatavates raadiosagedustes ei teki seadmevahelisi konflikte.

c. Raadiosageduste loendi vastavust tegelikule olukorrale kontrollitakse regulaarselt, vajadusel loend kaasajastatakse.

INF.13.M8 Hoone tehnilise halduse objektide loend [arhitekt]

a. Hoone tehnilise halduse süsteemi komponendid on kaardistatud ja kantud hoone tehnilise halduse objektide loendisse.

b. Iga objekti kohta on kirjeldatud vähemalt:
   - tootja andmed;
   - riistvara ja tarkvara andmed;
   - andmevahetusliidesed;
   - juurdepääsu reguleerimine;
   - korralised hooldused ja hooldustsükkel;

- vastutajate ja tehnilise toe kontaktandmed.

c. Loendisse kantakse täiendavalt kõik hoone tehnilise halduse taristu komponendid.

INF.13.M9 CAFM tarkvara kasutamise kord [arhitekt]

a. Hoone ressursihaldustarkvara (Computer Aided Facilities Management, CAFM) kasutatakse ainult tarkvara kasutamise korras kirjeldatud tingimustel.

b. CAFM tarkvara pääsuõigused on üksnes volitatud isikutel. Eriti oluline on see juhul, kui protsessis osalevad ka välise partneri töötajad.

INF.13.M10 Hooneteabe digitaalse modelleerimise tarkvara (BIM) turvaline haldus [arhitekt]

a. Hooneteabe digitaalseks modelleerimise tarkvara (Building Information Modeling, BIM) rakendamiseks on koostatud BIM kasutuselevõtukava (BIM Execution Plan).

b. BIM kasutuselevõtukava sisaldab vähemalt järgmist:
   - kasutatava BIM tarkvara kirjeldus;
   - seonduvad rollid ja kasutajad, kasutajate kohustused;
   - BIM integreerimine teiste süsteemidega (nt CAFM-ga);
   - BIM tehnilised spetsifikatsioonid (nt tarkvara failivormingud).

c. Kõik BIM andmed on asja- ja ajakohased.

d. Tundlik BIM teave (nt sisseetungituvastussüsteemi andmed) on juurdepääsetav ainult selleks volitatud töötajatele.

e. Enne BIM tarkvara kasutuseks kinnitamist on hinnatud tarkvara turvalisust. Tarkvara kasutuselevõtt on kooskõlastatud infoturbejuhiga.

INF.13.M11 Hoonete tehnilise halduse protsessi turbe tugevdamine

a. Hoonete tehnilise halduse (ingl *Technical Building Management,* TBM) protsessi infoturbe tugevdamise (ingl *hardening*) meetmed on dokumenteeritud.

b. Infoturbe tugevdamine hõlmab vähemalt järgnevat:
   - tootja infoturbe nõuete ja soovituste järgimine;
   - paroolide turvaline haldus;
   - turvaliste protokollide kasutamine;
   - tarbetute protokollide, liideste ja teenuste desaktiveerimine;
   - turvauuendite paigaldamine.

c. Tootja tagab hoone tehnilise halduse rakendusele turvauuendite väljastamise kogu rakenduse planeeritud kasutusea vältel.

d. Teadaolevate turvanõrkustega TBM-rakendus eemaldatakse kasutuselt. Kui see pole võimalik, eraldatakse hoone tehnilise halduse rakendus ülejäänud IT-süsteemidest võrgu segmentimisega.

e. TBM turvameetmete toimimist kontrollitakse regulaarselt. Vajadusel muudetakse olemasolevaid või lisatakse juurde uusi infoturbe meetmeid.

INF.13.M12 Hoonete tehnilise halduse rakenduse turvaline konfigureerimine

a. Enne hoonete tehnilise halduse rakenduse kasutuselevõtmist on veendutud rakenduse konfiguratsiooni turvalisuses.

b. Konfiguratsioonimuudatused testitakse ning nende käidukeskkonda paigaldamine toimub eelneva kooskõlastuse alusel.

c. Hoonete tehnilise halduse rakenduste konfiguratsioonid on varundatud. Vajadusel on võimalik taastada rakenduse viimasele muudatusele eelnev konfiguratsioon.

d. Konfiguratsiooni taastamist on testitud kas testsüsteemis või süsteemiuuendite paigaldamiseks võimaldatud hooldusaegade raames.

e. Hoonete tehnilise halduse rakenduste tarkvarauuendid ja konfiguratsioonimuudatused jõustatakse kõikides sama tüüpi rakendustes automaatselt ja võimalikult üheaegselt.

f. Eelseisvast konfiguratsioonimuudatustest teavitatakse kõiki asjaosalisi (sh tõrkeotsingu ja kasutajatoe töötajaid), eriti kui hoone tehnilise halduse rakenduse konfiguratsiooni muudatus puudutab juurdepääsumehhanisme või andmevahetusparameetreid.

g. Võimaliku rikke korral on halduril võimalik rakenduse konfiguratsiooni muuta ja rakendus taaskäivitada.

h. Hoonete tehnilise halduse rakenduste konfiguratsioonide vastavust tehnilistele spetsifikatsioonidele kontrollitakse regulaarselt. Kontrolli tulemused dokumenteeritakse, kõrvalekalded spetsifikatsioonidest parandatakse esimesel võimalusel.

INF.13.M13 Hoonete tehnilise halduse süsteemi turvaline liidestamine [arhitekt]

a. Kui põhjendatud juhul on vajalik hoonete tehnilise halduse süsteemi lisada piiratud usaldusväärsusega rakendus (nt rakendus, millel enam pole tootja tuge), piiratakse rakenduse võrguliiklust volitamata juurdepääsu takistamiseks tulemüüriga.

b. Hoonete tehnilise halduse süsteemi komponentide üldise turvalisuse eest vastutab tehnikatalitus.

INF.13.M14 Hoonete tehnilise halduse erirollide ja -volituste haldus

a. Hoonete tehnilise halduse süsteemi rollide määramisel ja volituste andmisel rakendatakse meetmeid moodulist „ORP.4 *Identiteedi- ja õiguste haldus“.*

b. Rolliga seotakse ainult minimaalselt vajalik hulk rakenduste pääsuõiguseid.

c. Hoonete tehnilise halduse süsteemi komponentide tootjate ja väliste hoolduspartnerite juurdepääs on võimalikult piiratud (võimalusel lubatud ainult lugemisõigusega juurdepääs).

d. Tehniliste kasutajate rollid (st rollid seadmevaheliseks andmevahetuseks) on dokumenteeritud. Tarbetud tehnilised kasutajad on desaktiveeritud.

INF.13.M15 Hoonete tehnilise halduse süsteemi kaitse kahjurvara eest

a. Hoone tehnilise halduse süsteemi kaitseks rakendatakse meetmeid moodulist OPS.1.1.4 *Kaitse kahjurprogrammide eest*.

b. Kui kahjurvaratõrje tarkvara pole võimalik kasutada (nt kui süsteem ei võimalda installida kolmandate poolte tarkvara või nappide arvutiressursside tõttu), on rakendatud sobivad alternatiivsed kaitsemeetmed (nt regulaarne varundus ja juurdepääsu piiramine).

c. Enne välise andmekandja ühendamist hoonete tehnilise halduse süsteemi komponendiga kontrollitakse andmekandjat pahavara suhtes.

INF.13.M16 Hoonete tehnilise halduse süsteemi muudatuste haldus

a. Hoonete tehnilise halduse süsteemi kavandatav muudatus arvestab kõigi asjaosaliste huve ja on kõigi osapooltega (sh välised hooldus- ja andmevahetuspartnerid) piisavalt aegsasti kooskõlastatud.

b. On koostatud juhend juhuks, kui ebaõnnestunult läbiviidud muudatust ei ole võimalik tagasi pöörata või kui endise olukorra taastamine on tehtav ainult suurte jõupingutustega.

c. Enne hoonete tehnilise halduse süsteemi muudatuse rakendamist tuleb läbi viia testid, mis hõlmavad ka süsteemi pöördprojekteerimise võimalust. Testi spetsiifika ja sügavus sõltub süsteemi keerukusest ja hõlmatud süsteemikomponentidest (vt INF.13.M22 *Hoonete tehnilise halduse süsteemi testimine*).

INF.13.M17 Hoonete turvalised hooldus- ja remonditööd

a. Hoonete regulaarsete hoolduste läbiviimiseks on koostatud hooldusplaan, mis muuhulgas sisaldab ka hooldus- ja remonditööde turvaaspekte.

b. On määratud hoonete hoolduse ja remondi eest vastutajad.

c. Väliste partnerite teostatud hooldus- ja remonditööde läbiviimist koordineerib organisatsiooni volitatud töötaja. Kõik hooldustööd on eelnevalt tehnikatalitusega kooskõlastatud, tööde vastuvõtmine akteeritakse.

d. Hoonetes tehtud hooldus- ja remonditööd on dokumenteeritud.

INF.13.M18 Ennetavad hooldustööd hoonete tehnilises halduses [arhitekt]

a. On määratud hooldusvälbad hoonete tehnilise halduse süsteemi komponentide regulaarseks hoolduseks.

b. Hooldustööde käigus veendutakse, kas süsteemi komponendid toimivad määratud parameetrite piires ning kas komponentide kasutusaeg pole läbi saamas.

INF.13.M19 Hoonete tehnilise halduse süsteemi seire

a. Eelanalüüsi käigus on määratud, millised hoonete tehnilise halduse süsteemi komponendid on võimalik kaasata ühtsesse seiresüsteemi ja milliseid näitajaid seire käigus jälgitakse.

b. Seire alla kuuluvate süsteemide ja vaadeldavate näitajate asjakohasust ja piisavust hinnatakse regulaarselt.

c. Olekuteateid ja muid seireandmeid edastatakse ainult turvaliste sidekanalite kaudu.

INF.13.M20 Hoonete tehnilise halduse süsteemi sündmuste käsitlemine [arhitekt]

a. Hoonete tehnilise halduse süsteemi sündmused liigitatakse ja klassifitseeritakse sündmuse kaalukuse (sh võimaliku mõju) järgi.

b. Sündmuste automaatseks klassifitseerimiseks on kehtestatud mõõdikute lävendväärtused.

c. Olenevalt sündmuse kaalukusest on määratud teavitusteed ja lepitud kokku sündmustele reageerimise kord.

INF.13.M21 Hoonete tehnilise halduse süsteemi logimine

a. Kõik oluliseks liigitatud hoonete tehnilise halduse süsteemi sündmused (sh kõik turvasündmused) logitakse vastavalt moodulile OPS.1.1.5 *Logimine*.

b. Kõik eeliskontoga sisselogimised ja süsteemi komponentide konfiguratsioonimuudatused logitakse.

c. Hoonete tehnilise halduse süsteemi logiandmed talletatakse keskses logiserveris.

d. Logiandmed edastamisel kasutatakse turvalisi sidekanaleid.

e. Turvakriitilistest sündmustest teavitatakse vastutavaid haldureid automaatselt.

INF.13.M22 Hoonete tehnilise halduse süsteemi testimine [arhitekt]

a. Hoonete tehnilise halduse süsteeme ja haldusprotsesside toimimist testitakse vähemalt enne süsteemi kasutuselevõttu ja pärast oluliste süsteemimuudatuste jõustamist.

b. Hoonete tehnilise halduse süsteemi mittefunktsionaalsete nõuete testimise käigus testitakse muuhulgas ka vastavust infoturbe nõuetele. Testitakse vähemalt järgnevaid infoturbe nõudeid:

   - kasutajakontode nõutud paroolikeerukuse järgimist;
   - vaikeparooli vahetamist süsteemi kasutuselevõtul;
   - võrguprotokollide ja -tehnoloogiate turvalisust;
   - krüpteerimise rakendamist (kus krüpteerimine on võimalik ja vajalik).

c. Valitud testilood ja testimise tulemused dokumenteeritakse.

INF.13.M23 Hoonete tehnilise halduse süsteemi turvanõrkuste ja -uuendite teabe seire

a. Haldurid jälgivad regulaarselt teavet hoonete tehnilise halduse süsteemi teadaolevate nõrkuste ning riist- ja tarkvara turvauuendite väljalaske kohta.

b. Hoonete tehnilise halduse süsteemi komponendid on konfigureeritud eesmärgiga võimalikult vähendada teadaolevate nõrkuste ärakasutamist ning minimeerida võimalike intsidentide põhjustatud kahjusid.

c. Süsteemi turvanõrkuste avastamiseks viiakse läbi turvakontrolle- ja skaneerimisi. Hoonete tehnilise halduse süsteemide turvaskaneerimisel tootmiskeskkonnas on arvestatud võimalike kaasnevate tehniliste tõrgetega (nt teavitatakse testi läbiviimisest töötajaid ette).

INF.13.M24 Hoonete tehnilise halduse süsteemi andmete turvaline pilvtöötlus [arhitekt]

a. Hoonete tehnilise halduse süsteemide rakendamisel pilvteenusena järgitakse mooduligrupis „OPS.2 *Käidutööd teenusena*“ esitatud meetmeid.

b. Pilvekorralduse mudeli ja teenuseandja valimisel on arvestatud kehtivaid turvanõudeid ja regulatsioone.

c. Sõltumata tehnilise halduse süsteemi andmete asukohast omab organisatsioon hooneandmete üle täielikku kontrolli.

d. Teenusega seotud turvaaspektid on määratletud teenuseandjaga sõlmitud lepingus.

3.4 Kõrgmeetmed

INF.13.M25 Hoonete tehnilise halduse süsteemi testkeskkond [arhitekt] (C-I-A)

a. Hoonete tehnilise halduse süsteeme testitakse testkeskkonnas enne nende käidukeskkonnas (ingl *operational environment*) kasutuselevõttu.

b. Testkeskkonna puudumisel on välja töötatud protseduurid käidukeskkonda lisatud riist- ja tarkvara tõrgete ja vigade tõhusaks käsitlemiseks ja muudatusele eelneva olukorra kiireks taasteks.

INF.13.M26 Hooneteabe digitaalse modelleerimise tarkvara (BIM) valideerimine [arhitekt] (C-I-A)

a. Kui hooneteabe digitaalse modelleerimise tarkvara (Building Information Modeling, BIM) sisaldab turvalisuse seisukohast olulist teavet, on BIM arhitektuurile, BIM juurutamisele ja käitamisele kehtestatud täiendavad turvameetmed.

b. Täiendavad BIM turvameetmed võivad sisaldada järgnevat:
   - üksikasjalikumaid rollideks jagamise ja volitamise reegleid;
   - turvalisi autentimismeetodeid(nt mitmikautentimine);
   - andmete krüpteerimist;
   - võrgu segmentimist;
   - BIM sündmuste detailset logimist.

INF.13.M27 Privaatpilve kasutamine hoonete tehnilise halduse süsteemis [arhitekt] (C-I-A)

a. Hoonete tehnilise halduse süsteemid on koondatud usaldusväärse pilvteenuse tarnija privaatpilve (ingl *private cloud*). Privaatpilv võib olla ka organisatsioonisisene.

b. Hoonete tehnilise halduse süsteemi andmed ei asu avalikus pilves (ingl *public cloud*).

c. Enne välise pilvteenuse tarnija kasutamist on veendutud teenuse turvataseme vastavuses organisatsiooni turvanõuetele.

d. Vajadusel on võimalik teenuseandjat vahetada, vastav protseduur on kirjeldatud pilvteenuse tarnijaga sõlmitud lepingus.

INF.13.M28 Intellektitehnika turvaline kasutamine hoonete tehnilises halduses (C-I-A)

a. Intellektitehnikat (ingl *artificial intelligence*, AI) kasutavad komponendid, nende funktsionaalsus ja toimepõhimõtted on dokumenteeritud.

b. Hoonete tehnilises halduses kasutatakse ainult tõestatult turvalist intellektitehnikat, nt on läbi viidud AI funktsioonide testimine suurendatud koormuste ning vigaste sisendparameetritega.

c. Enne AI kasutuselevõttu on veendutud, et organisatsiooni andmeid ei töötle volitamata osapooled (nt kas andmeid ei saadeta analüüsiks välise teenuseandja serverisse).

d. Pilvepõhise intellektitehnika kasutamisel järgitakse kehtivaid regulatsioone.

INF.13.M29 Hoonete tehnilise halduse süsteemi integreerimine SIEM lahendusega [IT-talitus] (C-I-A)

a. Turvateabe ja -sündmuste halduse (ingl *security information and event management*, SIEM) lahenduse olemasolul on hoonete tehnilise halduse süsteemi sündmused kaasatud SIEM lahendusse.

b. TBM protsessi sündmusi analüüsitakse reaalajas koos teiste IT-süsteemide sündmuste ja logiandmetega.

INF.13.M30 Hoonete tehnilise halduse süsteemi läbistustestimine (C-I-A)

a. Hoonete tehnilise halduse süsteemi ja süsteemi toetava taristu turbe kontrollimiseks viiakse läbi läbistustestimisi.
b. Läbistustestimised tehakse testkeskkonnas enne TBM süsteemi kasutuselevõttu ning täiendavalt pärast oluliste süsteemimuudatuste teostamist.
c. Tootmiskeskkonnas tehakse TBM süsteemide läbistustestimist ainult äärmisel vajadusel, testikava kooskõlastatakse kõigi mõjutatud osapooltega.
d. Läbistustestimise raames testitakse ka hoonete tehnilise halduse süsteemi AI funktsioone (eesmärgiga panna andmeid manipuleerides AI vääraid otsuseid tegema).

INF.14 Hooneautomaatikasüsteemid

1 Kirjeldus

1.1 Eesmärk

Esitada meetmed hooneautomaatikasüsteemide (ingl *Building Automation and Control System*, BACS) turvaliseks kavandamiseks, evitamiseks, käitamiseks ja arendamiseks. BACS hõlmab hoone funktsioonide juhtimise, automatiseerimise, optimeerimise, kasutusmugavuse ja energiatõhususe suurendamisega seotud funktsioone. Tehnosüsteemid on tavaliselt kasutatavad ka eraldi, kuid võivad olla ka integreeritud kesksesse hooneautomaatikasüsteemi.

1.2 Vastutus

Hooneautomaatikasüsteemide turvameetmete rakendamise eest vastutab tehnikatalitus.

Lisavastutajad

Arhitekt, IT-talitus.

1.3 Piirangud

Moodulis esitatud meetmed kohalduvad kõigile hooneautomaatikasüsteemiga liidestatud tehnosüsteeme sisaldavatele hoonetele. Moodul sisaldab ka hooneautomaatikasüsteemi võrgu ja võrgukomponentidega seonduvaid infoturbeaspekte.

Hoone tehnoseadmete ja -süsteemide (kütte-, jahutus-, ventilatsiooni-, konditsioneerimis-, vee-, valgustus-, tulekaitse- ja nõrkvoolusüsteemid) üldise halduse (ingl Technical Building Management, TBM) turvaaspekte käsitletakse moodulis INF.13 *Hoonete tehniline haldus*.

Hoonete füüsilist turvalisust käsitletakse moodulis INF.1 *Hoone üldiselt*.

Kui hooneautomaatikasüsteemid kuuluvad välisele partnerile (nt büroohoone või -ruumide rentimisel), rakendatakse täiendavalt meetmeid moodulist OPS.2.3 *Väljastellimine*.

Käidutehnoloogia keskkonnas kasutatavatele hooneautomaatikasüsteemidele rakenduvad meetmed mooduligrupist IND (nt IND.2.3 *Andurid ja täiturid* ja IND.2.7 *Ohutusautomaatika*).

Võrguturbe üldised meetmed on esitatud moodulis NET.1.1 Võrgu arhitektuur ja lahendus, võrgukomponentide turve mooduligrupis NET.3 *Võrgukomponendid*.

Hooneautomaatikasüsteemi komponentide turvalise kaughoolduse meetmeid kirjeldatakse moodulites OPS.1.2.5 *Kaughooldus* ja IND.3.2 *Tööstusautomaatika komponentide kaughooldus*.

Kui BACS andmeid töödeldakse pilves, rakendatakse täiendavaid meetmeid moodulist OPS.2.2 *Pilvteenuste kasutamine*.

2 Ohud

2.1 Hooneautomaatikasüsteemi ebapiisav kavandamine

Hooneautomaatikasüsteemi (BACS) kavandamisel tehtud vead võivad kaasa tuua materiaalse ja rahalise kahju. Kahju võib tekkida, kui BACS ei toimi ootuspäraselt (nt jätab reageerimata edastatud alarmteatele).

Tehnosüsteemide kavandamisel kõikide kehtivate regulatsioonide ja nõuete mittearvestamisel ei vasta hooneautomaatikasüsteem tehnilistele nõuetele ning seeläbi põhjustada süsteemis tõrkeid. Ebasoodsal hetkel toimuv lukustussüsteemi rike võib jätta inimesed pikemaks ajaks suletud ruumi kinni ning seeläbi ohustada inimeste elu ja tervist.

2.2 Tehnosüsteemide liidestamisel hooneautomaatikasüsteemiga tehtud vead

Tehnosüsteemide poolt genereeritud alarmid või automaatsed teavitused võivad käivitada tegevusi teistes tehnosüsteemides. Kui kriitiliste tehnosüsteemide (nt ohutusautomaatika süsteemid, automaatsed tulekahjusignalisatsioonisüsteemid) liidestamisel teiste süsteemidega on tehtud vigu või liidestes esinevad tõrked, võib see ohustada hoones viibijate elu ja tervist.

Hooneautomaatika juhtsüsteem võib tehnosüsteemi poolt saadetud teateid valesti tõlgendada või jätta teadetele reageerimata. Näiteks kui andmekeskuse tulekahjusignalisatsiooni käivitumisel ei rakendu akustilised ja/või optilised häiresüsteemid, ei pruugi andmekeskuses viibivad inimesed ruumist välja saada enne kui ruum on täidetud kustutusgaasiga.

2.3 Ebaturvaliste süsteemikomponentide või sideprotokollide kasutamine

Hooneautomaatikasüsteemi poolt juhitavate tehnosüsteemide komponendid võivad olla amortiseerunud või ei saa tootja toe aegumise tõttu enam tarkvarauuendeid. Turvanõrkused muudavad süsteemi rünnetele avatuks. Kuna tehnosüsteemide pääsuõiguste andmine ei ole keskselt hallatav, on oht, et süsteemile võivad juurde pääseda volitamata isikud. Uuendamata süsteemikomponentide vahelises andmesides kasutatavad protokollid on tihti vananenud ja võivad omakorda sisaldada turvanõrkusi.

Risk on veelgi suurem, kui hooneautomaatikasüsteemi või üksiku tehnosüsteemi tootja pole juba algselt turvalisusele piisavat tähelepanu pööranud.

2.4 Hooneautomaatikasüsteemi väär seadistus

Vääralt või kõiki võimalikke olukordi läbi mõtlemata konfigureeritud hooneautomaatikasüsteem võib põhjustada häireid ja katkestusi äriprotsessides, tekitada otsest materiaalset kahju või ohustada hoones viibijate tervist.

Näiteks võib vääralt konfigureeritud kliimaseade tekitada teatud tingimuste kokkusattumisel ruumide ülekuumenemise. Kui hoone elektrisüsteemi ja tulekustutussüsteemi automaatikasüsteemid ei toimi omavahel kooskõlas, võib see tekitada olulisi elektriseadmete kahjustusi või ruumis viibijate kehavigastusi.

2.5 Hooneautomaatikasüsteemi komponentidevaheliste liideste manipuleerimine

Hooneautomaatikasüsteemi komponentide vahelise andmeside manipuleerimine või valeteadete genereerimine võib tekitada hooneautomaatikasüsteemis ekslikke protsesse. Näiteks manipuleeritud tulekahjusignalisatsiooni teade võib põhjustada kõikide uste automaatse avamise, mis võimaldab volitamata isikutel märkamatult hoonesse siseneda.

2.6 Hooneautomaatikasüsteemi juurdepääsu ebapiisav turve

Kui tehnosüsteemide pääsuõiguste andmine pole keskselt hallatav ega kontrollitav, kasvab hooneautomaatikasüsteemile volitamata isikute juurdepääsu oht.

Hooneautomaatika komponendid võivad andmeid vahetada nii lokaalse arvutivõrgu kui erinevate juhtmevabade andmesideühenduste (WLAN, Bluetooth, raadioside). Kui andmesidekanalid on turvamata, võib ründaja avatud juurdepääsuvõimalusi kasutada hooneautomaatikasüsteemi manipuleerimiseks, organisatsiooni sisevõrku tungimiseks, kahjurvara levitamiseks või teenusetõkestusrünnete korraldamiseks.

2.7 Ebapiisavalt turvatud juhtpaneelid

Kui hooneautomaatikasüsteemi juhtimiseks kasutatavad lülitid või juhtpaneelid ei asu füüsiliselt kaitstud asukohas, on tehnosüsteemi juhtimine võimalik füüsiliselt üle võtta. Näiteks on võimalik väravavahi ruumi sisse tungides avada uksed või autode sissesõiduvärava.

Volitamata juurdepääsu hooneautomaatikasüsteemile võib ründaja saada ka juhtpaneeli füüsiliste liideste (nt LAN või USB-liideste) ärakasutamisel.

2.8 Ebapiisavalt turvatud kaugjuurdepääsud

Sageli on hooneautomaatikasüsteemil olemas kaugjuurdepääs, mida tootja või tootetuge osutava partnerorganisatsiooni töötajad kasutavad kiireks abistamiseks või süsteemi kaugseireks. Kui selline püsivalt avatud kaugjuurdepääs pole piisavalt turvatud, võib ründaja seda kasutada hooneautomaatikasüsteemile ja sealtkaudu ka organisatsiooni IT-süsteemidele juurde pääsemiseks.

3 Meetmed

3.1 Elutsükkel

Kavandamine

INF.14.M1 Hooneautomaatikasüsteemi kavandamine

INF.14.M7 Hooneautomaatikasüsteemi turvaeeskiri

INF.14.M8 Hooneautomaatikasüsteemi nõuete spetsifikatsioon

INF.14.M9 Hooneautomaatikasüsteemi kontseptsioon

Evitus

INF.14.M2 Hooneautomaatikasüsteemi turvaline kasutuselevõtt

INF.14.M3 Tehnosüsteemide turvaline liidestamine hooneautomaatikasüsteemiga

INF.14.M4 Erisused ohutuvastussüsteemide liidestamisel hooneautomaatikasüsteemiga

INF.14.M10 Hooneautomaatikasüsteemi sisemiste sõltuvuste vähendamine

INF.14.M13 Hooneautomaatikasüsteemi võrgu segmentimine

INF.14.M19 Hooneautomaatikasüsteemile aadressivahemike eraldamine

Käitus

INF.14.M5 Hooneautomaatikasüsteemi dokumentatsioon

INF.14.M6 Hooneautomaatikasüsteemi võrgu eraldamine

INF.14.M11 Avatud juurdepääsude ja portide kaitsmine

INF.14.M12 Turvaliste võrguprotokollide kasutamine

INF.14.M14 Hooneautomaatikasüsteemi juurdepääsu reguleerimine

INF.14.M15 Hooneautomaatikasüsteemi spetsiifiliste võrkude turve

INF.14.M16 Traadita andmeside kaitse hooneautomaatikasüsteemi võrgus

INF.14.M17 Mobiilside kaitse hooneautomaatikasüsteemi võrgus

INF.14.M18 Turvaline andmevahetus väliste hooneautomaatikasüsteemidega

INF.14.M20 Leviedastuse minimeerimine hooneautomaatikasüsteemi võrgus

INF.14.M21 Teabe autentsuse kontroll hooneautomaatikasüsteemides

INF.14.M23 Kestlike süsteemikomponentide kasutamine

INF.14.M24 Hooneautomaatikasüsteemi komponentide kellade sünkroniseerimine

INF.14.M25 Hooneautomaatikasüsteemi seire

INF.14.M26 Hooneautomaatikasüsteemi logimine

Avariivalmendus

INF.14.M22 Hooneautomaatikasüsteemi ja tehnosüsteemide autonoomse toimimise tagamine

INF.14.M27 Hooneautomaatikasüsteemide avariihaldus

Lisanduvad kõrgmeetmed

INF.14.M28 Hooneautomaatika võrkude füüsiline eraldamine

INF.14.M29 Ärikriitiliste tehnosüsteemide eraldamine

INF.14.M30 Hooneautomaatikasüsteemi sõltumatu ajaserver

3.2 Põhimeetmed

INF.14.M1 Hooneautomaatikasüsteemi kavandamine [arhitekt]

a. Hooneautomaatikasüsteemi (ingl *Building Automation and Control System*, BACS) kavandamine toimub hoonega seotud ehitustööde (uusehituste, hoone laienduste või renoveerimise) kavandamisest varem või sellega samal ajal.

b. BACS kavandamise käigus määratletakse kõik tehnosüsteemid, mis hooneautomaatikasüsteemiga liidestatakse või automatiseeritakse. Lisaks tehnosüsteemidele võivad hooneautomaatikasüsteemi koosseisu kuuluda täiendavaid andureid ja andmeallikaid (nt andmeliides ilmaprognoosi saamiseks).

c. Hooneautomaatikasüsteemi kavandamisel arvestatakse vähemalt järgmiste aspektidega:

- hoone kasutusotstarve ja sellest tulenevad nõuded;

- hoone segmentimine eraldi kontrollitavateks aladeks;
- korralduslikud nõuded ja regulatsioonid;
- hoone ehituslikud ja tehnilised tingimused;
- BACS koosseisu kuuluvad tehnosüsteemid;
- tehnosüsteeme mõjutavad keskkonnatingimused;
- kasutatav BACS tehnoloogia ja arhitektuur;
- BACS komponendid;
- vajalikud sidevõrgud;
- hooneautomaatikasüsteemi võrguarhitektuur;
- liidestused teiste süsteemidega;
- kasutatavad andmesideliidesed ja protokollid;
- elektritoite ja puhvertoiteallikate (UPS) vajadus;
- pilvteenuste kasutus;
- andmete talletamise ja varunduse nõuded;
- nõutavad turvameetmed;
- vajalikud rollid pääsuõiguste halduseks.

d. BACS on kavandatud sellisena, et erinevate kasutusele võetavate tehnoloogiate, andmesideliideste ja protokollide hulk oleks võimalikult väike ning süsteemide koostöövõime võimalikult suur.

e. Hooneautomaatikasüsteemis kasutatakse ainult turvalisi ja standardseid protokolle ja andmesideliideseid.

INF.14.M2 Hooneautomaatikasüsteemi turvaline kasutuselevõtt

a. Hooneautomaatikasüsteemi kasutuselevõtu eelselt on koostatud üksikasjalik kava kõigi hõlmatud tehnosüsteemide koordineeritud liidestamiseks hooneautomaatikasüsteemiga.

b. On kokku lepitud, kuidas ja milliste andmevahetusliideste kaudu hakkab toimuma suhtlus hooneautomaatikasüsteemi haldurite ja tehnosüsteemidele ning seotud taristule tehnilist tuge osutavate partnerorganisatsioonide vahel.

c. Hooneautomaatikasüsteemi andmevahetusliidesed on dokumenteeritud.

d. BACS süsteemisiseste muudatuste kavandamisel uuendatakse BACS dokumentatsiooni ja teavitatakse eelseisvast muudatusest kõiki mõjutatud organisatsioonisiseseid ja -väliseid osapooli.

INF.14.M3 Tehnosüsteemide turvaline liidestamine hooneautomaatikasüsteemiga

a. Kõigi hooneautomaatikasüsteemide, tehnosüsteemide ja nendega seotud komponentide puhul on määratletud, mis toiminguid on igal üksikul süsteemikomponendil lubatud käivitada ning kuidas see teisi komponente mõjutab.

b. Tehnosüsteemide kriitilistele protsessidele on määratud parameetrivahemikud (nt kütteseadme minimaalne ja maksimaalne temperatuur), mida BACS ei tohi ületada.

c. Kui tehnosüsteemi andmed on hooneautomaatikasüsteemi toimimiseks vajalikud, kuid tehnosüsteemi ei saa BACS-iga integreerida, on andmete hooneautomaatikasüsteemi saamiseks leitud alternatiivne lahendus.

d. Ühes hoones mitme hooneautomaatikasüsteemi kasutamisel on määratletud, kas ja kuidas süsteemid omavahel andmeid vahetavad.

e. Tehnosüsteemide liidestamisel hooneautomaatikasüsteemiga on arvestatud erinevate tehnoloogiate kasutusest tulenevaid erisusi. Avariiolukorras on tehnosüsteem võimeline toimima autonoomselt.

f. Protsesside toimimist ja süsteemikomponentide andmevahetust on hoolikalt testitud. Testimise käigus ilmnenud vead on parandatud enne BACS tootmiskeskkonnas kasutuselevõttu.

g. Tehnosüsteemide ja hooneautomaatikasüsteemi liidestus on täielikult dokumenteeritud (vt INF.14.M5 *Hooneautomaatikasüsteemi dokumentatsioon*).

INF.14.M4 Erisused ohutuvastussüsteemide liidestamisel hooneautomaatikasüsteemiga [arhitekt]

a. Ohutuvastussüsteemid (nt valve- ja tulekahjusignalisatsioonisüsteemid) on liidestatud hooneautomaatikasüsteemiga selliselt, et BACSi toimimine või mittetoimimine ei mõjuta ohutuvastussüsteemide funktsioneerimist. BACS võib kasutada ohutuvastussüsteemist saadud andmeid, kuid mitte vastupidi.

b. Võrguühendust või traadita andmesideühendust kasutavad ohutuvastussüsteemid on paigutatud füüsiliselt eraldatud võrgusegmenti. Võrgusegmendis on lubatud ainult ohutuvastussüsteemide tööks ja häirete edastamiseks vajalik andmeside.

c. Ohutuvastussüsteemid toimivad ka juhul, kui kõrgema taseme võrguühendus (nt internetiühendus) on katkenud.

INF.14.M5 Hooneautomaatikasüsteemi dokumentatsioon

a. Kõigi kasutatavate hooneautomaatikasüsteemi komponentide (sh tehnosüsteemid ja taristukomponendid) kasutamine, juurdepääs, omavahelised sõltuvused ja andmeliidesed on dokumenteeritud.

b. On olemas dokumentatsioon BACS füüsiliste liideste, andmesideliideste, protokollide ja juurdepääsuvõimaluste kohta, mis on desaktiveeritud.

c. Hooneautomaatikasüsteemi dokumentatsioon on kõikide asjaosalistega kooskõlastatud ning volitatud töötajatele kättesaadav.

d. Dokumentatsiooni asja- ja ajakohasust ning tegeliku olukorra vastavust dokumentatsioonile kontrollitakse regulaarselt. Lahknevuste ilmnemisel selgitatakse välja lahknevuse põhjus ja tehakse vajalikud parandused.

INF.14.M6 Hooneautomaatikasüsteemi võrgu eraldamine [arhitekt, IT-talitus]

a. Hooneautomaatikasüsteemi võrk on kontorivõrgust ja muudest organisatsiooni võrkudest vähemalt loogiliselt eraldatud.

b. Kogu andmeside ja üleminekud BACS ja teiste IT-süsteemide vahel on kontrollitud ja kaitstud tulemüüriga. Kaugjuurdepääsuks ja väliseks andmevahetuseks on soovitatav luua hooneautomaatikasüsteemi DMZ (ingl *demilitarized zone*).

c. Kui BACS hõlmab erinevaid hooneid või hoonestuid, kasutatakse andmesideks turvatud laivõrgu (ingl *wide area network*, WAN) ühendusi, nt kasutades VLAN-i (ingl *virtual local area network*, VLAN). BACS andmeside avalikus võrgus on kaitstud VPN-iga (ingl *virtual private network*, VPN).

d. Organisatsioonivälised isikute BACS komponentidele juurdepääs on reguleeritud vastavalt moodulile OPS.1.2.5 *Kaughooldus*.

3.3 Standardmeetmed

INF.14.M7 Hooneautomaatikasüsteemi turvaeeskiri

a. Lähtudes üldise turvapoliitikast ja hoonete tehnilise halduse turvanõuetest (INF.13.M4 *Hoonete tehnilise halduse turvaeeskiri*) on koostatud hooneautomaatikasüsteemi turvaeeskiri.

b. Hooneautomaatikasüsteemi turvaeeskiri sisaldab vähemalt järgmisti turvanõudeid:
   - tehnosüsteemide turvaline liidestus hooneautomaatikasüsteemiga;
   - BACS komponentide nõutav turvaspetsifikatsioon;
   - turvanõuetele mittevastavate komponentide käsitlemine;
   - BACS juurdepääsu turve;
   - BACS rollid ja turvaline kasutajate autentimine
   - BACS andmeside turve, sh nõuded protokollidele;
   - BACS logimine ja seire;
   - BACS arenduse ja testimise nõuded.

c. Kõik hooneautomaatika valdkonna töötajad on hooneautomaatikasüsteemi turvaeeskirjaga tutvunud ning järgivad seda oma töös.

d. Hooneautomaatikasüsteemi turvaeeskirja täitmist kontrollitakse regulaarselt, eeskirja ajakohastatakse vastavalt vajadusele.

INF.14.M8 Hooneautomaatikasüsteemi nõuete spetsifikatsioon

a. Hooneautomaatikasüsteemi turvaeeskirja (vt INF.14 M7 *Hooneautomaatikasüsteemide turvaeeskiri*) alusel on koostatud iga hooneautomaatikasüsteemi jaoks nõuete spetsifikatsioon. Nõuete spetsifikatsiooni koostamisel on arvestatud ka hoone arhitektuurist ja organisatsiooni äriprotsessidest tulenevaid erinõudeid.

b. Hooneautomaatikasüsteemi nõuete spetsifikatsiooni kasutatakse BACS kavandamisel ja hankimisel, aga samuti ka uute hoonete kavandamisel ja projekteerimisel.

c. Hooneautomaatikasüsteemi nõuete spetsifikatsioon on dokumenteeritud. Nõuete spetsifikatsiooni ajakohastatakse seoses BACS riistvara ja tarkvara arendamise ning tehnoloogia üldise arenguga.

d. Kasutatava hooneautomaatikasüsteemi arhitektuur, ülesehitus ja komponendid on vastavuses nõuete spetsifikatsiooniga. Vastavust kontrollitakse regulaarselt.

INF.14.M9 Hooneautomaatikasüsteemi kontseptsioon

a. Organisatsioonis on välja töötatud hooneautomaatikasüsteemide turvaeeskirjal ning nõuete spetsifikatsioonil põhinev üldine hooneautomaatikasüsteemi kontseptsioon.

b. Hooneautomaatikasüsteemi kontseptsioon sisaldab dokumenteeritult kõiki meetmes „INF.14.M1 *Hooneautomaatikasüsteemi kavandamine“* kirjeldatud aspekte. Lisaks tehnilistele nõuetele arvestatakse hooneautomaatikasüsteemi kontseptsioonis ka organisatsioonilisi nõudeid.

c. Kontseptsioonis on kirjeldatud kõik hooneautomaatikasüsteemiga integreeritud ja liidestatud tehnosüsteemid ja nende liidestamiseks vajalikud sideühendused.

INF.14.M10 Hooneautomaatikasüsteemi sisemiste sõltuvuste vähendamine [arhitekt]

a. Hooneautomaatikasüsteem on kavandatud sellisena, et BACSi ühe valdkonna funktsionaalsus toimiks teistest hooneautomaatika valdkondadest võimalikult sõltumatult.

b. Ühe BACS funktsiooni tõrke poolt põhjustatud mõju teistele hooneautomaatika valdkondadele on minimeeritud.

c. Ühte hoonestusse kuuluvate hoonete hooneautomaatikasüsteemid on eraldi juhitavad.

INF.14.M11 Avatud juurdepääsude ja portide kaitsmine [arhitekt]

a. Hooneautomaatikasüsteemi komponentidele juurdepääs läbi USB- ja võrguportide ning muude avatud liideste on kaitstud tehniliste turvameetmetega.

b. Volitamata ja tundmatute komponentide ühendamine hooneautomaatikasüsteemi võrku on piiratud (vt INF.14.M13 *Hooneautomaatikasüsteemi võrgu segmentimine*).

c. Kõik ühenduskatsed ja õnnestunud ühendused kajastuvad hooneautomaatikasüsteemi sündmuste logis.

d. Võrkupääs on reguleeritud standardil IEEE 802.1X põhinevate või samaväärsete turvamehhanismidega. Volitamata võrgukomponente ei saa hooneautomaatikasüsteemi võrgusegmentidesse lisada.

e. BACS süsteemikomponendi lokaalsete liideste ja konsooliportide volitamata juurdepääsu piiramiseks kasutatakse pordilukke või lukustatud seadmekappe.

f. Hooneautomaatikasüsteemi komponendi hoolduseks vajalikud juurdepääsud avatakse ainult ajutiselt, hoolduse läbiviimise ajaks.

INF.14.M12 Turvaliste võrguprotokollide kasutamine

a. Hooneautomaatikasüsteemi komponentide juhtimiseks ja hoolduseks väljastpoolt turvatud võrgusegmente kasutatakse ainult turvalisi protokolle (nt ajakohase TLS versiooniga krüpteeritud HTTPS või FTPS protokolle).

b. Ethernetil põhinev andmeside väljastpoolt turvatud võrgusegmente on krüpteeritud usaldusväärsete krüptomehhanismidega (vt NET.3.3 *Virtuaalne privaatvõrk (VPN)*)

c. Ebaturvalisi protokolle kasutavad andmesideliidesed on desaktiveeritud.

INF.14.M13 Hooneautomaatikasüsteemi võrgu segmentimine [arhitekt]

a. Hooneautomaatikasüsteemi võrk on vastavalt kaitsetarbele jaotatud üksikuid hooneautomaatikasüsteeme või tehnosüsteemide komponente sisaldavateks eraldatud võrgusegmentideks.

b. Segmentidevaheliseks andmesideks on koostatud reeglid. Üleminekud on kaitstud vähemalt dünaamiliste paketifiltritega (ingl *stateful packet filtering*).

c. Võrgu segmentimine on põhjalikult dokumenteeritud.

INF.14.M14 Hooneautomaatikasüsteemi juurdepääsu reguleerimine

a. Hooneautomaatikasüsteemi pääsuhaldus on rakendatud vastavalt moodulile ORP.4 *Identiteedi ja õiguste haldus*.

b. Hooneautomaatikasüsteemi keskne autentimislahendus haldab juurdepääse kõigile olulistele BACS komponentidele.

c. Hooneautomaatika rollide ja volituste süsteem võimaldab luua erinevate juurdepääsuõigustega kasutajaid, lähtuvalt organisatsiooni töötajate ning väliste tehnilise toe osutajate vajadustest.

d. Kõik kasutatavad hooneautomaatikasüsteemi komponendid võimaldavad komponentide volitamata kasutamist piirata.

e. On keelatud kasutada BACS komponente, millel juurdepääsupiirangud puuduvad või mille tootja vaikeparooli pole võimalik muuta.

INF.14.M15 Hooneautomaatikasüsteemi spetsiifiliste võrkude turve

a. Hooneautomaatikasüsteemi spetsiifiliste võrkude (nt BACnet, KNX, M-Bus) puhul on rakendatud turvameetmed, mis tagavad võrgusegmendi turvatasemega samaväärse turvataseme (nt BACnet puhul tagab hetkel piisava turbe BACnetSC ja TLS 1.3).

b. Hooneautomaatikasüsteemi spetsiifiliste võrkude lüüsid (ingl *gateway*) on konfigureeritud läbi laskma ainult vajalikku andesidet ning kasutavad kinnistatud pääsuloendit (ingl *Access Control List*, ACL).

c. Kui hooneautomaatikasüsteem sisaldab integreeritud turvamehhanisme (nt autentimiseks või andmete krüpteerimiseks), on need turvamehhanismid kasutusele võetud.

d. Piisamatute turvamehhanismidega hooneautomaatikasüsteemid vahetatakse välja niipea kui see on tehniliselt võimalik. Seniks on nad paigutatud tulemüüriga eraldatud võrgusegmenti.

INF.14.M16 Traadita andmeside kaitse hooneautomaatikasüsteemi võrgus [arhitekt]

a. Traadita andmesidet kasutatavate BACS võrkude (nt BLE, BACnet Zigbee, EnOcean) andmeside kaitseks on rakendatud asjakohaseid autentimis- ja krüptomehhanisme.

b. Üleminekud kaablipõhisele võrgule on realiseeritud tulemüüri funktsionaalsust omavate BACS komponentidega.

c. Traadita andmesidevõrgud ja nende poolt kasutatavad sagedusvahemikud on registreeritud. Võrguseadmed seadistatud nii, et need võimalikult vähe häiriks teiste traadita andmesidevõrkude toimimist (seda eriti 2,4 GHz sagedusalas).

d. BACS võrgu kavandamisel on arvestatud füüsilistest takistustest (nt metallkattega klaasid, raudbetoonsein) põhjustatud raadiolainete levihäiretega.

INF.14.M17 Mobiilside kaitse hooneautomaatikasüsteemi võrgus [arhitekt]

a. Kui BACS kasutab andmesidekanalina avalikku mobiilsidevõrku (nt LTE või 5G mobiilsidetehnoloogiat), on suhtlus piiratud ainult volitatud osapoolte ja määratud IP-aadressidega.

b. Kui avalikus mobiilsidevõrgus ei ole võimalik BACS võrke teisiti eraldada, kasutatakse võrkude eristamiseks rakenduslüüse (ingl *application level gateway*, ALG).

c. BACS komponendid kasutavad avalikku mobiilsidevõrku ainult juhul, kui see on nende toimimiseks hädavajalik, tavaseadistuses on BACS komponentide mobiilside piiratud. Püsiva andmesideühenduse asemel kasutatakse BACS komponentide poolt algatatud ajutisi andmesideseansse.

d. Võimaluse korral kasutatakse BACS andmeside tarbeks mobiilsideoperaatori poolt eraldatud mobiilside taristut või virtuaalset võrgupiirkonda, mis on mõeldud kasutamiseks ainult automaatikaseadmetele.

e. Autonoomse mobiilsidetehnoloogiaid kasutava privaatmobiilsidevõrgu (nt ülikoolilinnaku 5G võrk) kasutamisel BACS andmesidevõrguna on BACS võrk teistest võrkudest eraldatud, kõik üleminekud mobiilsidevõrgu ja teiste tehnoloogiat kasutava võrgu vahel on kaitstud tulemüüriga.

INF.14.M18 Turvaline andmevahetus väliste hooneautomaatikasüsteemidega

a. Hooneautomaatikasüsteemi andmeside välise BACS-süsteemiga on võimalik ainult määratud andmevahetusliideste kaudu. Kõik kasutatavad liidesed ja andmesidekanalid on dokumenteeritud ja kasutamiseks kinnitatud.

b. Andmevahetuse osapooled autenditakse, andmeside on krüpteeritud.

c. Liidestused väliste BACS-süsteemidega on piiratud minimaalselt vajalikuni.

INF.14.M19 Hooneautomaatikasüsteemile aadressivahemike eraldamine [arhitekt]

a. Hooneautomaatikasüsteemi komponentidele eraldatud IP-aadresside vahemikust piisab kõikidele organisatsiooni BACS komponentidele.

b. Eraldatud aadressivahemik on kontorivõrgu ja teiste IT-võrkude seadmetele antud IP-aadressidest selgelt eristatav. Aadressiruumi on võimalik vastavalt vajadusele jagada alamvõrkudeks.

c. Staatilisi IP-aadresse kasutavad hooneautomaatikasüsteemi komponentide IP-aadressid on dokumenteeritud.

d. Hooneautomaatika süsteemikonfiguratsioonide dubleerimisel on süsteemid võimalike aadressikonfliktide vältimiseks paigutatud eraldi võrgusegmentidesse. Süsteemidevahelises andmevahetuses kasutatakse rakenduslüüse (ingl *application level gateway*, ALG) või võrguaadresside teisendust (*Network Address Translation,* NAT).

INF.14.M20 Leviedastuse minimeerimine hooneautomaatikasüsteemi võrgus [arhitekt]

a. BACS võrkudes on võrgukoormuse vältimiseks võetud kasutusele meetmed IPv4 võrgu OSI Layer 2 ja OSI Layer 3 tasemel leviedastuse (ingl *broadcast*) minimeerimiseks.

b. Kui leviedastus on tehniliselt vajalik, tuleks see suunata ainult vajalikesse alamvõrkudesse. Leviedastuse adressaatide vähendamiseks kasutatakse võrgu segmentimist. Leviedastuse saatjad ja vastuvõtjad on eraldatud nendest BACS komponentidest, mida leviedastus võib potentsiaalselt häirida.

c. Hooneautomaatikasüsteemi IPv6 võrgus kasutatakse andmepakettide multisaate (ingl *multicast*) või monosaate (ingl *unicast*) marsruutimist

INF.14.M21 Teabe autentsuse kontroll hooneautomaatikasüsteemides

a. BACS-süsteemis toimub pidev sisendandmete valideerimine (kas kuvatav aeg, koht, väärtus, olek või sündmus vastab selle, mida on eeldati).

b. Simuleeritud või "külmutatud" väärtustega andmed tuvastatakse ning saadetakse vastav hoiatusteade, edasine protsess sõltub BACS-süsteemi kriitilisusest ja kaitsetarbest.

INF.14.M22 Hooneautomaatikasüsteemi ja tehnosüsteemide autonoomse toimimise tagamine [arhitekt]

a. Hooneautomaatikasüsteemid olema konfigureeritud nii, et nende toimimine ei sõltuks ühestki teisest tehnosüsteemist ega hooneautomaatikasüsteemist (nt küttesüsteem peab jätkama oma tööd ka siis, kui temperatuurianduritelt ei tule enam uut teavet).

b. Kui BACS komponentide vahelised sõltuvused siiski eksisteerivad, on kasutusele võetud meetmed sõltuvusest tulemevate mõjude vähendamiseks.

c. BACSiga integreeritud tehnosüsteemid jätkavad BACSi häirete puhul tööd ja täidavad oma funktsioone määratud parameetrite piires edasi isegi pärast pikaajalist andmeühenduse puudumist BACS süsteemiga.

d. Kui hooneautomaatikasüsteemiga seotud komponendid (nt teatud IoT-komponendid) vajavad toimimiseks katkematut internetiühendust, tuleks kaaluda süsteemi muutmist või väljavahetamist.

INF.14.M23 Kestlike süsteemikomponentide kasutamine

a. Hooneautomaatikasüsteemi komponendid on kavandatud vastupidavusvaruga, st süsteem on suuteline toimima pikka aega ka tavapärastest raskemates keskkonnatingimustes.

b. Hooneautomaatikasüsteemi komponentide konstruktsioon on füüsiliselt vastupidav. Kui see on kaheldav, on BACS komponendi kaitseks rakendatud täiendavaid meetmeid (nt on komponent paigutatud täiendavasse kaitsekasti).

c. BACS komponendid omavad tootjate poolt antud kinnitusi või sõltumatute testi organisatsioonide poolt väljaantud sertifikaate, et komponent vastab füüsilise vastupidavuse nõuetele.

INF.14.M24 Hooneautomaatikasüsteemi komponentide kellade sünkroniseerimine

a. Automaatse mõõtmise, juhtimise ja reguleerimise tagamiseks on hooneautomaatikasüsteemi ühendatud komponentide ja tehnosüsteemide kellad sünkroniseeritud (vt OPS.1.2.6 *Kellade sünkroniseerimine NTP-serveriga*).

b. Omavahel liidestatud hooneautomaatikasüsteemid kasutavad kellade sünkroniseerimiseks samasid ajaservereid. Kui hooneautomaatikasüsteem laieneb hoonestule või mitmetele kinnistutele, on kellade sünkroniseerimine tagatud kõigis hõlmatud hoonetes.

c. Kõik hooneautomaatikasüsteemi komponendid tõlgendavad kellaaega ühtses tüüpvormingus (võttes arvesse ajavööndeid ning talve- ja suveaegade vaheldumist).

d. Hooneautomaatikasüsteemi on paigutatud lokaalne ajaserver, mis jätkab BACS komponentidele kellaaja pakkumist pärast keskse või kõrgema taseme NTP-serveriga side katkemist.

e. Hooneautomaatikasüsteemis ei kasutata SNTP-d (Simple Network Time Protocol), kuna see lihtsustatud protokoll vähendab kellaaja sünkroniseerimise täpsust.

f. Kui hooneautomaatikasüsteem vahetab andmeid reaalajas kõrget ajalist täpsust nõudvate tehnosüsteemidega, tuleks kaaluda NTP asemel täppisaja protokolli PTP (Precision Time Protocol, PTP) kasutamist.

INF.14.M25 Hooneautomaatikasüsteemi seire

a. Kõik olulised BACS komponendid on lisatud seiresüsteemi. Hooneautomaatikasüsteemide käideldavust ja olekuparameetrite püsimist määratud piirväärtuste raames jälgitakse pidevalt.

b. Veateadete ja määratud piirväärtustest hälbimisest teavitab seiresüsteem hooneautomaatikasüsteemi haldureid.

c. Eelnevalt määratletud sündmuste korral saadetakse vastutajatele viivitamata (nt SMS sõnumiga) automaatne häireteade. Sellised sündmused on näiteks:
   - hooneautomaatikasüsteemi olulise funktsionaalsuse kadu;
   - BACS komponendi rike;
   - toiteallika kriitiline olek (nt pinge kõikumine);
   - võrguühenduse katkestus.

d. Seireandmeid ja BACS olekuteavet edastatakse ainult läbi turvaliste andmesidekanalite.

INF.14.M26 Hooneautomaatikasüsteemi logimine

a. Hooneautomaatikasüsteemi logimisel rakendatakse meetmeid moodulist OPS.1.1.5 *Logimine*.

b. Täiendavalt logitakse oluliste BACS komponentide olekumuudatused ja turvasündmused.

c. Logitakse kõik käsitsi või automaatselt tehtud hooneautomaatikasüsteemi või selle komponentide konfiguratsioonimuudatused.

d. On määratud, kas ja kuidas hooneautomaatikasüsteemi logiandmed edastatakse kesksesse logiserverisse ja/või SIEM (Security Information and Event Management) süsteemi.

e. Logiandmeid edastatakse ainult läbi turvaliste andmesidekanalite.

INF.14.M27 Hooneautomaatikasüsteemide avariihaldus

a. Organisatsioon on analüüsinud, kuidas hooneautomaatikasüsteemi avarii mõjutab äriprotsesse ja organisatsiooniülese avariivalmenduse kavandamist.

b. Hooneautomaatikasüsteemi üksiku komponendi rikke või ründe tagajärjel tekkinud mõjud teistele tehnosüsteemidele ja BACS komponentidele on võimalikult minimeeritud.

c. Hooneautomaatikasüsteemi avarii korral käitumiseks on koostatud hooneautomaatikasüsteemi avariihalduse tegevuskava (vt DER.4 *Avariihaldus*).

d. Avariihalduse tegevuskava sisaldab hooneautomaatikasüsteemi ja mõjutatud tehnosüsteemide toimimise eest vastutavaid töötajaid ning kontaktandmeid nendega ühendust võtmiseks.

e. Avariihalduse tegevuskavas on kirjeldatud, kuidas tagatakse hooneautomaatikasüsteemi avarii korral oluliste tehnosüsteemide avariitöö.

f. Hooneautomaatikasüsteemi oluliste komponentide töö taastamiseks pärast avariid on koostatud taasteplaanid.

g. Avariist taastumiseks on üle kõikide BACS ja tehnosüsteemide määratud vajalik taaskäivitusjärjestus. Taaskäivitusjärjestus on dokumenteeritud ka süsteemikomponentide taaste- ja taaskäivitusplaanides.

3.4 Kõrgmeetmed

INF.14.M28 Hooneautomaatika võrkude füüsiline eraldamine [arhitekt] (C-I)

a. Suurema kaitsetarbe puhul on hooneautomaatikasüsteemi võrgud realiseeritud füüsiliselt eraldiseisvate tsoonidena (vt NET.1.1 *Võrgu arhitektuur ja lahendus*).

b. Andmevahetus kaitstud hooneautomaatikavõrgu ja madalama kaitsetarbega võrkude vahel on piiratud minimaalselt vajalikuni. Internetipääs kaitstud hooneautomaatikavõrgust on blokeeritud.

c. Hooneautomaatikasüsteemi tootja või välise hoolduspartneri juurdepääs kaitstud hooneautomaatika võrku on rangelt reguleeritud.

d. Isoleeritud hooneautomaatikavõrgu võrguhäirete või -intsidentide seire ja halduse korraldamiseks on kaalutud spetsialiseeritud turbekeskuse (ingl *Security Operation Center*, SOC) loomist.

INF.14.M29 Ärikriitiliste tehnosüsteemide eraldamine (C-I)

a. Ärikriitiline (kõrgendatud turbevajadusega) tehnosüsteem on paigutatud eraldatud võrgusegmenti.

b. Ärikriitilise tehnosüsteemi andmesidet reguleeritakse võrgusegmendi ette paigutatud *Layer 2* tulemüüriga.

INF.14.M30 Hooneautomaatikasüsteemi sõltumatu ajaserver (I-A)

a. Hooneautomaatikasüsteemi võrgus on rakendatud sõltumatu, otse aatom- või raadiokellaga (Stratum kiht 0) ühendatud ajaserver.

b. Hooneautomaatikasüsteemi täiendavad ajaserverid sünkroniseerivad oma kellad hooneautomaatikasüsteemi keskse ajaserveriga.

4 Lisateave

Lühend	**Publikatsioon**
[ISO]	EVS-EN ISO 16484-1:2020 - Building automation and controls sytems (BACS)