

SISUKORD

Eesti infoturbestandardi 2021. a versioonis on:

- 1) organisatsiooni infoturbe halduse süsteemi nõuded;
- 2) rakendusjuhend;
- 3) etalonturbe kataloog;
- 4) auditeerimise juhend.

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

ISMS. Nõuded

Sisukord

- [1 Sissejuhatus](#)
- [1.1 Käsitlusala](#)
- [1.2 Sihtgrupp](#)
- [1.3 Normiviited](#)
- [1.4 Aukoht standardi dokumentatsioonis](#)
- [2 Terminoloogia](#)
- [3 Jaotiste lühiülevaade](#)
- [4 E-ITS olemus](#)
- [4.1 Infoturbe halduse süsteem](#)
- [5 Turbeprotsessi tsükli algatamine](#)
- [5.1 Juhtkonna kohustumus](#)
- [6 Turbeprotsessi kavandamine ja plaanimine](#)
- [6.1 Infoturvapoliitika](#)
- [6.2 Infoturvaeesmärgid](#)
- [6.3 Turbeprotsessi korraldus](#)
- [6.4 Infoturbealane koolitus](#)
- [6.5 Ressursside eraldamine](#)
- [6.6 Juhtkonna kinnitus](#)
- [6.7 Turbeprotsessi dokumenteerimine](#)
- [7 Riskihaldus](#)
- [7.1 Etalonturbe modelleerimine](#)
- [7.2 Etalonturbe väline riskihaldus](#)
- [8 Meetmete rakendamine](#)
- [9 Käigushoid](#)
- [10 Infoturbeprotsessi täiustamine](#)
- [10.1 Sõltumatu läbivaatus](#)
- [11 Jätkutegevused](#)
- [11.1 E-ITS auditeerimine](#)
- [11.2 ISO/IEC 27001 vastavuse sertifitseerimine](#)
- [12 Lisateave](#)

1 Sissejuhatus

Eesti infoturbestandard (edaspidi standard või E-ITS) on eestikeelne ja Eesti õigusruumile vastav alus infoturbe käsitlemiseks. E-ITS aluseks on Saksa päritolu [BSI IT-Grundschutz](#) etaloniturse meetod. E-ITS koostamisel on arvestatud vajadusega saavutada vastavus standardi [ISO/IEC 27001](#) nõuetega.

1.1 Käsitlusala

Dokument „E-ITS Infoturbe halduse süsteem. Nõuded” esitab nõuded ning juhised organisatsiooni infoturbe halduse süsteemi (ingl *Information Security Management System*, ISMS) käivitamiseks, rakendamiseks, käigushoiuks ja täiustamiseks.

E-ITS vastavuse saavutamiseks tuleb täita jaotistes 5–10 esitatud nõuded.

E-ITS ei tegele riigisaladuse ega salastatud välisteabe turbe korraldamisega.

1.2 Sihtgrupp

ISMS nõuete dokumendi peamised sihtgrupid on:

- standardi evitajad: infoturbejuhid, äriprotsessijuhid, üksuste juhid, IT-töötajad;
- audiitorid;
- konsultandid.

Standardi osi saab kasutada käsiraamatuna IT-süsteemide arenduses, halduses või õppeprotsessides.

1.3 Normiviited

Dokumendi lahutamatuks osaks on E-ITS etaloniturse kataloog, millesse on koondatud parimad praktikad infoturbeprotsessi loomiseks ja käigushoidmiseks.

1.4 Asukoht standardi dokumentatsioonis



Joonis 1. Dokumendi asukoht standardi dokumentatsioonis

2 Terminoloogia

Mõistepesade kaupa on esitatud kiirvasted, mis hõlbustavad kasutajal dokumendis orienteerumist. Standardi aktsepteeritud sõnavara on esitatud [E-ITS sõnastikus](#).

Tabel 1. Terminite kiirvasted

Nr	Termin või lühend	Lähtekeeles (inglise / saksa)	Lühike definitsioon
1	konfidentsiaalsus	<i>confidentiality</i>	Teabe kättesaamatus või paljastamatus volitamata isikutele, olemi-tele või protsessidele. Üks kolmest infoturbe põhikomponendist, märgitakse tähega C lühendis C-I-A.
			Teabe õigsus ja täielikkus, lubamatute muudatuste puudumine,

2	terviklus	<i>integrity</i>	hõlmab ka autentsust ja salgamatust. Üks kolmest infoturbe põhikomponendist, märgitakse tähega I lühendis C-I-A.
3	käideldavus	<i>availability</i>	Teabe omadus olla volitatud olemi nõudel õigel ajal kättesaadav ja kasutuskõlblik. Üks kolmest infoturbe põhikomponendist, märgitakse tähega A lühendis C-I-A.
4	kahju	<i>loss</i>	Soovimatu muutuse mõõt, riskianalüüsi aluskomponent, esmane infoturbevajadust otsustav tegur
5	alusohud	- (inglisekeelne termin puudub)	Standardi väljatöötaja poolt riskide kaalutlemisel kasutatud ohud; etalon turbe meetmete koostamise alus
6	risk	<i>risk</i>	Ohu võimekus tekitada organisatsioonile kahju.
7	ISMS	<i>Information Security Management System</i>	Infoturbe halduse süsteem. Def (EVS-ISO/IEC 27000:2015): Infoturbe halduse süsteem koosneb poliitikatest, protseduuridest, juhustest ning nendega seotud ressursidest ja tegevustest, mida organisatsioon kollektiivselt haldab, püüdes kaitsta oma infovarasid. ISMS on suunatud ärieesmärkide saavutamisele ning kujutab endast süstemaatilist lähenemist infoturbe rajamisele, käigushoiule, seirele, hooldamisele ja täiustamisele. See põhineb riski kaalutlemisel ja selle aktsepteerimisel tasemetel, mis tagavad riskide toimiva käsitlemise ja halduse.
8	infoturvapoliitika	<i>information security policy</i>	Organisatsiooni keskne infoturbealane dokument; sätestab arengusuunad ning taotletavad sihid, määratleb lubatu ning lubamatu.
9	käsitlusala	<i>scope</i>	ISMS kontekstis: organisatsiooni poolt kaitstavad elemendid: taristu, korraldus, personal, tehnilised komponendid
10	kaitseala*	<i>Informationsverbund</i> (saksa)	Turbekontseptsiooni koostamise ja rakendamise käsitlusala. Organisatsioon liigitab kaitsealasse kogumi sihtobjekte, mida turbeprotsess hakkab edaspidi kaitsma.
11	sihtobjekt*	<i>Zielobjekt</i> (saksa)	Kaitseala allosa – igasugune infosüsteemi kuuluv, kaitsetarbega vara (äriprotsess, rakendus, IT-lahenduse komponent, komponendirühm, hoone, kinnistu, allüksus). Sihtobjektile vastendatakse etalonmoodul (id).
12	protsess	<i>process</i>	Omavahel seotud või interakteeruvate tegevuste kogum, mis muundab lähtematerjali tulemiteks (EVS-ISO/IEC 27000:2015).
13	äriprotsess	<i>business process</i>	Organisatsiooni tegevuse element, mingi eesmärgi saavutamisele suunatud tegevuste, toimingute või protseduuride kogum. Äriprotsessi tulemusena võidakse luua sise- või väliskliendile väärtust toodete või teenustena.
14	kaitsetarve	<i>protection requirement</i> (ingl), <i>Schutzbedarf</i> (saksa)	Vara väärtusest tulenev vajadus seda kaitsta. ISO/IEC 21964: andmete ja teabe omadus, väljendab vajadust kaitsta teda kahju eest, mille võib tekitada konfidentsiaalsuse, tervikluse ja/või käideldavuse rikkumine. Standard BSI 200 laiendab kaitsetarve ka äriprotsessile.
15	teave	-	Teadmus inimesele sobival kujul ja inimsuhtluses. Eesti keel eristab teavet informatsioonist kui teadmuse masinale sobivast kujust (inglise keeles vahet teha ei saa). Seejuures andmetel puudub kontekst ja tähendus, tabel/informatsioonil on see olemas.
16	missiooni-kriitiline teave	-	Teave, mille puudumine või häiring a) takistab organisatsioonil oma ülesannete täitmist ning b) võib olukorra jätkudes ohustada organisatsiooni olemasolu.

(*) – etalon turbe spetsiifiline mõiste

3 Jaotiste lühiülevaade

Nõuete dokumendi struktuur on esitatud joonisel 2.



Joonis 2. ISMS. Nõuete dokumendi struktuur

Jaotises 4 E-ITS olemus kirjeldatakse E-ITS standardit ning selgitatakse selle suhet riskihaldusega ja standardiga ISO/IEC 27001. Lisaks esitatakse infoturbe halduse süsteemi lühikirjeldus.

Jaotises 5 Turbeprotsessi tsükli algatamine esitatakse nõuded infoturbeprotsessi tsükli igakordsele algatamisele ning juhtkonna kohustumusele.

Jaotises 6 Turbeprotsessi kavandamine ja plaanimine esitatakse nõuded infoturbe protsessi kavandamisele ja plaanimisele ning selle korraldusstruktuuridele.

Jaotises 7 Riskihaldus esitatakse nõuded infoturbe halduse süsteemi riskihaldusele, sh etalonturbe modelleerimisele ning täiendavale välisele riskihaldusele.

Jaotises 8 Meetmete rakendamine esitatakse nõuded riskihalduse abil väljaselgitatud meetmete rakendamisele.

Jaotises 9 Käigushoid esitatakse nõuded infoturbeprotsessi pidevaks käigushoidmiseks.

Jaotises 10 Infoturbeprotsessi täiustamine esitatakse nõuded infoturbe protsessi täiustamiseks ning sõltumatu läbivaatuse korraldamiseks.

Jaotises 11 Jätkutegevused kirjeldatakse võimalusi infoturbe halduse süsteemi toimimisele välise kinnituse saamiseks – auditeerimist ja sertifitseerimist.

Jaotis 12 Lisateave loetleb viited rakendaja jaoks vajalikule lisateabele.

4 E-ITS olemus

E-ITSi eesmärk on tagada avalike ülesannete täitmiseks kasutatavate äriprotsesside ja infosüsteemide kõikehõlmav kaitse ning saavutada infoturbe ühtlane tase nende kõigis osades.

E-ITSi haldab Riigi Infosüsteemi Amet. E-ITS on eestikeelne. E-ITS vaadatakse läbi ja uuendatakse üks kord aastas. E-ITSil on riiklik tugi ning kooskõla teiste Eesti õigusaktidega.

E-ITSi põhimeetod on BSI IT-Grundschutz päritolu etalonturbe. E-ITS lähenemine infoturbele põhineb tegevusriskide haldamisel.

Tulenevalt [Eesti Küberturvalisuse seadusest](#) on organisatsioonil infoturbe piisava taseme saavutamiseks kaks alternatiivset teed:

E-ITS etalonturbe

Etalonturbe toimingud jagunevad kaheks:

- 1 - Äriprotsesside toimimiseks vajalikud sihtobjektid seatakse vastavusse etalonmoodulitega, mille tulemusel tüüpsete ohtude riskikäsitus toimub tüüpmeetmete rakendamisega. Sellega saavutatakse toimiv turbehaldus valdavas osas organisatsiooni äriprotsessides.
- 2 - Äriprotsesside toimimiseks vajalike *ebatüüpsete** etalonturbesse sobimatute või normaalselt kõrgema kaitsetarbega sihtobjektide osas sooritatakse etalonturbe väline riskianalüüs täiemahulise riskihalduse abil. Kasutatav meetodika kinnitatakse organisatsiooni juhtkonna poolt. Ebatüüpsetele sihtobjektidele rakendatakse infoturbe meetmeid vastavalt etalonturbe välise riskihalduse tulemustele.

Vajadus E-ITS rakendatust auditeerida võib tuleneda: õigusakti, valdkonna standardi või lepingus sätestatud kohustusest. Auditeerida võib ka organisatsiooni enda soovil.

(*) - *Ebatüüpne ning vahetut riskikäsitlust nõudev sihtobjekt on vähemalt üks järgmistest: a) sihtobjekti kaitsetarve osutub infoturbe ühe või enama põhikomponendi (C-I-A) osas suureks või väga suureks; b) sihtobjekti ei õnnestu vastendada ühegagi olemasolevatest moodulitest, enamasti uudsuse või erilise tõttu; c) sihtobjekti kasutusviis erineb etalonmoodulis kirjeldatust.*

ISO/IEC 27001 standard

Läheneemisviis sobib eelkõige organisatsioonidele, kus on tekkinud vajadus tõendada oma ISMS vastavust rahvusvaheliselt tunnustatud standardile. Meetmed rakendatakse vastavalt riskikaalutlemise tulemustele. Meetmetena saab kasutada E ITS standardturbeviisi meetmeid, kui väljajätmade puhul tagatakse vastavus ISO/IEC 27001 nõuetega. ISO/IEC 27001 ISMS rakendatust tõendatakse vastavusauditi sertifikaadiga.

4.1 Infoturbe halduse süsteem

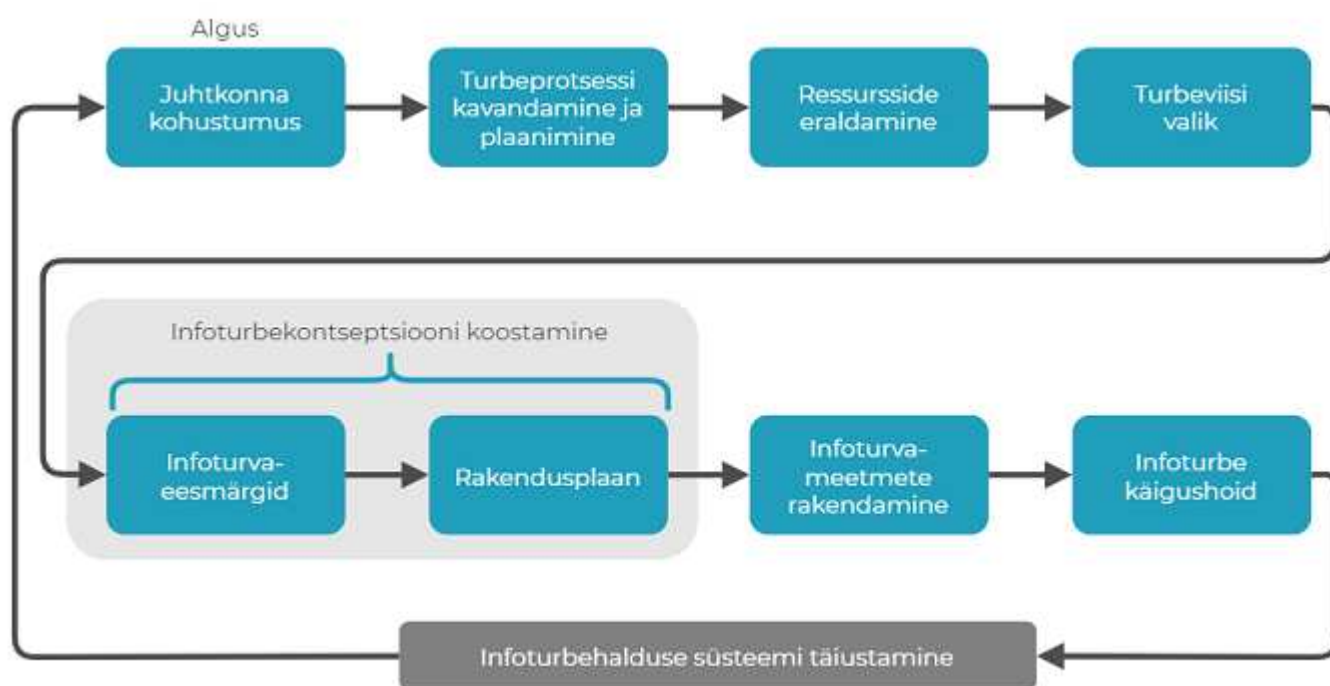
Infoturbe halduse süsteem (ISMS, *Information Security Management System*) on organisatsiooni juhtimise osa, mis tegeleb infoturbe rajamise, juurutamise, rakendamise, seire ja täiustamisega.

ISMS hõlmab:

- organisatsiooni struktuuri, protsesse, protseduure ja tavasid;
- poliitikaid ja plaanimistegevusi;
- kohustusi;
- ressursse ja varasid.

Infoturbe halduse süsteemi protsesse ja sooritatavaid tegevusi on kujutatud joonisel 3. ISMS tegevusi sooritatakse vajadusel paralleelselt. Infoturbe täiustamise käigus naastakse igakordselt protsessi algusesse.

ISMS teostusjuhised on esitatud E-ITS etalonturbe kataloogis, moodulis [ISMS.1 Turbehaldus](#).



Joonis 3. ISMS käivitamise ja uuendamise tegevused

5 Turbeprotsessi tsükli algatamine

Infoturbe lähtub organisatsiooni eesmärkidest ja tegutsemisviisidest. Infoturbe eestvedajaks (ingl *leadership*) on organisatsiooni tippjuhtkond.

Infoturbeprotsess algatatakse organisatsioonis juhtkonna otsusega, algatamisotsus dokumenteeritakse.

Infoturbeprotsessi algatamisel luuakse infoturbejuhi roll ja nimetatakse selle täitja. Infoturbejuht korraldab organisatsiooni infoturbealaseid tegevusi. Infoturbejuhi nimetamata jätmisel täidab seda rolli juhtkond.

Infoturbe keskendub teabe ja sellest sõltuvate äriprotsesside kaitsmisele ning sellest tulenevalt infotöötlaste või infotehnoloogia kaitsmisele. Seetõttu kaardistab organisatsioon esmalt äriprotsessid ja alles siis võtab arvele oma äriprotsessidega seotud varad.

5.1 Juhtkonna kohustumus

Kuna organisatsiooni äriprotsesside toimimise eest vastutab juhtkond, siis juhtkond vastutab ka äriprotsesse ohustavate sündmuste käsitlemise, sh infoturbe halduse eest. Infoturbealase vastutuse võtmist juhtkonnas nimetatakse juhtkonna kohustumuseks (ingl *commitment*).

Juhtkonna kaasatus tagab infoturbe integreerituse kaitseala kõigisse protsessidesse ning infoturbe jätkusuutlikkuse. Juhtkond vastutab infoturbe elluviimise, käigushoidmise ning täiendamise eest. Selleks määrab juhtkond turbealased õigused ja kohustused ning eraldab ressursid.

Juhtkond peab saama infoturbe kohta regulaarselt, õigeaegselt ja sobivas ulatuses järgmist teavet:

- a) organisatsiooni ja selle teabe turvariskid ning nendega seotud toimed ja kulud;
- b) turvaintsidentide toime äriprotsessidele;
- c) seadusest ja lepingutest tulenevad turvanõuded;
- d) tegevusalale tüüpilised infoturbe protseduurid;
- e) infoturbe hetkeseis ja sellest tulenevad tegevussoovitused;
- f) infoturbeprotsessi täiendusettepanekud;
- g) huvipooltega seotud kohustused ja tagasiside.

Infoturbealaseid tegevusi plaanib ja koordineerib infoturbejuht.

Äriprotsessi infoturbe meetmete rakendamist korraldab protsessijuht. Rakendatav infoturbe peab olema normaalse tööprotsessi osa ning olema kooskõlas töö eesmärkidega.

Infoturbeprotsessi peavad olema kaasatud kõik töötajad. Töötajate motiveerimiseks ning koolitamiseks kaasatakse ISMSi rakendamisse personaliosakond ning protsessijuhid.

6 Turbeprotsessi kavandamine ja plaanimine

6.1 Infoturvapoliitika

Infoturvapoliitika on organisatsiooni infoturbe juhtdokument, milles esitatakse infoturbealane kohustumus ning sõnastatakse organisatsiooni infoturbe sihid (ingl *goal*), vajadused ja põhimõtted (ingl *principle*). Infoturvapoliitika põhimõtteid kasutatakse organisatsiooni väärtuste kaitseks.

Organisatsiooni kaitstavad väärtused tuletatakse organisatsiooni põhieesmärkidest ja üldisest keskkonnast. Põhieesmärgid tulenevad ettevõtte puhul ärieesmärkidest, avaliku sektori asutuse puhul põhikirjast või põhimäärusest.

Organisatsiooni väärtustena võetakse arvesse vähemalt järgmist:

- toimingute, sealhulgas teabekäitluse kõrge usaldatavus (käideldavus, terviklus, konfidentsiaalsus jne);
- organisatsiooni hea maine;
- investering tehnoloogiasse, teabesse, tööprotsessidesse ja teadmusesse;
- töödeldav informatsioon (selle suur või korvamatu väärtus vajab kaitset);

- regulatsioonide ja lepingute nõuete täitmine;
- inimeste füüsiline ja vaimne heaolu.

Organisatsiooni infoturvapoliitika koostamisel arvestatakse:

- a) organisatsiooni eesmärgid ja strateegiat;
- b) organisatsiooni struktuuri;
- c) organisatsiooni olemasolevaid haldussüsteeme, nt kvaliteedihaldus, riskihaldus, keskkonnahaldus;
- d) õigusalasid raamtingimusi, sh kohalikud ja rahvusvahelised õigusaktid, valdkondlikud määrused;
- e) klientide, tarnijate, partnerite jt huvipoolte nõudeid;
- f) tegevusala turvastandardeid ja -praktikaid.

Infoturvapoliitika sisaldab infoturvaeesmärgid või loob raami infoturvaeesmärkide püstitamiseks.

Infoturvapoliitika kinnitab juhtkond. Infoturvapoliitika tehakse teatavaks töötajatele ning vajadusel teistele huvipooltele.

Organisatsioon vaatab infoturvapoliitika perioodiliselt üle ja ajakohastab vajadusel.

Joonis 4 selgitab infoturvapoliitika põhilisi elemente.



Joonis 4. Infoturvapoliitika elemendid

6.2 Infoturvaeesmärgid

Infoturvaeesmärgid (ingl *security objective*) sisaldavad infoturvapoliitikast lähtuvat kirjeldust, mis osas, milliste toimingutega ja mis ajaks kavatsetakse mõõdetavad eesmärgid saavutada.

Organisatsioon kasutab infoturvaeesmärkide sõnastamisel järgnevat teavet:

- a) äriprotsessid, protsessijuhid, protsesside kirjeldus ja äriprotsesside seosed organisatsiooni eesmärkidega;
- b) äriprotsesside sõltuvused ning äriprotsesside omavahelised seosed;
- c) äriprotsessidega seotud varad;
- d) äriprotsesside ning alusteabe kaitsetarvet konfidentsiaalsuse, tervikluse ja käideldavuse jt infoturbe komponentide osas;

- e) organisatsiooni tegevusriskid, nt turu hetkeseis, konkurentsiolukord ja muud turuspetsiifilised sõltuvused;
- f) olemasolev infoturbedokumentatsioon.

Eelnimetatud teabe kogumiseks organisatsioon:

- a) kaardistab äriprotsessid ja võtab arvele varad;
- b) määrab organisatsiooni infoturbe kaitseala ja sihtobjektid;
- c) valib etaloniturbe korral turbeviisi (põhi-, standard-, tuumikuturve);
- d) määrab sihtobjektide kaitsetarbe;
- e) dokumenteerib infoturvaeesmärgid ning määrab eesmärkide saavutamise ajaraamid.

Organisatsioon sõnastab infoturvaeesmärgid ning ajakohastab neid vajadusel.

6.3 Turbeprotsessi korraldus

Infoturbeprotsessi rakendamiseks ja edendamiseks loob organisatsioon turbekorraldus- ja teavitusstruktuuri.

Infoturbe korraldusstruktuuriga määrab juhtkond:

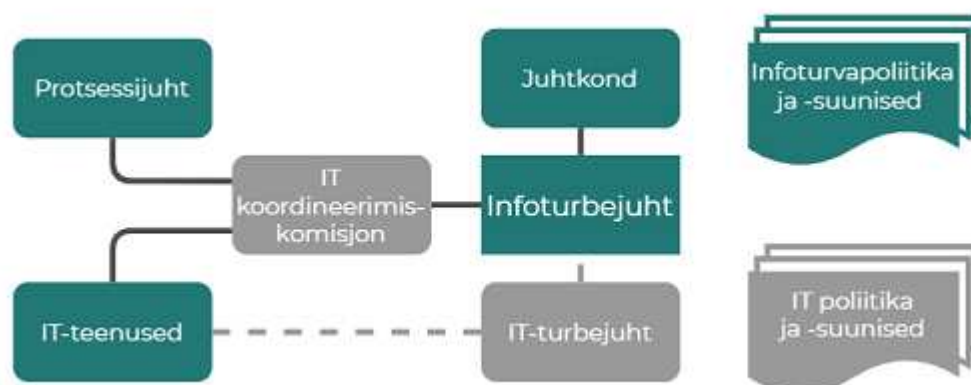
- a) rollid ja vajadusel rollipädevusnõuded;
- b) rollide täitjad;
- c) volitused ja vastutusalad.

Organisatsioon tagab rollide täitjate pädevuse ning vajalike pädevustõendite säilitamise.

Organisatsioon tuvastab sisemised ja välised infoturbe alased teavituse vajadused ning määrab teavitusviisid, osalevad rollid jm tingimused.

Turbekorraldus tehakse töötajatele teatavaks.

NÄIDE: Joonisel 5 on kujutatud üht võimalust infoturbealase töö korraldamiseks organisatsioonis. Igal äriprotsessil on protsessijuht. IT-koordineerimiskomisjon on korralduslikuks foorumiks, kus arutatakse IT-teenuste ja infoturbeaspektidega seonduvat. IT-turbejuht on nõutav vaid suurtes organisatsioonides, kus infoturbealase töö koordineerimine vajab eristamist IT-lahenduste turbealaste strateegiate täideviimisest. Halli värviga on märgitud elemendid, mida väiksem organisatsioon ei pruugi vajada.



*Joonis 5. Infoturbe korraldusstruktuuri näidis***6.4 Infoturbealane koolitus**

Vastavuses infoturvapoliitika eesmärkidega tagab organisatsioon kõikide töötajate vajaliku infoturbealase pädevuse ja pädevuse uuendamise.

Regulaarsete infoturvet käsitlevate koolituste eesmärk on motiveerida töötajaid järgima infoturbenõudeid, käsitlema teavet ning töövahendeid korrektselt ja vältima riskikäitumist.

6.5 Ressursside eraldamine

Juhtkond eraldab rahalised ja mitterahalised ressursid infoturbeprotsessi läbiviimiseks. Juhtkond aktsepteerib töötajate põhitööga kaasnevaid infoturbekohustusi.

6.6 Juhtkonna kinnitus

Juhtkond kinnitab infoturvapoliitika, turvaeesmärgid ning ressursside eraldamise infoturbele.

6.7 Turbeprotsessi dokumenteerimine

Dokumenteermise abil tagatakse infoturbeprotsessi jätkusuutlikkus ja jälgitavus. Dokumente tuleb koostada taasesitatavas, ajakohastamist võimaldavas ning versioonihaldusega kaetud viisil. Tuleb tagada, et käibelt on kõrvaldatud vananenud dokumendid ja versioonid.

Organisatsioon kehtestab dokumentide koostamise, vormistamise ja hoidmise reeglid.

Poliitikad ja eeskirjad vaadatakse üle vähemalt üks kord aastas ning muudatused kinnitab juhtkond. Korrad ja protseduurijuhendid hoitakse tegelike protsessidega kooskõlas.

Organisatsioon loob ja säilitab tegevusdokumentatsiooni, mis tekib infoturbeprotsessi käigus.

Dokumenteeritakse:

- turbeprotsessi alusdokumendid ja väljatöötamise kulg (konteksti jäädvustamiseks),
- otsused (et tagada otsuste ja meetmete jälitatavus),
- infoturbesündmused (osutamaks täiustamise võimalustele),
- organisatsiooni reaktsioon sündmustele ja otsustele (et demonstreerida parandusmeetmete toimivust),
- muu teave, mida organisatsioon ise peab vajalikuks säilitada infoturbe halduse toimivuse huvides.

Turbeprotsessi dokumentatsioon on volitatutele kättesaadav ning kaitstud kõrvalise juurdepääsu eest.

7 Riskihaldus

Etalonturbe kontseptsioon lähtub põhimõttest, et infoturvaohud ja kaitstavad varad on erinevate organisatsioonide puhul tüüpsed. E-ITS etalonturbe kataloog esitab moodulitesse koondatud eelanalüüsitud meetmekomplektid, mis katavad tüüpsete sihtobjektide riskihalduse ning infoturvavajadused.

Ebatüüpsetele ning kõrgendatud kaitsetarbega sihtobjektidele tuleb rakendada etalonturbe välist riskihaldust.

Organisatsioon määratleb kaitsetarbe määramise põhimõtted, sh riski aktsepteerimise kriteeriumid, kaitsetarbe komponendid (vähemalt konfidentsiaalsus, terviklus, käideldavus ehk C-I-A).

Sihtobjektide kaitsetarve tuvastatakse ja dokumenteeritakse.

Riskihalduse käik ja tuvastatud või määratud meetmete rakendamise otsused dokumenteeritakse korratavuse ja võrreldavuse eesmärgil.

7.1 Etalonturbe modelleerimine

Organisatsioon vastendab kaitsealasse kuuluvad iga sihtobjekti etalonturbe kataloogi ühe või mitme mooduliga. Moodulite rakendamise järjekord määratakse lähtuvalt organisatsiooni infoturvapoliitikast ja reaalsest vajadusest.

Moodulist sihtobjekti turvameetmete tuvastamisel arvestatakse:

- a) turbeviisi;
- b) sihtobjekti kaitsetarvet;
- c) meetme seost infoturbeprotsessi elutsükliga.

Etalonturbe kataloogi protsessimoodulite kõik rühmad käsitletakse väljajäetudeta, st iga väljajätt peab olema põhjendatud. Süsteemimoodulid rakendatakse vastavuses kaitseala määratlusega.

7.2 Etalonturbe väline riskihaldus

Organisatsioon suunab etalonturbe välisesse riskihaldusse sihtobjektid, mille jaoks puudub etalonturbe kataloogis sobiv moodul. Täiendavalt suunatakse välisesse riskihaldusse sihtobjektid, kui sihtobjekti puhul on täidetud üks järgmistest tingimustest:

- a) kaitsetarve on suur või väga suur;
- b) kaitsetarve on määramata või ebaselge;
- c) kasutusviisid ei ole vastavuses etalonturbe kataloogi moodulite kirjeldustega;
- d) etalonturbe kataloogi meetmed osutuvad turvaeesmärkide täitmisel puudulikuks (jääkrisk pole aktsepteeritav).

Organisatsioon määrab etalonturbe välise riskihalduse protsessi. Riskihalduse asjaolud, kulg ning tulemused dokumenteeritakse.

Etalonturbe väline riskihaldus määrab sihtobjektidele lisaturvameetmeid sihtobjekti kaitsetarbest ja infoturvaeesmärkidest lähtuvalt.

8 Meetmete rakendamine

Tehnilised meetmed rakendatakse kõigile kaitseala sihtobjektidele. Organisatsioonilised meetmed integreeritakse organisatsiooni kõigisse protsessidesse.

Meetmete rakendamise eest vastutab vastava protsessi juht või etalonturbe kataloogis nimetatud vastutajarolli täitja. Rakendamist koordineerib ja nõustab infoturbejuht.

Organisatsioon hindab tuvastatud ja määratud meetmete:

- a) ressursside ühekordseid ja korduvaid kulusid;
- b) sobivust, teostatavust, piisavust, võimalikku turvakasu ja meetmete omavahelisi mõjusid.

Infoturvaeesmärkidele vastavalt määrab organisatsioon meetmete rakendusplaanis:

- a) rakendamise otsused;
- b) teostusjärjekorra;
- c) vastutajad;
- d) tähtjad.

Organisatsioon teadvustab ja aktsepteerib jääkriskid ning kinnitab rakendusplaani eelarve.

Meetmed rakendatakse vastavalt rakendusplaanile. Meetmete rakendatuse määr ning rakendamise etapid dokumenteeritakse ajakohase ülevaate ning hilisema jälitatavuse eesmärgil.

Organisatsioon tagab meetmetes kirjeldatud korduvate ja regulaarsete tegevuste võrreldavuse, järjepidevuse ja õigeaegsuse.

9 Käigushoid

Organisatsioon tagab infoturbeprotsessi ning turvameetmete pideva ja jätkusuutliku toimimise.

Jälgitakse ja mõõdetakse:

- a) infoturvaeesmärkide ning -meetmete sobivust, tõhusust;
- b) ressursside kasutamist.

Organisatsioon reageerib muutustele organisatsiooni eesmärkides, regulatsioonide nõuetes, lepingulistes kohustustes ning ümbritsevas infoturbeolukorras. Protsessijuhid tagavad infoturvet puudutava teabe õigeaegse edastamise asjakohaste rollide täitjatele.

Seiratakse protsesside ning süsteemide töö käigus tekkinud teavet. Olulistele infoturbe sündmustele reageeritakse ja need registreeritakse.

Seire, ülevaatuste ja kontrollide dokumenteeritud tulemusi ning järeldusi kasutab organisatsioon infoturbeprotsessi ja -meetmete täiustamise ning muutmise ettepanekute koostamisel.

Infoturbeprotsessi käigus ilmnenu asjaoludest ning nende muutustest teavitatakse vajalikus ulatuses:

- a) juhtkonda
- b) määratud rollide täitjaid
- c) töötajaid
- d) teisi huvipooli.

10 Infoturbeprotsessi täiustamine

Organisatsioon kontrollib perioodiliselt infoturbeprotsessi, infoturvapoliitika ja infoturvaeesmärkide sobivust ja asjakohasust.

Infoturbeprotsessi täiustamise põhjused on muuhulgas:

- a) organisatsiooni eesmärkide ja nõuete muutused;
- b) infoturvapoliitika ja infoturvaeesmärkide muutused;

- c) turvaolukorra muutused;
- d) regulatsioonide ja standardite muutused;
- e) kaitseala ning kaitsetarbe olulised muutused;
- f) infoturbeprotsessi käigus ilmnenu asjaolud, sh intsidentide, läbivaatuste, auditeerimiste järelused ja ettepanekud;
- g) vajadus E-ITS auditeerimiseks või rahvusvahelise ISO/IEC 27001 sertifikaadi taotlemiseks.

Organisatsiooni juhtkond otsustab infoturbeprotsessi täiustamise ning protsessi tsükli algusesse naasmise.

10.1 Sõltumatu läbivaatus

Organisatsioon korraldab regulaarselt infoturbeprotsessi tulemite ja seisundi sõltumatu läbivaatuse. Läbivaatusel hinnatakse organisatsiooni infoturbealalduse vastavust:

- a) siinse dokumendiga (E-ITS *ISMS. Nõuded*);
- b) organisatsiooni infoturbepoliitikaga.

Läbivaatuse läbiviijaks on vastavalt infoturbepoliitikale kas sise- või välisaudiitor. Võimalusel välditakse rakendaja ning kontrollija rollide huvide konflikti.

Organisatsioon määrab sõltumatu läbivaatuse käsitusala ja eesmärgid. Läbivaatuse läbiviimisel arvestatakse:

- a) organisatsiooni eesmäärke;
- b) regulatsioonide nõudeid ning lepingulisi kohustusi;
- c) organisatsiooni infoturvapoliitikat ja -eesmäärke;
- d) varasemate läbivaatuste tulemusi.

Läbivaatuse tulemused ja ettepanekud dokumenteeritakse täiustamise ning jälitatavuse eesmärgil. Tulemusi arvestatakse organisatsiooni protsesside täiustamisel.

11 Jätkutegevused

11.1 E-ITS auditeerimine

Auditeerimine viiakse läbi vastavalt [E-ITS auditeerimisjuhendile](#).

E-ITS rakendatuse auditeerimist viiakse läbi:

- a) kohustuslikult – regulatsioonidest lähtuvalt või
- b) lepinguliste kohustuste täitmiseks või
- c) vabatahtlikult – vastavalt organisatsiooni eesmärkidele ja infoturvapoliitikale.

E-ITS auditeerimise nõuded, sh läbiviija (välisaudiitori pädevus), sageduse jm osas tulenevad regulatsioonidest.

Audiitori hinnang on tõendiks organisatsiooni infoturbe toimivuse kohta.

11.2 ISO/IEC 27001 vastavuse sertifitseerimine

Organisatsiooni eesmärkidest ning infoturvapoliitikast lähtuvalt võib organisatsioon taotleda äriprotsesside infoturbe halduse süsteemi sertifitseerimist vastavuses rahvusvahelise standardi ISO/IEC 27001 nõuetele.

12 Lisateave

Alljärgnevalt on esitatud allikad, kus leidub abi infoturbeprotsessi korraldamiseks:

[E-ITS Rakendusjuhend](#)

E-ITS Etalonturbe kataloog, <https://eits.ria.ee/>

[E-ITS Riskihaldusjuhend](#)

[E-ITS Auditeerimisjuhend](#)

[E-ITS Alusotude kataloog](#)

[E-ITS Standardi terminoloogiasõnastik](#)

[ISO/IEC 27001:2017 Infotehnoloogia. Turbemeetodid. Infoturbe halduse süsteemid. Nõuded](#)

[BSI IT Grundschutz](#)

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

Juhend

RAKENDUSJUHEND

Sisukord

[RAKENDUSJUHEND](#)

[1 Käsitlusala](#)

[1.1 Asukoht standardi dokumentatsioonis](#)

[2 Jaotiste lühiülevaade](#)

[3 Eesti infoturbestandardi eesmärk](#)

[3.1 Standardi olemus](#)

[3.2 Standardi ülesehitus ja sisemine struktuur](#)

[4 Turbe teoreetilised alused](#)

[4.1 Turvaprobleem](#)

[4.2 Risk](#)

[4.3 Etalonturbe põhialused](#)

[5 Astmikud ja liigitusskeemid](#)

[5.1 Infoturbe komponendid](#)

[5.2 Kaitsetarve](#)

[5.3 Etalonturbe liigitused](#)

[5.4 Turvameetmete sobivus](#)

[5.5 Rakendusotsus ja meetmete teostatuse määr](#)

[6 Etalonturbe ressursid](#)

[6.1 Etalonturbe kataloog ja moodulirühmad](#)

[6.2 Moodulid ja nende ülesehitus](#)

[6.3 Meetmete teostusjärjekord](#)

[6.4 Täiendavad soovitusel etalonturbe kataloogi kasutamiseks](#)

[7 Etalonturbe turbeviisid](#)

[7.1 Põhiturve](#)

[7.2 Standardturve](#)

[7.3 Tuumikuturve](#)

[7.3.1 Varade tuumiku piiritlemine](#)

[8 Etalonturbeprotsessi lühikirjeldus](#)

[8.1 Etalonturbe protsessi erinevused turbeviiside lõikes](#)

[9 Etalonturbeprotsessi käivitamine](#)

[9.1 Infoturbeprotsessi algatamine](#)

[9.1.1 ISMS käivitamine etalonturbe koosseisus](#)

[9.2 Turbeprotsessi dokumenteerimine](#)[9.3 Äriprotsesside ja varade arvelevõtt](#)[9.3.1 Äriprotsesside arvelevõtt](#)[9.3.2 Alusteabe ja sihtobjektide arvelevõtt](#)[9.3.2.1 Äriprotsesside alusteave](#)[9.3.2.2 IT süsteemid ja rakendused](#)[9.3.2.3 Sideühendused](#)[9.3.2.4 Muud olulised ressursid](#)[9.3.2.5 Muud sõltuvused](#)[10 Etalonturbe protsess](#)[10.1 Ettevalmistused etalonturbeks ja varade arvelevõtt](#)[10.2 Samm 1 – kaitseala piiritlemine](#)[10.3 Samm 2 – kaitseala struktuurianalüüs](#)[10.4 Samm 3 – kaitsetarbe määramine](#)[10.5 Samm 4 – kaitseala modelleerimine ja meetmete tuvastamine](#)[10.6 Etalonturbe väline riskihaldus](#)[10.7 Samm 5 – turvameetmete kinnitamine](#)[10.8 Samm 6 – turvameetmete rakendamine](#)[10.9 Samm 7 – turbe käigushoid](#)[10.10 Samm 8 – infoturbeprotsessi täiustamine](#)[10.11 E-ITS auditeerimine](#)[10.12 ISO/IEC 27001 vastavuse sertifitseerimine](#)[11 Lisateave](#)[Lisa A Etalonturbe kataloogi ülevaade](#)[Lisa B Kahjustsenaariumide küsimustik](#)[Lisa C Dokumentatsiooni näidisloend](#)[Lisa D Rollide nimekirj](#)

1 Käsitlusala

Eesti infoturbestandard (E-ITS) on eestikeelne ja Eesti õigusruumile vastav alus infoturbe käsitlemiseks. E-ITS aluseks on Saksa päritolu BSI *IT-Grundschutz* **etalonturbe meetod**. Samaaegselt on E-ITS on vastavuses standardi ISO/IEC 27001 nõuetega.

E-ITS rakendusjuhend on etalonturbe rakendajale mõeldud abimaterjal. Rakendusjuhendi suunised on sõltumatud organisatsiooni suuruselt ja tegevusvaldkonnast.

Rakendusjuhend annab juhised infoturbe korralduse kavandamiseks, infoturbe haldussüsteemi (**ISMS** – *Information Security Management System*) käivitamiseks ja etalonturbe rakendamiseks ja käigushoiuks organisatsioonis. Dokument esitab sel eesmärgil protseduurisammud.

Rakendusjuhendi sihtrühm on infoturbe halduse töötajad, spetsialistid, konsultandid ning infoturbe eest vastutavad isikud.

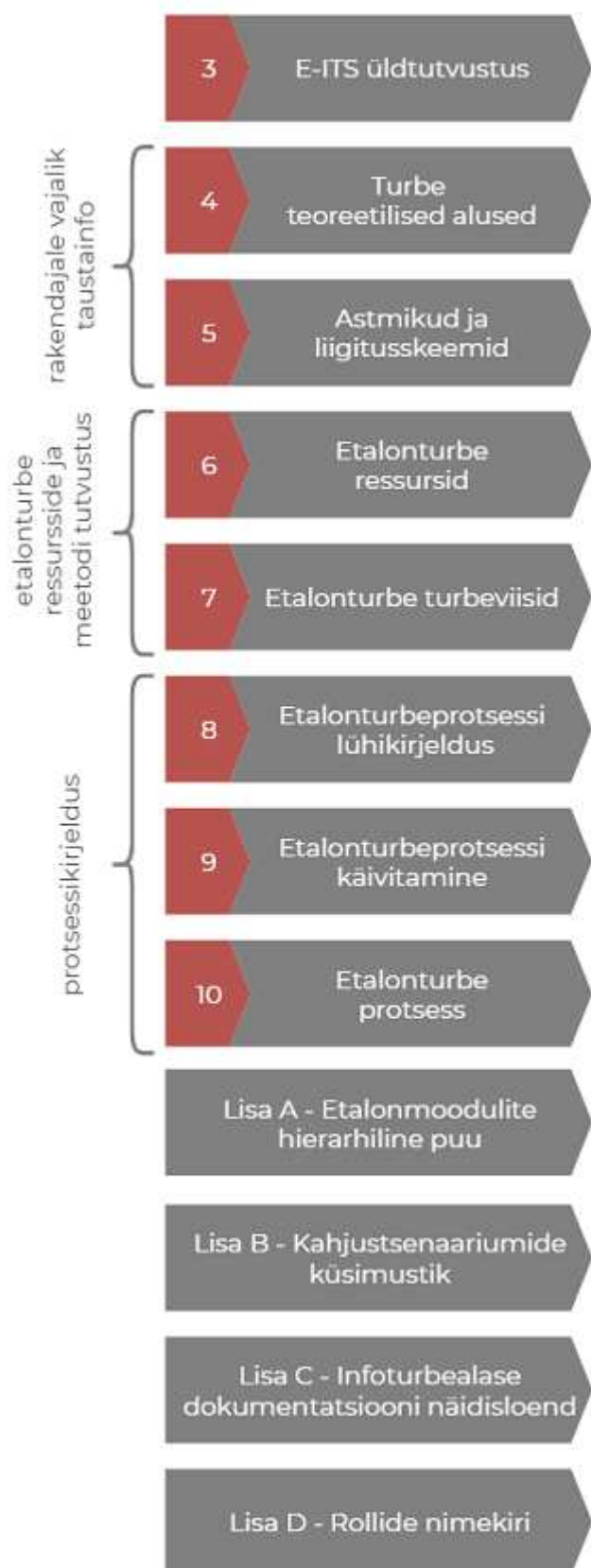
Lisaks võivad rakendusjuhendit abimaterjalina kasutada protsessi- või üksustejuhid, kes peavad organisatsioonis arvestama infoturbe aspekte ja korraldama infoturbemeetmete rakendamise.

1.1 Asukoht standardi dokumentatsioonis



Joonis 1. Rakendusjuhendi asukoht standardi dokumentatsioonis

2 Jaotiste lühiülevaade



Jaotises 3 Üldtutvustus antakse lühiülevaade Eesti infoturbestandardi eesmärgist ja tutvustatakse selle lähtekohti.

Jaotises 4 Turbe teoreetilised alused selgitatakse infoturbe sh etalonturbe alusmõisteid.

Jaotises 5 Astmikud ja liigitusskeemid kirjeldatakse etalonturbe rakendamiseks vajalikke konventsioone ja notatsioone.

Jaotis 6 Etalonturbe ressursid tutvustab etalonturbe kataloogi, selle ülesehitust ning iga mooduli sisemist struktuuri. Selgitatakse põhi-, standard- ning kõrgmeetmete erinevust ning moodulite teostusjärjestust.

Jaotis 7 Etalonturbe turbeviisid annab ülevaate põhi-, standard- ning tuumikuturbe turbeviisidest.

Jaotis 8 Etalonturbeprotsessi lühikirjeldus annab ülevaate etalonturbeprotsessi sammudest turbeviiside lõikes.

Jaotis 9 Etalonturbeprotsessi käivitamine kirjeldab infoturbeprotsessi käivitamist etalonturbes, vastavuses dokumendis E-ITS [ISMS. Nõuded](#) määratletud infoturbe halduse süsteemiga ning vaatleb etalonturbe ja ISMS sulandumist. Samuti sõnastatakse etalonturbeprotsessi dokumenteerimismõisted ja varade arvelevõtu juhised.

Jaotis 10 Etalonturbe protsess kirjeldab etalonturbe rakendamise samme.

Lisas A – etalonmoodulite hierarhiline puu.

Lisas B – kahjustsenaariumide küsimustik.

Lisas C – infoturbedokumentatsiooni näidisloend.

Lisas D – kasutatud infoturberollide nimekiri.

3 Eesti infoturbestandardi eesmärk

Eesti infoturbestandardi (E-ITS) siht on arendada ning edendada Eesti avaliku sektori asutuste, aga ka erafirmade infoturbe taset, esitades eestikeelne ja Eesti õigusruumile vastav alus infoturbe käsitlemiseks, mis samalaadset on kooskõlas rahvusvaheliselt tunnustatud infoturbe halduse standardiga ISO/IEC 27001. E-ITS arendamisel on aluseks võetud Saksa päritolu BSI *IT-Grundschutz* etalonturbe süsteem.

Auditeeritud vastavus E-ITS-iga võimaldab organisatsioonil kinnitada ja demonstreerida oma infoturbe toimivust ja jätkusuutlikkust, nt andmevahetuse partneritele ja klientidele.

3.1 Standardi olemus

Nii E-ITS kui ISO/IEC 27001 nõuavad, et organisatsioonil oleks toimiv infoturbe halduse süsteem (vt [jaotis 9.1](#) ja moodul [ISMS](#) etalonturbe kataloogist). ISMS tagab infoturbe protsessi jätkusuutlikkuse organisatsioonis, loob võimekuse intsidentidest õppida ning arvesse võtta väliskeskkonnas toimunud muutusi. Standardite põhinõuete omavaheline kooskõla annab võimaluse standardi ISO/IEC 27001 rakendamiseks, kui selleks tekib vajadus.

E-ITS kasutab riskihalduse lihtsustamiseks **etalonturbe meetodit**. Etalonturbe puhul on põhilised riskihaldusotsused ära teinud standardi väljatöötaja. Etalonturbe esitab etalonmeetmed tüüpsetele organisatsioonidele tüüpsete **ohtude** (*threats*) vastu. Kahjustsenaariume põhjustavad ohud loetleb standard **alusohitudena** (vt [E-ITS Alusohitude kataloog](#)). Infoturbemeetmed etalonturbe kataloogis pakuvad kaitset alusohitude nimekirjas loetletud ohtude eest.

Etalonturbes käsitlemata ja uute ohtude eest kaitsmiseks nõuab E-ITS organisatsioonilt **etalonturbe välist riskihaldust**. Samuti on väline riskihaldus nõutav, kui äriprotsessides kasutatav teave tingib kõrgendatud

kaitsetarbe (kaitsetarve: suur või väga suur). E-ITS võimaldab organisatsioonil riskide kaalutlemiseks (*risk assessment*) ning käsitlemiseks (*risk treatment*) valida sobiva riskihaldusmeetodi. Seejuures E-ITS sisaldab [riskihaldusjuhendit](#).

Rakendaja ülesanne on arvele võetud **sihtobjekte** puudutavate meetmete tuvastamine etalonturbe kataloogist. Etalonturbe rakendamiseks tuleb need **meetmed** (*controls*) teostada. Etalonturbe rakendamine ei vabasta organisatsiooni kohustusest riske hallata, ent võimaldab suurema osa riskihaldusest sooritada lihtsustatud meetodil.

E-ITS võimaldab organisatsioonil demonstreerida oma infoturbealast küpsust. Sel eesmärgil tuleb organisatsiooni infoturbe halduse süsteem kas:

- auditeerida E-ITS [ISMS. Nõuded](#) järgi (vt E-ITS [Auditeerimisjuhend](#)) või
- sertifitseerida ISO/IEC 27001 alusel.

Avalikus sektoris sätestatakse auditeerimiskohustus õigusaktiga, muudel juhtudel tuleb auditeerimist lugeda vajaduspõhiseks tõendamiskohustuseks (nt lepingust tulenev kohustus).

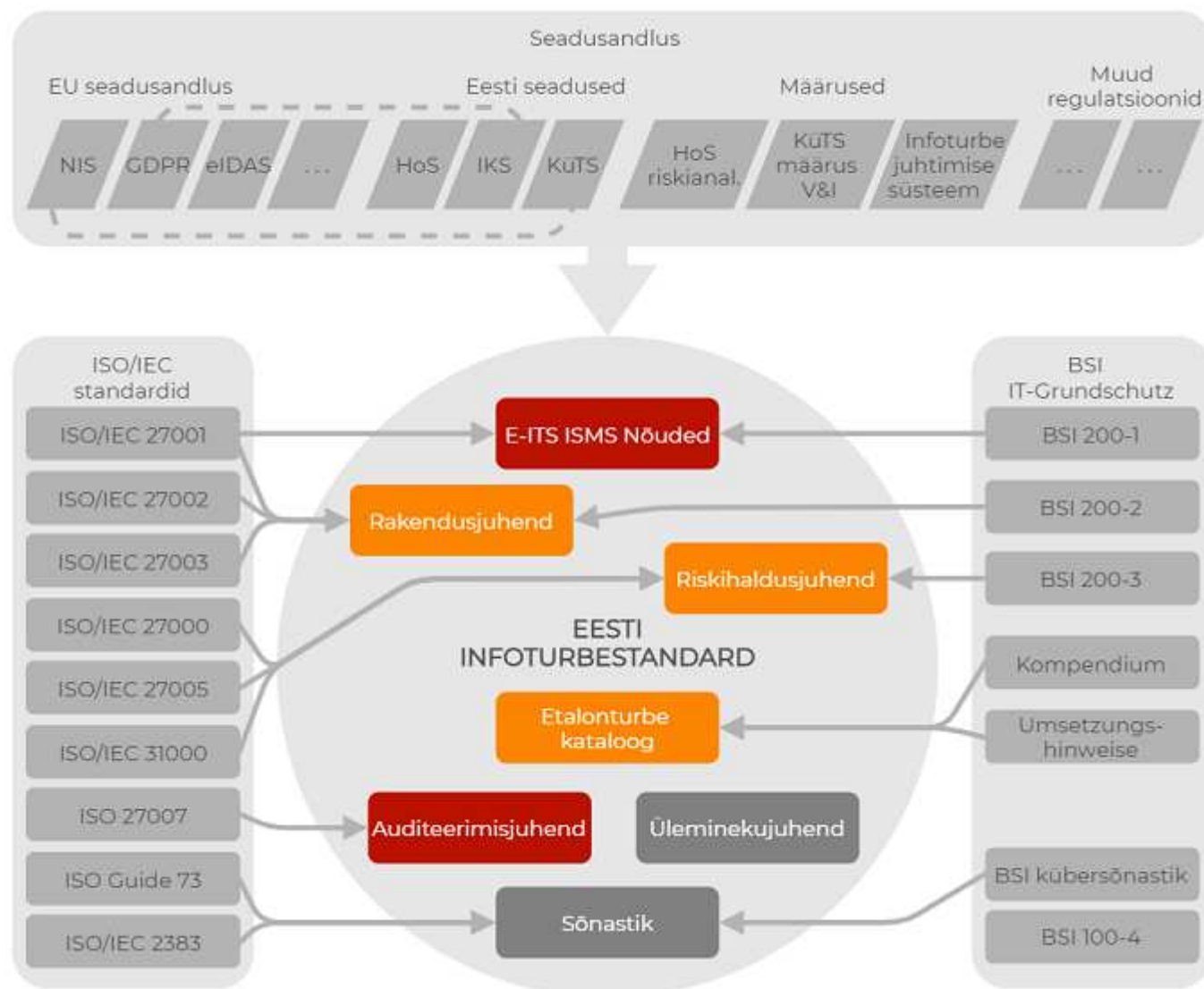
3.2 Standardi ülesehitus ja sisemine struktuur

Standardi omanik ja uuendaja on Riigi Infosüsteemi Amet. Standardi ülesehituse põhimõtted järgivad etalonturbe BSI *IT-Grundschutz* süsteemi. Tabelis 1 on loetletud Eesti infoturbestandardi olulisemad dokumendid.

Tabel 1. E-ITS dokumendid

Nr	Nimetus	Sisu	Sihtgrupp	Vastavus
1	Lühijuhend	Lühike tutvustus	Juhtkond, esmatutvujad	
2	Infoturbe halduse süsteem. Nõuded (ISMS Nõuded)	Standardi nõuded	Infoturbe töötajad, protsessijuhid, IT-töötajad	BSI 200-1
3	Rakendusjuhend	Ülevaade etalonturbe rakendamisest	Turbehalduse töötajad, infoturbe ja IT spetsialistid	BSI 200-2, ISO/IEC 27001
4	Etalonturbe kataloog	Infoturvameetmed	Riskihalduse ja turbehalduse töötajad, protsessijuhid, infoturbe ja IT spetsialistid	BSI Kompendium, Umsetzungshinweise
5	Riskihaldusjuhend	Etalonturbega sobiva riskihalduse kirjeldus.	Infoturbehalduse töötajad, spetsialistid, konsultandid, isikud, protsessijuhid	ISO/IEC 27001, BSI 200-3
6	Auditeerimisjuhend	E-ITS vastavus-auditi põhimõtted, ja läbiviimine	Audiitorid, infoturbejuhid, organisatsioonide juhid ja otsustajad	BSI auditeerimiskeemid
7	Üleminekujuhend	E-ITS soovitusel ISKE kasutajatele. E-ITS—ISKE ning E-ITS—ISO/IEC 27001 vastavustabelid	Infoturbejuhid	ISKE, E-ITS, ISO/IEC 27001
8	Alusohitude kataloog	Etalonturbe riskihalduses arvestatud ohud	Riskihalduse ja turbehalduse töötajad	BSI Gefährdungskataloge des IT Grundschutzes
9	Alusohitude viitetabel	Alusohitude seosed moodulitega	Infoturbejuhid, audiitorid.	BSI Kompendium
10	ISO27001- E-ITS	ISO27001 ja E-ITSi meetmete vastavus kasutatav	Infoturbejuhid, audiitorid	

Joonis 3 väljendab, millistest ISO/IEC standardidest ja BSI *IT-Grundschutz* dokumentidest on lähtutud E-ITS juhendite ning dokumentide koostamisel. E-ITSi hoitakse vastavuses kohalduvate Eesti ja EU regulatsioonidega.



Joonis 3. E-ITS dokumentide seos õigusaktide ja standarditega

4 Turbe teoreetilised alused

Jaotises esitatakse infoturbealuse alusmõisted, mis abistavad rakendajat E-ITSist arusaamisel ning erialasel suhtlemisel.

4.1 Turvaprobleem

Organisatsioon, isik või riik vajab oma olemasoluks ja tegutsemiseks varasid.

Vara (*asset*) on miski, millel on omaniku jaoks väärtus (ISO 28002, ISO 55000 jt). Varad on näiteks:

- teave
- andmed
- tarkvara

- füüsiline vara (taristu, hoone, riistvara, sisseseade)
- rahaline vara
- teenus
- inimressurss (inimesed, kvalifikatsioon, oskused, kogemused)
- oskusteave
- mitteaineline vara (maine, kuvand).

Vara rikkumine, hävimine või lubamatu kasutamine tekitab kahju selle omanikule või kasutajale, vahel ka kolmandatele isikutele.

Kahju (*loss*) on vara väärtuse langus (ISO/IEC TR 27016), kahjustuse või kaotuse kvantitatiivne mõõt (EVS-ISO/IEC 2382). Kahju ähvardavad tekitada ohud.

Oht (*threat*) on võimaliku kahjustuse allikas (EVS-ISO/IEC Juhend 73). Ohtude realiseerumise takistamine nõuab ressursse, niisiis tekitab kulusid. Kulud ei tohi olla tõrjutavast kahjust suuremad.

Turvaprobleem on kahjude ja nende tõrjumise kulude mõistliku suhte leidmise tehnilis-majanduslik ülesanne. Ülesande teeb keeruliseks lähteandmete puudulikkus, eriti ohtude realiseerumise juhuslikkus.

Määramatus on lähteandmete ja/või analüüsiprotsessi ebakindlus (ISO 11231). Määramatus võib väljenduda teabe puudulikkuses või ebatäpsuses.

4.2 Risk

Risk on määramatuse **toime** eesmärkidele (EVS-ISO/IEC Juhend 73).

Toime on positiivne või negatiivne kõrvalekalle oodatavast (EVS-ISO/IEC Juhend 73).

Negatiivne toime on **kahju** ülalmääratletud tähenduses. Positiivne toime on **šanss**, st eesmärgi saavutamist edendav võimalus.

Formaliseeritult esitades on risk kahe muutuja funktsioon:

- **risk = f(toime, võimalikkus).**

Riski väärtuse leidmise teeb keeruliseks ja kulukaks võimalikkuse hindamine piisava täpsusega.

Määramatust tuleb uurida täpsemalt, kasutades mõõtmist.

Võimalikkus (*likelihood*) on millegi juhtumise võimalus, mis on kvalitatiivselt või kvantitatiivselt määratletud, mõõdetud või määratud (EVS-ISO/IEC Juhend 73).

Võimalikkuse kvantitatiivsed mõõdud on

- juhtumise teoreetiline **tõenäosus** või
- juhtumise empiiriline **sagedus**

mingil määratud ajavahemikul, näiteks aastas.

Turvameede (*security control*) – riski muutev abinõu (EVS-ISO/IEC Juhend 73).

4.3 Etalonturbe põhialused

Enamik süsteeme on tüüpilised ja korduvad: samad varad, samad ohud sama võimalikkusega. Seetõttu on riskianalüüsi tulemid taaskasutatavad.

Etalonturve on tüüpjuhtudeks ettevalmistatud, riskianalüüsi läbinud valmis moodulitesse jaotatud turvameetmete kogum.

Mudel:

- reaalmaailma protsessi, seadme või mõiste esitus (ISO/IEC/IEEE 24765),
- millegi esitus, mis jätab ära mingid esitatava objekti aspektid (IEEE 1320.2).

Modelleerimine – tegelikkuse mingi osa esitamine mudeliga. Etalonturbes valitakse modelleerimisel etalonturbe kataloogist moodulid ning seatakse need vastavusse sihtobjektidega.

Sihtobjekt on etalonturbes modelleeritav komponent. Oma olemuselt on sihtobjektid varad, millele rakendatakse etalonturbe meetmeid. Sihtobjektis võivad varad olla grupeeritud oma põhiomaduste ja kaitsetarbe alusel.

Etalonmudel – kogum suhteliselt sõltumatute moodulitena koostatud süsteemi- ja protsessimooduleid, mis näitavad iga modelleeritava komponendi peamisi ohte ja vajalikke turvameetmeid.

5 Astmikud ja liigitusskeemid

Jaotisse on koondatud olulised elemendid ja mitmesugused liigitused, mida on vaja teada enne etalonturbe rakendamist.

5.1 Infoturbe komponendid

Infoturbe jagamist komponentideks läheb vaja **kaitsetarbe** täpsel määramisel. Infoturbevajadus jaotatakse kolmeks eraldi komponendiks, mis on loetletud tabelis 2.

Tabel 2. Infoturbe põhikomponendid

Eestikeelne nimetus	Tähistus	Ingliskeelne nimetus
konfidentsiaalsus	C	confidentiality
terviklus	I	integrity
käideldavus	A	availability

Tähistust (C-I-A) kasutatakse:

- kaitsetarbe väljendamiseks,
- etalonturbe kataloogi kõrgmeetme asjakohasuse näitamiseks infoturbe komponendi osas.

Kasutatavad liigitused dokumenteeritakse .*

(*) - Organisatsiooni ja äriprotsesside spetsiifikast lähtuvalt võib infoturbe põhikomponentidele lisaks vajadusel eristada täiendavaid infoturbe komponente: privaatsust (privacy), jälitatavust (accountability), auditeeritavust (auditability), autentsust (authenticity), usaldusväärset (trustworthiness), salgamatust (non-repudiation) ning ohutust (safety). E-ITS nimetatud lisakomponentide tarbeks kahjustsenaariume ei paku. Kui organisatsioon otsustab lisakomponente kasutada, siis tuleb asjakohased kahjustsenaariumid ise välja töötada.

5.2 Kaitsetarve

Kaitsetarve väljendab äriprotsessi infoturbe vajadust. Hinnang äriprotsessi kaitsetarbele tuleneb eelkõige **äriprotsessi poolt töödeldava teabe** kaitsetarbest, sh andmekogu turvaklassist. Kaitsetarve määramine

võib toimuda näiteks äritoime analüüsi (BIA - *Business Impact Analysis* - äritoime analüüs) tulemuste põhjal.

Kaitsetarbe hinnang on kvalitatiivne, see antakse kolmeastmelisel skaalal. Äriprotsessile omistatud kaitsetarbe kandub tavaliselt edasi kõigile selle äriprotsessis kasutatavatele varadele.

Kaitsetarbe tähistatamist selgitab tabel 3.

Tabel 3. Kaitsetarbe määrangud

Arvuline tähistus	Lühend	Taseme nimetus	Kirjeldus	Pikem selgitus
1	N	normaalne	Kahjustuse toime on piiratud ja ohjatatav.	Etalonturbe meetmed osutuvad asjakohasteks ja mõistlikeks ning üldiselt nende rakendamisest piisab.
2	S	suur	Kahjustuse toimed võivad olla tõsised. St kuni 1,5% aasta eelarvest	Etalonturbe meetmetest ei pruugi alati piisata. Tuleb läbida etalonturbe väline riskianalüüs ning vajadusel määrata lisaturvameetmed.
3	VS	väga suur	Kahjustuse toimed võivad ulatuda katastroofilise tasemeni, ähvardades organisatsiooni olemasolu. St rohkem kui 1,5% aasta eelarvest.	Etalonturbe meetmetest ei piisa kindlasti. Riskianalüüs on kohustuslik, konkreetsele ohule tuleb määrata individuaalsed turvameetmed.

E-ITS nõuab sihtobjekti kaitsetarbe määramist turvalisuse kolme põhikomponendi (C-I-A) osas (vt jaotis 5.1).

Kaitsetarbe määramisel äriprotsessi tasemel on abiks *Kahjustsenaariumide küsimustik* (vt [Lisa B](#)). Kaitsetarbe määramise protseduuri käsitleb [jaotis 10.4](#).

Kaitsetarvet saab esitada kokkuvõtva maatriksina, vt tabel 4.

Tabel 4: Kaitsetarbe maatriks

		Kaitsetarbe tase			
		N	S	VS	Kokku
Infoturbe komponent	C	1	2	3	C1
	I	1	2	3	I3
	A	1	2	3	A2
	Kaitsetarbe				C1-I3-A2

NB! Üldistatult tähendab „kaitsetarbe S” või „kaitsetarbe VS” sihtobjekti kaitsetarvet vähemalt ühe infoturbe komponendi suhtes S või VS. Täpsem määratlus komponenthaaval on tarvilik kõrgmeetmete tuvastamisel ning välises riskihalduses.

Organisatsioon kinnitab kaitsetarbe sobiva liigitusskeemi, sh infoturbekomponendid ning vajadusel ka kaitsetarbe tasemete nimetused (kui standardsed nimetused mingil põhjusel ei sobi).

Kaitsetarbe komponenthaval määramise tulemus on oluline sisend mõnede meetmete rakendamisel (meetmes nimetatud) ja normaalsest suurema kaitsetarbega sihtobjektidele riskihaldust läbi viies.

5.3 Etalonturbe liigitused

- Etalonturbe kataloog on jaotatud moodulirühmadeks – ISMS, CON, ORP, OPS, DER; INF, NET, SYS, APP, IND. Moodulirühmas on vastava valdkonna moodulid.
- Moodulis on turvameetmed jaotatud kolmeks: **põhimeetmed, standardmeetmed, kõrgmeetmed**.
- Etalonturbe turbeviise on kolm: **põhiturve, standardturve, tuumikuturve**. Turbeviise vaadeldakse [jaotistes 7](#).

Etalonturbe ressursse kirjeldatakse [jaotises 6](#).

5.4 Turvameetmete sobivus

Etalonturbe kataloogis sisalduvate turvameetmete sobivust on moodulite koostamisel hinnatud. Välise riskihalduse läbimisel lisanduvaid lisaturvameetmeid tuleb hinnata sobivuse suhtes. Hindamine viiakse läbi enne lisaturvameetmete ühendamist etalonturbe moodulite meetmetega.

Meetmete sobivuskontrolli käsitletakse [jaotises 10.7](#). Sobivuskategooriad on loetletud tabelis 5.

Tabel 5: Lisameetmete sobivuskategooriad

Nimetus	Sobivuskategooria selgitus
toimivus	Meetmed kaitsevad võimalike ohtude eest ka tegelikult. Vajalik kaitsetarve on kaetud.
kõlblikkus	Meetmeid saab praktikas teostada. Nad ei pidurda korraldusprotsesse ülemäära ega nõrgenda teisi turvameetmeid.
tarvitatavus	Meetmed on kergesti mõistetavad, hõlpsasti kasutatavad ning ei ole veaaltid. Kasutajatel ei ole meetmetest lihtne mööda hiilida.
vastuvõetavus	Meetmed on ühtemoodi rakendatavad kõigile kasutajatele, nad ei diskrimineeri ega kahjusta kedagi.
kuluefektiivsus	Meetmete teostuse kulud ja keerukus on kooskõlas mõjutatavate sihtobjektide kaitsetarbega. Kasutatavate ressurssidega saavutatakse optimaalne tulemus.

5.5 Rakendusotsus ja meetmete teostatuse määra

Rakendusotsusega plaanitud ja teostatud meetmete üle peetakse arvestust. Meetmete rakendamise teostatuse määra arvestus tagab infoturbe halduse olukorra pideva jälgitavuse.

Tabel 6 defineerib teostatuse märke, mis on esitatud nn „**PEARO** põhimõttel“. Rakendusotsus meetmete mitterakendamisest (sh „Ei ole vajalik“) vajab eraldi põhjendamist taasesitatavas vormis.

Tabel 6: Meetmete teostatuse märke

Teostatusmärged	Märke sisu	Kommentaar
P	P ole asjakohane	Meetme teostamine pole vajalik ega konkreetsete sihtobjektide puhul asjakohane (näiteks teenuste aktiveerimise tõttu). Meetme mitterakendamine ei avalda mõju asutuse infoturbele.
E	E i ole rakendatud	Meede on teostamata või teostatud ebaolulisel määral, kuid vajab rakendamist.
A	A ksepteeritud risk	Meede on rakendamata ja seotud risk on saanud juhtide tasemel akseptearingu, mille kohta on ka kirjalik märke.

R	Rakendatud	Turvameede on teostatud täielikult, tõhusalt ja otstarbekalt.
O	Osaliselt	Meede on teostatud vaid osaliselt.

6 Etalonturbe ressursid

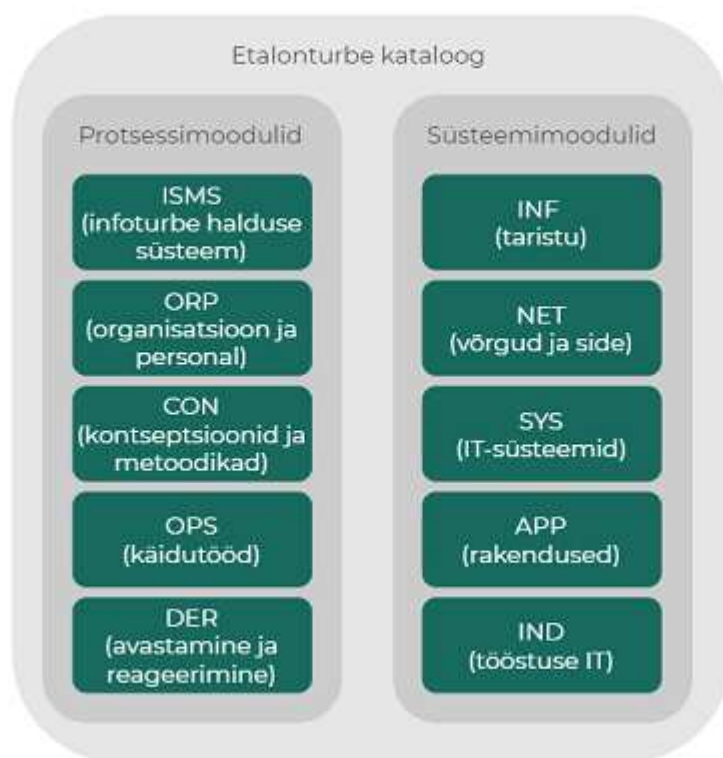
Etalonturbe põhimõisteid on selgitatud [jaotises 4.3](#).

Etalonturbe keskne tegevus on **modelleerimine**. Selle käigus seatakse sihtobjektid vastavusse (vastendatakse) etalonturbe kataloogi moodulitega ning tuvastatakse rakendusplaani kantavad meetmed.

6.1 Etalonturbe kataloog ja moodulirühmad

Etalonturbe kataloog esitab ohtude tõrjeks kasutatavad meetmed moodulitena. Moodulid on koondatud teemade alusel rühmadesse. Moodulirühmade tähised (nt ISMS, OPS, INF) vastavad käsitletavate valdkondade ingliskeelsetele lühenditele.

Eristatakse organisatsiooni protsessidega seotud protsessimoodulite rühmi ning tehnoloogiaga seotud süsteemimoodulite rühmi, vt joonis 4.



Joonis 4. Etalonturbe kataloog, moodulirühmade jagunemine

Ülevaate moodulirühmade sisesest hierarhiast leiab etalonturbe kataloogist, vt [Lisa A](#).

6.2 Moodulid ja nende ülesehitus

Moodulis esitatakse teave ühe konkreetse teema või valdkonna kohta.

Mooduleid kasutatakse infosüsteemi sihtobjektide modelleerimisel ning rakendatavate meetmete tuvastamiseks.

Moodulid järgivad ühtset malli.

Mooduli kirjeldus

- **Eesmärk** – aitab tuvastada mooduli ja rakendaja sihtobjekti eesmärkide vastavust.
- **Vastutajad** – vaikumisi roll kui meetme juures pole märgitud vastutajat (rollid vt [Lisa D](#)).
- **Lisavastutajad** – meetmetega seotud lisarollid. Lisavastutajad esitatakse meetme kirjelduses (rollid vt [Lisa D](#)).
- **Piirangud** – mooduli välistused või soovitusel seotud moodulite kaasamiseks.

Ohud – mooduli riskianalüüsil arvestatud ohud, seosed alusohtudega.

Meetmed

- **Elutsükk** – meetmete rakendamise järjekorra määramise sisend.
- **Põhimeetmed** – kohustuslikud meetmed, vastab põhiturbeviisile.
- **Standardmeetmed** – põhimeetmetele lisanduvad meetmed, vastab standardturbeviisile.
- **Kõrgmeetmed** – põhi- ja standardmeetmetele lisanduvad meetmed, kasutatakse suure või väga suure kaitsetarbega sihtobjektide puhul. Kõrgmeetmele on lisatud asjakohane infoturbe põhikomponendi tähis või tähised (C-I-A). Tähised viitavad milliste kaitsetarbe komponentide saavutamiseks on meede vajalik, vt [jaotised 5.1 ja 5.2](#).

Lisateave – viited välistele abimaterjalidele, regulatsioonidele.

Standard- ja kõrgmeetmed on koostatud silmas pidades etaloniturbet kõiki alusohte (vt E-ITS [Alusohtude kataloog](#)). Põhimeetmed pakuvad kaitset vaid olulisemate ohtude eest ja on mõeldud standardi rakendamise alustamiseks piiratud ajaperioodil.

Kõrgmeetmeid rakendatakse, kui tuvastatakse „suur” või „väga suur” kaitsetarve või välises riskihalduses määrati lisaturvameetmed.

Mõnikord tuleb meetmete tuvastamisel arvesse võtta, millise infoturbekomponendi tõttu meede määrati. Näiteks, kui kõrgmeetmete vajadus tekkis tervikluskalutlustel, siis puudub rakendajal vajadus teostada käideldavusnõuetest ajendatud kõrgmeetmeid. Infoturbekomponent, mille saavutamisele meede on suunatud, on sellisel juhul meetme juures otsesõnu nimetatud.

Ühele sihtobjektile tuleb rakendada kõiki asjakohaseid mooduleid, st ühele sihtobjektile võib vastata mitu moodulit. Näiteks Windows serverile 2012 tuleb rakendada mooduleid [SYS.1.1 Server üldiselt](#) ning [SYS.1.2.2 Windows server 2012](#).

Sihtobjektile täpse mooduli vaste puudumisel (näiteks sihtobjektile Windows server 2019) võib kasutada lähimat sihtobjektiga sobivat moodulit, kuid meetmete asjakohasust ning täielikust tuleb eraldi hinnata välise riskihalduse käigus.

6.3 Meetmete teostusjärjekord

Moodul [ISMS.1](#) (turbehaldus) ning moodulirühm DER (avastamine ja reageerimine) on erandlikud, **need tuleb rakendada sõltumata organisatsioonis kasutatavatest rakendustest või tehnoloogiatest**.

Moodulite rakendamise järjekorra määrab organisatsioon ise lähtudes reaalistest vajadustest.

Mõned turvameetmetest tuleks teostada võimalikult varakult, sest neile tuginevad järgmised moodulid. Rakendusplaanis järjestab organisatsioon meetmed kasutades sisendina muuhulgas:

- moodulis olevat elutsükli,
- meetmete ning sihtobjektide omavahelisi sõltuvusi,
- organisatsiooni infoturvaeesmärke.

Tuvastatud ja täitmiseks järjestatud meetmed koondatakse rakendusplaani, mis seejärel täpsustub kuupäevade ja vastutajatega.

6.4 Täiendavad soovitusel etalonturbe kataloogi kasutamiseks

- Vastendamisel jäetakse kõrvale kõik mitteasjakohased moodulid. Näiteks: kui organisatsiooni kõik serverid on Linux serverid, siis Windows serverite moduleid ei vaadelda.
- Moodulist kantakse rakendusplaani kõik turbeviisile vastavad meetmed. Mitterakendamise otsus (nt pole asjakohane) fikseeritakse rakendusplaanis meetmete teostatuse määrana (vt [jaotis 5.5](#)).
- Välise riskihalduse tulemusena või organisatsiooni strateegiast tulenevalt võib tekkida vajadus sihtobjektile määrata lisaturvameetmeid, mis lisatakse samuti rakendusplaani.
- Tuleb teadvustada ja võimalusel vältida rollikonflikte – meetme rakendaja ning kontrollija peaksid olema erinevad isikud.
- Etalonturbe kataloogi uuendatakse kord aastas. Rakendaja peab mõistliku aja jooksul oma tegevusplaanides arvestama võimalike uuendustega ning vastavalt ajakohastama organisatsiooni infoturbe meetmete rakendusplaani.

7 Etalonturbe turbeviisid

E-ITS etalonturbemetoodika kirjeldab kolme turbeviisi:

- **põhiturbe,**
- **standardturbe,**
- **tuumikuturbe.**

Põhiturbe ja standardturbe erinevad peamiselt rakendamisele kuuluvate meetmete hulga, sh dokumenteerimise nõuete osas, ja regulaarsete infoturbe halduse jätkusuutlikkust tagavate tegevuste osas. Tuumikuturvet võib vaadelda kui ülemineku protsessi põhiturbest standardturbele, kus standardturvet rakendatakse esialgu vaid varade tuumikule ja kõigele muule rakendatakse põhiturvet.

Organisatsioon valib alustamiseks ühe turbeviisi. Turbeviisi valikul tuleb lähtuda regulatsioonidest ja kaitsetarbest, aga ka organisatsiooni infoturbe küpsusest. Alustamiseks valitud turbeviis ei sõltu organisatsiooni suuruselt.

Infoturbe halduse protsess on tsükliline. Iga tsükli alustamisel tuleb hinnata turbeviisi sobivust ning vajadusel valida infoturbe eesmärkidele vastav.

- **Kohustuslik on tagada põhiturbe rakendamine, aga eesmärk on standardturbe rakendamine ja pidev täiendamine.**

Joonis 5 kujutab kolme turbeviisi erinevust graafiliselt. Põhiturvet rakendatakse kõigile äriprotsessidele.

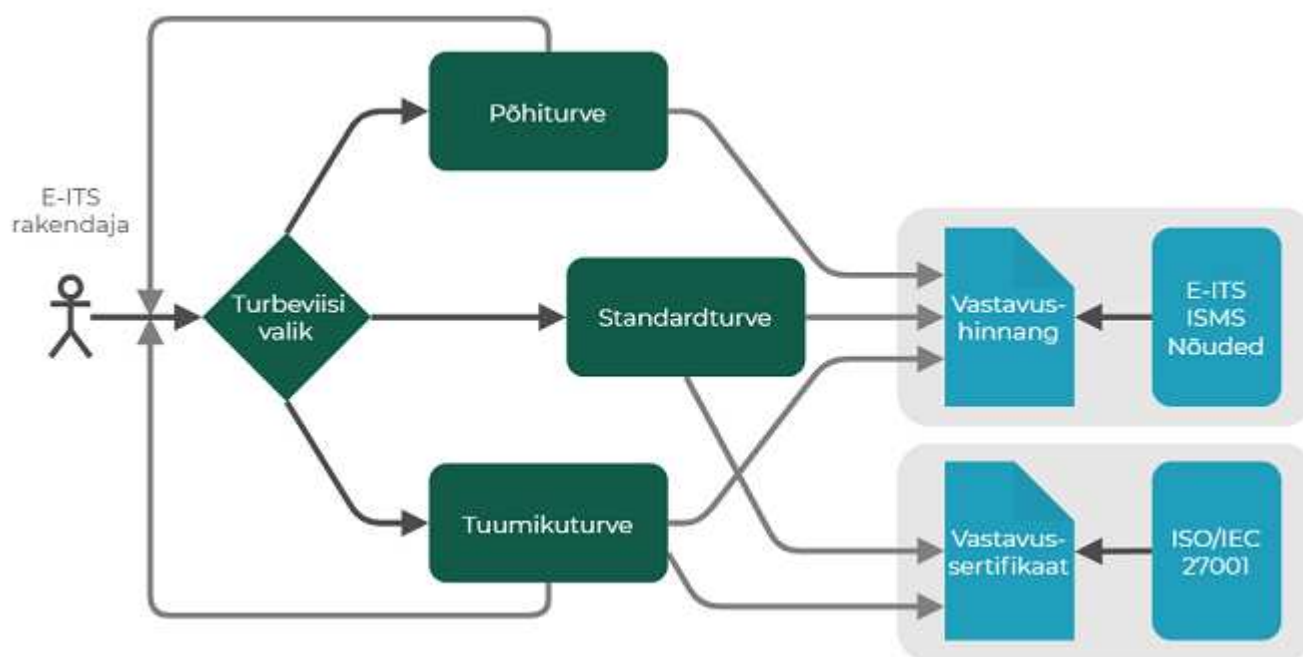
Standardturbe (vt joonise vasakpoolne osa) tagab äriprotsessides rakendatud infoturbe jätkusuutlikkuse.

Tuumikuturbe (vt joonise parempoolne osa) rakendatakse, kui põhiturbe ei rahulda varade tuumiku kaitsetarvet ning standardturvet ei suudeta kõigis protsessides rakendada.



Joonis 5. Etalonturbe turbeviiside erinevused

Joonis 6 kujutab E-ITS rakendamisteid vastavushinnangu või sertifitseerimiseni. E-ITSi vastavushinnagu saab taotleda kõigi turbeviiside puhul, vastav turbeviis fikseeritakse vastavushinnangus. Põhiturve ei võimalda ISO27001 vastavuse saavutamist. Küll aga võib saavutada E-ITSi meetmete rakendamisega varade tuumikule konkreetsetes kaitsealas ISO27001 vastavuse, mida on võimalik vajadusel sertifitseerida. Standardturbe korrektne rakendamine võimaldab tõendada ka ISO27001 vastavust.



Joonis 6. E-ITS rakendamise teed

Järgmises kolmes alajaotises kirjeldatakse turbeviiside iseärasusi. Turbeviiside rakendussammude erinevusi kirjeldatakse [jaotises 8.1](#).

7.1 Põhiturve

Põhiturve tagab organisatsiooni üldise ja elementaarse esialgse turbe.

Põhiturve turbeviisina sobib organisatsioonile, kui:

- infoturbe rakendamine on algusjärgus või madalal küpsusastmel;
- eeldatav kaitsetarbe tase on **normaalne** (mitte suur või väga suur);
- äriprotsessid ei sisalda infoturbe kõrgeid riske;

- varade vargus, häving või rikkumine ei ohusta organisatsiooni toimimist või olemasolu või avalike ülesannete täitmist;
- väiksemad turvaintsidendid (sh põhjustatud rahaline kahju) on talutavad ja ei ohusta organisatsiooni olemasolu.

Põhiturbe valimisel rakendatakse etalonturbe põhimeetmed etalonturbe kataloogi moodulitest. Suure või väga suure kaitsetarbe tuvastamisel tuleb valida juba algusest peale standardturve või tuumikuturve.

Juurutatud põhiturbe on lähtepunktiks standardturbe rakendamisele.

7.2 Standardturve

Standardturve tagab infoturbeprotsessi jätkusuutlikkuse organisatsiooni kõigis äriprotsessides. Selleks nõuab standardturve süsteemset infoturbeprotsessi dokumenteerimist. See tagab infoturbe halduse jätkusuutlikkuse ka inimeste vahetumise korral.

Standardturve on etalonturbe rakendamise lõppeesmärk sõltumata algselt valitud või eelnevast turbeviisist.

Standardturve turbeviisina sobib organisatsioonile, kui:

- organisatsioonis on rakendatud ISMS (näiteks ISKE või ISO/IEC 27001);
- infoturbe organisatsioonis on saavutanud piisava küpsusastme, on loodud infoturbe korraldus ja olulistel aladel on rakendatud turvameetmed;
- organisatsioonile ei ole vastuvõetavad turvaintsidendid, mis tuntavalt mõjutavad äriprotsesse, tekitavad rahalist või muud kahju.

Standardturbe valimisel rakendatakse etalonturbe kataloogi põhi- ja standardmeetmed ning vajadusel ka kõrgmeetmeid. Riskianalüüsi tulemusena võib olla vajalik rakendada lisaturvameetmeid, vt jaotis [10.6 Etalonturbe väline riskihaldus](#).

Standardturbe rakendamine võimaldab organisatsioonil jõuda ISO/IEC 27001 sertifikaadi taotlemiseni.

7.3 Tuumikuturve

Tuumikuturve tähendab kaitseala piiritletud osas (kriitiliste äriprotsesside ja varade tuumiku osas) standardturbe rakendamist. Ülejäänud kaitsealal rakendatakse põhiturvet.

Tuumikuturve sobib organisatsioonile eelkõige siis, kui tundlike andmete olemasolu tõttu jääks põhiturbe ebapiisavaks, kuid puudub ressurss standardturbe koheseks rakendamiseks organisatsiooni kõigile äriprotsessidele.

Tuumikuturve sobib organisatsioonile, kui:

- organisatsiooni äriprotsessidest mõned on **suure** või **väga suure** kaitsetarbega;
- organisatsioon suudab määratleda äriprotsessid, mille riskipotentsiaal teabe turvalisuse seisukohast on kõrge;
- organisatsioonil leidub varasid, mille vargus, häving või rikkumine ohustab organisatsiooni toimimist või olemasolu;
- väiksemaid ning organisatsiooni toimimist mitteohustavaid turvaintsidente tajutakse aktsepteeritavatena.

Tuumikuturbe valimisel rakendatakse etalonturbe kataloogi põhimeetmeid kogu kaitseala ulatuses. Varade tuumiku osas rakendatakse kohalduvate moodulite standardmeetmed ning vajadusel ka kõrgmeetmeid. Riskianalüüsi tulemusena võib olla vajalik rakendada lisaturvameetmeid, vt jaotis [10.6 Etalonturbe väline riskihaldus](#).

Tuumikuturbe rakendamine võimaldab organisatsioonil jõuda ISO/IEC 27001 sertifikaadi taotlemiseni piiratud käsitlusala ulatuses.

7.3.1 Varade tuumiku piiritlemine

Tuumikuturbe valimisel kinnitab organisatsiooni juhtkond varade tuumiku. Varade tuumiku piiritlemisel arvestatakse teavet ja äriprotsesse. Ettepaneku liigitada teave varade tuumikusse võivad teha vastutavad spetsialistid ja turbejuhid.

Harilikult kuuluvad varade tuumiku hulka:

- missioonikriitilistes **äriprotsessides** töödeldav **teave**;
- äriprotsessid, mille kaitsetarve on normaalsest tunduvalt suurem, seda kas konfidentsiaalsuse, tervikluse, käideldavuse või privaatsuse seisukohast;
- lühiajaliselt selgelt määratletud perioodi jooksul kriitilised protsessid ja seotud varad (nt valimised);
- teave ja äriprotsessid, mille vargus, hävimine, paljastamine või rikkumine ohustavad organisatsiooni toimimist või olemasolu.

Varade tuumiku näited:

- äriprotsessid, mida käitatakse seadusest tulenevate nõuete täitmiseks, äriotsuste üksikasjad, strateegilised hankedokumendid, finantsplaanid;
- ärisaladused -- ehituskavad, tooteretseptid, tootearenduse üksikasjad, patenditaotluste taustmaterjal, disainikavandid jms;
- kaitsealuste taimede, ohustatud inimeste või salastatud süsteemide asukohateave (NB! Riigisaladusi töödeldakse Riigisaladuse ja salastatud välisteabe seaduse nõuetest tulenevalt);
- isikute privaatne alusteave e-identiteedi süsteemides;
- isikute eriliiki kuuluv teave;
- krüptograafiline materjal, näiteks organisatsiooni võtmeloomevõti või elektrooniliste isikusertifikaatide väljastamise võtmed;
- serverite halduspääsu andmed.

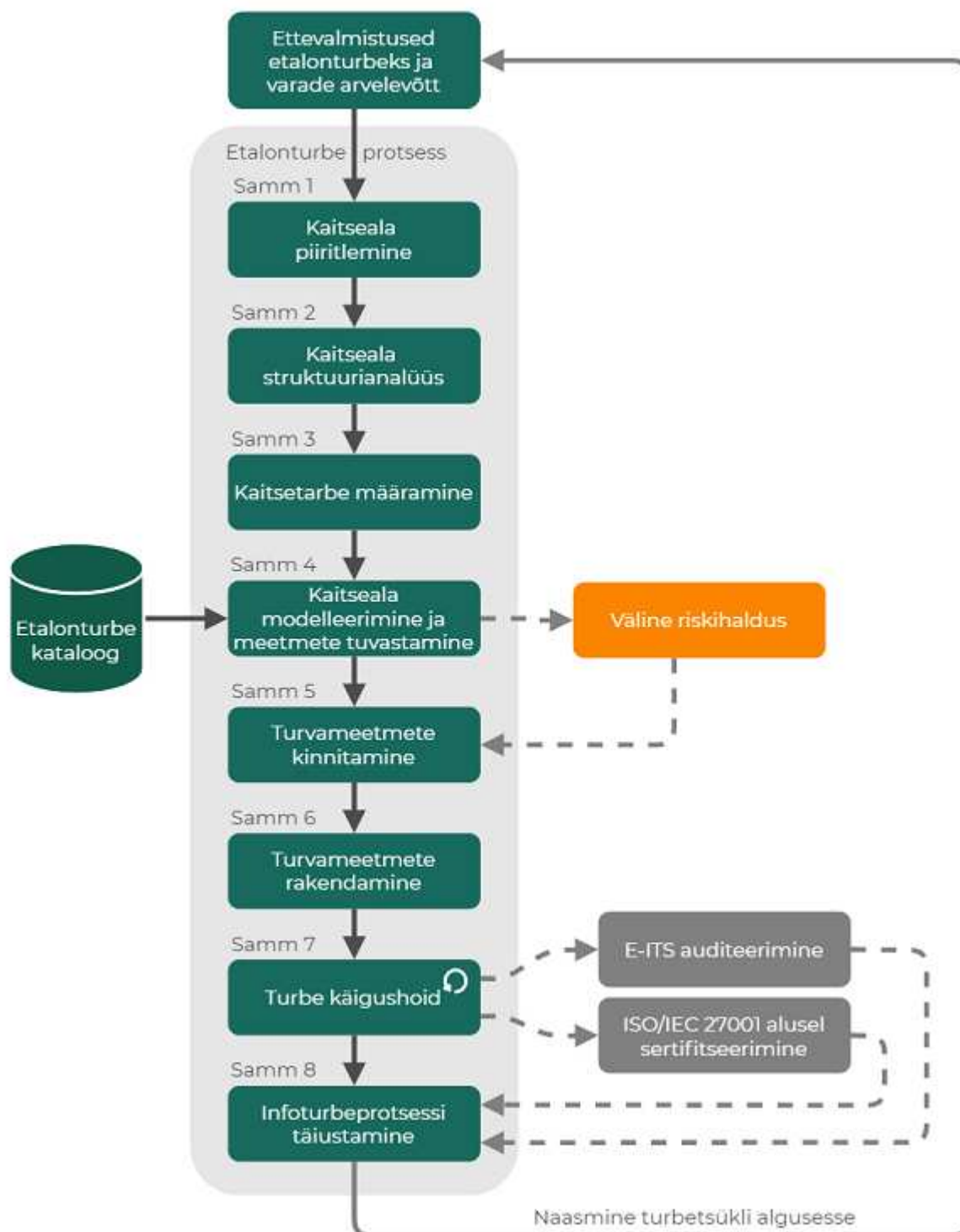
Varade tuumiku piiritlemisel võib olla abi järgmistest väidetest:

- varade tuumiku hulka kuuluvad teave või äriprotsessid;
- varade tuumiku hulka kuuluv teave võib olla esmapilgul märkamatu: näiteks üksikfail, andmekogu, struktureeritud või struktureerimata teave (nt käsitsi kirjutatud sedel, suuline teade, töötajate teadmised, võimed);
- eeldatakse, et varade tuumiku ja nendega seotud ressursside kaitsetarvet ei ole võimalik rahuldada põhiturbe abil;
- äriprotsessi ja teabe kaitsetarve võib ajas muutuda – näiteks informatsioon uudistoodete kohta ja aastaaruannete mustandid;
- äriprotsessi ja teabe kaitsetarve võib olla nii suur, et vastutajal ei ole õigust varasid hallata, kuigi on kohustus kaitsta;
- lisaks ründajatele võib varade tuumikut ohustada ka keskkond.

Varade tuumiku piiritlemisel tuleb sisendina arvesse võtta kõiki seotud protsesse ja nende sisend- ja väljundteavet, tarneahelaid jmt. Varade arvelevõttu kirjeldatakse [jaotises 9.3](#).

8 Etalonturbeprotsessi lühikirjeldus

Etalonturbe protsess on ülevaatlikult esitatud joonisel 7. Etalonturbe protsessi sammude täpsem kirjeldus on [jaotises 10](#). Etalonturbe kataloogi kirjeldus on [jaotises 6](#). Etalonturbe välise riskihalduse jaoks on soovitatav kasutada E-ITS [Riskihalduse juhendit](#). Ettevalmistust etalonturbeks tuleb alustada dokumendi E-ITS [ISMS. Nõuded](#) alusel, rakendusjuhendis selgitab seda [jaotis 9](#).



Joonis 7. Etalonturbe protsessi ülevaade

8.1 Etalonturbe protsessi erinevused turbeviiside lõikes

Etalonturbe alustamiseks valitud turbeviisid on kirjeldatud [jaotises 7](#). Turbeviisist sõltub läbitavate sammude hulk. Tabel 7 kirjeldab, millised sammud tuleb läbida.

Tabel 7. Etalonturbe protsessi sammud turbeviiside lõikes

Etalonturbe samm	Etalonturbe tegevus	Turbeviis	Turbeviis	Turbeviis	Turbeviis	Kommentaariid
		Põhiturbe	Standardturbe	Tuumikoturbe - varade	Tuumikoturbe - muud	

				tuumiku osas	varad	
-	Ettevalmistused etalonturbeks, varade arvelevõtt					Vt jaotis 9 Etalonturbeprotsess käivitamine
1	Kaitseala piiritlemine					Tuumikuturbe korral rakendatakse kaitseala piiritletud osas standardturvet. Ülejäänud kaitseala rakendatakse põhiturvet.
2	Kaitseala struktuurianalüüs					Põhiturbe puhul vaid minimaalne ülevaatus
3	Kaitsetarbe määramine					Põhiturbe puhul eeldatakse kaitsetarvet kuni N . Kõrgem kaitsetarve nõuab turbeviisina standard- või tuumikuturbe kasutamist.
4	Kaitseala modelleerimine ja meetmete tuvastamine					Põhiturbe puhul jäetakse vahele võrdlus ohtudega. Vt samm 3 kommentaari.
VÄLINE	Etalonturbe väline riskihaldus		vajadusel	vajadusel		Põhiturbe puhul eeldatakse kaitsetarvet N , kus riskianalüüsi võib vahele jätta. Standard- ja tuumikuturbe puhul oleneb riskianalüüsi vajadus sihtobjektide kaitsetarbest (>N).
5	Turvameetmete kinnitamine					
6	Turvameetmete rakendamine					
7	Turbe käigushoid					Põhiturbe tagab vaid alustamise ja on eelduseks standardturbele, mis tagab ka käigushoiu
8	Infoturbeprotsessi täiustamine					Turbe jätkusuutlikkuse tagamiseks peaks liikuma standardturbe suunas.
						Auditeerimise

-	E-ITS auditeerimine	vajadusel	vajadusel	vajadusel	vajadusel	vajadus tuleneb regulatsioonidest, lepingutest või organisatsiooni strateegiast.
-	ISO/IEC 27001 alusel sertifitseerimine		vajadusel	vajadusel		Vajadus tuleneb lepingutest, regulatsioonidest vms ja on organisatsiooni strateegiline otsus

9 Etalonturbeprotsessi käivitamine

Etalonturbe protsessi rakendamise eel on:

- algatatud infoturbeprotsess (sh on käivitatud ISMS);
- määratletud turvapoliitika ja infoturbe korraldus;
- arvele võetud äriprotsessid, nende aluseks olev teave ja äriprotsesse teenindavad varad.

Organisatsioon dokumenteerib infoturbeprotsessi vajalikus ulatuses oma infoturbealduse toimimise jälgimiseks ja jätkusuutlikkuse tagamiseks.

Käivitamisfaasi eesmärk on tagada nimetatud eelduste täidetud.

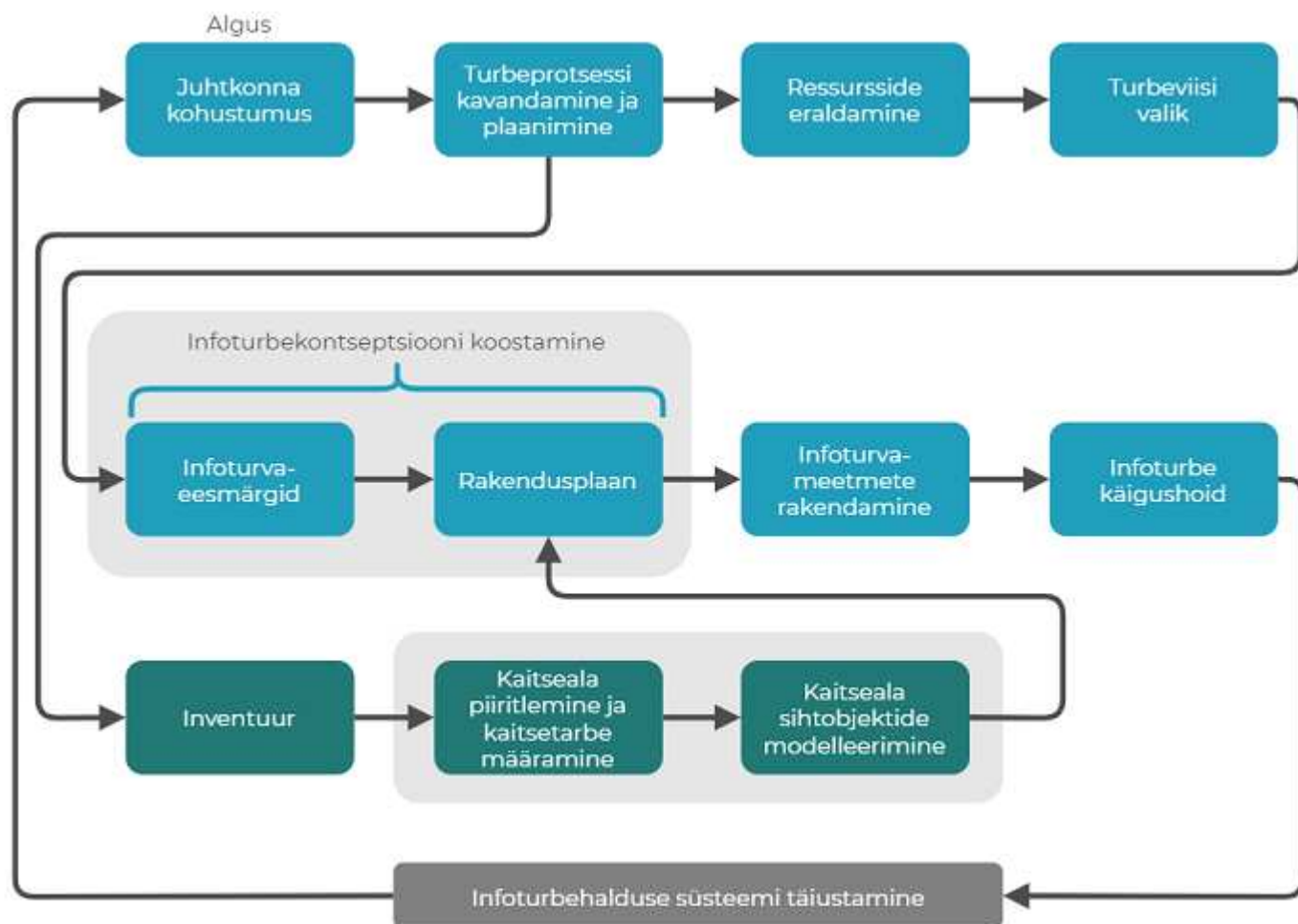
9.1 Infoturbeprotsessi algatamine

Infoturbeprotsess käivitatakse vastavalt dokumendile E-ITS [ISMS. Nõuded](#). Nõuete dokumendis käsitletakse ka infoturbeprotsessi osi, mis ei ole etalonturbeprotsessis kirjeldatud. Etalonturbe protsessile eelneva ettevalmistava sammu kirjeldus on [jaotises 10.1](#).

9.1.1 ISMS käivitamine etalonturbe koosseisus

Joonis 8 kujutab toiminguid, mis tuleb E-ITS rakendamisel sooritada. Sinise värviga on märgitud infoturbe haldussüsteemi üldised elemendid, roheline värviga etalonturbe spetsiifilised tegevused. Varade arvelevõtt on siin tinglikult liigitatud etalonturbe osaks, kuigi seda saab käsitleda ka turbeprotsessi kavandamise ja plaanimise osana.

Kujutatud toimingutest mõningaid saab sooritada ka paralleelselt. Näiteks võib turbeprotsessi kavandamine ja plaanimine toimuda üheaegselt varade arvelevõtu ning infoturbe korralduse loomisega. Sealjuures tuleb hoolitseda, et paralleelselt sooritatavate tegevuste tulemused püsiks koostööaladena.



Joonis 8. Etalonturbe meetoodika sulandumine ISMS raamistikku

9.2 Turbeprotsessi dokumenteerimine

Dokumenteeritud poliitikad, eeskirjad ja protsessijuhendid on infoturbe halduse süsteemi lahutamatu osa, et tagada infoturbe halduse jätkusuutlikkus ka siis kui inimesed vahetuvad või varasemaid otsuseid ununevad.

Dokumente tuleb koostada taasesitatavas, ajakohastamist võimaldavas ning versioonihaldusega kaetud viisil. Eelistada tuleks elektroonilist dokumentatsiooni. Peetakse vaid sellist dokumentatsiooni, mida suudetakse jätkusuutlikult hallata ja uuendada.

Dokumenteerimise abil tagatakse infoturbe protsessi jätkusuutlikkus ja jälgitavus. Näiteks:

- juhtkonna või infoturbejuhi vahetumisel sujuva ülemineku tagamine;
- meetmete rakendamise järjepidev kontrollimine;
- varade ülevaate omamine, sh litsentsidest, teenus- ja tarnelepingutest, tark- ja riistvarast;
- intsidentide asitõendite ja reageerimise otsuste kogumine;
- infoturbe rakendamine protsessides kogu organisatsiooni ulatuses;
- jne.

Organisatsiooni ise kehtestab dokumentide koostamise, vormistamise ja hoidmise reeglid. Juhtkond kinnitab poliitikad ja eeskirjad ning nende muudatused. Üldreeglina vaadatakse poliitikaid ja eeskirju üle vähemalt üks kord aastas. Kordasid ja protseduurijuhendeid uuendatakse koheselt pärast protsessis tehtud muudatusi. Igal dokumendil peaks olema omanik, kelle vastutuseks on dokumendi õigeaegse läbivaatuse, uuendamise ja levitamise korraldamine.

Alusdokumentatsiooni hulka kuuluvad:

- **Poliitikad** – määravad üldised nõuded ja tegevussuunad, kuid ei keskendu üksikute protsesside või tegevuste kirjeldamisele. Poliitika võib olla üldine (nt “Infoturvapoliitika”) või valdkonnapõhine (nt “Võrguturbe poliitika”).
- **Eeskirjad** – poliitikaga vastavuses olevad konkreetset tegevusjuhendid, mis kirjeldavad poliitikate elluviimiseks vajalikke tegevusi, osalejaid ning rolle.
- **Korrad** – kokkulepped teatud protsessi või protsesside jada teostamiseks. **Korrad võivad olla vabamas stiilis ja/või esitatud muu dokumentatsiooni osana.** Teatud juhtudel tuleneb kord organisatsiooni kultuurist (“meil tehakse seda tegevust niimoodi”) ning sel juhul ei esitata korda kirjalikult. Mitte-taasesitatav vorm on aktsepteeritav, kui korra järgimist on võimalik tõendada. Riskide vältimiseks on soovitatav korrad formuleerida kirjalikult.
- **Protsessijuhendid** – esitavad detailsed ja täpsed sammud tegevuste läbiviimiseks. Protsessijuhendid on alati kirjalikud, nad võivad olla mõne nõutud dokumendi osaks või on dokumendi lahutamatuks lisaks (nt IT-süsteemi taasteplaani osana käsitletav varukoopia pealt taastamise protsessi juhend).

Lisaks tuleb luua ja säilitada infoturbeprotsessi tegevusdokumentatsioon, mis tekib protsessi käigus, nt:

- otsused, kavad, plaanid;
- juhtkonnale kommunikeeritud infoturbeteave;
- kaitsetarbe omistamise, järelvalve aktid;
- nõuete, meetmete, intsidentide nimekirjad;
- inventuuride tulemused.

Näidisloetelu organisatsioonis peetavast infoturbealasest dokumentatsioonist on esitatud [Lisa C](#).

9.3 Äriprotsesside ja varade arvelevõtt

Arvelevõtt tähendab, et varad saavad loetletud ja identifitseeritud ning et tuvastatakse nende otstarve, asukoht ja vastutajad.

Varade olemust ja liike selgitatakse [jaotises 4.1](#).

Inventuur sooritatakse kahes järgus. Esmalt võetakse arvele äriprotsessid.

Seejärel võetakse arvele äriprotsessi aluseks olev teave (sh andmekogud), kaitseala sihtobjektid ning nende omavahelised sõltuvused. Arvele tuleb võtta IT-süsteemid, rakendused, taristu, sideühendused, äriprotsessi toimimiseks vajalikud ressursid (nt pädevused, oskused, asutuse välised kontod sh teistes asutustes või sotsiaalmeedias, olulise toorme või sisendteabe lepingud).

Varade arvelevõtuks on soovitatav taaskasutada juba olemasolevaid protsesside ja varade kirjeldusi, inventuuride tulemusi, võrguskeeme, raamatupidamise andmeid vms.

Inventuuri käigus tuleb arvestada ka füüsilisest perimeetrist väljapoole ulatuvaid kasutusviise ja asukohti, sh kaugtöövahendid, pilvteenused jms.

Inventuuri käigus kogutakse vähemalt järgmised andmed:

- äriprotsessi nimetus ja vajadusel selgitav lühikirjeldus;
- äriprotsessi eest vastutav üksus;
- äriprotsessi alusteave;
- IT-süsteemide nimetused, platvormid, paigalduskohad;
- virtuaalsed IT-süsteemid;
- rakenduste nimetused ja otstarve;
- füüsilised ja virtuaalsed võrgud (sideühendused);
- automaatikasüsteemide nimetused ja otstarve;
- muud asjassepuutuvad objektid;
- ruumid: liik, number, hoone.

Loenduse käigus tuleb koostada kaitsealasse kuuluvate võrkude skeem.

9.3.1 Äriprotsesside arvelevõtt

Äriprotsesside arvelevõtu tulemusel saab organisatsioon struktureeritud ülevaate oma äriprotsessidest ning esmase pildi äriprotsessides kasutatavast teabest. Tuvastatakse äriprotsesse teenindavad rakendused, andmekogud või andmebaasid. Äriprotsesside kaardistus on oluline sisend kaitseala määratlemisel.

Äriprotsesside arvelevõtmisel:

- koostatakse äriprotsesside loetelu, sh kirjeldus, protsessijuht või kontaktisik, esialgne turbealane informatsioon;
- tuvastatakse äriprotsesside poolt vajatav alusteave, sh teabevoos tehniline allikas (teenus, andmekogu, andmebaas vms), sh väliste partnerite omad, teabeallika valdaja või kontaktisik;
- tuvastatakse äriprotsesside seosed neid teenindavate rakenduste ja andmeallikatega;

Informatsioon äriprotsesside kohta kogutakse protsessijuhtide ja juhtkonna abiga. Tehniliste varade arvelevõtt toimub järgimises etapis.

9.3.2 Alusteabe ja sihtobjektide arvelevõtt

Varade arvelevõtu eesmärgiks on tuvastada ja detailselt arvele võtta äriprotsesside alusteave ning äriprotsesse teenindavad varad (sh andmekogud). Etalonturbes vaadeldakse edaspidi neid turvameetmete **sihtobjektidena**.

Arvelevõtmise sisendina kasutatakse eelnevas etapis äriprotsesside kohta kogutud infot ja seoseid. Arvelevõtmisel registreeritakse sh:

- **sihtobjekti nimetus,**
- **unikaalne tunnus,**
- **vastutajad ning kontaktisikud,**
- **seosed teiste sihtobjektidega,**
- **piirangud ja märkused.**

9.3.2.1 Äriprotsesside alusteave

Äriprotsesside aluseks olevad andmekogud, andmeallikad ja andmebaasid registreeritakse, sh andmeallika liik (andmebaas, andmeteenus, andmekogu vms), andmete liik (nt isikuandmed, ärisaladus). Arvele võetakse ka kõik pilvteenustes talletatavad andmed.

9.3.2.2 IT süsteemid ja rakendused

Võetakse detailselt arvele kõik IT-süsteemid ja rakendused. Inventuuril kaasatakse rakenduste pea- ja lõppkasutajaid. Tehakse järgmist:

- tuvastatakse ja registreeritakse rakendused, mida käsitletav äriprotsess vajab;
- võetakse arvele virtuaalsed või pilves peetavad rakendused;
- kaardistatakse andmeallikad, IT süsteemid ja teenused, millele rakendus tugineb;
- selgitakse välja võimalikud mitteametlikud andmeallikad ja IT süsteemide seosed, sh andmed, mida töötaja hangib käsitsi või peab omaalgatuslikult, näiteks töökohaarvutis või pilves, sh töölase rolliga seotud sotsiaalmeedia kontod.

Rakenduste uurimisel tuvastatakse sageli täiendavaid andmeallikaid, mida äriprotsesside uurimisel ei märgatud. See on tingitud asjaolust, et äriprotsesse ja IT-süsteeme haldavad eri isikud.

9.3.2.3 Sideühendused

Tuleb arvele võtta nii füüsilised kui virtuaalsed ühendused. Hõlmata tuleb nii universaalteenused kui sihtotstarbelised ühendused (üüriliinid, raadioligid). Ühenduste hulka liigitatakse ka raadioeetrit või avalikku teenust kasutavad ühendused (WiFi, WiMax, mobiilside). Tehakse järgmist:

- ühendused võetakse arvele ja vajadusel dokumenteeritakse ka graafiliselt;
- tuvastatakse missioonikriitilise teabe edastuseks ning missioonikriitiliste äriprotsesside teenindamiseks kasutatavad ühendused;
- märgistatakse missioonikriitilised ühendused sellistena.

9.3.2.4 Muud olulised ressursid

Arvele tuleb võtta töötajate oskused ja kvalifikatsioon, mis on vajalikud äriprotsessi sooritamiseks. Seda tehakse äriprotsessi, mitte isikuandmete põhisel (nt ametikoha kirjeldused või ametijuhendid).

Juhul kui äriprotsessid olenevad välistest teenustest, siis on vaja arvele võtta nii teenused kui ka nende aluseks olevad lepingud. Inventuurile lisatakse kokkuvõtte lepingutega tagatud ressurssidest ja organisatsiooni lepingulistest kohustustest.

9.3.2.5 Muud sõltuvused

Alljärgnevalt loetletakse sihtobjektid, mille arvelevõtmise vajadus pole alati ilmne.

Võrguskeemi koostamisel kasutatakse olemasolevaid arvutivõrgu skeeme neid vajadusel ajakohastades ja täiendades. Vajadusel lisatakse või koostatakse eraldi võrguskeemid muude võrkude sh automaatika- ja esemevõrgusüsteemide (IoT, sh ka ventilatsiooni-, kütte- või muud seireandurid), valvekaamera- ning pääslasüsteemid kohta.

Tehniliste süsteemide ja seadmete arvelevõtt ei piirdu klassikaliste arvutite, serverite ja võrguseadmetega. Arvele tuleb võtta ka nn muud seadmed, s.t. tööstusautomaatika (ICS / SCADA), esemevõrgu (IoT) seadmed, automaatikaseadmed, videovalve- ja läbipääsusüsteemid, valvesignalisatsioon jne. Seadmed seostatakse teiste sihtobjektidega, sh serverid, võrgud, rakendused jms.

Võetakse arvele nii kontori-, lao- ja tootmisruumid kui ka tugiteenuste (ventilatsioon, pääsla) osutamiseks kasutatavad ruumid. Tuleb:

- lisada inventuurinimekirja IT-, automaatika- ja esemevõrgusüsteemide toimimiseks vajalikud kinnistud, hooned ja ruumid;
- võtta arvele muud ruumid, kus/kuhu talletatakse või kus muul viisil käideldakse kaitset vajavat informatsiooni (nt varukoopiate seifi asukoharuum);
- märkida üles iga ruumi asukoht, iseärasused ning vastutajad;
- vajadusel määratleda kaugtöö asukohad või kodukontorid üldnimetusena, mis seostatakse nendes asukohtades kasutamiseks mõeldud sihtobjektidega.

10 Etalonturbe protsess

Etalonturbe protsess on esitatud sammudena. Protsessi läbitakse tsükliliselt.

Infoturbejuht koordineerib sammude läbimist vastavalt valitud turbeviisile (vt [jaotis 8](#)).

Iga sammu alguses on loetletud peamised osalejad, tegevused, sisendid ja väljundid. Infoturbejuht osaleb vajadusel igas sammus konsultandina.

Dokumentide tähised ja selgitused on esitatud [Lisa C](#).

10.1 Ettevalmistused etalonturbeks ja varade arvelevõtt

Osalejad	Juhtkond, infoturbejuht, protsessijuhid, IT-talitus
Sisend	
	E-ITS ISMS. Nõuded
	Regulatsioonid
	Infoturbedokumentatsioon, teenuslepingud, intervjuud, vaatlused, kaardistus
	T06 Iga üksiku (arvelevõetud) äriprotsessi üksikasjad
	T08 Olulised lepingud partnerite ja klientidega
Tegevused	
	Infoturbe algatamine organisatsioonis
	ISMS nõuetega tutvumine, ISMS käivitamine
	Turvapoliitika ja -eesmärkide koostamine - esialgsed versioonid või olemasoleva täiendamine
	Analüüs, intervjuud, vaatlused, kaardistamine
	Äriprotsesside ja varade arvelevõtt
Väljund	
	N01 N01.1 Infoturvapoliitika ja -eesmärgid – esialgsed versioonid või olemasoleva täiendamine
	N02 Infoturbeprotsessi kontseptsioon
	N03 Varade loetelu (ja nende omavahelised seosed)
	N04 Ebatraditsiooniliste varade loetelu
	N08 Infoturbe korraldusstruktuuri kirjeldus
	N12 Võrguskeem
	T06 Iga üksiku (arvelevõetud) äriprotsessi üksikasjad
	T10 Infoturbe ja turbeprotsessi kohta tehtud otsused

Lisainfo:

Organisatsiooni infoturbeprotsessi algatamisel ja täiendamisel tuleb lähtuda dokumendist E-ITS [ISMS. Nõuded](#). Lühidalt on ISMS käivitamist kirjeldatud [jaotistes 9.1 ja 9.2](#).

Etalonturbe protsess eeldab, et läbi on viidud järgnevad tegevused:

- on tutvunud dokumendiga E-ITS [ISMS. Nõuded](#), et aru saada infoturbehalduse olemusest;
- juhtkond on võtnud infoturbe alal kohustumuse;
- on valitud turbeviis (põhi-, standard- või tuumikuturve, vt [jaotis 7](#));
- on koostatud turvapoliitika, dokumenteerimise põhimõtted (vt [jaotis 9.2](#));
- on heaks kiidetud infoturbekorraldus ja organisatsioonile vajalikud rollid (vt rollide nimekiri [Lisa D](#));
- juhtkond on võimaldanud ISMS rakendamiseks vajalikud ressursid – personal, aeg (sh koolitused), töövahendid. Meetmete rakendamise eelarve koostatakse ja kinnitatakse [sammus 5](#).

Otsused dokumenteeritakse.

Varade olemust selgitab ja varade liigid loetleb [jaotis 4.1](#). Juhised varade arvelevõtuks on kirjeldatud [jaotises 9.3](#).

Varade arvelevõtu käigus:

- kaardistatakse äriprotsessid;

- võetakse arvele varad, sh äriprotsesside aluseks olev teave, andmekogud, süsteemid, rakendused, taristu, ruumid, ressursid ja tarne- ning teenuslepingud;
- dokumenteeritakse äriprotsessid ja seosed varade vahel, sh äriprotsesside omavahelised seosed; äriprotsesside seosed varadega; varade omavahelised seosed, sh võrguskeem.

Varade arvelevõtuks on soovitatav taaskasutada juba olemasolevaid protsesside ja varade kirjeldusi, inventuuride tulemusi, võrguskeeme, raamatupidamise andmeid vms.

Arvelevõtu detailsus ja ajakohasuse hoidmine peaks vastama organisatsiooni vajadustele ja nõuetele. Infoturbeprotsessi käigus võib varade loetelu täieneda või muutuda.

Inventuuri käigus tuleb arvestada ka füüsilisest perimeetrist väljapoole ulatuvaid kasutusviise ja asukohti, sh kaugtöövahendid, pilvelahendused jms.

10.2 Samm 1 – kaitseala piiritlemine

Osalejad	Protsessijuhid, juhtkond
Sisend	
	N01 N01.1 Infoturvapoliitika ja -eesmärgid
	N03 Varade loetelu (ja nende omavahelised seosed)
	N04 Ebatraditsiooniliste varade loetelu -- koos äriprotsesside ning varade seostega
	N12 Võrguskeem
Tegevused	
	Kaitseala koosseisu kuuluvad sihtobjektide määratlemine
	Kaitseala sihtobjektide loetelu dokumenteerimine
Väljund	
	N02 Infoturbeprotsessi kontseptsioon
	N07 Kaitseala kirjeldus – sihtobjektide loetelu

Lisainfo:

Kaitsealaks nimetatakse turvapoliitika käsitlusala, mille ulatuses rakendatakse turvameetmed. Kaitseala moodustamiseks piiritletakse loetelu äriprotsessidest, IT süsteemidest, rakendustest, ressurssidest ja sõltuvustest (sh liidestused välispartneritega). Etalonturbes nimetatakse kaitsealasse kuuluvaid varasid **sihtobjektideks**.

Etalonturbe protsessi järgmistes sammudes käsitletakse vaid neid sihtobjekte, mis on määratud kaitseala koosseisu.

Tuumikuturbe korral piiritletakse tervikkaitseala ning eraldi kaitseala varade tuumiku osas.

Kaitseala tuleb üheselt määratleda ja sellisena dokumenteerida.

10.3 Samm 2 – kaitseala struktuurianalüüs

Osalejad	Protsessijuhid, IT-talitus
Sisend	
	N01 N01.1 Infoturvapoliitika ja -eesmärgid
	N07 Kaitseala kirjeldus
Tegevused	
	Sihtobjektide tähtsuse analüüs äriprotsesside jaoks

	Sihtobjektide rühmitamine
Väljund	
	N02 Infoturbeprotsessi kontseptsioon – täpsustamine
	N07 Kaitseala kirjeldus -- sihtobjektide loetelu täpsustamine

Lisainfo:

Struktuurianalüüsi eesmärgiks on tagada, et kaitsetarbe määramisel oleks piisav ettekujutus kaitseala koosseisust ja keerukusest. Struktuurianalüüsi tulemuste põhjal määratletakse sihtobjektide kaitsetarve ning asutakse sihtobjekte modelleerima (vt [jaotis 10.5](#)).

Struktuurianalüüs vaatleb arvelevõetud äriprotsesse, teavet ja sihtobjekte kogumis ning koos toimiva infoturbe korraldusega. Kogumit analüüsitakse, et mõista sihtobjektide tähendust äriprotsesside võtmes. Analüüsi tulemusi kasutatakse turbekontseptsiooni täpsustamiseks.

Sarnased sihtobjektid rühmitatakse (näiteks sarnaseid ülesandeid täitvad Linuxi serverid). See võimaldab lihtsustada sarnaste sihtobjektidega tehtavaid tegevusi järgnevates sammudes. Rühmitatud sihtobjektide tüüp ja koosseis tuleb dokumenteerida. Rühmitamisel võib juhinduda etalonoturbe kataloogi moodulite loendist.

Dokumenteerituse detailsus peab vastama kaitsetarbe määramise vajadusele.

10.4 Samm 3 – kaitsetarbe määramine

Osalejad	Protsessijuhid
Sisend	
	N01 N01.1 Infoturvapoliitika ja -eesmärgid
	N05 Infoturbe aluskomponentide valik
	N07 Kaitseala kirjeldus -- sihtobjektide loetelu
	Kahjustsenaariumide küsimustik (Lisa B)
Tegevused	
	Äriprotsesside ja teabe esmase kaitsetarbe täpsustamine
	Sihtobjektide kaitsetarbe määramine (seadmed ja süsteemid; ruumid jne)
	Kõrgema kaitsetarbega sihtobjektide: koondamine turvatsoonidesse/ suunamine välisesse riskihaldusse
Väljund	
	N07 Kaitseala kirjeldus -- sihtobjektide loetelu täiendamine kaitsetarbega
	T22 Äriprotsessidele kaitsetarbe kinnitamise akt

Lisainfo:

Kaitsetarve väljendab organisatsiooni äriprotsessides töödeldava teabe konfidentsiaalsuse, tervikluse ja käideldavuse vajadust. Kaitsetarbe tasemed on kirjeldatud [jaotises 5.2](#). Sihtobjektidele määratakse rakendatavad turvameetmed kaitsetarbe alusel.

Kaitsetarbe määramisel võib arvestada ka infoturbe täiendavaid komponente, vt [jaotis 5.1](#).

Äriprotsessi ja temaga seostatud teabe kaitsetarbe määratlemisel tehakse järgmist:

- Veendutakse, kas esmane kaitsetarve on asjakohane.
- Äriprotsessidele ja teabele esitatud nõuete ning kahjustsenaariumide küsimustiku ([Lisa B](#)) abil kontrollitakse kaitsetarbe asjakohasust.

- Äriprotsesside kaitsetarve "pärandatakse" sihtobjektidele. Mitut äriprotsessi teenindavale sihtobjektile määratakse kõrgeim kaitsetarve. Siinjuures arvestatakse sihtobjektide omavahelisi sõltuvusahelaid ja koostoimeid.
- Kaitsetarbe määrangud koos põhjendustega dokumenteeritakse.

Kui äriprotsessi sihtobjektide hulgas on mõni andmekogu, tuleb kaitsetarbe määramisel arvestada selle turvaklassi.

Kaitsetarbe määratlus sihtobjektidele infoturbe komponentide (C-I-A) suhtes võib osutada oluliseks mõne meetme rakendamisel, kus see on eraldi mainitud etalonmeetme sees. Lisaks on komponentide haaval määratletud kaitsetarve oluline kõigi suure ja väga suure kaitsetarbega sihtobjektidele etalonturbe välise riskihalduse läbiviimisel ja meetmete väljatöötamisel.

Kaitsetarbe määramise tulemused dokumenteeritakse koos põhjendustega.

10.5 Samm 4 – kaitseala modelleerimine ja meetmete tuvastamine

Osalejad	Infoturbejuht
Sisend	
	E-ITS Etalonturbe kataloog
	E-ITS Alusohitude kataloog
	N02 Infoturbeprotsessi kontseptsioon (turbekontseptsioon)
	N07 Kaitseala kirjeldus
Tegevused	
	Sihtobjektide vastendamine etalonturbe kataloogi moodulitega
	Sihtobjektidele moodulitest meetmete tuvastamine vastavalt turbeviisile ja kaitsetarbele (vajadusel tsoneerimine kaitsetarbist lähtudes)
	Vajadusel sihtobjektide suunamine välisesse riskianalüüsi
Väljund	
	T02 Turbekontseptsiooni rakendusplaan – meetmete, sihtobjektide ja vastutajate seosed, sihtobjektide suunamine välisesse riskianalüüsi, tsoneerimise otsused
	T03 Moodulite kinnis(ta)tus sihtobjektidele
	T11 Infoturvameetmete nimekiri – võib olla T02 rakendusplaani osa

Lisainfo:

Modelleerimise käigus tuvastatakse etalonturbe kataloogist vajalikud moodulid ning seatakse need vastavusse sihtobjektidega. Etalonturbe kataloogi kõik protsessimoodulid käsitletakse väljajäetudeta. Süsteemimoodul rakendatakse, kui kaitsealas on vastavad sihtobjektid esindatud.

Moodulite ülesehitust ning kasutamise suuniseid kirjeldatakse [jaotises 6.2](#).

Modelleerimise käigus:

- Tutvutakse moodulis toodud ohtude nimekirjaga, et aru saada moodulis sisalduvate meetmete eesmärkidest.
- Vastendatakse moodulid ja sihtobjektid. Protsessimoodulite sihtobjektideks on reeglina organisatsiooni protsessid.

Meetmete tuvastamisel:

- Moodulist tuvastatakse turbeviisile vastavad meetmed ja märgitakse need rakendusplaani koos rakendamise eest vastutajatega. Põhiturbe puhul kuuluvad rakendamisele põhimeetmed, standardturbe korral nii põhi- kui standardmeetmed.
- Kui sihtobjekti kaitsetarve on suur (S) või väga suur (VS), siis hinnatakse lisaks põhi- ja standardmeetmetele kõrgmeetmete piisavust. Suure kaitsetarbe puhul piisab enamasti etalonturbe kataloogi meetmetest. Väga suure kaitsetarbe puhul võivad riskihalduse tulemusena lisanduda lisaturvameetmed.

Meetme sihtobjektile mitesobivuse otsus (meede ei ole asjakohane) dokumenteeritakse.

Etalonturbe välisesse riskihaldusse suunamise toimub kui täidetud on vähemalt üks tingimus:

- sihtobjekti kaitsetarve on **suur** või **väga suur**;
- ilmnenu on ohud, mida mooduli ohtude sektsioon ei käsitle;
- kasutatakse tehnoloogiaid, mida moodulid ei kata;
- sihtobjekti kasutatakse viisil, mida moodulid ei kata;
- kui meede eeldatavalt ei tõrju ohtu.

Rakendusplaanis kajastatakse moodulite, sihtobjektide ja meetmete seosed ning rakendamise eest vastutajad.

Rakendusplaani võib pidada tabelina, sisuhalduskeskkonnas või muus struktureeritud vormis.

10.6 Etalonturbe väline riskihaldus

Osalejad	Protsessijuht
Sisend	
	E-ITS Etalonturbe kataloog
	Riskihaldusjuhend
	T02 Turbekontseptsiooni rakendusplaani
	N01 N01.1 Infoturvapoliitika ja -eesmärgid
	N02 Infoturbeprotsessi kontseptsioon (turbekontseptsioon)
	N07 Kaitseala kirjeldus
Tegevused	
	Riskianalüüs
Väljund	
	Lisaturvameetmed

Lisainfo:

Etalonturbe välise vahetu riskihalduse ülesanne on riskianalüüsile tuginedes määrata lisaturvameetmed. Etalonturbe väline riskihaldus viiakse läbi vastavuses E-ITS riskihaldusjuhendiga.

10.7 Samm 5 – turvameetmete kinnitamine

Osalejad	Organisatsiooni juhtkond, protsessijuhid, infoturbejuht, IT-talitus
Sisend	
	N02 Infoturbeprotsessi kontseptsioon (turbekontseptsioon)
	T02 Turbekontseptsiooni rakendusplaani.
	Lisaturvameetmed
Tegevused	
	Lisaturvameetmete sobivuse hindamine ja rakendusplaani lisamine

	Meetmete teostusjärjekorra määramine
	Meetmete rakendamiseks vajalike ressursside ja kulude hindamine
	Rakendusplaani, teostusjärjekorra ja eelarve kooskõlastamine
Väljund	
	T02 Turbekontseptsiooni rakendusplaan – täiendatud: lisaturvameetmed, kulud, jääkriskid
	T04 Turvameetmete teostusjärjestus – võib sisalduda T02 rakendusplaanis
	T11 Infoturvameetmete nimekiri -- võib sisalduda T02 rakendusplaanis
	T10 Infoturbe ja turbeprotsessi kohta tehtud otsused

Lisainfo:**Lisaturvameetmete ühendamine rakendusplaaniga**

- kontrollitakse lisandunud meetmete sobivust, kategooriaid vt [jaotisest 5.4](#);
- kontrollitakse lisaturvameetme vastavust infoturbepoliitika ja -eesmärkidega.

Riskianalüüsi tulemusel määratud lisameetmed lisatakse senisele rakendusplaanile.

Meetmete teostusjärjestuse plaanimiseks

- rühmitatakse või koondatakse sarnased meetmed;
- määratakse ja põhjendatakse turvameetmete teostusjärjestus, arvestades meetmete ja sihtobjektide omavahelisi sõltuvusi ja võimalikult kiiret turvakasu;
- määratakse asendavad turvameetmed neile, mida ei ole võimalik teostada.

Meetmete teostusjärjestus dokumenteeritakse.

Eelarve koostamine ja jääkriskide hindamine

- hinnatakse teostatavatele turvameetmetele **ühekordsed ja korduvad kulud** (sh rahalised ja mitterahalised);
- hinnatakse mitteteostatavate meetmete põhjustatud ja muud jääkriskid;
- riskiomanikud (protsessijuhid) aktsepteerivad jääkriskid.

Talumatu jääkriski ilmnemisel võib olla tarvilik tagasi pöörduda etaloniturbe välise riskihalduse sammu algusse.

Juhtkond teadvustab ja aktsepteerib jääkriskid ning kinnitab rakendusplaani ja eelarve.

10.8 Samm 6 – turvameetmete rakendamine

Osalejad	Protsessijuhid, IT-talitus, infoturbejuht
Sisend	
	Etaloniturbe kataloog – meetmete kirjeldused
	T02 Turbekontseptsiooni rakendusplaan
	T04 Turvameetmete teostusjärjestus
	T05 Rakendusplaani järelevalve kava
	T11 Infoturvameetmete nimekiri
	N07 Kaitseala kirjeldus
	N08 Infoturbe korraldusstruktuuri kirjeldus
Tegevused	

	Rakendusplaani elluviimine ja elluviimise koordineerimine
	Meetmete elluviimise jälgitavuse tagamine
	Meetmete teavitus- ja koolitustegevus
	Infoturbekontseptsiooni täiustamine – vajadusel
Väljund	
	T02 Turbekontseptsiooni rakendusplaani – täiendamine rakendatuse ja muutuste osas
	T11 Infoturvameetmete nimekiri
	Infoturbedokumentatsioon, selle loomine ning täiendamine turvapoliitikale ja -eesmärkidele vastavas ja organisatsioonile vajalikus ulatuses

Lisainfo:

Turbekontseptsiooni teostus tähendab kataloogist tuvastatud meetmete ja lisaturvameetmete elluviimist (rakendamist) vastavalt infoturvaeesmärkidele ning rakendusplaanile.

Muuhulgas:

- koolitatakse meetmetest mõjutatud personali, et tõsta personali teadlikkust;
- tagatakse infoturvaeesmärkide mõõtmise (seire);
- tagatakse tegevuste regulaarsus vastavalt meetme kirjeldusele ning organisatsiooni vajadustele (suurusest ja spetsiifilisest lähtuvalt);
- turbeta tegevused dokumenteeritakse organisatsioonile vajalikus ulatuses;
- koordineeritakse turvameetmete teostamise käiku ja tähtaegadest kinnipidamist;
- seiratakse teostatud turvameetmete toimivust ja tõhusust; kontrollitakse, kas turvameetmeid aktsepteeritakse; vajadusel tehakse plaanides korrektsioone;
- tagatakse turbeta tegevuste ja nende tulemite konfidentsiaalsus.

Meetmete rakendatuse määra infot hoitakse rakendusplaanis ajakohasena (vt [jaotis 5.5](#)).

10.9 Samm 7 – turbe käigushoid

Osalejad	Protsessijuhid, IT-talitus, infoturbejuht
Sisend	
	Infoturbe dokumentatsioon
	N01 N01.1 Infoturvapoliitika ja -eesmärgid
	N07 Kaitseala kirjeldus
	N08 Infoturbe korraldusstruktuuri kirjeldus
	T02 Turbekontseptsiooni rakendusplaani
	T05 Rakendusplaani järelevalve kava
	T11 Infoturvameetmete nimekiri
Tegevused	
	Ohuinfo ja kohustuste muutumise jälgimine ning sellele reageerimine
	Pidev meetmete ja ISMS toimivuse jälgimine
	Regulaarne juhtkonna teavitamine infoturbe olukorrast
Väljund	
	N01 N01.1 Infoturvapoliitika ja -eesmärgid – täiustamise ettepanekud
	N02 Infoturbeprotsessi kontseptsioon (turbekontseptsioon) – täiustamise ettepanekud
	T02 Turbekontseptsiooni rakendusplaani – parandused, täiendused
	T09 Juhtkonnale kommunikeeritud infoturvateave

	T11 Infoturvameetmete nimekiri – parandused, täiendused
	T12 Infoturbe (seisu) ülevaatus
	Infoturbe dokumentatsiooni täiustamise otsus

Lisainfo:

Käigushoid on pidev ja paralleelne tegevus, seda ei katkestata infoturbeprotsessi teiste sammude läbimisel.

Ohusituatsiooni või raamtingimuste muutumisel tuleb turbekontseptsiooni (ning sellest tulenevalt ka turvameetmeid) vastavalt muuta või kohandada.

Infoturbe käigushoidmiseks ja pidevaks täiustamiseks, tuleb muuhulgas:

- teadvustada ning võimalusel vältida meetme teostaja ja kontrollija rollide konflikti;
- seirata ning perioodiliselt kontrollida organisatsiooni turvaeesmärkide ja turbeviisi sobivust ja ajakohasust;
- perioodiliselt kontrollida ressursside kasutamist ning turvameetmete tõhusust ja kuluefektiivsust;
- kontrollida välise riskihalduse protsessi toimivust, kui selline protsess on alatatud;
- infoturbekontseptsioonist lähtudes (sh regulaarsus, eesmärk) töödelda ning analüüsida logiinfot (tegevusinfo, süsteemiinfo, võrguinfo, ründeinfo) ning selle põhjal tuvastada ja uurida kõrvalekaldeid, intsidente ja täiustada turvameetmeid;
- jälgida üldist turbesituatsiooni, kasutatavate toodete turva- ja uuendusteavitusi;
- suunata järeldused seire ja kontrollide tulemustest täiustustena tagasi infoturbeprotsessi;
- hoida juhtkonda regulaarselt kursis infoturbe olukorraga.

Infoturbedokumentatsiooni ajakohastatakse organisatsioonile vajalikus ulatuses.

10.10 Samm 8 – infoturbeprotsessi täiustamine

Osalejad	Infoturbejuht, juhtkond
Sisend	
	Täiustamise ettepanekud
	T12 Infoturbe (seisu) ülevaatus
	N01 N01.1 Infoturvapoliitika ja -eesmärgid
	N02 Infoturbeprotsessi kontseptsioon (turbekontseptsioon)
Tegevused	
	Infoturbe täiustamise ettepanekute läbivaatus
	Turbekontseptsiooni ja turbeviisi muutmise otsused
	Ettevalmistus uueks etalonturbe tsükliks
Väljund	
	T10 Infoturbe ja turbeprotsessi kohta tehtud otsused

Lisainfo:

Organisatsiooni turbekontseptsiooni tuleb uuendada vastavalt äriprotsesside ning nende kasutatavate varade muutustele. Olulised muutused turbekontseptsioonis tähendavad naasmist etalonturbe protsessi algusse ning kogu infoturbeprotsessi uuendamist uutel eeldustel.

Turbekontseptsiooni uuendamisel võib olla tarvis uuendada ka etalonturbe välist riskihaldusprotsessi, kui see on kasutusel.

Kohustuslik on tagada põhiturbe rakendamine, aga eesmärgiks on standardturbe rakendamine ja infoturbe pidev täiendamine. Turbeviiside kirjeldust vt [jaotis 7](#).

10.11 E-ITS auditeerimine

Osalejad	Auditirühm (sise- või välisaudiitor), protsessijuhid, juhtkond, infoturbejuht
Sisend	
	Infoturbe dokumentatsioon, intervjuud, vaatlused
	E-ITS-J3 Auditeerimisjuhend
	Alusotude viitetabel
	T12 Infoturbe (seisu) ülevaatus
Tegevused	
	Auditi plaanimine
	Auditi läbiviimine
	Järeltegevused (parandustegevused, vajadusel järelaudit)
Väljund	
	T13 Kontrollide (nii sisemiste kui välimiste) tulemused
	Auditiraport ja -kinnitus sõltumatult osapoolelt

Lisainfo:

Organisatsiooni infoturbehaldust auditeeritakse dokumendi E-ITS [ISMS. Nõuded](#) alusel. Auditeeritakse infoturbe halduse süsteemi toimivust, mitte meetmete komplekti. Auditeerimist käsitleb E-ITS [Auditeerimisjuhend](#) ja DER moodul. Audiitori hinnang on kasutatav tõendina partnerile või järelevalve organisatsioonidele infoturbe teostuse olukorra ja riskide realiseerumisel toimetuleku võimekuse kohta.

10.12 ISO/IEC 27001 vastavuse sertifitseerimine

Osalejad	Välisaudiitor, juhtkond, sertifitseerimisorganisatsioon
Sisend	
	Infoturbe dokumentatsioon
	ISO/IEC 27001
Tegevused	
	Auditi plaanimine (eelnevalt veenduda ISO/IEC 27001 vastavuses, vajadusel täiendada ISMSi)
	Auditi läbiviimine
	Järeltegevused (parandustegevused, vajadusel järelaudit)
Väljund	
	Rahvusvaheliselt tunnustatud infoturbe halduse toimimist kinnitav sertifikaat parandusettepanekud

Lisainfo:

Sertifitseerimine toimub **vaid** organisatsiooni enda soovil või välistest nõuetest tulenevalt. Rahvusvahelise infoturbe halduse sertifikaadi saamiseks tuleb organisatsioonil taotleda oma äriprotsesside sertifitseerimist standardi ISO/IEC 27001 nõuete vastu. Sertifikaadi taotlemine ja säilitamine on juhtkonna otsus ja infoturbe strateegiline eesmärk.

11 Lisateave

[E-ITS ISMS. Nõuded](#)

[E-ITS Riskihaldusjuhend](#)

E-ITS Etalonturbe kataloog, vaata <https://eits.ria.ee/>

[E-ITS Auditeerimisjuhend](#)

[E-ITS Rakendusjuhend](#)

[E-ITS Alusotude kataloog](#)

[E-ITS Alusotude viitetabel](#)

Eesti infoturbestandard. Etalonturbe kataloog. [ISMS.1: Turbehaldus](#)

BSI IT Grundschutz - https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html

[ISO/IEC 27001:2017 Infotehnoloogia. Turbemeetodid. Infoturbe halduse süsteemid. Nõuded](#)

ISO/IEC 27005

[Standardi terminoloogiasõnastik](#)

Lisa A Etalonturbe kataloogi ülevaade

Hierarhiline ülevaade etalonturbe moodulitest on järgnevalt esitatud piltidena. Puu vasakus harus on kujutatud protsessimoodulid, paremas harus süsteemimoodulid.

[Protsessimoodulid](#)

[Süsteemimoodulid](#)

Lisa B Kahjustsenaariumide küsimustik

(Mugandatud tõlge standardist BSI 200-2)

Infoturvaohht võib lisaks tehniliste nõrkuste ärakasutamisele realiseeruda palju laiema valiku stsenaariumide järgi. Järgnevalt on esitatud kahjustsenaariumide põhised näidisküsimused, mis aitavad määrata kaitsetarvet.

Neid küsimusi tuleks organisatsiooni iseärasuste põhjal sobitada ja vajadusel täiendada.

Allpool on vaadeldud kuut kahjustsenaariumi:

- [01 - õigusaktide, eeskirjade või lepingute rikkumine;](#)
- [02 - isiku teabelise enesemääramisõiguse rikkumine;](#)
- [03 - isiku füüsilise puutumatuse rikkumine;](#)
- [04 - ülesannete täitmise võime kahjustamine;](#)
- [05 - sisemised või välised negatiivsed toimed;](#)
- [06 - rahalised tagajärjed.](#)

Lisa C Dokumentatsiooni näidisloend

Näidisloetelu on tinglikult jagatud kaheks.

- [Alusdokumentatsioon](#) – poliitikad, põhimõtted, liigitusastmikud jne.

- [Tegevusdokumentatsioon](#) – otsused, operatiivne dokumentatsioon, infoturbeintsidentide materjalid, läbivaatuste ja ülevaatuste aktid jne.

Märkus: Loetelu on orienteeritud keskmisele ja suuremale organisatsioonile. Väiksematel organisatsioonidel tuleb loetelu optimeerida ja dokumente kombineerida.

Lisa D Rollide nimekiri

[Rollisõnastik](#)

[Lisa D Rollide nimekiri](#)

Lisa A Moodulid puukujuliselt

Lisa A Etalonturbe kataloogi ülevaade

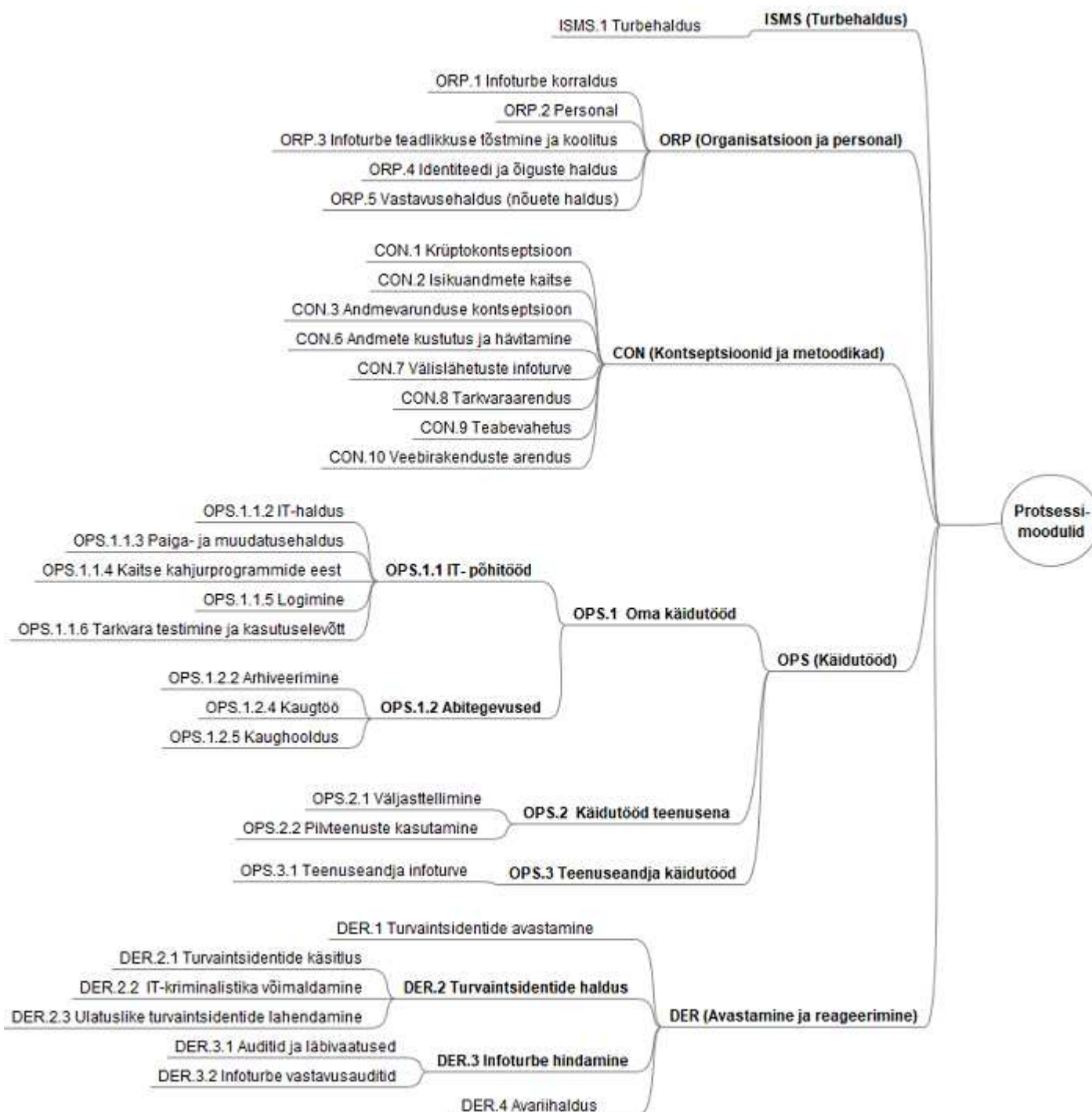
Hierarhiline ülevaade etalonturbe moodulitest on järgnevalt esitatud piltidena. Puu vasakus harus on kujutatud protsessimoodulid, paremas harus süsteemimoodulid.

Sisukord

[Joonis A 1. Etalonturbe moodulid puukujuliselt. Protsessimoodulid](#)

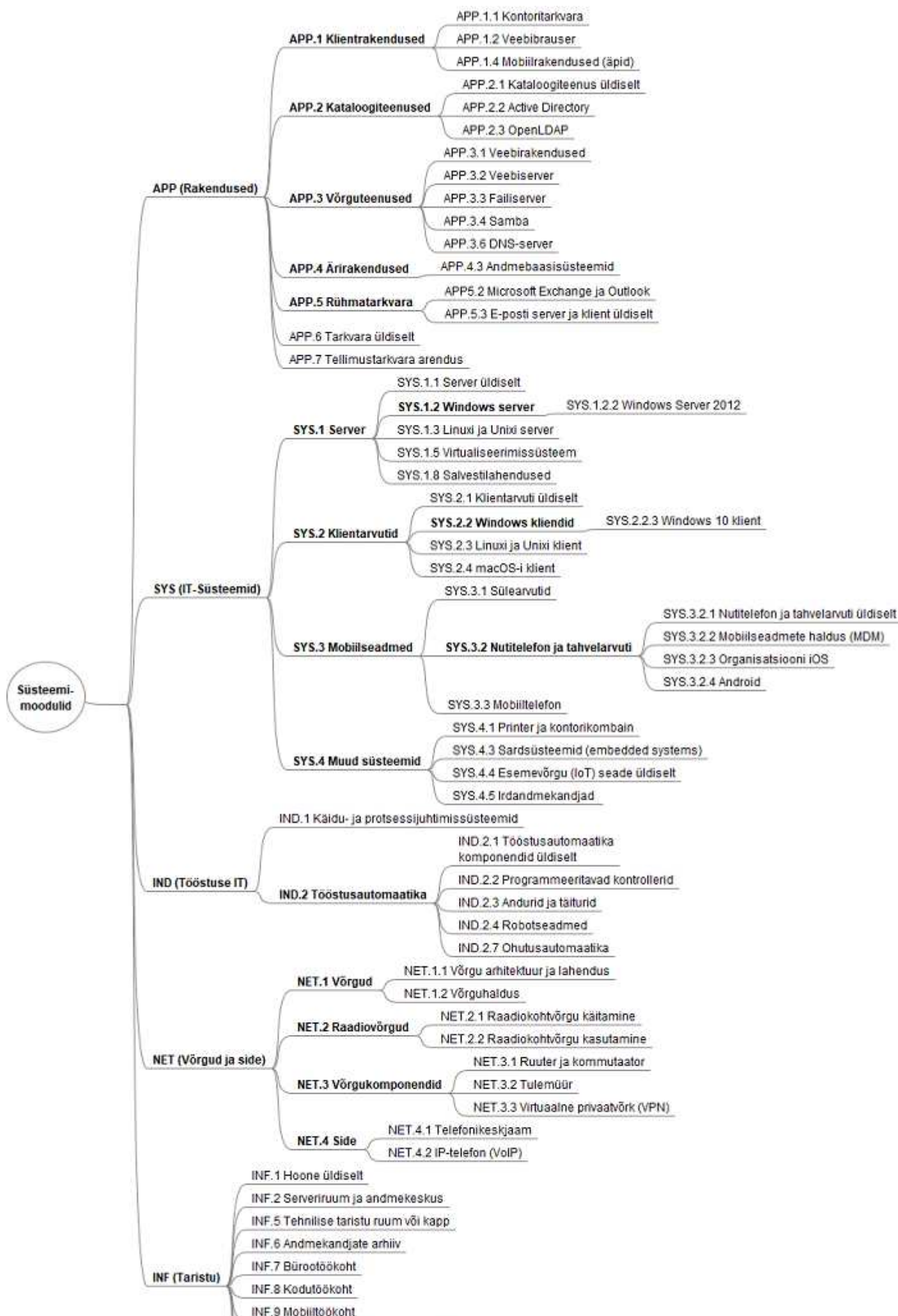
[Joonis A 2. Etalonturbe moodulid puukujuliselt. Süsteemimoodulid](#)

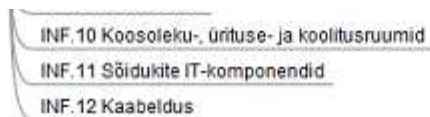
Joonis A 1. Etalonturbe moodulid puukujuliselt. Protsessimoodulid



[Etalonturbe moodulid puukujuliselt. Protsessimoodulid. pdf](#)

Joonis A 2. Etalonturbe moodulid puukujuliselt. Süsteemimoodulid





[Etalonturbe moodulid puukujuliselt. Süsteemimoodulid. pdf](#)

Lisa B Kahjustsenaariumid

Lisa B Kahjustsenaariumide küsimustik

(Mugandatud tõlge standardist BSI 200-2)

Infoturvaohht võib lisaks tehniliste nõrkuste ärakasutamisele realiseeruda palju laiema valiku stsenaariumide järgi. Järgnevalt on esitatud kahjustsenaariumide põhised näidisküsimused, mis aitavad määrata kaitsetarvet.

Neid küsimusi tuleks organisatsiooni iseärasuste põhjal sobitada ja vajadusel täiendada.

Allpool on vaadeldud kuut kahjustsenaariumi:

Sisukord

[Kahjustsenaarium 01 - "Õigusaktide, eeskirjade või lepingute rikkumine"](#)

[Kahjustsenaarium 02 - "Teabelise enesemääramisõiguse rikkumine"](#)

[Kahjustsenaarium 03 - "Isiku füüsilise puutumatuse rikkumine"](#)

[Kahjustsenaarium 04 - "Ülesannete täitmise võime kahjustamine"](#)

[Kahjustsenaarium 05 - "Negatiivsed sisemised või välised toimed"](#)

[Kahjustsenaarium 06 - "Rahalised tagajärjed"](#)

Kahjustsenaarium 01 - "Õigusaktide, eeskirjade või lepingute rikkumine"

Selliste rikkumiste tulemuseks võib olla konfidentsiaalsuse, tervikluse või käideldavuse kadu. Kahjustuse tõsidus sõltub juhtumiga organisatsioonile kaasnevatest juriidilistest tagajärgedest.

Eestis kehtivate õigusaktide näiteid:

- [Isikuandmete kaitse seadus](#) (IKS), [Küberturbe seadus](#) (KüTS), andmekogude põhimäärused

Asjakohaste eeskirjade näiteid:

- halduseeskirjad, määrused, teenistuseeskirjad

Lepingute näiteid:

- andmetöötamise teenuseleping, ärisaladuse leping

Kahjustuse tagajärgede ja ulatuse hindamiseks saab kasutada järgmisi küsimusi.

Tabel 1. Kahjustsenaarium 01 - "Õigusaktide, eeskirjade või lepingute rikkumine"

	Küsimused
Konfidentsiaalsuse kadu:	
	Kas õigusaktid nõuavad selle teabe konfidentsiaalsust?
	Kas teabe paljastumine võib tuua kaasa kohtumenetluse või suure kahjutasunõude?

	Kas on lepinguid, mis nõuavad teatava teabe konfidentsiaalsuse säilitamist?
Tervikluse kadu:	
	Kas õigusaktid nõuavad selle teabe terviklust?
	Mil määral oleks terviklusriike vastuolus seaduste või eeskirjadega?
Käideldavuse kadu:	
	Kas selle rakenduse tõrge võib põhjustada eeskirjade või isegi õigusaktide rikkumist?
	Kas õigusaktid nõuavad mingi teabe pidevat kättesaadavust (24/7)?
	Kas on seatud mingeid tähtaegu, mida tuleb selle rakenduse kasutamisel järgida?
	Kas mõne lepingu tingimused käsitlevad tähtaegu?

Kahjustsenaarium 02 - "Teabelise enesemääramisõiguse rikkumine"

IT-süsteemide teostamisel ja käitamisel esineb risk, et rikutakse teabelist enesemääramis-õigust või isegi väärkasutatakse isikuandmeid.

Teabelise enesemääramisõiguse rikkumise näited on:

- isikuandmete lubamatu kogumine, ilma seadusliku põhjuse või isiku nõusolekuta (vt IKS ja GDPR nõuded);
- teabe lubamatu kogumine andmetöötluse või isikuandmete edastuse käigus (vt IKS ja GDPR nõuded);
- isikuandmete lubamatu paljastamine;
- isikuandmete kasutamine muul eesmärgil kui kogumisel nimetatud;
- isikuandmete tervikluskadu IT-süsteemides või andmeedastusel.

Kahjustuse tagajärgede ja ulatuse hindamiseks saab kasutada järgmisi küsimusi.

Tabel 2. Kahjustsenaarium 02 - "Teabelise enesemääramisõiguse rikkumine"

	Küsimused
Konfidentsiaalsuse kadu:	
	Millist kahju võib inimesele tekitada olukord, kus tema isikuandmeid ei käidelda konfidentsiaalsetena?
	Kas mingeid isikuandmeid töödeldakse lubamatutel eesmärkidel?
	Kas on võimalik, et isikuandmete töötlemisel seadusliku põhjusega saab neist andmeist siiski järeldada näiteks inimese tervislikku seisundit või majanduslikku olukorda?
	Millist kahju võib põhjustada talletatud isikuandmete väärkasutus?
Tervikluse kadu:	
	Millist kahju võib inimesele tekitada ta isikuandmete stiihiline või sihilik rikkumine?
	Kui ruttu isikuandmete tervikluskadu märgatakse?
Käideldavuse kadu:	
	Kas on võimalik, et mingi rakenduse tõrke või andmeedastuse häiringu puhul lähevad isikuandmed kaotsi või muutuvad säärases ulatuses, et see mõjutab kahjulikult isiku sotsiaalset positsiooni või tekitab talle isiklikku või majanduslikku kahju?

Kahjustsenaarium 03 - "Isiku füüsilise puutumatuse rikkumine"

IT-süsteemide või rakenduste väärtalitus võib otseselt tekitada inimestele traumasid, invaliidsust või kaasa tuua surma. Kahjustuse ulatust tuleb hinnata isiku otsese kahjustuse põhjal.

Sellised rakendused ja IT-süsteemid on näiteks:

- meditsiinilise seire arvutid,
- meditsiinilise diagnostika süsteemid,
- lennujuhtimise arvutid,
- liikluse juhtimise süsteemid.

Kahjustuse tagajärgede ja ulatuse hindamiseks saab kasutada järgmisi küsimusi.

Tabel 3. Kahjustsenaarium 03 - "Isiku füüsilise puutumatuse rikkumine"

	Küsimused
Konfidentsiaalsuse kadu:	
	Kas selle teabe paljastamine võib inimest füüsiliselt või psühholoogiliselt kahjustada?
Tervikluse kadu:	
	Kas programmi või andmete manipuleerimine võib inimeste tervist kahjustada?
Käideldavuse kadu:	
	Kas mingi rakenduse või IT-süsteemi tõrge ähvardab otseselt inimeste tervist?

Kahjustsenaarium 04 - "Ülesannete täitmise võime kahjustamine"

Organisatsiooni võimet oma ülesandeid täita võib oluliselt mõjutada mõne rakenduse käideldavuse kadu või teabe või andmete tervikluse kadu. Selles kontekstis sõltub tekitatava kahjustuse tõsidus kahjustuse kestusest ja antavate teenuste kitsenemise ulatusest.

Näiteid selle kohta:

- seadusega ette nähtud avalik ülesanne jääb määratud tähtaja jooksul sooritamata;
- tarnete hiline mine tellimuste töötluse hilistuste tõttu;
- defektne toodang väärade juhtimisparameetrite tõttu;
- puudulik kvaliteedi tagamine testimissüsteemi tõrke tõttu.

Kahjustuse tagajärgede ja ulatuse hindamiseks saab kasutada järgmisi küsimusi.

Tabel 4. Kahjustsenaarium 04 - "Ülesannete täitmise võime kahjustamine"

	Küsimused
Konfidentsiaalsuse kadu:	
	Kas on mingit teavet, mille konfidentsiaalsus on ülesande täitmiseks oluline (õiguskaitseteave, uurimistulemused)?
Tervikluse kadu:	
	Kas teabe muutumine takistaks ülesannete täitmist määral, et organisatsioon ei saaks enam toimida?
	Kas ülesannete täitmine rikutud teabega tekitaks olulist kahju? Kui kiiresti õnnestub lubamatud muudatused andmetes avastada?
	Kas rikutud teave vaadeldavas rakenduses võib tekitada vigu teisteski rakendustes?

	Millised on tagajärjed kui andmete loomine omistatakse valele isikule?
Käideldavuse kadu:	
	Kas on teavet, mille käideldavuse vähenemisel oleksid tõsised tagajärjed organisatsioonile või selle äriprotsessidele?
	Kas rakenduste tõrge võib nii tõsiselt mõjutada organisatsiooni tegevust, et asjaomastele ei ole ooteajad enam vastuvõetavad?
	Kas selle rakenduse tõrge võib mõjutada teisi rakendusi?
	Kui oluline on organisatsioonile, et rakendused ja programmid töötaksid alati ning et andmed oleksid alati kättesaadavad?

Kahjustsenaarium 05 - "Negatiivsed sisemised või välised toimed"

Ühe turvakomponendi kadu kolme põhilise (konfidentsiaalsuse, tervikluse, käideldavuse) hulgast võib kaasa tuua mitmesugused sisemised ja välised negatiivsed toimed, näiteks:

- organisatsiooni maine kaotus;
- usalduse kadu organisatsiooni suhtes;
- töömoraali langus;
- kahjustuvad partnerorganisatsiooniga siduvad ärisuhted;
- kaob usaldus organisatsiooni töö kvaliteedi suhtes;
- konkurentsipositsiooni kaotus.

Kahjustuse suurus sõltub usalduse kaotuse tõsidusest ja sisemise või välise toime levikust.

Niisugusel kahjustusel võib olla mitmesuguseid põhjusi:

- organisatsiooni teovõimetus IT-süsteemi tõrke tõttu;
- väär publitseerimine manipuleeritud andmete tõttu;
- väär tellimine laoarvestusprogrammide vigade tõttu;
- konfidentsiaalsuslepete rikkumine;
- valede inimeste süüdistamine;
- ühe allüksuse teovõimetus teiste protsesside vigade tõttu;
- tagaotsitava isiku andmete edastus huvitatud kolmandatele;
- konfidentsiaalsete andmete lekitamine ajakirjandusele.

Kahjustuse tagajärgede ja ulatuse hindamiseks saab kasutada järgmisi küsimusi.

Tabel 5. Kahjustsenaarium 05 - "Negatiivsed sisemised või välised toimed"

	Küsimused
Konfidentsiaalsuse kadu:	
	Millised on tundliku teabe lubamatu avaldamise tagajärjed organisatsioonile?
	Kas konfidentsiaalse teabe kaotus võib nõrgendada konkurentsipositsiooni?
	Kas konfidentsiaalse teabe paljastumine võib panna kahtlema organisatsiooni usaldatavuses?
	Kas teabe avaldamine võib tekitada poliitilist või sotsiaalset ebaturvalisust?
	Kas teabe lubamatu avaldamine võib kaotada töötajate usalduse organisatsiooni vastu?
Tervikluse kadu:	
	Millist kahju võib tekitada väär või puuduliku teabe töötlus, levi või edastus?

	Kas teabe rikkumine saab avalikult teatavaks?
	Kas rikutud teabe avaldamine võib tekitada prestiiži langust?
	Kas rikutud teabe avaldamine võib tekitada poliitilist või sotsiaalset ebaturvalisust?
	Kas rikutud teabe avaldamine võib halvendada toote kvaliteeti ja seeläbi prestiiži langust?
Käideldavuse kadu:	
	Kas rakenduste tõrge piiraks kolmandatele pakutavaid infoteenuseid?
	Kas teabe käideldamatus või äriprotsesside tõrge võib takistada organisatsiooni ärieesmärkide saavutamist?
	Kui kiiresti saab teabe käideldamatus või äriprotsesside tõrge märgatavaks väljaspool?

Kahjustsenaarium 06 - "Rahalised tagajärjed"

Otsene või kaudne rahaline kahju võib tekkida kaitset vajava teabe konfidentsiaalsuse kadumisel, teabe muutumisel või rakenduste tõrke korral. Põhjuste näiteid:

- uurimis- ja arendustulemuste lubamatu edasiandmine,
- rahandust mõjutavate andmete manipuleerimine arvestussüsteemis,
- müügitulu vähenemine IT-juhitava tootmissüsteemi tõrke tõttu,
- teabe lubamatu saamine turustusstrateegia dokumentidest või käibeandmetest,
- reisibüroo tellimissüsteemi tõrge,
- e-kaubanduse serveri tõrge,
- panga maksetehingute katkemine,
- riistvara vargus või hävimine.

Kogukahju koosneb otsestest või kaudsetest kuludest näiteks omandi kahjustamise tõttu, kahjutasu-nõuetest ja lisakuludest (näiteks taasteks).

Tabel 6. Kahjustsenaarium 06 - "Rahalised tagajärjed"

	Küsimused
Konfidentsiaalsuse kadu:	
	Kas konfidentsiaalse teabe avaldamine põhjustaks kahjutasunõudeid?
	Kas on mingit äriprotsessi- või rakenduse teavet, mis annaks kolmandate (näiteks konkurentide) kätte sattumisel neile rahalist kasu?
	Kas rakendustega salvestatakse väärtuslikke uurimisandmeid? Mis juhtuks nende loata kopeerimisel ja edasiandmisel?
	Kas tundliku teabe enneaegne avaldamine võib tekitada kahju?
Tervikluse kadu:	
	Kas arvestusega seotud andmeid manipuleerides saab tekitada rahalist kahju?
	Kas väära teabe avaldamine võib põhjustada kahjutasunõudeid?
	Kas rikutud tellimisandmed võivad tekitada rahalist kahju (näiteks täppisajastusega tootmisel)?
	Kas rikutud teave võib viia väärade äriotsusteni?
Käideldavuse kadu:	
	Kas rakenduste või äriprotsesside tõrge kahjustaks tootmist, laohaldust või turustust?
	Kas rakenduste või äriprotsesside tõrke puhul tekiks rahaline kahju hilinevad maksete või intressikao tõttu?

	Kui palju maksaks IT-süsteemide remont või taaste nende tõrke, defekti, hävimise või varguse korral?
	Kas rakenduste või äriprotsesside tõrge võib põhjustada maksevõimetust või lepingutrahvi?
	Kui paljusid olulisi kliente mõjutaks rakenduste või äriprotsesside tõrge?

Lisa C Dokumentide näidisloend

Lisa C Dokumentatsiooni näidisloend

Näidisloetelu on tinglikult jagatud kaheks.

- Alusdokumentatsioon – poliitikad, põhimõtted, liigitusastmikud jne.
- Tegevusdokumentatsioon – otsused, operatiivne dokumentatsioon, infoturbeintsidentide materjalid, läbivaatuste ja ülevaatuste aktid jne.

Märkus: Loetelu on orienteeritud keskmisele ja suuremale organisatsioonile. Väiksematel organisatsioonidel tuleb loetelu optimeerida ja dokumente kombineerida.

Sisukord

[Alusdokumentatsioon](#)
[Tegevusdokumentatsioon](#)

Alusdokumentatsioon

Tabel C-1. Alusdokumentatsiooni näidisloend

Nr	Nimetus	Peamine sihtrühm	Märkused
N01	Infoturvapoliitika	Huivatud osapooled	Ülemise taseme dokument, sisaldab keskseid määranguid - mida, miks ning mis eesmärgil tehakse ning et üldse tehakse (pühendumuskinnitus)
N01.1	(Info) turvaeesmärgid	Turbehaldus, juhtkond	Ülemise taseme sihid, mis organisatsioonis infoturvet kujundavad. Enamasti loetletakse üles infoturvapoliitikas
N01.2	Infoturbe strateegia	Turbehaldus	Kuidas, missuguse ideoloogia, metoodika abil kavatakse sihid saavutada. Enamasti leiab mainimist ka infoturvapoliitikas
N02	Infoturbeprotsessi kontseptsioon (turbekontseptsioon)	Turbehaldus, töötajad	Taktikalise taseme üksikasjalik kirjeldus eesmärkide saavutamise võtetest.
N03	Varade loetelu (ja nende omavahelised seosed)	Turbehaldus, juhtkond	Inventuuri tulemus, sisaldab äriprotsesse ja varasid: äriprotsessidesse kaasatud teavet, IT süsteeme, rakendusi, võtab arvesse ka keskkonda (lepingulised kohustused), ressursse (elekter, tööjõud). Arvestatakse ka väljapoole perimeetrit jäävaid seadmeid ja kasutusvõimalusi
N04	Ebatraditsiooniliste varade loetelu	Turbehaldus, ärisuunad	Sideliinid, virtuaalrakendused, IoT, SCADA/ICS, läbipääsusüsteemid, valvesignalisatsioon, video-valvesüsteemid, võrgustatud kohvimasinad, kontori-, tehnoloogia- ning laoruumid (põhjus eraldi käsitlemiseks - sageli unustatakse just need varad kaitsealast välja)
N05	Infoturbe aluskomponentide	Turbehaldus	Tüüpiline organisatsioon piirdub kolme nn C-I-A komponendiga. Mõnel juhul võidakse vajada lisakomponente nagu privaatsus, auditeeritavus, jälitatavus, autentisus/usaldusväarsus, salgamatus,

	valik		ohutus, legaalsus vms
N06	Turbeprotsessiks vajalikud klassifikaatorid	Turbehaldus	Kaitsetarbe tasemete nimetused (juhul kui need erinevad E-ITS väljapakututest)
N07	Kaitseala kirjeldus	Turbehaldus	Turbeprotsessiga hõlmatavate ressursside piiritus (ka: IS, käsitusala)
N08	Infoturbe korraldusstruktuuri kirjeldus	Turbehaldus, juhtkond, töötajad	Suhtluskanalid, rollid, organisatsiooniskeemid
N09	Tööprotseduurid ja organisatsiooni eeskirjad	Kõik töötajad	Näited: e-maili ja Interneti kasutamise turvapoliitika, käitumisjuhised kahjurvaraga nakatumise ja inimestega manipuleerimise vältimiseks, töötajate käitumisreeglid turvaintsidendi kahtluse puhuks
N10	Autentimispoliitika	Kõik töötajad	Reeglid autentimisvahenditele. Vahendid, mis on nõrgemad kui 2FA tase, tuleb eranditena dokumenteerida ning allutada regulaarsele kontrollile
N11	Turvaintsidentide avastamise korraldus (avastamine, reageerimine)	Turbehaldus, kõik töötajad	Määratleb töökorralduse. Suures organisatsioonis võib tekkida vajadus erinevate juhendite loomiseks tavatöötajatele ning IT-töötajatele.
N12	Võrguskeem	IT, turbehaldus	Plaanimistaseme dokument, mis on eelkõige vajalik kaitseala struktuuri analüüsimisel. Võrgu füüsiline ja loogiline ülesehitus, seadmetega seostamine koos oluliste identifikaatorite äranäitamisega. Eraldi markeeritakse missioonikriitiline side.

Tegevusdokumentatsioon

Tabel C-2. Tegevusdokumentatsiooni näidisloend

Nr	Nimetus	Peamine sihtrühm	Märkused
T01	Turvapoliitika teostamise etapiline tegevusplaan.	Turbehaldus, juhtkond	Planeerimise alus
T02	Turbekontseptsiooni rakendusplaan.	Turbehaldus, ärisuund	Eelmisest detailsem, koos ressursivajadusega. Vajalik, et isikutele korraldusi anda ning tagada vahendid
T03	Moodulite kinnis(ta) tus sihtobjektidele	Turbehaldus	Etalonturbe meetodi spetsiifilise vahesammu dokumenteerimine (tabeli kujul)
T04	Turvameetmete teostusjärjestus	Turbehaldus, riskihaldus	Turvameetmete teostusjärjestuse määratlused ja põhjendused. Hoolikuse dokumenteerimiseks panna kirja ka alternatiivsed seisukohad.
T05	Rakendusplaani järelevalve kava	Turbehaldus	Ajakohase ülevaate tagamiseks.
T06	Iga üksiku (arvelevõetud) äriprotsessi üksikasjad.	Äripool	Taasteprotseduuride võimaldamiseks, aga ka esimese lähenemisena inventuuri ülesandele
T07	Turbeprotsessi käigus tehtud otsused.	Turbehaldus, juhtkond, audit	Turbeprotsessi otsuste jälitatavuse ja korratavuse tagamiseks
	Olulised lepingud	Juristid,	Nõuded tuleks lepingutest eraldi välja tuua äriprotsessi mõistmise

T08	partnerite ja klientidega	ärisuunad; Turbehaldus	eesmärgil ning et olla kindel nende arvessevõtus
T09	Juhtkonnale kommunikeeritud infoturvateave	Audit	Teabe aja- ning asjakohasuse kontrolliks.
T10	Infoturbe ja turbeprotsessi kohta tehtud otsused (sh juhtkonnatasemel)	Juhtkond	Jälgitavuse, korratavuse tagamiseks.
T11	Infoturvameetmete nimekiri	Turbehaldus, audit	Vajalik aruandluseks ja kontrolliks. Iga üksik turvameede tuleb dokumenteerida. Eesmärk: põhjuslik ja ajaline jälitatavus. Iga meetme puhul tuleb säilitada jälitatavus (miks, mis riski tõttu, mis nõue, kuidas meede kaitseb jne)
T12	Infoturbe (seisu) ülevaatus	Turbehaldus	Ülevaatus toimingut kirjeldav dokument
T13	Kontrollide (nii sisemiste kui välimiste) tulemused	Turbehaldus	Et tagada avastatud probleemide tundmine ja võimalus neist õppida, ka nõuetele vastavuse kontroll, meetmete efektiivsuse kontroll jne
T14	(Infoturva) intsidentide nimekiri ja lahendamise materjalid	Turbehaldus, juhtkond, audit	Et tagada intsidentidest õppimise võimalus. Sisaldab järeldusi, rakendatud parandusmeetmeid ja viiteid järelkontrollile
T15	Kasutajaõigused	Turbehaldus, ärisuunad, audit	Detailselt dokumenteeritakse nii õiguste maatriks, neid koondavad rollid (rühmad) kui ka iga pääsuõiguse andmine ja eemaldamine. Tuleb tagada nii fakti, aja kui ka põhjuse jälitatavus
T16	Muudatustehalduse sündmused	IT	Muudatused nii äriprotsessides kui ka IT süsteemides tuleb arvele võtta ning säilitada sisuline informatsioon (näiteks ITILi metoodika kohaselt), tagada fakti, aja, ja põhjuse jälitatavus
T17	Andmekandjate inventuur	Turbehaldus, IT	Ükshaaval ja seerianumbriga arvele võtta vähemalt järgmised andmekandjad: a) varundus, b) arhiveerimine, c) andmevahetus partneritega, d) paigaldusmeedia, e) töötajatele kasutamiseks lubatud irdmeedia
T18	Väliste teenuseandjate ja - tarnijate pädevustunnistused ja sertifikaadid	Äri, IT, turbehaldus	Hankeahela turvalisuse tagamiseks.
T19	Talitluspidevuse käsiraamatud	Rakenduse või süsteemi kohane	Tuleb loetleda ning ühtlasi teha kättesaadavaks ka ajakohased paberkoopiaid
T20	Krüptograafilised võtmed ja sertifikaadid	Turbehaldus, sisekontroll	Ükshaaval arvele võtta (v.a. automaatselt genereeritavad): seerianumber ja räsi, täpne otstarve, kehtivus, aegumistähtaeg, kasutus-atribuudid, vastutaja
T21	Krüptograafilised algoritmid	Turbehaldus	Arvele võtta murdumise ennetamise ja asendamise planeerimiseks.
T22	Äriprotsessidele kaitsetarbe kinnitamise akt	Turbehaldus	Kaitsetarbe formaalne määramine ja kinnitamine on etalonturbe protseduuri kohustuslik samm
T23	Alluvatele varadele ja ressurssidele kaitsetarbe omistamise akt	Turbehaldus	Kaitsetarve määratakse IT-süsteemidele, rakendustele, teabele, kõigile arvelevõetud sihtobjektidele ja ressurssidele, sealhulgas ruumidele

T24 Kontrolljälg, logid	Turbehaldus	Konsolideerida viisil, mis võimaldab edasist automaattöötlust ning tagab kogutu konfidentsiaalsuse
-------------------------	-------------	--

Lisa D Rollid

Lisa D Rollide nimekiri

Rollide nimekirja kasutamisest: kui etalonturbe kataloogist valitakse meede, mille kirjeldus sisaldab vastutajana mõnda konkreetset rolli, siis tuleb tagada, et selle rolli täitja organisatsioonis oleks nimetatud, seda ka juhul, kui vastava nimetusega ametikohta ei eksisteeri.

Tinglikult loetakse, et iga täitmata rolli eest vastutab organisatsiooni juht isiklikult.

Tabel D-1. Rollinimekiri koos selgitustega

Roll	Määratlus (v2021)
Andmekaitespetsialist	Organisatsiooni juhtkonna määratud isik, kes hoolitseb isikuandmete käitluse seaduslikkuse eest.
Arendaja	Tarkvara, riistvara või süsteemide kavandamise, väljatöötuse, testimise ja hooldusega tegelev isik (nt tarkvaraarhitekt, programmeerija) või üksus.
Arhitekt	Keerukate valdkondlike tööde (nt ehitiste, andmesidevõrkude) turvalise kavandamise ja plaanimise eest vastutaja.
Auditirühm	Audiitoritest ja tehnilistest ekspertidest koosnev rühm auditite tegemiseks.
Avariijuht	Organisatsiooniülese avariiahalduse loomise, rakendamise, käigushoiu ja toe eest vastutaja ning kõigi avariiahalduse tegevuste juht.
Ehitusfirma	Rajatiste ja ehitiste tegija või paigaldaja.
Ehitusjuht	Ehituslike meetmete teostuse eest vastutaja.
Haldusosakond	Organisatsiooni allüksus, mis kavandab ja korraldab tsentraalseid haldustegevusi ja haldab tugiteenuseid (nt paljundust, transporti, posti, puhastustöid).
Hankeosakond	Hangete algatamise (sh töövahendite ja IT-süsteemide hankimisega) ning hanke järelevalvega tegelev allüksus ja üksuse juht.
Hooldepersonal	Tehnilisi süsteeme hooldama määratud töötajad või välise teenuse andjad.
Infoturbe läbivaatuse rühm	Infoturbe läbivaatust sooritav töörühm, mille koosseisus on asjakohaseid tehnilisi spetsialiste.
Infoturbejuht	Organisatsiooni juhtkonna määratud isik, kes juhtkonna nimel koordineerib ja edendab infoturbetegevust organisatsioonis.
IT-talitus	Organisatsioonisisest infotehnoloogiat paigaldav, käitlev, seirav ja hooldav allüksus ja üksuse juht.
Kasutaja	Organisatsiooni töötaja, kes kasutab oma töö tegemiseks infotehnoloogiat.
Käidutehnoloogia talitus	Tööstusprotsesside kavandamise, toimimise, halduse ja seirega tegelev üksus (sh personal ja tehnoloogia).
Organisatsiooni juhtkond	Organisatsiooni juhtimistasand, sh tippjuhtkond.
Personaliosakond	Tööjõu plaanimise, värbamise, arvestuse ja arendamisega ning töötajate isiklike küsimustega tegelev allüksus ja selle juht.
Tehnikatalitus	Hoone või kinnistu tehnilise taristu (sh elektri- ja sidesüsteemid) eest hoolitsev allüksus ja selle juht.
Testija	Ettemääratud testimisplaani, protseduure ja kriteeriume rakendades uue või muudetud tarkvara või riistvara testimise sooritaja.
	Organisatsiooni liige (töötaja), sh väljaspool organisatsiooni töötav ning tööandja

Töötaja	IT-süsteeme kasutav isik.
Tuleohutusspetsialist	Vastutaja ja kontaktisik kõigis tuleohutuse küsimustes.
Ülemus	Töötaja, keda organisatsioon on volitanud käsutama tema alluvusse määratud töötajaid.
Vastavushaldur	Organisatsioonile kohaldatavate õiguslike, lepinguliste ja muude nõuete väljaselgitaja ning nende täitmise kontrollija (ingl <i>Compliance Manager</i>)
Vastutav spetsialist	Ühe või mitme äriprotsessi või tehnilise protseduuri kavandamise ning läbiviimise eest vastutaja, protsessijuht (nt paikamise ja muudatuste haldaja, arhiivihaldur, avalike suhete juht).

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetusskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

INF. Taristu

INF.1: Hoone üldiselt

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

1.1 Eesmärk

Esitada organisatsiooni tüüpilise hoone tehnilisi ja organisatoorseid turvaaspekte käsitlevad meetmed. Seejuures võetakse arvesse hoonete kogu elutsükli, alustades nõuete koostamisest, kavandamisest, rajamisest, kasutamisest kuni remondi ja väljakolimiseni.

1.2 Vastutus

„Hoone üldiselt“ meetmete täitmise eest vastutab tehnikatalitus.

Lisavastutajad

Ehitusjuht, ehitusfirma, infoturbejuht, organisatsiooni juhtkond, töötaja, arhitekt, haldusosakond, tuleohutusspetsialist.

1.3 Piirangud

Hoone side- ja elektriikaabeldust 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

Sisukord

[2.1 Tuli](#)[2.2 Äike](#)[2.3 Vesi](#)[2.4 Ilmastikust ja loodusõnnetustest tulenevad ohud](#)[2.5 Keskkonnaohud](#)[2.6 Lubamatu sissepääs](#)[2.7 Ehituseeskirja rikkumine](#)[2.8 Puudulikud tuletõkked](#)[2.9 Elektrikatkestus](#)

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 kaheksa 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 kliimaatilised 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 pealtkuulamiseseadme, 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 paigaldada 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

Sisukord

3.1 Elutsükel

3.2 Põhimeetmed

[INF.1.M1 Hoone turbe kavandamine \[arhitekt, infoturbejuht\]](#)

[INF.1.M2 Elektrisüsteemi sobivus](#)

[INF.1.M3 Tuleohutusnõuete järgimine \[tuleohutusspetsialist\]](#)

[INF.1.M4 Hoone tulekahjusignalisatsioon \[arhitekt, tuleohutusspetsialist\]](#)

[INF.1.M5 Käsikustutid \[tuleohutusspetsialist\]](#)

[INF.1.M6 Akende ja uste sulgemine \[töötaja\]](#)

[INF.1.M7 Sisepääsu reguleerimine ja -kontroll \[haldusosakond, infoturbejuht\]](#)

[INF.1.M8 Suitsetamiskeeld \[töötaja\]](#)

[INF.1.M10 Standardite ja eeskirjade järgimine \[ehitusfirma, ehitusjuht\]](#)

[INF.1.M27 Sissemurdmiskaitse](#)

3.3 Standardmeetmed

[INF.1.M9 Hoonete turbe programm \[arhitekt\]](#)

[INF.1.M12 Pääsmike ja võtmete haldus](#)

[INF.1.M13 Tehnosüsteemidele juurdepääsu reguleerimine](#)

[INF.1.M14 Piksekaitsesüsteem](#)

[INF.1.M15 Juhistike ja torustike paigutusskeemid](#)

[INF.1.M16 Kaitset vajavate hooneosade otstarbe mittenäitamine](#)

[INF.1.M17 Suitsutõkestus \[arhitekt\]](#)

[INF.1.M18 Tuleohutuse läbivaatused \[tuleohutusspetsialist\]](#)

[INF.1.M19 Tuleohutuse eest vastutava töötaja õigeaegne teavitamine \[tuleohutusspetsialist\]](#)

[INF.1.M20 Tulekahju korral tegutsemise plaan ja tuleohutusõppused \[tuleohutusspetsialist\]](#)

[INF.1.M36 Taristu dokumentatsiooni regulaarne uuendamine](#)

3.4 Kõrgmeetmed

[INF.1.M22 Turvalised uksed ja aknad \(C-I-A\)](#)

[INF.1.M23 Turvatsoonid \[arhitekt\] \(C\)](#)

[INF.1.M24 Automaatne vee-eemaldus \(A\)](#)

[INF.1.M25 Sobiva asukoha valimine \[organisatsiooni juhtkond\] \(A\)](#)

[INF.1.M26 Valve- ja turvateenistus \(C-I-A\)](#)

[INF.1.M30 Sobiva hoone valimine \(C-I-A\)](#)

[INF.1.M31 Turvaline väljakolimine \[haldusosakond\] \(C\)](#)

[INF.1.M34 Häire- ja hoiatussüsteem \(A\)](#)

[INF.1.M35 Välisperimeetri kaitsmine \[arhitekt\] \(C-A\)](#)

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 ukсед 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

INF.1.M35 Välisperimeetri kaitsmine

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 jätmed.

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]

a. Kui hoones ei ole inimesi, hoitakse aknad suletud ja välisüksed (ka rõdu- või terrassiüksed) lukustatud.

b. Uste ja akende sulgemise kord on töötajaile teada ja selle täitmist kontrollitakse regulaarselt.

INF.1.M7 Sisepääsu 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 [töötajad]

- 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 välisüksed on kaitstud pääsukontrollisüsteemiga ja neid ei jäeta lahti.

INF.1.M10 Standardite ja eeskirjade järgimine [ehitusfirma, ehitusjuht]

- 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 võredegaga;
 - 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]

- 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;

- 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

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, avariilukorras 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 ukseksidid ei näita ruumide tegelikku otstarvet.

INF.1.M17 Suitsutõkestus [arhitekt]

a. Konstruksiooni 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 ukse ja aknad (C-I-A)

a. Hoonete ukse ja aknad vastavad vähemalt kaitseklassile RC2 standardi EVS-EN 1627 järgi.

b. Andmekeskuse olemasolul vastavad selle ukse 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 kriminoogeensus.

INF.1.M26 Valve- ja turvateenistus (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 (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 suuremõduliste 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“

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

INF. Taristu

INF.2: Serveriruum ja andmekeskus

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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

Andmekaitse spetsialist, 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

Sisukord

[2.1 Andmekeskuse kavandamisvead](#)

[2.2 Lubamatu sissepääs](#)

[2.3 Puudulik seire](#)

[2.4 Andmekeskuse ebasobiv mikrokliima](#)

[2.5 Tuli](#)

[2.6 Vesi](#)

[2.7 Puuduv või puudulik sissemurdmistõrje](#)

[2.8 Elektrikatkestus](#)

[2.9 Ebapuhas keskkond](#)

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. Õhukonditsioneeride 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 sisemurdmistõrje 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 tolmu keskkonnas kiiremini ja neil on rohkem tõrkeid.

3 Meetmed

Sisukord

[3.1 Elutsükel](#)

[3.2 Põhimeetmed](#)

[INF.2.M1 Nõuete kehtestamine \[tehnikatalitus, arhitekt\]](#)

[INF.2.M2 Tuletõkkesektsioonid \[arhitekt\]](#)

[INF.2.M3 Puhvertoiteallikas \(UPS\) \[tehnikatalitus\]](#)

[INF.2.M4 Toite avariilüliti \[tehnikatalitus\]](#)

[INF.2.M5 Õhutemperatuuri ja -niiskuse reguleerimine \[tehnikatalitus\]](#)

[INF.2.M6 Pääsu reguleerimine \[tehnikatalitus\]](#)

[INF.2.M7 Uste ja akende lukustus ja turve \[töötaja, tehnikatalitus\]](#)

[INF.2.M8 Tulekahjusignalsatsioon \[arhitekt, tuleohutusspetsialist\]](#)

[INF.2.M9 Tulekustutussüsteem ja kustutusvahendid \[tehnikatalitus, tuleohutusspetsialist\]](#)

[INF.2.M10 Taristu ülevaatus ja hooldus \[tehnikatalitus, hooldepersonal\]](#)

[INF.2.M11 Taristu seire \[tehnikatalitus\]](#)

[INF.2.M17 Tulekahju varajane tuvastamine \[arhitekt, tehnikatalitus\]](#)

[INF.2.M29 Juhistiku kontroll \[arhitekt, tehnikatalitus\]](#)

[3.3 Standardmeetmed](#)

[INF.2.M12 Andmekeskuse perimeetri turve \[arhitekt, tehnikatalitus\]](#)

[INF.2.M13 Valvesüsteem \[tehnikatalitus\]](#)

[INF.2.M14 Avariitoitegeneraator \[arhitekt, tehnikatalitus\]](#)

[INF.2.M15 Liigvoolukaitse \[arhitekt, tehnikatalitus\]](#)

[INF.2.M16 Andmekeskuse keskkonnatingimused \[arhitekt, tehnikatalitus\]](#)

[INF.2.M19 Tehnilise taristu testimine \[tehnikatalitus\]](#)

[3.4 Kõrgmeetmed](#)

[INF.2.M21 Varuandmekeskus \(A\)](#)

[INF.2.M22 Tolmutõrje \[tehnikatalitus\] \(I-A\)](#)

[INF.2.M23 Andmekeskuse turvaline kaabeldus \[tehnikatalitus\] \(A\)](#)

[INF.2.M24 Videovalvesüsteem \[arhitekt, tehnikatalitus, andmekaitsespetsialist\] \(I-A\)](#)

[INF.2.M25 Puhvertoiteallikate dubleerimine \[arhitekt\] \(A\)](#)

[INF.2.M26 Avariitoitegeneraatori dubleerimine \[arhitekt\] \(A\)](#)

[INF.2.M28 Kõrgendatud nõuetele vastav valvesüsteem \[arhitekt\] \(I-A\)](#)

3.1 Elutsükel

Kavandamine

INF.2.M1 Nõuete kehtestamine

INF.2.M12 Andmekeskuse perimeetri turve

INF.2.M13 Valvesüsteem

Evitus

INF.2.M2 Tuletõkkeseksioonid

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 Nõuete 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 niiskustahemikus, selleks on soovitatav 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. Õhukonditsioneeride 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 tulekustutussüsteem. Ilma automaatse tulekustutussüsteemita serveriruumidesse on paigaldatud tulekahju varaseks tuvastamiseks tule- ja suitsuandurid.
- b. Serveriruumi on paigaldatud vajaliku suurusega ning ettenähtud kustutusainega käsikustutid.
- c. Tulekustutiteid on piisav arv ning need on paigutatud kergesti juurdepääsetavatesse kohtadesse. Tulekustutini on võimalik jõuda vähem kui kolme minutiga.
- d. Andmekeskusesse või serveriruumi pääsuõigust omavad töötajad oskavad käsikustutiteid ja tulekustutussüsteemi ohutult kasutada.

e. 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 suitsutõkkeseksatsioonide 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 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. Liigvoolukaitsed 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. Avariilukordade 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. Kontrollle 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"

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

INF. Taristu

INF.5: Tehnilise taristu ruum või kapp

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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

Sisukord

[2.1 Halb planeering](#)[2.2 Lubamatu juurdepääs](#)[2.3 Ebapiisav ventilatsioon](#)[2.4 Tuli](#)[2.5 Vesi](#)[2.6 Elektrikatkestus](#)[2.7 Äike ja liigpinge](#)[2.8 Elektromagnetilised häiringud](#)[2.9 Elektrostaatilised häiringud](#)

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 mitteamestamine 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 märkimisväärsed kahjustusi või hävida täielikult. Selle tulemusena katkevad äriprotsessid, mis ruumis asuvatest seadmetest 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 induktsooniefekti 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

Sisukord

[3.1 Elutsükel](#)

[Lisanduvad kõrgmeetmed](#)

[3.2 Põhimeetmed](#)

[INF.5.M1 Tehnilise taristu ruumi turbe kavandamine \[arhitekt\]](#)

[INF.5.M2 Tehnilise taristu ruumi sobiv asukoht ja suurus \[arhitekt\]](#)

[INF.5.M3 Pääsu reguleerimine ja kontroll \[tehnikatalitus, IT-talitus\]](#)

[INF.5.M4 Sissemurdmiskaitse \[arhitekt, tehnikatalitus\]](#)

[INF.5.M5 Kaitse elektromagnetiliste häiringute eest \[arhitekt\]](#)

[INF.5.M6 Tuletundlikkuse vähendamine \[töötaja, arhitekt\]](#)

[INF.5.M7 Ruumi otstarbekohane kasutamine \[töötaja, arhitekt\]](#)

[INF.5.M9 Sobiv elektrivarustussüsteem \[tehnikatalitus\]](#)

[INF.5.M16 Puhvertoiteallikas \(UPS\) \[tehnikatalitus\]](#)

[3.3 Standardmeetmed](#)

[INF.5.M8 Kontrollimatu elektrostaatilise laengu vältimine \[arhitekt\]](#)

[INF.5.M10 Sobiv õhutemperatuur ja -niiskus \[tehnikatalitus\]](#)

[INF.5.M11 Kommunaal- ja gaasitorustike vältimine \[arhitekt, tehnikatalitus\]](#)

[INF.5.M12 Ühenduskanalite kaitse juhuslike kahjustuste eest \[arhitekt\]](#)

[INF.5.M13 Kaitse tule- ja suitsukahjustuste eest \[arhitekt, tehnikatalitus\]](#)

[INF.5.M14 Naaberalade tuleohu minimeerimine \[arhitekt, tehnikatalitus\]](#)

[INF.5.M15 Pikse- ja liigpingekaitse \[arhitekt, tehnikatalitus\]](#)

[INF.5.M17 Taristu ülevaatus ja hooldus \[tehnikatalitus, IT-talitus, hooldepersonal\]](#)

[3.4 Kõrgmeetmed](#)

[INF.5.M18 Tehnilise taristu ruumi asukoht \[arhitekt\]](#)

[INF.5.M19 Tehnilise taristu varuasukoht \[arhitekt\]](#)
[INF.5.M20 Laiendatud sissemurdmiskaitse \[arhitekt\]](#)
[INF.5.M22 Varutoide \[arhitekt\]](#)
[INF.5.M23 Avariitoitegeneraator \[arhitekt, tehnikatalitus, hooldepersonal\]](#)
[INF.5.M24 Ventilatsioon ja jahutus \[arhitekt, tehnikatalitus, hooldepersonal\]](#)
[INF.5.M25 Tugevam kaitse tule- ja suitsukahjustuste eest \[arhitekt\]](#)
[INF.5.M26 Elektrivarustuse seire \[arhitekt, tehnikatalitus\]](#)

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. Vältitakse 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 elektritarvibimist 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 konstruktsioonelementidel (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]

<https://eits.ria.ee/et/versioon/2021/etalonturbe-kataloog/inf-taristu/inf5-tehnilise-taristu-ruum-vooi-kapp/>

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. Liigpingekaitseadmeid 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 suitsutõkkeseksioonide vaheliste kaabli- ja toruläbiviikude tuletõkestust kontrollitakse regulaarselt.

c. Taristu ülevaatused ja hooldetööd dokumenteeritakse.

3.4 Kõrgmeetmed

INF.5.M18 Tehnilise taristu ruumi asukoht [arhitekt]

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. Avariilukorra 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 tuletõkkeseksioonides ning neil on üksteisest sõltumatud õhukonditsioneerimissüsteemid.

INF.5.M20 Laiendatud sissemurdmiskaitse [arhitekt]

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 elektri kaablid 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. Elektrivarustus on peajaotuskilbist kuni tehnilise taristu ruumi elektritarvititeni dubleeritud eraldi tuletõkkeseptsioonis asuvate toiteliinidega.
- b. Madalpinge jaotussüsteemis on varuliinide lisamise võimalus.

INF.5.M23 Avariitoitegeneraator [arhitekt, tehnikatalitus, hooldepersonal]

- 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. 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. Tehnilise taristu ruumi piirdekonstruktsioon, õhuklapid ja toiteliinid peavad tulele ja suitsule vastu vähemalt 90 minutit.
- b. Väga suure kaitsetarbe korral käsitletakse üksikuid ruume iseseisvate tuletõkkeseptsioonidena.
- c. Kaablitrassid väljapool tehnilise taristu ruumi paiknevad eraldi tuletõkkeseptsioonides.
- d. Tehnilise taristu ruumidesse on paigutatud tsentraalse tulekahjusignalsatsiooniga ühendatud tule- ja suitsuandurid.
- e. Ventilatsioonikanalitesse on paigutatud suitsuanduritele reageerivad tuletõkkeklapid.
- f. Väga suure kaitsetarbe korral on tehnilise taristu ruumi paigaldatud automaatne tulekustutussüsteem.
- g. Tulekahjusignalsatsioon, suitsuandurid ja automaatne kustutussüsteem on ühendatud puhvertoiteallika ja avariitoitegeneraatoriga.

INF.5.M26 Elektrivarustuse seire [arhitekt, tehnikatalitus]

- 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"

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetusskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

INF. Taristu

INF.6: Andmekandjate arhiiv

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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

Sisukord

[2.1 Lubamatu temperatuur ja õhuniiskus](#)

[2.2 Eeskirjade puudumine või puudulikkus](#)

[2.3 Lubamatu sissepääs kaitset vajavatesse ruumidesse](#)

2.4 Vargus

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 märkamatu 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

Sisukord

3.1 Elutsükel

3.2 Põhimeetmed

[INF.6.M1 Käsikustutid \[tuleohutusspetsialist\]](#)

[INF.6.M2 Sissepääsu reguleerimine ja kontroll \[tehnikatalitus\]](#)

[INF.6.M3 Kaitse tolmu ja määrdumise eest \[töötaja\]](#)

[INF.6.M4 Akende ja uste sulgemine ja lukustamine \[töötaja\]](#)

3.3 Standardmeetmed

[INF.6.M5 Kaitsekapid \[töötaja\]](#)

[INF.6.M6 Veetorude vältimine \[tehnikatalitus\]](#)

[INF.6.M7 Sobiv sisekliima \[tehnikatalitus\]](#)

[INF.6.M8 Turvalised ukse ja aknad \[arhitekt\]](#)

3.4 Kõrgmeetmed

[INF.6.M9 Valvesüsteem \[tehnikatalitus\] \(C-I-A\)](#)

3.1 Elutsükel

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]

- b. Andmekandjate arhiivis asuvad ainult veetorud, mis on vältimatult vajalikud.
- c. Andmekandjate arhiivi läbivate veetorude lekkekindlust kontrollitakse regulaarselt.
- d. On rakendatud meetmed lekete varajaseks tuvastamiseks (lekkeandurid) ja kahjude vähendamiseks (vee äravoolukanalid).
- e. Suure kaitsetarbega arhiivi tarbeks on koostatud intsidendihalduse kava, mis määratleb, keda lekke korral informeeritakse 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”

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetusskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

INF. Taristu

INF.7: Bürootöökoht

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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

Bürootöökohta 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

Sisukord

[2.1 Lubamatu sissepääs](#)

[2.2 Ebasobivad töötingimused](#)[2.3 Küllastajate ja välispersonaliga seotud ohud](#)[2.4 IT varade manipuleerimine või hävitamine](#)[2.5 Vargus](#)[2.6 Kaabelduse korraldamatus](#)

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 suuruselt 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 Küllastajate ja välispersonaliga seotud ohud

Ka isikud, kes viibivad bürooruumides küllastajana 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 bürooruume 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 bürooruumides 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

Sisukord

[3.1 Elutsükk](#)

[3.2 Põhimeetmed](#)

[INF.7.M1 Sobiva bürooruumi valimine \[ülemus\]](#)

[INF.7.M2 Akende sulgemine ja uste lukustamine \[töötaja, haldusosakond\]](#)

[INF.7.M6 Korras töökoht \[töötaja\]](#)

[3.3 Standardmeetmed](#)

[INF.7.M3 Toite- ja sidekaablite turvaline paigutus](#)

[INF.7.M5 Ergonoomiline töökoht \[haldusosakond, ülemus\]](#)

[INF.7.M7 Dokumentide ja andmekandjate hoiustamise kord \[töötaja, tehnikatalitus\]](#)

[3.4 Kõrgmeetmed](#)

[INF.7.M8 Vargusvastased vahendid \[töötaja\] \(C-I-A\)](#)

3.1 Elutsükk

Kavandamine

INF.7.M1 Sobiva bürooruumi 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 bürooruumi valimine [ülemus]

- Büroorumidena kasutatakse ainult selleks kasutusotstarbeks ettenähtud ja vastavalt sisustatud ruume.
- Ruumi turve ja pääsukontrollisüsteemid vastavad ruumis käideldava teabe kaitsetarbele.
- Üldkasutatavad büroorumid on eraldatud kõrge kaitsetarbega aladest.

INF.7.M2 Akende sulgemine ja uste lukustamine [töötaja, haldusosakond]

- Töövälisel ajal on bürooruumi aknad suletud.
- Juhul, kui büroorumis hoitakse konfidentsiaalset teavet, lukustavad töötajad ruumist lahkudes ukse.
- Tule- ja suitsutõkkeused on alati suletud.
- 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 töökaitsevenõuetele.

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.

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

INF. Taristu

INF.8: Kodutöökoht

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

1.1 Eesmärk

Esitada meetmed organisatsiooni teabe kaitseks ja turvalise taristu rajamiseks kodutöökohas. Üldjuhul on kodutöökoht juurdepääsetav ka pereliikmetele, külalistele ja koduloomadele.

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

Sisukord

[2.1 Kodus töötamise eeskirja puudumine või puudulikkus](#)

[2.2 Lubamatu sissepääs kodutöökohta](#)

[2.3 Ebasobivad töötingimused](#)

[2.4 Andmekandjate ja dokumentide ebaturvaline transport](#)

[2.5 Andmekandjate ja dokumentide ebaturvaline kõrvaldamine](#)

[2.6 IT-seadmete, andmete või tarkvara manipuleerimine või rikkumine](#)

[2.7 Vargusohk kodutöökohas](#)

2.1 Kodus töötamise eeskirja puudumine või puudulikkus

Kui kodus töötamiseks puuduvad konkreetsed tegevusjuhised, võib IT-süsteemide kasutamine ebaõnnestuda ja seeläbi tekkida pikemaajalisi 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 ebatavalisse asukohta, näiteks koduarvutisse, millele võivad pääseda ligi ka teised pereliikmed. Tekib oht andmete konfidentsiaalsusele ja terviklusele.

2.2 Lubamatu sissepääs kodutöökohas

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 tootlikkust 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 ebatavaline 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 kättesse 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 ebatavaline 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 mahu. Hävitatud IT-komponentide asendamine kodutöökohas nõuab aega ja IT-töötajate ressursi, 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

Sisukord

[3.1 Elutsükkel](#)

[3.2 Põhimeetmed](#)

[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](#)

[3.3 Standardmeetmed](#)

[INF.8.M4 Kodutöökoha õige korraldus](#)

[3.4 Kõrgmeetmed](#)

[INF.8.M5 Konfidentsiaalsete andmete turvaline kõrvaldamine \(C\)](#)

[INF.8.M6 Suure kaitsetarbega töödokumentide turvaline käitus \(C-I-A\)](#)

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

Väljavahtamine

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 ukسلukud).

c. Kui töötaja kodutöökohal ei viibi, on tööruumi aknad suletud ja ukسل 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.

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetusskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

INF. Taristu

INF.9: Mobiiltöökoht

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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.3.2.1 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

Sisukord

[2.1 Eeskirjade puudumine või puudulikkus](#)

[2.2 Keskkonnast tingitud kahjulikud mõjud](#)

[2.3 IT-seadmete, -tarvikute ja -süsteemide manipuleerimine või hävitamine mobiiltöökohal](#)

[2.4 Töötaja kättesaadavuse piiratus](#)

[2.5 Andmekandjate ja dokumentide ebaturvaline transport](#)

[2.6 Andmekandjate ja dokumentide ebaturvaline kõrvaldamine](#)

[2.7 Andmete konfidentsiaalsuse kadu](#)

[2.8 Andmekandjate ja dokumentide vargus või kaotamine](#)

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 kättesse 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, tolmu 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 kättesse 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 paber kandjal 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 konkurentsiolekorra.

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

Sisukord

[3.1 Elutsükel](#)

[3.2 Põhimeetmed](#)

[INF.9.M1 Mobiiltöökoha sobivuse kriteeriumid \[IT-talitus\]](#)

[INF.9.M2 Mobiilseadmete kasutamise eeskiri \[personaliosakond\]](#)

[INF.9.M3 Kaitse lubamatu juurdepääsu eest \[haldusosakond, töötaja\]](#)

[INF.9.M4 Organisatsioonivälise IT-süsteemiga töötamise kord \[IT-haldus, töötaja\]](#)

[3.3 Standardmeetmed](#)

[INF.9.M5 Mobiilseadme kaotusest teatamine \[töötaja\]](#)

[INF.9.M6 Konfidentsiaalse teabe turvaline kõrvaldamine \[töötaja\]](#)

[INF.9.M7 Mobiiltöö õiguslikud raamtingimused \[personaliosakond\]](#)

[INF.9.M8 Mobiiltöökoha turvanõuete kehtestamine \[IT-haldus\]](#)

[INF.9.M9 Mobiilseadmete ja andmekandjate krüpteerimine \[IT-haldus, kasutaja\]](#)

[INF.9.M12 Ekraanifiltri kasutamine \[töötaja\]](#)

[3.4 Kõrgmeetmed](#)

[INF.9.M10 Vargusvastaste vahendite rakendamine \[töötaja\] \(C-I-A\)](#)

[INF.9.M11 Mobiiltöö keeld ebaturvalistes oludes \[IT-haldus\] \(C-I-A\)](#)

3.1 Elutsükel

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 organisatsiooniväliste 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]

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 ebaturvalistes 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.

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

INF. Taristu

INF.10: Koosoleku-, ürituse- ja koolitusruum

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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 *Raadiovõrgud* 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

Sisukord

[2.1 Eeskirjade puudumine või puudulikkus](#)[2.2 IT-seadmete ühildumatus](#)[2.3 Külastajatest tulenevad ohud](#)[2.4 Lahtised kaablid](#)[2.5 Vargus](#)[2.6 Teabe konfidentsiaalsuse kadu](#)

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 organisatsiooniväliste 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 tähelepanematus tõttu. Külastaja võib näiteks tualettruumi otsides eksida uksega ja siseneda bürooruumi, milles asuval markertahvil 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 juhatakse 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 organisatsiooni 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 märkamatu varastada.

2.6 Teabe konfidentsiaalsuse kadu

Tehniliste tõrgete, töötajate tähelepanematus või teadmatuse tõttu on võimalik IT-seadme salvestuskandjal (nt kõvaketas), irdkandjal (nt mälupulk või DVD), paberandjal või joonistustahvilil 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

Sisukord

[3.1 Elutsükel](#)

[3.2 Põhimeetmed](#)

[INF.10.M1 Koosoleku-, ürituse- ja koolitusruumi turvaline kasutamine \[tehnikatalitus, IT-haldus\]](#)

[INF.10.M3 Akende ja uste sulgemine \[töötaja\]](#)

[3.3 Standardmeetmed](#)

[INF.10.M4 Koosoleku-, ürituse- ja koolitusruumide turvaline asukoht](#)

[INF.10.M5 Toite- ja sidekaablite turvaline paigutus](#)

[INF.10.M6 Turvalise võrkupääsu korraldus \[IT-haldus\]](#)

[INF.10.M7 Koolitus- ja esitlusarvutite turvaline konfiguratsioon \[IT-haldus\]](#)

[INF.10.M8 Ruumikasutuse registreerimise kord](#)

[3.4 Kõrgmeetmed](#)

[INF.10.M9 Koolitus- ja esitlusarvutite algseadistamine \[IT-haldus\] \(C-A\)](#)

[INF.10.M10 Mobiiltelefonide keeld \(C\)](#)

3.1 Elutsükel

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

INF.10.M10 Konfidentsiaalsusvajadusega koosolekute turve

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 ukseid 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 ukseid lisaks ka lukustatud.

b. Ajutisel lahkumisel otsese järelevalveta koosoleku-, ürituse- ja koolitusruumidest lukustatakse ukseid 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 tavapärasest tööd ei segaks.

d. Konfidentsiaalset teavet käsitlevad koosolekud peetakse selleks sobivaks tunnistatud ja vastavat märget omavates koosolekuruumides, kus on rakendatud meetmeid pealtkuulamise piiramiseks (nt seinade 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*).

INF.10.M10 Mobiiltelefonide keeld (C)

a. Korraldaja võib keelata konfidentsiaalsetele nõupidamistele mobiiltelefonide ja nutiseadmete kaasavõtmise.

b. Mobiilseadmete turvaliseks hoiustamiseks väljaspool nõupidamisruumi on paigaldatud lukustatavadapid.

c. Vajaduse korral kasutatakse mobiilsideseadmete avastamiseks detektorseadet.

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetusskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

INF. Taristu

INF.11: Sõidukite IT-komponendid

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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, andmekaitse spetsialist, vastutav spetsialist, IT-talitus, töötaja.

1.3 Piirangud

Moodul käsitleb sõidukeid üldiselt. Eriotstarbeliste sõidukitele (nt kiirabiauto, päästekooper, 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

Sisukord

[2.1 Puuduv või puudulik sõiduki kasutamise kord](#)

[2.2 Ohutusnõuete eiramine](#)

[2.3 Ebaturvaline andmevahetus](#)

[2.4 Sõiduki lubamatu või ebaturvaline ümberseadistus](#)

[2.5 Sõiduki vargus ja volitamata juurdepääs](#)

[2.6 Sõiduki hoolduse ja IT-komponentide uuenditega seotud ohud](#)

[2.7 Kasutaja andmete kõrvaldamata jätmine](#)

[2.8 Sobimatud keskkonnatingimused](#)

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 automaatsete 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 informeerimata, 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 raadioliidest 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 sõiduki juhi 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 märkamatu 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, parandada 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 ukse ja auto käivitada ilma autentset autovõtit omamata. Sissemurdmise ja ärandamise oht on suurem selliste sõidukite 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

Sisukord

[3.1 Elutsükel](#)

[3.2 Põhimeetmed](#)

[INF.11.M1 Sõiduki hanke kavandamine \[vastutav isik, hankeosakond, andmekaitse spetsialist\]](#)
[INF.11.M2 Korrakohane hooldus ja IT-komponentide uuendamine \[vastutav isik, IT-talitus\]](#)
[INF.11.M3 Sõiduki infoturbe juhendid \[IT-talitus, vastutav isik, kasutaja, andmekaitse spetsialist\]](#)
[INF.11.M12 Vargusvastase kaitse vahendid \[vastutav spetsialist, töötaja\]](#)

3.3 Standardmeetmed

[INF.11.M4 Sõidukite infoturbe eeskirja jõustamine \[vastutav spetsialist, IT-talitus\]](#)
[INF.11.M5 Sõidukite inventariloend](#)
[INF.11.M6 Detailsed tegevusjuhised \[vastutav isik, kasutaja\]](#)
[INF.11.M7 Sõiduki turvaline kasutamine \[vastutav isik, kasutaja\]](#)
[INF.11.M8 Sõiduki kaitse ilmastikumõjude eest \[kasutaja, vastutav spetsialist\]](#)
[INF.11.M9 Sõiduki kasutusvalmiduse tagamine \[vastutav spetsialist\]](#)
[INF.11.M10 Sõidukite kasutusest kõrvaldamise kord \[IT-talitus, vastutav spetsialist\]](#)

3.4 Kõrgmeetmed

[INF.11.M11 Asendamise kord \[vastutav spetsialist\] \(A\)](#)
[INF.11.M13 Sõiduki kaitse kahjulike välismõjude eest \[vastutav spetsialist\] \(A\)](#)
[INF.11.M14 Konfidentsiaalse teabe kaitse \[IT-talitus, vastutav spetsialist\] \(C-I-A\)](#)
[INF.11.M15 Sõiduki liideste kaitse \[IT-talitus, vastutav spetsialist\] \(C-I-A\)](#)
[INF.11.M16 Tulekustutussüsteem \[vastutav spetsialist\] \(A\)](#)
[INF.11.M17 Sõidukisisese võrgu eraldamine \(C\)](#)

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, andmekaitespetsialist]

- 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 autoriseeritud 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, andmekaitespetsialist]

- 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 andmesideliidest 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. Ülevaatus 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 avariolukorra ja IT-komponentide rikke korral.
- b. Juhised avariolukorra 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 kasutusaaja 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 juhaks 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*).

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetusskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

INF. Taristu

INF.12: Kaabeldus

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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

Sisukord

- [2.1 Kaabli süttimine](#)
 - [2.2 Kaabelduse aladimensioneerimine](#)
 - [2.3 Kaabelduse puudulik dokumenteerimine](#)
 - [2.4 Jaotusseadmete puudulik turve](#)
 - [2.5 Kaablikahjustused](#)
 - [2.6 Pinge võnkumine, liig- ja alapinge](#)
 - [2.7 Liigne pikendusjuhtmete kasutamine](#)
 - [2.8 Lubamatud ühendused](#)
 - [2.9 Liinihäiringud](#)
 - [2.10 Pealtkuulamine ja manipuleerimine](#)
-

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 voolotaluvuse (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, andmemahutade 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 igal inimesel 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 elektritarveteid. 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

Sisukord

[3.1 Elutsükel](#)

[3.2 Põhimeetmed](#)

[INF.12.M1 Sobiva kaablitüübi valimine \[IT-talitus, tehnikatalitus\]](#)

[INF.12.M2 Kaabelduse kavandamine \[IT-talitus, tehnikatalitus\]](#)

[INF.12.M3 Asjatundlik kaablipaigaldus \[IT-talitus, tehnikatalitus\]](#)

[INF.12.M10 Kaabelduse dokumenteerimine ja märgistus \[IT-talitus, tehnikatalitus\]](#)

[INF.12.M11 Jaotusseadmete dokumentatsioon \[IT-talitus, tehnikatalitus\]](#)

[INF.12.M13 Elektritarvitite süttimise vältimine \[tehnikatalitus\]](#)

[3.3 Standardmeetmed](#)

[INF.12.M4 Tasandusvoolude vältimine varjetes \[tehnikatalitus\]](#)

[INF.12.M5 Kaabelduse nõuete analüüs \[IT-talitus, tehnikatalitus\]](#)

[INF.12.M6 Kaabelduse vastuvõtmine \[IT-talitus, tehnikatalitus\]](#)

[INF.12.M7 Liigvoolukaitse \[tehnikatalitus\]](#)

[INF.12.M8 Liigsete kaablite kõrvaldamine \[IT-talitus, tehnikatalitus\]](#)

[INF.12.M9 Kaablite tuleohutus \[tehnikatalitus\]](#)

[INF.12.M12 Elektripaigaldiste ja ühenduste ülevaatus \[IT-talitus, tehnikatalitus\]](#)

[INF.12.M16 Turvalised kaitsekapid \[tehnikatalitus\]](#)

[3.4 Kõrgmeetmed](#)

[INF.12.M14 Dubleeritud toide \[tehnikatalitus\] \(A\)](#)

[INF.12.M15 Kaabelduse füüsiline turve \[IT-talitus, tehnikatalitus\] \(I-A\)](#)

[INF.12.M17 Sidekaablite dubleerimine \[IT-talitus\] \(A\)](#)

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 Elektritavite 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 täismöödus kaablirenne kohe ei paigaldata, tuleks sein- ja laeläbiviikude läbimöödud 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 töötappides 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 kaitselemendi (liigvoolukaitselüliti) järel tohib mõjuda maksimaalselt nii palju liigvoolust põhjustatud energiat, kui selle järel paiknevad elektritarvitid (sh järgmised liigvoolukaitselülidid) suudavad taluda.

c. Elektrisüsteemide liigvoolukaitse vastab kohalduvatele standarditele ja eeskirjadele.

d. Liigvoolukaitse kava hõlmab ka avariitoitegeneraatoreid ja puhvertoiteallikaid.

e. Liigvoolukaitselülite toimimist kontrollitakse perioodiliselt ja lisaks ka kaitse puudulikkusele viitavate sündmuste ilmnemisel. Vajadusel asendatakse liigvoolukaitselülidid 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 elektri kaablid (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. Ülevaatus tehes järgitakse valdkonnapõhiseid standardeid ja õigusakte.

c. Ülevaatus 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 ülevaatus 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 tuletõkkeseptsioonides.

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"

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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

Sisukord

[2.1 Lubamatu juurdepääs kesksetele võrguhalduskomponentidele](#)

[2.2 Lubamatu juurdepääs võrgukomponentidele](#)

[2.3 Lubamatu sekkumine võrguhalduse sisse](#)

[2.4 Võrgukomponentide süsteemiaja puudulik sünkroniseerimine](#)

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 sisse

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

Sisukord

[3.1 Elutsükel](#)

[3.2 Põhimeetmed](#)

[NET.1.2.M1 Võrguhalduse kavandamine](#)

[NET.1.2.M2 Võrguhalduse nõuete spetsifitseerimine](#)

[NET.1.2.M6 Regulaarne andmevarundus](#)

[NET.1.2.M7 Sündmuste logimine](#)

[NET.1.2.M8 Aja sünkroniseerimine](#)

[NET.1.2.M9 Võrguhalduse side turve](#)

[NET.1.2.M10 SNMP-side piiramine](#)

[NET.1.2.M11 Võrguhalduse juhend](#)

[3.3 Standardmeetmed](#)

[NET.1.2.M12 Võrguhalduse dokumenteerimine](#)

[NET.1.2.M13 Võrguhalduse kontseptsioon](#)

[NET.1.2.M14 Võrguhalduse rakendusplaan](#)

[NET.1.2.M15 Võrguhalduse taristu turvalise kasutamise kord](#)

[NET.1.2.M16 Võrguhalduslahenduste turvaline konfigureerimine](#)

[NET.1.2.M17 Regulaarne võrguhalduse ülevaatus](#)

[NET.1.2.M18 Võrguhalduse koolitus \[ülemus\]](#)

[NET.1.2.M21 Võrguhalduse side lahusus](#)

[NET.1.2.M22 Haldusfunktsioonide piiramine](#)

[NET.1.2.M24 Võrgukomponentide keskne konfiguratsioonihaldus](#)

[NET.1.2.M25 Võrgukomponentide seire](#)

[NET.1.2.M26 Sündmuste teavitus, alarmeerimine ja logimine](#)

[NET.1.2.M27 Võrguhalduse avariivalmendus](#)

[NET.1.2.M28 Haldustööjaamade turvaline paigutus ainukanaliga halduse puhul](#)

[NET.1.2.M29 Virtuaalsed kohtvõrgud \(VLAN\) haldustsoonis](#)

[3.4 Kõrgmeetmed](#)

[NET.1.2.M30 Halduslahenduse kõrgkäideldavus \(A\)](#)

[NET.1.2.M31 Turvalised protokollid \(C-I-A\)](#)

[NET.1.2.M32 Haldusvõrgu füüsiline eraldamine \[arhitekt\] \(C-I-A\)](#)

[NET.1.2.M33 Haldussegmenti füüsiline eraldamine \[arhitekt\] \(C-I-A\)](#)

[NET.1.2.M35 Asitõendite turve \(C-I-A\)](#)

[NET.1.2.M36 Võrguhalduse logimise liidestamine turvateabe ja -sündmuste halduse \(SIEM\) lahendusega \(C-I-A\)](#)

[NET.1.2.M37 Kõiki asukohti hõlmav aja sünkroniseerimine \(C-I\)](#)

[NET.1.2.M38 Võrguhalduse taristu asenduslahendused \(A\)](#)

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 Aja 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 Haldussegmenti 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 kõikumus;
- automaatprotsesside veateated (nt konfiguratsiooni levitamise korral);
- võrgukomponentide kättesaadavushäired.

NET.1.2.M8 Aja sünkroniseerimine

a. Kõigis võrguhalduse komponentides ja nendega seotud võrgukomponentides on aeg sünkroniseeritud ning kasutatakse sama ajavööndit.

b. Kohtvõrgu kõigis kohtades sünkroniseeritakse aega 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 protokollile andmestikule on lubatud ainult vajalikele haldusserveritele.

d. Kui SNMP protokollile 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. Ülevaatus käigus kontrollitakse võrguhalduse dokumentatsiooni ajakohasust, vastavust hetkeseisule ning tegelikele protseduuridele.

c. Ülevaatus 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 käideldavusriike;
- 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 Haldussegmenti 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 liidestite 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 võrgustenaariumid. Riskid, kavandamismeetodid ja reguleerimisküsimused"

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

NET. Võrgud ja side

NET.1: Võrgud ja side

NET.1.1: Võrgu arhitektuur ja lahendus

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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 privaatlilvede ja hübriidpilvede meetmed on esitatud moodulis [OPS.2.2 Pilvteenuste kasutamine](#). Sidevahendite infrastruktuuri meetmeid käsitletakse moodulis [NET.4.2 IP-telefon \(VoIP\)](#).

2 Ohud

Sisukord

[2.1 Sideühenduse tõrge või puudulik sooritusvõime](#)

[2.2 Sisevõrgule juurdepääsu puudulik turve](#)

[2.3 Võrgu asjatundmatu teostus](#)

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 läbimõttlemata konfiguratsioon teevad võrku tunginud ründaja avastamise keeruliseks. Ründaja võib võrgus nähtamatuks jäädes organisatsiooni võrguliiklust jälgida, andmeid varastada ja manipuleerida.

3 Meetmed

Sisukord

[3.1 Elutsükel](#)

[3.2 Põhimeetmed](#)

[NET.1.1.M1 Võrgu turvapoliitika \[IT-talitus, infoturbejuht\]](#)

[NET.1.1.M2 Võrgulahenduse dokumentatsioon \[IT-talitus\]](#)

[NET.1.1.M3 Võrgu tehniliste nõuete spetsifitseerimine](#)

[NET.1.1.M4 Võrgu tsoneerimine](#)

[NET.1.1.M5 Klientide ja serverite võrgusegmentide eraldamine \[IT-talitus\]](#)

[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.M13 Võrgu teostuskava](#)

[NET.1.1.M14 Võrgu kavakohane teostus](#)

[NET.1.1.M15 Võrgu vastavuskontroll \[infoturbejuht\]](#)

[3.3 Standardmeetmed](#)

[NET.1.1.M10 Demilitaartsoon \(DMZ\)](#)

[NET.1.1.M16 Võrgu arhitektuuri dokumenteerimine](#)
[NET.1.1.M17 Võrgulahenduse spetsifitseerimine](#)
[NET.1.1.M18 Internetiühenduse P-A-P-struktuuri \(paketifilter-rakenduslüüs-paketifilter\) kasutamine](#)
[NET.1.1.M19 Taristuteenuste eraldamine](#)
[NET.1.1.M20 Alamvõrgud IPv4/IPv6 lõppseadmetele](#)
[NET.1.1.M21 Haldusvõrkude eraldamine](#)
[NET.1.1.M22 Segmentimise eeskiri](#)
[NET.1.1.M23 Võrgusegmentide eraldamine](#)
[NET.1.1.M24 Võrkude loogiline eraldamine VLAN-iga](#)
[NET.1.1.M25 Võrgu arhitektuuri ja võrgulahenduse detailplaneerimine](#)
[NET.1.1.M26 Võrgu käitusjuhend \[IT-talitus\]](#)
[NET.1.1.M27 Võrgu arhitektuuri arvestamine avariivalmenduses \[IT-talitus\]](#)
3.4 Kõrgmeetmed
[NET.1.1.M28 Kõrgkäideldavad võrgu- ja turvakomponendid \(A\)](#)
[NET.1.1.M29 Võrguühenduste kõrgkäideldav teostus \(A\)](#)
[NET.1.1.M30 Hajusa ummistusründe tõrje \(A\)](#)
[NET.1.1.M31 Võrgusegmentide füüsiline eraldamine \(C-I-A\)](#)
[NET.1.1.M32 Haldusvõrgu segmentide füüsiline eraldamine \(C-I-A\)](#)
[NET.1.1.M33 Võrgu alamsegmentid \(C-I-A\)](#)
[NET.1.1.M34 Võrgupõhised krüptograafilised vahendid \(C-I\)](#)
[NET.1.1.M35 Võrgupõhise lekketõrje rakendamine \[infoturbejuht\] \(C-I\)](#)
[NET.1.1.M36 Virtuaalse kohtvõrguga eraldamise keeld väga suure kaitsetarbe korral \(C-I-A\)](#)

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 alamsegmentid

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 muudatuseettepanekud 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.M1 *Võrgu turvapoliitika*).

b. Turvapoliitika või äri vajaduste 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 paketi filtriga (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 turvapoksi või vastavat võimekust omava keskse tulemüüri.

b. P-A-P-struktuuri (paketi filter-rakenduslüüs-paketi filter) kasutamise korral on väljaminev andmeside suunatud läbi P-A-P turvapokside.

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 dimensionimine 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 privaatsilvega;
 - ühendused pilvteenustega (vt [OPS.2.2 Pilvteenuste kasutamine](#) ja [OPS.3.1 Teenuseandja infoturvet](#));
 - 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 realiseerimise 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 rakenduslüüsides 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 rakenduslüüsides ja turvaprokside siseründeid.
- d. VPN-lüüsisist sisevõrku suunatud autenditud ja usaldusväärsed võrkupääsud ei läbi rakenduslüüsi ega P-A-P-struktuuri turvaprokside.

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 protokoll.

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 paketiltriga.
- 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 testimiskeskondade segmendid;
- klientarvutite võrgusegmentist võrkupääsu reguleerimine;
- raadioühendused ja spetsialiseeritud sidekanalid;
- virtualiseerimishostid ja virtuaalmasinad;
- mitut võrgusegmenti teenindavate seadmete (nt koormusejaotur) integreerimine;
- võrgusegmentide vaheliste sidestuskomponentide (nt dünaamilise paketiltriga tulemüür) turvafunktsioonid.
- segmentide võrgutehniline teostus.

NET.1.1.M23 Võrgusegmentide eraldamine

a. Erineva kaitsetarbega IT-süsteemid asuvad erineva turvasemega 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 turvasemega võrgusegmentid 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 segmentid on põhivõrgust kommutaatoritega ja/või ruuteritega füüsiliselt eraldatud, üksnes loogiline eraldamine pole lubatud.

NET.1.1.M33 Võrgu alamsegmentid (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 privaatvõrgu (VPN) kasutamine lubatud.

4 Lisateave

Lühend	Publikatsioon
[ISO27033]	EVS-ISO/IEC 27033-3:2013 "Infotehnoloogia. Turbemeetodid. Võrguturve. Osa 3: Tüüpsed võrgustsenaariumid. Riskid, kavandamismeetodid ja reguleerimisküsimused"

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetusskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

NET. Võrgud ja side

NET.2: Raadiovõrgud

NET.2.1: Raadiokohtvõrgu käitamine

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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 käsitus](#).

2 Ohud

Sisukord

- [2.1 Raadiokohtvõrgu ühenduse tõrge või häiring](#)
 - [2.2 Raadiokohtvõrgu kavandamisvead](#)
 - [2.3 Raadiokohtvõrgu kasutamise korra puudumine](#)
 - [2.4 Ebaturvalised autentimisprotseduurid](#)
 - [2.5 Raadiokohtvõrgu taristu seadistusvead](#)
 - [2.6 Puuduvad või ebapiisavad raadiokohtvõrgu turvamehhanismid](#)
 - [2.7 Raadiokohtvõrgu side pealtkuulamine](#)
 - [2.8 Tegelikult pääsupunkti matkimine \(kahjurpääsupunkt\)](#)
 - [2.9 Kaitsmata pääs pääsupunktist kohtvõrku](#)
 - [2.10 Riistvara kahjustused](#)
 - [2.11 Pääsupunkti vargus](#)
-

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 sagedusala 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 teadmatusel 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 kontrolleri) 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 Tegelikult 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 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

Sisukord

[3.1 Elutsükel](#)

[3.2 Põhimeetmed](#)

[NET.2.1.M1 Raadiokohtvõrkude kavandamine](#)
[NET.2.1.M2 Sobiv raadiokohtvõrgu standard \[arhitekt\]](#)
[NET.2.1.M3 Turvaline krüptomehhanism \[arhitekt\]](#)
[NET.2.1.M4 Pääsupunktide turvaline paigaldus \[tehnikatalitus\]](#)
[NET.2.1.M5 Pääsupunkti turvaline seadistus](#)
[NET.2.1.M6 Raadiokohtvõrgu taristu turvaline seadistus](#)
[NET.2.1.M7 Turvaline raadiokohtvõrgu arhitektuur \[arhitekt\]](#)
[NET.2.1.M8 Raadiokohtvõrgu intsidendikäsitluse kord](#)

3.3 Standardmeetmed

[NET.2.1.M9 Raadiokohtvõrgu turvaline ühendamine kaabelvõrguga \[arhitekt\]](#)
[NET.2.1.M10 Raadiokohtvõrgu turvajuhend](#)
[NET.2.1.M11 Sobivad raadiokohtvõrgu komponendid](#)
[NET.2.1.M12 Raadiokohtvõrgu sobiv haldus](#)
[NET.2.1.M13 Raadiokohtvõrgu regulaarne turvakontroll](#)
[NET.2.1.M14 Raadiokohtvõrgu komponentide regulaarne läbivaatus](#)

3.4 Kõrgmeetmed

[NET.2.1.M15 Raadiokohtvõrgu turve virtuaalse privaatsvõrguga \(VPN\) \(C-I\)](#)
[NET.2.1.M16 Raadiokohtvõrgu ja kaabelvõrgu vahelise ühenduse lisaturve \(C-I-A\)](#)
[NET.2.1.M17 Pääsupunktide ühenduse turve \(C\)](#)
[NET.2.1.M18 Raadiokohtvõrgu sissetungituvastuse ja -tõrje tööriistad \(C-I-A\)](#)

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 Jaotussüsteemi rajamine

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 privaativõrguga (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 pikselööök) 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. Avariivalmendumise 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 kommutaatoritega (ingl *switch*) 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 meetet 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, konfigurierida 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 käsitus](#)).

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 privaatsvõrguga (VPN) (C-I)

a. Raadiokohtvõrgu (WLAN) taristu andmeside turbeks kasutatakse virtuaalset privaatsvõrku (ingl *virtual private network*, VPN).

b. VPN rakendamisel järgitakse meetmeid moodulist [NET.3.3 Virtuaalne privaatsvõrk \(VPN\)](#).

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“

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetusskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

NET. Võrgud ja side

NET.2: Raadiovõrgud

NET.2.2: Raadiokohtvõrgu kasutamine

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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 Infoturbe teadlikkuse tõstmine ja koolitus](#) ning [DER.2.1 Turvaintsidentide käsitletus](#).

2 Ohud

Sisukord

[2.1 Eeskirjade tundmise puudulikkus](#)[2.2 Turvameetmete eiramine](#)[2.3 Raadiovõrgu andmeside pealtkuulamine](#)[2.4 Sideühenduse andmete analüüs](#)[2.5 Õige pääsupunkti teesklemine \(kahjurpääsupunkt\)](#)

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 veebilehetele, 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

Sisukord

[3.1 Elutsükkel](#)[3.2 Põhimeetmed](#)[NET.2.2.M1 Raadiokohtvõrgu kasutamise eeskiri \[IT-talitus\]](#)[NET.2.2.M2 Raadiokohtvõrgu kasutajate teadlikkuse tõstmine ja koolitus \[ülemus, IT-talitus\]](#)[NET.2.2.M3 Raadiokohtvõrgu kasutamine avalikes raadiokohtvõrkudes \[IT-talitus\]](#)[3.3 Standardmeetmed](#)[NET.2.2.M4 Raadiokohtvõrgu turvasündmuste puhul käitumise kord](#)[3.4 Kõrgmeetmed](#)

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 ebatavalistes tingimustes kitsendatud õigustega kasutajakontot. Administraatori õigustega kasutajal on oma arvutist välistesse ebatavalistesse 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 privaativõrgu (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)“

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetusskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

NET. Võrgud ja side

NET.3: Võrgukomponendid

NET.3.1: Ruuter ja kommutaator

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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

Sisukord

- [2.1 Hajus ummistusrünne \(DDoS\)](#)
 - [2.2 Manipuleerimine](#)
 - [2.3 Ruuteri või kommutaatori konfigureerimisvead](#)
 - [2.4 Puudulik kavandamine](#)
 - [2.5 Ühildumatud aktiivsed võrgukomponendid](#)
 - [2.6 MAC-tulv](#)
 - [2.7 Ründed STP protokolliga vastu](#)
 - [2.8 GARP-ründed](#)
-

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 ebatavalisi teenuseid. Kui ruuterid ja kommutaatorid võetakse kasutusele ebatavaliste 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 oskamatusel või tähelepanematusel teha seadistusvea, mille tulemusena tekib võimalus lubamatuks juurdepääsuks võrguressurssidele. Kui sisselogimiskuva paljastab seadme mudeli ning versiooninumbri, siis osutub võimalikuks sihtotstarbeliselt ära kasutada just konkreetset versiooni 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-lähteadressidega 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 protokoll vastu

STP (ingl *spanning tree protocol*, STP) ründe korral edastab ründaja sillaprotokoll 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 alatatada hajusaid ummistusründeid ja võltsitud sillaprotokoll 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

Sisukord

[3.1 Elutsükkel](#)

[3.2 Põhimeetmed](#)

[NET.3.1.M1 Ruuteri või kommutaatori turvaline baaskonfiguratsioon](#)

[NET.3.1.M4 Haldusliideste turve](#)

[NET.3.1.M5 Kaitse IP-pakettide fragmenteerimisrünnete eest](#)

[NET.3.1.M6 Ruuteri või kommutaatori avariijuurdepäas](#)

[NET.3.1.M7 Ruuterite ja kommutaatorite logimine](#)

[NET.3.1.M8 Regulaarne andmevarundus](#)

[NET.3.1.M9 Käidudokumentatsioon](#)

[3.3 Standardmeetmed](#)

[NET.3.1.M10 Ruuterite ja kommutaatorite turvajuhend \[infoturbejuht\]](#)

[NET.3.1.M11 Ruuteri või kommutaatori valimine](#)

[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.M18 Pääsuloendid](#)

[NET.3.1.M19 Kommutaatori portide turve](#)

[NET.3.1.M20 Turvalised marsruutimisprotokollid](#)

[NET.3.1.M21 Pääsuõiguste ja identiteedi haldus võrgutaristus](#)

[NET.3.1.M22 Ruuterite ja kommutaatorite avariivalmendus](#)

[NET.3.1.M23 Läbivaatused ja läbistustestimised](#)

[3.4 Kõrgmeetmed](#)

[NET.3.1.M24 Võrkupääsu reguleerimine \(I-A\)](#)

[NET.3.1.M25 Konfiguratsioonifailide tervikluse laiendatud kaitse \(I\)](#)

[NET.3.1.M26 Kõrgkäideldavuse tagamine \(A\)](#)

[NET.3.1.M27 Ärikriitiliste rakenduste jõudluse haldus \(A\)](#)

[NET.3.1.M28 Sertifitseeritud tooted \(C-I\)](#)

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 Haldusliideste turve

NET.3.1.M9 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 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. Varukoopiaid on avarii korral kättesaadavad.

NET.3.1.M9 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 olekukurnamisrüündeid (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 autentitakse. 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 käsitlemise juhend, mida regulaarselt ajakohastatakse.

b. Ruuterite ja kommutaatorite avariivalmendus on osa üldisest avariivalmenduse kontseptsioonist (vt [DER.4. Avariiahaldus](#)).

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 autentimismetodiga EAP-TLS (*Extensible Authentication Protocol* (EAP) - *Transport Layer Security* (TLS)).

b. Eeltoodud meetodit ei tohi kasutada koos standardi ebaturvaliste versioonidega IEEE 802.1x-2001 või 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.

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

NET. Võrgud ja side

NET.3: Võrgukomponendid

NET.3.2: Tulemüür

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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](#)“ tulemüüripetsiifiliste 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 [OPS.1.1.4 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

Sisukord

[2.1 Hajus ummistusrünne \(DDoS\)](#)

[2.2 Manipuleerimine](#)

[2.3 Tulemüürireeglite piirangust möödumine](#)

[2.4 Tulemüüri konfigureerimis- ja hooldusvead](#)

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

Tulemüüri kaitstud võrgusektsioonidele ligi pääsemiseks ja tulemüüri kaitsemehhanismidest läbitungimiseks võib ründaja alata 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

Sisukord

[3.1 Elutsükel](#)

[3.2 Põhimeetmed](#)

[NET.3.2.M1 Tulemüüride turvajuhend \[infoturbejuht\]](#)

[NET.3.2.M2 Tulemüürireeglid](#)

[NET.3.2.M3 Sobivad filtreerimisreeglid paketifiltris](#)

[NET.3.2.M4 Tulemüüri turvaline konfigureerimine](#)

[NET.3.2.M6 Tulemüüri haldusliideste turve](#)

[NET.3.2.M7 Tulemüüri avariijuurdepääs](#)

[NET.3.2.M8 Dünaamilise marsruutimise keelamine](#)

[NET.3.2.M9 Tulemüüri logimine](#)

[NET.3.2.M10 Killuründe tõrje paketifiltris](#)

[NET.3.2.M14 Käidudokumentatsioon](#)

[NET.3.2.M15 Tulemüüri hankimise kord](#)

[NET.3.2.M22 Aja turvaline sünkroniseerimine](#)

3.3 Standardmeetmed

[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 järjenumbriga äraarvamise tõrje paketifiltris](#)

[NET.3.2.M23 Tulemüüri seire ja seiretulemuste analüüs](#)

[NET.3.2.M24 Läbivaatused ja läbistustestimised](#)

[NET.3.2.M32 Tulemüüri avariivalmendus](#)

3.4 Kõrgmeetmed

[NET.3.2.M20 Põhiliste Interneti protokollide turve](#)

[NET.3.2.M21 Andmeliikluse ajutine dekripteerimine \(C-I\)](#)

[NET.3.2.M25 Tervikluskaitstud konfiguratsioonifailid \(C-I\)](#)

[NET.3.2.M26 Funktsioonilaienduste väljastellimine \(C-I-A\)](#)

[NET.3.2.M27 Erinevad operatsioonisüsteemid ja tulemüüritooted mitmeastmelises tulemüüri arhitektuuris \(C-I\)](#)

[NET.3.2.M28 Aktiivsisu keskne filtreerimine \(C-I\)](#)

[NET.3.2.M29 Kõrgkäideldavuse tagamise vahendid \(A\)](#)

[NET.3.2.M30 Ärikriitiliste rakenduste jõudluse haldus \(A\)](#)

[NET.3.2.M31 Sertifitseeritud tooted \(C-I\)](#)

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 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 Aja turvaline 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-lähteadressid 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 protokollid või pääsuloendi (ingl *access control list*, ACL) nurjunud autentimiskatsed, sh teenus, IP-lähteadressid 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 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 protokollid kasutamisel võimaldab paketifilter IPv6 laiendpäiste (ingl *IPv6 extension header*) kontrolli ja IPv6 konfigureerimist protokollile IPv4.

NET.3.2.M22 Aja turvaline 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 protokollu 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 haldusprotokollu 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 protokollu 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 läbivaatuse tehakse regulaarselt, läbivaatuse tulemused dokumenteeritakse.

NET.3.2.M32 Tulemüüri avariivalmendus

- a. Tulemüüri avariivalmendus on osa organisatsiooni üldisest avariivalmenduse kontseptsioonist (vt [DER.4. Avariiahaldus](#)).
- 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

- 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 protokollide 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 väljastellimine (C-I-A)

- a. Tulemüüri funktsioonilaiendused tellitakse ainult spetsialiseeritud riist- ja tarkvarana.

NET.3.2.M27 Erinevad operatsioonisüsteemid ja tulemüüritoote 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. Turvaprokseid 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“
--------	---

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

NET. Võrgud ja side

NET.3: Võrgukomponendid

NET.3.3: Virtuaalne privaatvõrk (VPN)

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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 Avariiahaldus](#) 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

Sisukord

[2.1 Virtuaalse kohtvõrgu rakenduskava puudumine või puudulikkus](#)

[2.2 Ebaturvaline virtuaalse kohtvõrgu teenuseandja](#)

[2.3 VPN klientrakenduse ebaturvaline seadistus](#)

[2.4 VPN-komponentide ebaturvaline tüüpseadistus](#)

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

Sisukord

[3.1 Elutsükel](#)

[3.2 Põhimeetmed](#)

[NET.3.3.M1 Virtuaalse privaatvõrgu rakendamise kava](#)

[NET.3.3.M2 Virtuaalse privaatvõrgu teenuseandja valimine \[infoturbejuht\]](#)

[NET.3.3.M3 Virtuaalse privaatvõrgu seadmete turvaline installimine](#)

[NET.3.3.M4 Virtuaalse privaatvõrgu turvaline seadistus](#)

[NET.3.3.M5 Tarbetute virtuaalse privaatvõrgu juurdepääsude tõkestamine](#)

[3.3 Standardmeetmed](#)

[NET.3.3.M6 Virtuaalse privaativõrgu nõuete analüüs](#)

[NET.3.3.M7 Virtuaalse privaativõrgu tehnilise teostuse kava](#)

[NET.3.3.M8 Virtuaalse privaativõrgu turvalise kasutamise juhend \[infoturbejuht\]](#)

[NET.3.3.M9 Virtuaalse privaativõrgu toodete valimise kord](#)

[NET.3.3.M10 Virtuaalse privaativõrgu turvaline käitus](#)

[NET.3.3.M11 Välisvõrgu turvaline ühendamine](#)

[NET.3.3.M12 Virtuaalse privaativõrgu kasutajate pääsuhaldus](#)

[3.4 Kõrgmeetmed](#)

[NET.3.3.M13 VPN-komponentide integreerimine tulemüüriga \(C-I\)](#)

3.1 Elutsükkel

Kavandamine

NET.3.3.M1 Virtuaalse privaativõrgu rakendamise kava

NET.3.3.M6 Virtuaalse privaativõrgu nõuete analüüs

NET.3.3.M7 Virtuaalse privaativõrgu tehnilise teostuse kava

NET.3.3.M8 Virtuaalse privaativõrgu turvalise kasutamise juhend

Soetus

NET.3.3.M2 Virtuaalse privaativõrgu teenuseandja valimine

NET.3.3.M9 Virtuaalse privaativõrgu toodete valimise kord

Evitus

NET.3.3.M3 Virtuaalse privaativõrgu seadmete turvaline installimine

NET.3.3.M4 Virtuaalse privaativõrgu turvaline seadistus

NET.3.3.M10 Virtuaalse privaativõrgu turvaline käitus

NET.3.3.M13 VPN-komponentide integreerimine tulemüüriga

Käitus

NET.3.3.M5 Tarbetute virtuaalse privaativõrgu juurdepääsude tõkestamine

NET.3.3.M11 Välisvõrgu turvaline ühendamine

NET.3.3.M12 Virtuaalse privaativõrgu kasutajate pääsuhaldus

Lisanduvad kõrgmeetmed

NET.3.3.M13 VPN-komponentide integreerimine tulemüüriga

3.2 Põhimeetmed

NET.3.3.M1 Virtuaalse privaativõrgu rakendamise kava

a. Enne virtuaalse privaativõrgu (ingl *virtual private network*, VPN) kasutuselevõttu on organisatsioon hinnanud virtuaalse privaativõrgu vajadust.

b. Enne virtuaalse privaativõrgu kasutuselevõttu on määratud:

- virtuaalse privaativõrgu käitusega seotud töötajate kohustused;
- VPN-i kasutajarühmad ja nende õigused;
- Pääsuõiguste andmise, muutmise ja tühistamise kord.

NET.3.3.M2 Virtuaalse privaativõrgu teenuseandja valimine [infoturbejuht]

a. Virtuaalse privaativõrgu teenuseandjaga on sõlmitud teenustasemelepped (ingl *service level agreement*, SLA) ja need on dokumenteeritud.

b. VPN-teenuseandjaga kokkulepitud teenustasemelepingu täitmist kontrollitakse regulaarselt.

NET.3.3.M3 Virtuaalse privaativõrgu 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 privaativõrgu funktsionaalsust ja turvamehhanismide toimimist testitakse enne virtuaalse kohtvõrgu kasutuselevõttu.

NET.3.3.M4 Virtuaalse privaativõrgu turvaline seadistus

a. Kõigi virtuaalse privaativõrgu klientseadmete, serverite ja ühenduste jaoks on spetsifitseeritud ja dokumenteeritud turvaline konfiguratsioon.

b. Virtuaalse privaativõrgu haldaja kontrollib regulaarselt IT-süsteemide VPN seadistuse turvalisust. Vajadusel muudetakse VPN-i konfiguratsiooni.

NET.3.3.M5 Tarbetute virtuaalse privaativõrgu 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 privaativõrgu nõuete analüüs

a. Virtuaalse privaativõrgu vajaduse hindamisele (vt NET.3.3.M1 *Virtuaalse privaativõrgu rakendamise kava*) tuginedes on läbi viidud virtuaalse privaativõrgu riist- ja tarkvarakomponentide nõuete analüüs.

b. Virtuaalse privaativõrgu nõuete analüüsis on arvesse võetud järgmist:

- hõlmatavad äriprotsessid;
- juurdepääsukanalid;
- identifitseerimis- ja autentimisprotseduurid;
- kasutajad ja kasutajaõigused;
- vastutused ja kohustused;
- teatamisteed.

NET.3.3.M7 Virtuaalse privaativõrgu tehnilise teostuse kava

a. On koostatud virtuaalse privaativõrgu 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 privaativõrgu turvalise kasutamise juhend [infoturbejuht]

a. Virtuaalse privaativõrgu kasutajate jaoks on koostatud virtuaalse privaativõrgu turvalise kasutamise juhend.

b. Kasutajad on virtuaalse privaativõrgu turvalise kasutamise osas koolitatud.

c. Töötajale VPN-pääsu loomisel õpetatakse teda VPN-i kasutama.

d. Kõik virtuaalse privaativõrgu kasutajad on kohustatud virtuaalse privaativõrgu turvalise kasutamise juhendit järgima.

NET.3.3.M9 Virtuaalse privaativõrgu toodete valimise kord

a. Virtuaalse privaativõrgu toodete valimisel on arvestatud organisatsiooni vajadusi erinevates asukohtades ja allüksustes, sealhulgas mobiilkasutajate ja kaugtöötajate vajadusi.

NET.3.3.M10 Virtuaalse privaativõrgu turvaline käitus

a. On dokumenteeritud virtuaalse privaativõrgu turvalise käituse (ingl *operation*) põhimõtted, milles on sätestatud virtuaalse privaativõrgu:

- 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 privaativõrgu kasutajate pääsuvaldus

a. Virtuaalse privaativõrgu kasutajate pääsuvaldus 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)“

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

NET. Võrgud ja side

NET.4: Side

NET.4.1: Telefonikeskjaam

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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 organisatsioonisisestest ja organisatsiooniväliste 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

Sisukord

[2.1 Sidesüsteemi pealtkuulamine](#)

[2.2 Ruumide pealtkuulamine sidesüsteemi kaudu](#)

[2.3 Sideteenuse vargus](#)

[2.4 Telefoniühenduse kuritarvitus](#)

2.1 Sidesüsteemi pealtkuulamine

Kui telefonikõnesid edastatakse krüpteerimata kujul, kaasneb oht, et ründaja võib kõnesid pealt kuulata. Telefonikeskjaamal on olemas funktsionaalsus, mis võimaldab telefonikõnesid märkamatu 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 mikrofonid saab aktiveerida ilma selle omaniku teadmata (nt käivitada telefoni „beebimonitori“ funktsioon).

Olemasolevasse sidesüsteemi võib ründaja lisada spetsiaalse pealtkuulamise seadme. 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

Sisukord

[3.1 Elutsükkel](#)

[3.2 Põhimeetmed](#)

[NET.4.1.M1 Telefonikeskjaama kasutuselevõtu kava \[IT-talitus\]](#)

[NET.4.1.M2 Sideteenuste tarnija valimine \[IT-talitus\]](#)

[NET.4.1.M5 Telefonikeskjaama logimine](#)

[NET.4.1.M15 Hädaabikõned telefonikeskjaama tõrke puhuks](#)

[3.3 Standardmeetmed](#)

[NET.4.1.M6 Telefonikeskjaama turvajuhend \[IT-talitus\]](#)

[NET.4.1.M7 Telefonikeskjaama turvaline paigutus](#)

[NET.4.1.M8 Tarbetute või turvakriitiliste funktsioonide piiramine ja blokeerimine](#)

[NET.4.1.M9 Sidesüsteemi turvalise kasutamise koolitus \[ülemus\]](#)

[NET.4.1.M10 Telefonikeskjaama konfiguratsiooni dokumenteerimine ja läbivaatus \[IT-talitus\]](#)

[NET.4.1.M11 Telefonikeskjaama ja sideseadmete kasutuselt kõrvaldamise kord \[IT-talitus\]](#)

[NET.4.1.M12 Konfiguratsioonifailide varundus](#)

[NET.4.1.M13 Telefonikeskjaama hankimise kord](#)

[NET.4.1.M14 Telefonikeskjaama avariivalmendus](#)

[NET.4.1.M16 Sidesüsteemi klientseadmete turve](#)

[3.4 Kõrgmeetmed](#)

[NET.4.1.M17 Telefonikeskjaama hoolduse turve \(C-I\)](#)

[NET.4.1.M18 Täiendav füüsiline turve \(C-I\)](#)

[NET.4.1.M19 Dubleerivad ühendused \(A\)](#)

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 organisatsiooniväliste 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 andmekaitse nõudeid.

c. Läbivaatuse tulemused esitatakse lisaks otsestele vastutajatele ka infoturbejuhile, andmekaitse spetsialistile 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 muudatust.

d. Telefonikeskjaama andmete taastamist varukoopiaalt 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. Avariiahaldus](#)).

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. Organisatsiooniväliste isikute ruumis viibimine (nimi, ettevõte, ajavahemik) registreeritakse.

NET.4.1.M19 Dupleerivad ühendused (A)

- a. Telefonikeskjaama välisühendus on dupleeritud.
- b. IP-põhine sidesüsteem on täiendavalt ja turvaliselt ühendatud analoogtelefonivõrguga.

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetusskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

NET. Võrgud ja side

NET.4: Side

NET.4.2: IP-telefon (VoIP)

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

1.1 Eesmärk

Esitada meetmed VoIP-põhise sidesüsteemi (ingl *Voice over IP*, VoIP) komponentide ja IP-telefoni kõneastuse 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

Sisukord

[2.1 VoIP-põhise sidesüsteemi vahetarkvara seadistusvead](#)

[2.2 VoIP-põhise sidesüsteemi komponentide väär konfiguratsioon](#)

[2.3 Kõnede pealtkuulamine](#)

[2.4 Telefoniühenduse kuritarvitus](#)

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 signaaliseadistuse 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 sisenumbritest salvestuseks kasutusel e-telefoniraamat, võib selle sisu lekkida.

3 Meetmed

Sisukord

[3.1 Elutsükkel](#)

[3.2 Põhimeetmed](#)

[NET.4.2.M1 VoIP-põhise sidesüsteemi kasutuselevõtu kava](#)

[NET.4.2.M3 VoIP-põhise sidesüsteemi turvaline haldus](#)

[NET.4.2.M4 VoIP-põhisele sidesüsteemile juurdepääsu kitsendamine](#)

[NET.4.2.M5 Vahetarkvara turvaline seadistamine](#)

[3.3 Standardmeetmed](#)

[NET.4.2.M7 VoIP-põhise sidesüsteemi turvajuhend \[infoturbejuht\]](#)

[NET.4.2.M8 VoIP-side krüpteerimine](#)

[NET.4.2.M9 VoIP-põhise sidesüsteemi komponentide valimise kord](#)

[NET.4.2.M11 IP-telefonide turvaline kasutamine \[kasutaja\]](#)

[NET.4.2.M12 VoIP-põhise sidesüsteemi komponentide turvaline kõrvaldamine](#)

[NET.4.2.M13 IP-telefoni tulemüür](#)

[3.4 Kõrgmeetmed](#)

[NET.4.2.M14 Signaalimise krüpteerimine \(C-I\)](#)

[NET.4.2.M15 SRTP protokollide turve \(C-I\)](#)

[NET.4.2.M16 Andmesidevõrgu ja VoIP-võrgu eraldamine \(C-I-A\)](#)

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 protokoll 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 ühendatakse 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);
- logimise nõuded (detailsus, turve, andmekaitse nõuded);
- uuendus- ja paikamise nõuded;
- haldusnõuded (protokollide tugi, haldusliidestus);
- krüpteerimise nõuded.

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 protokollide 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).

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

SYS. IT-süsteemid

SYS.2: Klientarvutid

SYS.2.1: Klientarvuti üldiselt

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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

Sisukord

[2.1 Kahjurprogrammid](#)

[2.2 Andmekadu keskse andmetalletuse puudumise tõttu](#)

[2.3 Väärkasutusest tingitud riistvaratõrked](#)

[2.4 Infotehnoloogia lubamatu kasutamine](#)

[2.5 Tarbetute rakenduste ja operatsioonisüsteemi komponentide installimine](#)

[2.6 Pealtkuulamine arvutimikrofoni ja -kaameraga](#)

[2.7 Seadmete ja süsteemide puudulik haldus](#)

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 kaotamine 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 öla 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. Praktikast 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

Sisukord

[3.1 Elutsükel](#)

[3.2 Põhimeetmed](#)

[SYS.2.1.M1 Kasutajate turvaline autentimine \[kasutaja\]](#)

[SYS.2.1.M3 Uuendite automaatpaigaldus](#)

[SYS.2.1.M6 Kahjurvaratõrje tarkvara](#)

[SYS.2.1.M8 Buutimise turve](#)

[SYS.2.1.M9 Klientarvuti turvalise kasutamise juhend](#)

[SYS.2.1.M42 Pilve- ja võrgufunktsioonide kasutamine](#)

[3.3 Standardmeetmed](#)

[SYS.2.1.M10 Klientarvutite kasutuselevõtu kava](#)

[SYS.2.1.M11 Klientarvuti hankimise kord](#)

[SYS.2.1.M13 Piiratud juurdepääs täitmiskeskonda](#)

[SYS.2.1.M14 Püsivara, operatsioonisüsteemi ja rakenduste uuendid ja paigad](#)

[SYS.2.1.M15 Klientarvuti turvaline install ja seadistus](#)

[SYS.2.1.M16 Tarbetute komponentide ja kontode desaktiveerimine](#)

[SYS.2.1.M18 Krüptoprotokollide kasutamine andmesides](#)

[SYS.2.1.M20 Haldusprotseduuride turve](#)

[SYS.2.1.M21 Arvutimikrofoni ja -kaamera kasutamise kord](#)

[SYS.2.1.M23 Klient-serveri teenuste eelistamine](#)

[SYS.2.1.M24 Väliste andmekandjate kasutamise piiramine](#)

[SYS.2.1.M26 Rakenduste turvaline käitus](#)

[SYS.2.1.M27 Klientarvuti kõrvaldamise kord](#)

[SYS.2.1.M29 Klientarvutite seire](#)
[SYS.2.1.M30 Klientarvuti etaloninstall](#)
[SYS.2.1.M34 Turvakriitiliste rakenduste kapseldamine](#)
[SYS.2.1.M43 Klientarvuti lokaalsed turvaseaded](#)
[SYS.2.1.M44 Keskne klientarvutite turvaseadete haldus](#)

3.4 Kõrgmeetmed

[SYS.2.1.M28 Klientarvuti sisu krüpteerimine \(C\)](#)
[SYS.2.1.M31 Lokaalne paketifilter \(C-I-A\)](#)
[SYS.2.1.M32 Lisameetmed rünnete tõrjeks \(C-I-A\)](#)
[SYS.2.1.M33 Rakenduste käitamise tõkestamine \(C-I\)](#)
[SYS.2.1.M35 Juursertifikaatide aktiivne haldus \(C-I\)](#)
[SYS.2.1.M36 Funktsiooni SecureBoot ja mooduli TPM rakendamine \(C-I\)](#)
[SYS.2.1.M37 Mitmikautentimise kasutamine \(C\)](#)
[SYS.2.1.M38 Integreerimine avariivalmendusega \(A\)](#)
[SYS.2.1.M39 Katkematu ja stabiilne toide \[tehnikatalitus\] \(A\)](#)
[SYS.2.1.M40 Hooldusdokumentatsioon \(A\)](#)
[SYS.2.1.M41 Klientarvuti kõvaketta salvestusruumi piiramine \(A\)](#)
[SYS.2.1.M45 Klientarvuti laiendatud logimine \(C-I-A\)](#)

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.M14 Püsivara, operatsioonisüsteemi ja rakenduste uuendid ja paigad

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 avariivalmendumusega

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 autentitud kasutajal.
- b. Mistahes tegevuse puhul klientarvutis on võimalik tuvastada tegevuse sooritaja.
- c. Autentimisandmeid (nt parooli) muuta saab üksnes selleks volitatud kasutaja.

- d. Klientarvutitele lubamatu juurdepääsu takistamiseks kasutatakse ekraanilukku.
- e. Kasutaja eemaloleku ajaks lukustab kasutaja arvuti juurest lahkudes ekraani.
- f. Ekraanilukk käivitub kasutaja poolt käsitsi aktiveerituna või automaatselt pärast ettemääratud ajavahemikku. Ajavahemiku pikkus sõltub arvutikasutaja tööpetsiifikast.
- g. Ekraaniluku avamine on võimalik vaid kasutaja autentimisega.
- h. 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;
- võrgühendused 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 andmekaitseõuetega.

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.

SYS.2.1.M13 Piiratud juurdepääs täitmiskeskonda

- a. Operatsioonisüsteemis tavakasutajale mittenähtav täitmiskeskond (salvestuspiirkonnad, püsivara alad, ingl *executable space*), on tavakasutajale juurdepääsematu.
- b. Täitmiskeskondades programmikoodi käivitamine on võimalik ainult vastava haldusõiguse olemasolul.
- c. BIOS-i või UEFI püsivara seaded on lubamatute muudatuste eest parooliga kaitstud.

SYS.2.1.M14 Püsivara, operatsioonisüsteemi ja rakenduste uuendid ja paigad

- a. Klientarvutites kasutatakse üksnes tootja tuge omavaid operatsioonisüsteeme ja rakendusi.
- b. Tuvastatud klientarvuti nõrkused kõrvaldatakse võimalikult kiiresti. Kui nõrkust pole võimalik kõrvaldada, võetakse tarvitusele nõrkust kompenseerivad meetmed.
- c. Uuendeid (ingl *update*) ja turbepaiku (ingl *security patch*) hangitakse üksnes usaldusväärsest allikast.
- d. Kui pärast uuendite installimist on vajalik teha klientarvuti taaskäivitus, planeeritakse uuendite installimine sobivale ajale ja teavitatakse sellest kasutajaid.

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 tavapärase haldustööde jaoks on koostatud haldusjuhised, 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 mikrofoni 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 lubatud 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 taasininstallimise 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 täitmiskeskonnas.

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 paketifiltrite 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. Avariiahaldus](#)).

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 toiteto 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.

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

SYS. IT-süsteemid

SYS.2: Klientarvutid

SYS.2.2: Windows kliendid

SYS.2.2.3: Windows 10 klient

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

1.1 Eesmärk

Esitada meetmed operatsioonisüsteemi Windows 10 kasutavates klientarvutites (klientides) olevate andmete kaitseks.

1.2 Vastutus

Windows 10 klientarvutile esitatud turvameetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Kasutaja.

1.3 Piirangud

Selle mooduli Windows 10 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

Sisukord

[2.1 Windowsile suunatud kahjurprogrammid](#)

[2.2 Integreeritud pilvefunktsioonid](#)

[2.3 Tarkvara ühilduvusprobleemid](#)

[2.4 Windows 10 telemeetriafunktsioonide väärkasutus](#)

[2.5 Raskendatud intsidendikäsitlus VSM \(Virtual Secure Mode\) kasutamisel](#)

2.1 Windowsile suunatud kahjurprogrammid

Tänu Windowsi operatsioonisüsteemide laialdasele levikule on Windows 10 puhul kasutamiseks loodud palju 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 sisaldab 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 10 vaikeseadena võimalust varundada *BitLocker*i 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 puhul esineda ühilduvusprobleeme. Seetõttu vana tarkvara enam Windows 10 kliendil 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 Windows 10 signeeritud draiveritega (ingl *driver*), mida ei pruugi vanade riistvarakomponentide jaoks enam saadaval olla.

2.4 Windows 10 telemeetriafunktsioonide väärkasutus

Windows 10 saadab Microsoftile pidevalt diagnostikaandmeid. Microsoft Windows 10 võib integreeritud telemeetriateenuse abil kliendile ka ise päringuid saata. Windows 10 Pro 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 10 Enterprise keskkonnas kasutatakse andmete kaitsmiseks ja juurdepääsu tõkestamiseks VSM (*Virtual Secure Mode*) virtualiseerimislahendust, halvenevad võimalused arvutiprotsesside analüüsiks. VSM abil kapseldatud protsesside andmetest ei saa IT-kriminalistika (ingl *computer forensics*) eesmärgil teha hilisemaks analüüsiks mälutõmmiseid (ingl *memory dump*), mistõttu on IT-intsidenti käsitlemine raskendatud.

3 Meetmed

Sisukord

[3.1 Elutsükk](#)

[3.2 Põhimeetmed](#)

[SYS.2.2.3.M1 Windows 10 pilvteenuste rakendamise kava](#)

[SYS.2.2.3.M2 Windows 10 sobiva versiooni valimine](#)

[SYS.2.2.3.M4 Telemeetria andmekaitse](#)

[SYS.2.2.3.M5 Windows 10 kahjurvara tõrje](#)

[SYS.2.2.3.M12 Faili- ja kataloogiõiguste haldus](#)

[3.3 Standardmeetmed](#)

[SYS.2.2.3.M6 Võrgukontode integreerimine \[kasutaja\]](#)

[SYS.2.2.3.M9 Keskne autentimine](#)

[SYS.2.2.3.M13 Funktsiooni *SmartScreen* desaktiveerimine](#)

[SYS.2.2.3.M14 Digitaalse assistendi *Cortana* desaktiveerimine \[kasutaja\]](#)

[SYS.2.2.3.M15 Windows 10 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 \[kasutaja\]](#)

[SYS.2.2.3.M20 UAC kasutamine eeliskontodega](#)

[3.4 Kõrgmeetmed](#)

[SYS.2.2.3.M21 Krüpteeringuga failisüsteemi EFS kasutamine \(C-I\)](#)

[SYS.2.2.3.M22 *Windows PowerShell* i kasutamine \(C-I-A\)](#)

[SYS.2.2.3.M23 Sisselogimisteabe lisaturve \(C-I\)](#)

[SYS.2.2.3.M24 Viimase pöördumise ajatembelduse aktiveerimine \(A\)](#)

[SYS.2.2.3.M25 Komponendi CUET kaugjuurdepääsufunktsioonide turvaline rakendamine \(C-I\)](#)

3.1 Elutsükk

Kavandamine

SYS.2.2.3.M1 Windows 10 pilvteenuste rakendamise kava

Soetamine

SYS.2.2.3.M2 Windows 10 sobiva versiooni valimine

Evitus

SYS.2.2.3.M4 Telemeetria andmekaitse

SYS.2.2.3.M5 Windows 10 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 Windows 10 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

3.2 Põhimeetmed

SYS.2.2.3.M1 Windows 10 pilvteenuste rakendamise kava

a. Windows 10 hankimise kavandamisel on otsustatud, milliseid pilvteenuseid ja millises ulatuses on lubatud kasutada.

SYS.2.2.3.M2 Windows 10 sobiva versiooni valimine

a. Windows 10 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 andmekaitseade

a. Telemeetriateenuste andmete edastamine operatsioonisüsteemi tootjale on seadistuses piiratud (Windows 10 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 10 kahjurvara tõrje

a. Kui IT-süsteemi kaitsmiseks kahjurvaraga nakatumise eest ei ole kasutusele võetud samaväärseid või rangemaid meetmeid, on Windows 10 klientidel aktiveeritud Microsofti kahjurvaratõrje (*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 10 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. Keskseks 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 keskest autentimisest on põhjendatud ja kooskõlastatud infoturbejuhiga.

SYS.2.2.3.M13 Funktsiooni *SmartScreen* desaktiveerimine

- a. Windows 10 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 Windows 10 sünkroonismehhanismide desaktiveerimine

- a. Kasutajaandmete sünkroonimine Microsofti pilvteenustega ja WLAN-paroolide ühiskasutus on desaktiveeritud.

SYS.2.2.3.M16 *Microsoft Store* turvaline kasutus

- a. Microsoft Store kasutamise lubatavust ja vastavust organisatsiooni andmekaitse- ja turvanõuetele on hinnatud.
- b. Kui Microsoft Store pole äppide Windows 10-sse installimiseks nõutav, on Microsoft Store desaktiveeritud.

SYS.2.2.3.M17 Automaatse sisselogimise keeld

a. Paroolide, sertifikaatide ja muu teabe salvestamine veebilehtedele ja IT-süsteemidesse automaatselt 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 algtada 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:

- lõikelaua kasutamine;
- printerite integreerimine;
- irdandmekandjate ja võrgudraivide 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 (*Encrypting File System*, EFS) turvalisus sõltub kasutajakonto paroolist, kaitstakse kasutajakontot tugeva parooliga.

b. Taasteagent (*Data Recovery Agent*) on spetsialiseeritud konto, taasteagendina ei kasutata halduskontot.

c. Taasteagendi privaativõit hoitakse turvaliselt süsteemist eemal välisel andmekandjal. Kõigist privaativõtmetest 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 PowerShell* i kasutamine (C-I-A)

a. *PowerShell* i ja WPS-faile tohivad käivitada ainult haldurid.

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, 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.

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

SYS. IT-süsteemid

SYS.2: Klientarvutid

SYS.2.3: Linuxi ja Unixi klient

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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 kasutatava 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

Sisukord

[2.1 Valideerimata allikatest pärit tarkvara](#)

[2.2 Skriptikeskkonna ärakasutamine](#)

[2.3 Ühistekide dünaamiline laadimine](#)

[2.4 Konfigureerimisvead](#)

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 Ühistekide dünaamiline laadimine

Käsk „LD_PRELOAD“ laadib valitud dünaamilise teegi (*dynamically linked shared object library*) enne muid tüüpteke, 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

Sisukord

[3.1 Elutsükel](#)

[3.2 Põhimeetmed](#)

[SYS.2.3.M1 Haldurite ja kasutajate autentimine \[kasutaja\]](#)

[SYS.2.3.M2 Sobiva distributiivi valimine](#)

[SYS.2.3.M4 Operatsioonisüsteemi tuuma uuendamine](#)

[SYS.2.3.M5 Tarkvarapakettide turvaline install](#)

[3.3 Standardmeetmed](#)

[SYS.2.3.M6 Irdseadmete automaatse failisüsteemiga sidumise keeld \[kasutaja\]](#)

[SYS.2.3.M7 Faili- ja kataloogiõiguste piiramine](#)

[SYS.2.3.M8 Rakenduste pääsuõiguste piiramine](#)
[SYS.2.3.M9 Paroolide turvaline kasutamine käsureal \[kasutaja\]](#)
[SYS.2.3.M11 Kõvaketta liigtäituvuse vältimine](#)
[SYS.2.3.M12 Linuxiga spetsiaalseadmete turvaline kasutamine](#)
3.4 Kõrgmeetmed
[SYS.2.3.M14 Lubamatute välisseadmete vältimine \(C-I-A\)](#)
[SYS.2.3.M15 Soovimatute failide käivitamise lisakaitse \(C-I\)](#)
[SYS.2.3.M17 Nõrkuste ärakasutuse lisatõrje \(C-I\)](#)
[SYS.2.3.M18 Tuuma lisaturve \(C-I\)](#)
[SYS.2.3.M19 Kõvaketta või failide krüpteerimine \(C-I\)](#)
[SYS.2.3.M20 Kriitiliste *SysRq*-funktsioonide piiramine \(C-I-A\)](#)

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 tootetoet (nt riistvarakomponentide draiverite näol) plaanitud kasutaja jooksul.
- c. Enimkasutatavad rakendused on distributiivi osa ja neid ei laeta valideerimata allikatest. Distributiivile lisaks paigaldatud rakendusprogrammidele on tagatud tootja tugi.
- d. Töölaseks kasutamiseks ei valita distributiive, 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 paketi halduri abil ja mitte üksikshaaval 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. Lubamatute rakenduste keelamiseks kasutatakse valgefiltreerimist (ingl *whitelisting*).
- 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 käsureaparametritena.

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 välisseadmeid (ingl *peripheral*) lubatakse kasutada keskselt hallatud valge nimekirja (ingl *whitelisting*) põhisel.
- b. Välisseadme toimimiseks vajalikud tuuma (ingl *kernel*) moodulid laaditakse ja aktiveeritakse ainult siis, kui seade on valges nimekirjas.

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.

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

SYS. IT-süsteemid

SYS.2: Klientarvutid

SYS.2.4: macOS-i klient

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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 kasutatava tarkvara (nt meilikliendid või kontoritarkvara) turbe meetmed on esitatud mooduligrupi APP.1 *Klientrakendused* asjakohastes moodulites.

<https://eits.ria.ee/et/versioon/2021/etalonturbe-kataloog/sys-itsüsteemid/sys2-klientarvutid/sys24-macosi-klient/>

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

Sisukord

[2.1 Kontrollimatu juurdepääs väljaspool organisatsiooni hoitavatele andmetele](#)

[2.2 Apple ID konto kuritarvitamine](#)

[2.3 Ründed raadioliidestele](#)

[2.4 Ründed elvaatefunktsiooni sisaldavatele rakendustele](#)

[2.5 Ebaturvalised protokollid macOS-is või macOS-rakendustes](#)

2.1 Kontrollimatu juurdepääs väljaspool organisatsiooni hoitavatele andmetele

macOS võimaldab mitmeid teenuseid (nt iCloud andmete salvestamiseks ja sünkroonimiseks), mida kasutatakse Apple'i keskserverites. Kuna kõik andmed ei ole enam täielikult organisatsiooni kontrolli all, on võimalus, et kõrvalised isikud võivad serveritele juurde pääseda, 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 ühilduvasse taasesitusseadmesse. 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

Sisukord

3.1 Elutsükkel**3.2 Põhimeetmed**[SYS.2.4.M1 macOS-i turvalise rakendamise kava](#)[SYS.2.4.M2 macOS-i turvafunktsioonide kasutamine](#)[SYS.2.4.M3 Kasutajakontode haldus \[kasutaja\]](#)**3.3 Standardmeetmed**[SYS.2.4.M4 Kõvaketta krüpteerimine](#)[SYS.2.4.M5 Turvalisust ohustavate funktsioonide desaktiveerimine](#)[SYS.2.4.M6 Ajakohane riistvara](#)[SYS.2.4.M7 Apple ID mitmikautentimine \[kasutaja\]](#)[SYS.2.4.M8 iCloudi keeld tundlike andmete hoiustamisel \[kasutaja\]](#)[SYS.2.4.M9 Täiendava turvatarkvara kasutamine](#)[SYS.2.4.M10 macOS-i personaalse tulemüüri kasutamine](#)[SYS.2.4.M11 Seadme turvaline kõrvaldamine](#)**3.4 Kõrgmeetmed**[SYS.2.4.M12 Püsivaraparool ja buutimiskaitse \(C-I-A\)](#)

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. FileVaulti 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. Tundlike andmeid on lubatud sünkroonida ainult organisatsiooni siseteenuste vahel.

c. Tundlike 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 andmekandjalt 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*“).

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

SYS. IT-süsteemid

SYS.3: Mobiilseadmed

SYS.3.1: Sülearvutid

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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 Linux'i distributiivid). Sülearvutid on levinud enamikes organisatsioonides ning asendavad sageli klassikalist lauarvutit.

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](#).

<https://eits.ria.ee/et/versioon/2021/etalonturbe-kataloog/sys-itsüsteemid/sys3-mobiilseadmed/sys31-sülearvutid/>

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

Sisukord

[2.1 Muutuvast kasutuskeskkonnast tingitud ohud](#)

[2.2 Sülearvuti kaotamine või vargus](#)

[2.3 Sülearvuti kasutajate vahetumine](#)

2.1 Muutuvast kasutuskeskkonnast tingitud ohud

Sülearvuteid võivad kahjustada keskkonnamõjud, näiteks liiga kõrge või liiga madal temperatuur, samuti tolmu 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 andmelekkkest 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

Sisukord

[3.1 Elutsükel](#)

[3.2 Põhimeetmed](#)

[SYS.3.1.M1 Sülearvutite mobiilse kasutamise kord](#)

[SYS.3.1.M3 Personaalne tulemüür](#)

[SYS.3.1.M5 Sülearvuti andmevarundus \[kasutaja\]](#)

[SYS.3.1.M9 Turvaline kaugjuurdepääs](#)

[3.3 Standardmeetmed](#)

[SYS.3.1.M6 Sülearvuti kasutamise eeskiri \[infoturbejuht\]](#)

[SYS.3.1.M7 Sülearvutite väljastuse ja tagastuse kord \[kasutaja\]](#)

[SYS.3.1.M8 Turvaline ühendamine andmesidevõrguga](#)

[SYS.3.1.M10 Andmete sünkroonimine](#)

[SYS.3.1.M11 Toite tagamine \[kasutaja\]](#)

[SYS.3.1.M12 Sülearvuti kaotusest teatamine \[kasutaja\]](#)

[SYS.3.1.M13 Sülearvuti sisu krüpteerimine](#)

[SYS.3.1.M14 Sülearvuti füüsiline turve \[kasutaja\]](#)

[SYS.3.1.M15 Sülearvuti valimise kord \[hankeosakond\]](#)

[3.4 Kõrgmeetmed](#)

[SYS.3.1.M16 Keskne sülearvutite haldus \(C-I\)](#)

[SYS.3.1.M17 Sülearvutite turvaline ladustamine \(A\)](#)

[SYS.3.1.M18 Varguskaitsevahendite kasutamine \(C-I-A\)](#)

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 privaativõrgu (VPN) kaudu (vt [NET.3.3 Virtuaalne privaativõrk](#)).

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 serveriressurse;
- 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 komplekselt 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 korra. 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. Keskseid 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.

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

SYS. IT-süsteemid

SYS.3: Mobiilseadmed

SYS.3.2: Nutitelefon ja tahvelarvuti

SYS.3.2.1: Nutitelefon ja tahvelarvuti üldiselt

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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 Mobiilirakendused \(äpid\)](#) ja [APP.1.2 Veebibrauser](#).

Meetmed kahjurvara eest kaitsmiseks on esitatud moodulis [OPS.1.1.4 Kaitse kahjurprogrammide eest](#).

2 Ohud

Sisukord

- [2.1 Ajakohastamata operatsioonisüsteem](#)
 - [2.2 Tarkvaranõrkused mobiilirakendustes \(äppides\)](#)
 - [2.3 Nutitelefonide või tahvelarvutite manipuleerimine](#)
 - [2.4 Nutitelefonide ja tahvelarvutite kahjurprogrammid](#)
 - [2.5 Veebipõhised ründed mobiilibrauseritele](#)
 - [2.6 Tervise- või asukohaandmete kuritarvitamine](#)
 - [2.7 Lukustatud ekraanil näidatavate andmete kuritarvitamine](#)
 - [2.8 Töötelefoni või tahvelarvutite kasutamine isiklikuks otstarbeks](#)
 - [2.9 Isikliku seadme kasutamisest \(BYOD\) tulenevad ohud](#)
 - [2.10 Tarkvara nõrkuste kasutamine volitamata juurdepääsuks](#)
-

2.1 Ajakohastamata operatsioonisüsteem

Mobiilsetes seadmetes kasutatavatele 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)

Nutitelefonide või tahvelarvutitega 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 Nutitelefonide või tahvelarvutite manipuleerimine

Ründaja võib nutitelefonile või tahvelarvutile juurde pääsedes seadmes olevaid andmeid sihipäraselt manipuleerida. Ta võib näiteks muuta seadme konfiguratsiooni, käivitada täiendavaid teenuseid või märkamatu 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 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 asukohta. 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 mobiilseadmete 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 isiklike 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 igal ajal võimalik avalikus käibes leiduvate vahendite ning juhendite abil.

3 Meetmed

Sisukord

[3.1 Elutsükel](#)

[3.2 Põhimeetmed](#)

[SYS.3.2.1.M1 Nutitelefonide ja tahvelarvutite turvanõuete kehtestamine \[infoturbejuht\]](#)

[SYS.3.2.1.M2 Pilvteenuste kasutamise kord](#)

[SYS.3.2.1.M3 Mobiilseadme turvaline aluskonfiguratsioon](#)

[SYS.3.2.1.M4 Lubamatu kasutuse tõkestamine \[kasutaja\]](#)

[SYS.3.2.1.M5 Operatsioonisüsteemi ja rakenduste ajakohastamine](#)

[SYS.3.2.1.M6 Privaatsussätete ja rakenduste juurdepääsude haldamine](#)

[SYS.3.2.1.M7 Turvasiindmusele reageerimise kord \[kasutaja\]](#)

[SYS.3.2.1.M8 Mobiilirakenduste installimise kord](#)

[3.3 Standardmeetmed](#)

[SYS.3.2.1.M9 Lisafunktsionaalsuse piiramine](#)

[SYS.3.2.1.M10 Mobiilseadmete kasutamise eeskiri \[kasutaja, infoturbejuht\]](#)

[SYS.3.2.1.M11 Nutitelefonide ja tahvelarvuti mälu krüpteerimine](#)

[SYS.3.2.1.M12 Anonüümsete seadmenimedede kasutamine](#)

[SYS.3.2.1.M13 Ekraanijagamise ja meedia ühiskasutuse kord](#)

[SYS.3.2.1.M16 Tarbetute sideliidestite desaktiveerimine \[kasutaja\]](#)

[SYS.3.2.1.M18 Biomeetiline autentimine](#)

[SYS.3.2.1.M19 Virtuaalassistentide kasutamise piiramine](#)

[SYS.3.2.1.M22 VPN-i kasutamine ühenduseks sisevõrguga](#)

[SYS.3.2.1.M28 Veebilehtede filtreerimine](#)

[SYS.3.2.1.M31 Mobiilmaksete käsitlemise kord](#)

[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](#)

[3.4 Kõrgmeetmed](#)

[SYS.3.2.1.M25 Täitmiskeskondade lahusus \(C-I\)](#)

[SYS.3.2.1.M26 PIM kasutamine \(C-I-A\)](#)

[SYS.3.2.1.M27 Kõrgturvaline mobiilseade \(C-I-A\)](#)

[SYS.3.2.1.M29 Organisatsioonipõhine pääsupunkt \(APN\) \(C-I-A\)](#)

[SYS.3.2.1.M30 Äppide installimise valge nimekiri \(C-I-A\)](#)

[SYS.3.2.1.M35 Mobiilseadmete tulemüür \(C-I-A\)](#)

3.1 Elutsükel

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

<https://eits.ria.ee/et/versioon/2021/etalonturbe-kataloog/sys-itsuesteemid/sys3-mobiilseadmed/sys32-nutitelefon-ja-tahvelarvuti/sys321-nutitelefon-ja-tahvelarvuti->

SYS.3.2.1.M10 Mobiilseadmete kasutamise eeskiri

SYS.3.2.1.M11 Nutitelefonide ja tahvelarvuti mälu krüpteerimine

SYS.3.2.1.M12 Anonüümsete seadmenimedega kasutamine

SYS.3.2.1.M13 Ekraanijagamise ja meedia ühiskasutuse kord

SYS.3.2.1.M16 Tarbetute sideliidestega 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 Täitmiskeskondade 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 andmekaitseõuetele. Vajadusel juurdepääs piiratakse või vastav funktsioon desaktiveeritakse.

d. Mobiilirakenduste juurdepääsuõiguste ülevaatus viiakse läbi vastavalt vajadusele.

SYS.3.2.1.M7 Turvasündmusele reageerimise kord [kasutaja]

- a. Kasutaja teavitab organisatsiooni kõigist nutitelefonide 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. Nutitelefoni ja tahvelarvutist on keelatud eemaldada sinna paigutatud haldustarkvara ja muuta mobiilseadme turvaseadeid.
- d. Eeskiri sätestab nutitelefonide ja tahvelarvutite juurimise (ingl *root*) keelu.

SYS.3.2.1.M11 Nutitelefonide ja tahvelarvutite mälu krüpteerimine

- a. Nutitelefonide ja tahvelarvutite püsिमälu (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. Virtuaalassistenti 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 privaativõrgu (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

<https://eits.ria.ee/et/versioon/2021/etalonturbe-kataloog/sys-itsusteemid/sys3-mobiilseadmed/sys32-nutitelefon-ja-tahvelarvuti/sys321-nutitelefon-ja-tahvelarvuti->

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 Täitmiskeskondade lahusus (C-I)

- a. Kui töötajad võivad organisatsiooni antud tööseadmeid kasutada ka isiklikuks tarbeks, siis on selleks loodud seadmes eraldi täitmiskeskond.
- b. Võimalusel kasutatakse lahutatud täitmiskeskondi ainult selleks sertifitseeritud seadmetes (nt *Common Criteria* alusel).
- c. Tööga seotud andmed asuvad eranditult töötstarbelises täitmiskeskonnas.
- d. Pärast määratud arvu järjestikuseid ebaõnnestunud mobiilseadme avamiskatseid kustutatakse mobiilseadmest töötstarbelise täitmiskeskonna 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 infotöötluks 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 protokoll CHAP (ingl *challenge-handshake authentication protocol*, CHAP).

SYS.3.2.1.M30 Äppide installimise valge nimekiri (C-I-A)

<https://eits.ria.ee/et/versioon/2021/etalonturbe-kataloog/sys-itsusteemid/sys3-mobiilseadmed/sys32-nutitelefon-ja-tahvelarvuti/sys321-nutitelefon-ja-tahvelarvuti->

a. Nutitelefonide või tahvelarvutite 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“

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetusskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

SYS. IT-süsteemid

SYS.3: Mobiilseadmed

SYS.3.2: Nutitelefon ja tahvelarvuti

SYS.3.2.2: Mobiilseadmete haldus (MDM)

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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

Sisukord

[2.1 Puudulik sünkroonimine](#)

[2.2 Vead mobiilseadmete halduses](#)

[2.3 Puudulik pääsuõiguste haldus](#)

[2.4 Asukohainfo lubamatu jälgimine mobiilseadmete halduse kaudu](#)

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 andmekaitseõuete 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 andmekaitseõueteid. 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

Sisukord

[3.1 Elutsükel](#)

[3.2 Põhimeetmed](#)

[SYS.3.2.2.M1 Mobiilseadmete halduse põhimõtted](#)

[SYS.3.2.2.M2 Mobiilseadmete aktsepteeritud mudelid](#)
[SYS.3.2.2.M3 MDM tarkvara valimine](#)
[SYS.3.2.2.M4 Mobiilseadmete integreerimine MDM tarkvaraga](#)
[SYS.3.2.2.M5 MDM kliendi installimine](#)
[SYS.3.2.2.M20 Mobiilseadmete halduse regulaarne läbivaatus](#)
[3.3 Standardmeetmed](#)
[SYS.3.2.2.M6 Logimine ja seadme oleku seire](#)
[SYS.3.2.2.M7 Mobiilirakenduste \(äppide\) installimine](#)
[SYS.3.2.2.M12 MDM-i turve](#)
[SYS.3.2.2.M21 Sertifikaatide haldus](#)
[SYS.3.2.2.M22 Mobiilseadmete kasutuselt kõrvaldamine](#)
[3.4 Kõrgmeetmed](#)
[SYS.3.2.2.M14 Äppide hindamine välise maineteenuse abil \(C-I\)](#)
[SYS.3.2.2.M17 Mobiilseadmete kasutamise seire \(I\)](#)
[SYS.3.2.2.M19 Geotarastuse kasutamine \(C-I\)](#)
[SYS.3.2.2.M23 Vastavusnõuete jõustamine \(C-I\)](#)

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 mobiilseadmete 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 seadistusega 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 ilmunisel 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.

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

SYS. IT-süsteemid

SYS.3: Mobiilseadmed

SYS.3.2: Nutitelefon ja tahvelarvuti

SYS.3.2.3: Organisatsiooni iOS

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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

Sisukord

[2.1 iOS seadme lahtimurdmine \(*jailbreaking*\)](#)

[2.2 Apple ID konto kuritarvitamine](#)

[2.3 Eelpaigaldatud rakenduste laialdased õigused](#)

[2.4 Biomeetrilise autentimise kuritarvitamine](#)

[2.5 Lukustatud ekraanil näidatavate andmete kuritarvitamine](#)

[2.6 Lubamatu juurdepääs väljaspool organisatsiooni hoitavatele andmetele](#)

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 tehase seadeid 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 süntoonitakse 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

Sisukord

[3.1 Elutsükk](#)

[3.2 Põhimeetmed](#)

[SYS.3.2.3.M1 iOS-põhiste seadmete rakendamise põhimõtted](#)

[SYS.3.2.3.M2 Pilvteenuste rakendamise kava](#)

[SYS.3.2.3.M7 Konfiguratsiooniprofiilide turve](#)

[3.3 Standardmeetmed](#)

[SYS.3.2.3.M10 Biomeetriline autentimine](#)

[SYS.3.2.3.M12 Apple ID anonüümimine](#)

[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](#)

[SYS.3.2.3.M21 Rakenduste lisamise ja kinnitamise kord](#)

[3.4 Kõrgmeetmed](#)

[SYS.3.2.3.M23 Konfiguratsiooniprofiili automaatne kustutamine \(C-I\)](#)

[SYS.3.2.3.M25 Teenuse AirPrint turvaline kasutamine \(C-I\)](#)

[SYS.3.2.3.M26 IT-süsteemidega lubamatu ühendamise vältimine \(C-I\)](#)

3.1 Elutsükk

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 keskeks 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 andmekaitsevenõuetega.
- 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 seadud 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 organisatsioonisisesest 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.

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

SYS. IT-süsteemid

SYS.3: Mobiilseadmed

SYS.3.2: Nutitelefon ja tahvelarvuti

SYS.3.2.4: Android

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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

Sisukord

[2.1 Juurimine \(rooting\) Androidiga seadmes](#)

[2.2 Androidiga seadmete kahjurvara](#)

[2.3 Ajakohastamata operatsioonisüsteem](#)

[2.4 Google konto kuritarvitamine](#)

[2.5 Eelpaigaldatud rakenduste laialdased õigused Androidis](#)

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 igaljuhul 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 seadme 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

Sisukord

[3.1 Elutsükk](#)[3.2 Põhimeetmed](#)[SYS.3.2.4.M1 Androidiga seadmete valimise kord](#)[3.3 Standardmeetmed](#)[SYS.3.2.4.M2 Arendaja sätete desaktiveerimine](#)[SYS.3.2.4.M3 Mitmekasutajarežiimi ja külalisrežiimi piiramine](#)[SYS.3.2.4.M5 Laiendatud turbeseaded](#)[3.4 Kõrgmeetmed](#)

3.1 Elutsükk

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.

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

SYS. IT-süsteemid

SYS.3: Mobiilseadmed

SYS.3.3: Mobiiltelefon

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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.

Nutitefonide ja nendes kasutatavate operatsioonisüsteemide turvanõuded on esitatud mooduligrupis SYS. 3.2 *Nutitefon ja tahvelarvuti*. Nutitefonidele rakendatakse kõiki meetmeid moodulist [SYS.3.2.1 Nutitefon ja tahvelarvuti üldiselt](#).

Andmesidepõhise telefonside aspekte käsitletakse moodulis [NET.4.2 Netitefon \(VOIP\)](#).

Kui vaadeldav mobiiltelefon kasutab virtuaalse privaativõrgu tehnoloogiaid, siis tuleb arvesse võtta ka moodulit [NET.3.3 Virtuaalne privaativõrk \(VPN\)](#).

2 Ohud

Sisukord

[2.1 Vead mobiiltelefonide hankimisel](#)

[2.2 Mobiiltelefoni kaotamine](#)

[2.3 Hooletus mobiiltelefoni käsitlemisel](#)

[2.4 Organisatsiooni mobiiltelefoni kasutamine isiklikuks tarbeks](#)

[2.5 Mobiiltelefoni tõrge](#)

[2.6 Ühendusandmete kuritarvitamine](#)

[2.7 Vestluste lubamatu salvestamine](#)

[2.8 Vananenud mobiiltelefonide kasutamine](#)

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 konkreetsetes 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 käsitlemisel

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 rikkal võib olla erinevaid põhjusi. Telefon võib hooletul käsitlemisel 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 pealtkuulamiseadet. 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 nutitelefoni pakkumine tunduvalt „nuputelefoni“ 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 originaalosaadega 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

Sisukord

[3.1 Elutsükel](#)

[3.2 Põhimeetmed](#)

[SYS.3.3.M1 Mobiiltelefonide kasutamise eeskiri](#)

[SYS.3.3.M2 Mobiiltelefoni blokeerimine seadme kaotamisel \[kasutaja\]](#)

[SYS.3.3.M3 Kasutajate koolitamine ja teadlikkuse tõstmine](#)

[SYS.3.3.M4 Mobiiltelefonide kasutuselt kõrvaldamise kord](#)

[SYS.3.3.M5 Mobiiltelefonide turvamehhanismide kasutamine \[kasutaja\]](#)

[SYS.3.3.M6 Mobiiltelefoni tarkvara ajakohastamine \[kasutaja\]](#)

[3.3 Standardmeetmed](#)

[SYS.3.3.M7 Mobiiltelefonide hankimise kord](#)

[SYS.3.3.M8 Tarbetute raadioliideste desaktiveerimine \[kasutaja\]](#)

[SYS.3.3.M10 Turvaline andmevahetus\[kasutaja\]](#)

[SYS.3.3.M11 Mobiiltelefoni avariivalmendus \[kasutaja\]](#)

[SYS.3.3.M12 Piisav mobiiltelefonide varu](#)

[3.4 Kõrgmeetmed](#)

[SYS.3.3.M9 Mobiiltelefonide toite tagamine \[kasutaja\] \(A\)](#)

[SYS.3.3.M13 Liikumise seire vältimine \[kasutaja\] \(C\)](#)

[SYS.3.3.M14 Telefoninumbri näitamise blokeerimine \[kasutaja\] \(C\)](#)

[SYS.3.3.M15 Kaitse mobiiltelefoniga pealtkuulamise eest \(C\)](#)

3.1 Elutsükel

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 seadme parooli või muu turvamehhanismiga.
- e. Pääsukood (sh PUK-koodid) ja teenuste parooli 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 kompleksust, 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 numbrit 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.

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

SYS. IT-süsteemid

SYS.4: Muud süsteemid

SYS.4.1: Printer ja kontorikombain

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

1.1 Eesmärk

Esitada meetmed printeri ja kontorikombaini turvaliseks kasutamiseks.

Tänapäevased printerid, koopiaimasinad ja kontorikombainid on keerukad võrgustatud seadmed ja sageli töödeldakse neis konfidentsiaalset teavet.

Märkus: edaspidi koopiaimasinaid eraldi ei mainita, aga paljusid selles moodulis toodud ohte ja meetmeid tuleb arvestada ja rakendada ka koopiaimasinate 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 koopiaimasinate 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

Sisukord

[2.1 Prinditud dokumentide lubamatu nähtavalejätmine](#)

[2.2 Metaandmete nähtavus](#)

[2.3 Salvestatud teabe ebapiisav kaitse](#)

[2.4 Krüpteerimata side](#)

[2.5 Dokumentide lubamatu edastamine](#)

[2.6 Dokumentide lubamatu kopeerimine ja skaneerimine](#)

[2.7 Ebapiisav võrguturve](#)

[2.8 Seadmete halduse ebapiisav turve](#)

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 väljatrükitud lähedalasuvasse prügikasti. Sealt võivad väljatrükitud 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 väärtalt. 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 märkamatuks 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 organisatsioonisisised 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

Sisukord

[3.1 Elutsükkel](#)

[3.2 Põhimeetmed](#)

[SYS.4.1.M1 Printerite ja kontorikombainide rakendamise kava](#)

[SYS.4.1.M2 Printeri ja kontorikombaini füüsilise juurdepääsu piiramine](#)

[SYS.4.1.M5 Printerite ja kontorikombainide kasutamise eeskiri \[infoturbejuht\]](#)

[SYS.4.1.M22 Prinditud dokumentide kasutuselt kõrvaldamise kord](#)

[3.3 Standardmeetmed](#)

[SYS.4.1.M4 Printerite ja kontorikombainide turvaeeskiri \[infoturbejuht\]](#)

[SYS.4.1.M7 Printeri ja kontorikombaini halduspääsu kitsendamine](#)

[SYS.4.1.M11 Printeri ja kontorikombaini võrguühenduse piiramine](#)

[SYS.4.1.M15 Andmete krüpteerimine printeris ja kontorikombainis](#)

[SYS.4.1.M16 Printeri ja kontorikombaini seisakuaja vähendamine](#)

[SYS.4.1.M17 Ajutiste andmete ja metaandmete turve](#)

[SYS.4.1.M18 Printeri ja kontorikombaini turvaline konfiguratsioon](#)

[3.4 Kõrgmeetmed](#)

[SYS.4.1.M14 Seadme kasutaja täiendav autentimine \(C-I-A\)](#)

[SYS.4.1.M20 Printeri ja kontorikombaini andmestiku täiendav turve \(C\)](#)

[SYS.4.1.M21 Printeri ja kontorikombaini laiendatud turve \(I-A\)](#)

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 teabelekena.

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 eraldi 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, PJJ) 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 kasutata püsivara ega tarkvara, millel pole konkreetse seadmetootja heakskiitu.

4 Lisateave

Siin lisainfot ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

SYS. IT-süsteemid

SYS.4: Muud süsteemid

SYS.4.3: Sardsüsteemid (embedded systems)

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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 käsitusallas 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

Sisukord

[2.1 Puudulikud turvanõuded sardsüsteemide väljatöötamisel](#)

[2.2 Sardsüsteemi turvamata sisend- ja väljundliidesed](#)

[2.3 Sardsüsteemi puudulik füüsiline turve](#)

[2.4 Sardsüsteemi riistvaratõrge või -viga](#)

[2.5 Sardsüsteemi tarkvarauuendite manipuleerimine](#)

[2.6 Sisseehitatud krüptosüsteemide kõrvalkanalrünne](#)

[2.7 Sardsüsteemi manipuleerimine sideliidese kaudu](#)

[2.8 Järeletehtud komponentide kasutamine](#)

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 märkamatuult 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 välgmälli (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 Sissehitatud 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 Sardüsteemi 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 mobiilsideliidese kaudu. Süsteemi tungida saab ka lokaalsete sideliidest, 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 väärtalt 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

Sisukord

[3.1 Elutsükel](#)

[3.2 Põhimeetmed](#)

[SYS.4.3.M1 Sardüsteemide rakendamise kord](#)

[SYS.4.3.M2 Sardüsteemi mittevajalike liidest ja teenuste desaktiveerimine \[arendaja\]](#)

[SYS.4.3.M3 Sardüsteemi turvasündmuste logimine](#)

[SYS.4.3.M5 Sardüsteemi kaitse kahjulike keskkonnamõjude eest \[arendaja, arhitekt\]](#)

[3.3 Standardmeetmed](#)

[SYS.4.3.M4 Sardüsteemi nõuete spetsifikatsioon \[hankeosakond\]](#)

[SYS.4.3.M6 Sardüsteemi programmikoodi turve \[arendaja\]](#)

[SYS.4.3.M7 Sardüsteemi funktsioonide turvaline teostus riistvaras \[arendaja, arhitekt, hankeosakond\]](#)

[SYS.4.3.M8 Sardüsteemi turvaline operatsioonisüsteem \[arendaja, arhitekt\]](#)

[SYS.4.3.M10 Sardüsteemi taaste](#)

[SYS.4.3.M11 Sardüsteemi turvaline kõrvaldamine](#)

[3.4 Kõrgmeetmed](#)

[SYS.4.3.M9 Krüptoprotsessorite ja kaasprotsessorite kasutamine \[arendaja, arhitekt\] \(C-I\)](#)

[SYS.4.3.M12 Usaldusväärne sardsüsteemi tarne- ja logistikaahel \[hankeosakond\] \(C-I-A\)](#)

[SYS.4.3.M13 Sertifitseeritud operatsioonisüsteem \[arendaja, arhitekt\] \(C-I-A\)](#)

[SYS.4.3.M14 Sardüsteemi buutimise turve ja autentimine \[arendaja, arhitekt\] \(C-I\)](#)

[SYS.4.3.M15 Sardüsteemi mäluhalduse turve \[arendaja, arhitekt\] \(C-I\)](#)

[SYS.4.3.M16 Sardüsteemi muukimisrünnete tõrje \(C-I\)](#)

[SYS.4.3.M17 Sardüsteemi moodulite enesetestimine \(I-A\)](#)

[SYS.4.3.M18 Sardüsteemi kõrvalkanalrünnete tõrje \(C\)](#)

3.1 Elutsükkel

Kavandamine

SYS.4.3.M1 Sardüsteemide rakendamise kord

SYS.4.3.M5 Sardüsteemi kaitse kahjulike keskkonnamõjude eest

SYS.4.3.M7 Sardüsteemi funktsioonide turvaline teostus riistvaras

Soetamine

SYS.4.3.M4 Sardüsteemi nõuete spetsifikatsioon

Evitus

SYS.4.3.M2 Sardüsteemi mittevajalike liideste ja teenuste desaktiveerimine

SYS.4.3.M6 Sardüsteemi programmikoodi turve

SYS.4.3.M8 Sardüsteemi turvaline operatsioonisüsteem

Käitus

SYS.4.3.M3 Sardüsteemi turvasündmuste logimine

SYS.4.3.M9 Krüptoprotsessorite ja kaasprotsessorite kasutamine

Kõrvaldamine

SYS.4.3.M11 Sardüsteemi turvaline kõrvaldamine

Avariivalmendus

SYS.4.3.M10 Sardüsteemi taaste

Lisanduvad kõrgmeetmed

SYS.4.3.M12 Usaldusväärne sardsüsteemi tarne- ja logistikaahel

SYS.4.3.M13 Sertifitseeritud operatsioonisüsteem

SYS.4.3.M14 Sardüsteemi buutimise turve ja autentimine

SYS.4.3.M15 Sardüsteemi mäluhalduse turve

SYS.4.3.M16 Sardüsteemi muukimisrünnete tõrje

SYS.4.3.M17 Sardüsteemi moodulite enesetestimine

SYS.4.3.M18 Sardüsteemi kõrvalkanalrünnete tõrje

3.2 Põhimeetmed

SYS.4.3.M1 Sardüsteemide rakendamise kord

a. Sardüsteemide rakendamiseks ja probleemideta halduse tagamiseks on määratud: • süsteemi kaitsetarve; • 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. On kehtestatud sardsüsteemide tervikluse ja töövõimelisuse testimise kord.

c. Sardüsteemide algseadistus on turvaline. Kasutatav konfiguratsioon on dokumenteeritud.

d. Kõigile kasutajatele ja halduritele on tutvustatud tõrgete, talitlushäirete või turvaintsidenti kahtluse korral tegutsemise juhiseid ja teavituskanaleid.

SYS.4.3.M2 Sardüsteemi 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. Tarbetud ja ebaturvalised protokollid ja teenused (NetBios, Telnet, http, ftp) on desaktiveeritud.

d. Sardüsteemi kasutava rakenduse juurdepääs sardsüsteemi liidestele on kaitstud turvalise autentimisega.

e. Sardüsteemi liidestega seotud nõrkuste tuvastamiseks kasutatakse pordiskannereid ja muid asjakohaseid võrguturbe rakendusi.

SYS.4.3.M3 Sardüsteemi turvasündmuste logimine

a. Sardüsteemi 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. Sardüsteemi logidele on juurdepääs üksnes määratud isikutel.

f. Logisid ja logiraamatu sissekandeid analüüsitakse regulaarselt ja intsidendipõhiselt.

SYS.4.3.M5 Sardüsteemi kaitse kahjulike keskkonnamõjude eest [arendaja, arhitekt]

a. Tulenevalt sardsüsteemi kasutusviisist ja -kohast kaitstakse sardsüsteemi tolmu, kuumuse, niiskuse ja muude kahjulike keskkonnamõjude eest.

b. Vajalike kaitsemeetmetega on arvestatud juba sardsüsteemi taristu kavandamise järgus.

c. Sardüsteemi 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, kooolitus jms);
- tehnilised ja majanduslikud nõuded (funktsioonid, reaalajanõuded, energiatarve, kulud jms);
- vastavus tööstusala standarditele ja tavadele (sertifikaatide olemasolu);
- füüsiline kaitstud 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. 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 usaldusväärust.

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. Sardüsteemi põhimälu on struktureeritud selliselt, et ühe programmi viga ei mõjuta teiste programmide või kogu süsteemi stabiilsust.
- b. Programmide andmepäas teiste programmide mälupiirkondadele on tõkestatud riistvaraliselt MPU (*Memory Protection Unit*, MPU) või MMU (*Memory Management Unit*, MMU) abil.
- c. Riistvaralise turbe puudumisel kontrollitakse mälu pöördumisi tarkvaraliselt. Kontrollimine võib toimuda pärast kompileerimist või programmi käituse ajal automaatsete kontrollidena.

SYS.4.3.M16 Sardüsteemi muukimisrünnete tõrje (C-I)

- a. Muukimisrünnete (ingl *tampering attack*) avastamiseks, registreerimiseks ja takistamiseks (ingl *tamper response*) kasutatakse sobivaid vahendeid.
- b. Sardüsteemi füüsiliseks kaitseks kasutatakse turvalisi korpuseid ning kinnitatakse sardüsteem 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 Sardüsteemi moodulite enesetestimine (I-A)

- a. Sardüsteemi 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 Sardüsteemi kõrvalkanalrünnete tõrje (C)

- a. Sardüsteemi 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.

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetusskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

SYS. IT-süsteemid

SYS.4: Muud süsteemid

SYS.4.4: Esemevõrgu (IoT) seade üldiselt

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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

Sisukord

[2.1 Luure esemevõrgu seadme kaudu](#)

[2.2 Automaathäälestuse \(UPnP\) kasutamine](#)

[2.3 Hajus ummistusrünne \(DDoS\)](#)

[2.4 Spionaaž esemevõrgu seadme tagaukse kaudu](#)

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

Sisukord

[3.1 Elutsükel](#)

3.2 Põhimeetmed[SYS.4.4.M1 IoT seadmete turvanõuete määramine](#)[SYS.4.4.M2 IoT seadme autentimine](#)[SYS.4.4.M5 IoT seadme võrkupääsu piiramine](#)**3.3 Standardmeetmed**[SYS.4.4.M6 IoT seadmete kaasamine organisatsiooni turvapoliitikasse \[infoturbejuht\]](#)[SYS.4.4.M7 IoT seadmete rakendamise kava](#)[SYS.4.4.M8 IoT seadmete hankimise kriteeriumid \[hankeosakond, infoturbejuht\]](#)[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](#)[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](#)[SYS.4.4.M20 Esemevõrgu seadme korrahane kasutuselt kõrvaldamine](#)**3.4 Kõrgmeetmed**[SYS.4.4.M21 Töökeskkond ja elektritoide \[tehnikatalitus\] \(I\)](#)[SYS.4.4.M22 Esemevõrgu seire \(A\)](#)[SYS.4.4.M23 Esemevõrgu seadmete audit \(C-I-A\)](#)[SYS.4.4.M24 IoT seadme veebiserveri turvaline konfiguratsioon ja kasutamine \(C-I-A\)](#)

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 kasutatavate 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.

a. Sisenevad ja väljuvad võrguühendused ja sihtkohad on piiratud ruuterite pääsuloenditega (ACL) ja tulemüüri reeglitega (nt valvekaamerale piisab ühendustest tootja uuendusserveri, videoandmete salvestuskoha ja haldussüsteemiga).

- b. Telneti (port 23) kaudu juurdepääs on blokeeritud.
- c. Marsruutimine on kitsendav, vaikemarsruudid on blokeeritud.
- d. Kõigis ruuterites on automaathäälestuse funktsioon UPnP desaktiveeritud.
- e. Esemevõrgu seadmed ja andurid asuvad eraldi võrgusegmendis, mis omab ühendust ainult halduse võrgusegmendiga.
- f. Kaugpöördumine esemevõrgu seadme poole toimub SSH (vaikeport 22) ja turvalise autentimisega.
- g. 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 kaitstud 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 protokollu 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 logismehhanisme.
- 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 võrgusegmen dist.
- 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.

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

SYS. IT-süsteemid

SYS.4: Muud süsteemid

SYS.4.5: Irdandmekandjad

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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. Irdandjate hulka kuuluvad muuhulgas välised kõvakettad, CD-d, DVD-d, mälukaartid, magnetlindid ja mälupulgad.

1.2 Vastutus

Irdandjate 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 töötleva (nt nutitelefonid) esitatakse moodulis [SYS.3.2.1 Nutitelefon ja tahvelarvuti üldiselt](#).

Turvalise andmevahetuse korraldamist irdandmekandjate abil käsitletakse moodulis [CON.9 Teabevahetus](#).

2 Ohud

Sisukord

[2.1 Hooletus teabe käitlemisel](#)

[2.2 Puudulik eeskirjade tundmine](#)

[2.3 Irdandmekandjate vargus või kaotamine](#)

[2.4 Defektsed andmekandjad](#)

[2.5 Kahjustus muutuva kasutuskeskkonna tõttu](#)

[2.6 Kahjurprogrammide levitamine](#)

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 kasutatavate tehnoloogiate tõttu alati 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, tolmu 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

Sisukord

[3.1 Elutsükkel](#)

[3.2 Põhimeetmed](#)

[SYS.4.5.M1 Töötajate teadlikkuse tõstmine](#)

[SYS.4.5.M2 Irdandmekandja kaotamisest või manipulatsioonist teatamine \[kasutaja\]](#)

[SYS.4.5.M12 Kahjurvaratõrje \[kasutaja\]](#)

[3.3 Standardmeetmed](#)

[SYS.4.5.M4 Irdandmekandjate kasutamise eeskiri](#)

[SYS.4.5.M5 Irdandmekandjate kaasavõtmise kord](#)

[SYS.4.5.M6 Irdandmekandjate halduse kord \[vastutav spetsialist\]](#)

[SYS.4.5.M7 Andmekandja turvaline kustutus enne ja pärast kasutamist \[vastutav spetsialist\]](#)

[SYS.4.5.M13 Andmekandja nõuetekohane märgistus \[kasutaja\]](#)

[3.4 Kõrgmeetmed](#)

[SYS.4.5.M10 Andmekandja krüpteerimine \(C-I\)](#)

[SYS.4.5.M11 Tervikluse kaitse kontrollkoodi või digitaalsignatuuriga \(I\)](#)

[SYS.4.5.M14 Turvaline transport ja pakend \(C-I-A\)](#)

[SYS.4.5.M15 Sertifitseeritud tooted \(C-I-A\)](#)

[SYS.4.5.M16 Spetsialiseeritud andmelüüsid \(C-I\)](#)

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 Kahjurvaratõrje

SYS.4.5.M7 Andmekandja turvaline kustutus enne ja pärast kasutamist

SYS.4.5.M13 Andmekandja nõuetekohane märgistus

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 tooted

SYS.4.5.M16 Spetsialiseeritud andmeliüüsid

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.

SYS.4.5.M12 Kahjurvaratõrje [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;
 - 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 andmekandjalt 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 Andmekandja nõuetekohane märgistus [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.

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 tooted (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.

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetusskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

SYS. IT-süsteemid

SYS.1: Server

SYS.1.1: Server üldiselt

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

1.1 Eesmärk

Esitada serverites töeldavate 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

Infoturbejuht, tehnikatalitus, hankeosakond.

1.3 Piirangud

Kui serveriteenuse või IT-süsteemi jaoks on välja töötanud eraldiseisev etalonturbe moodul, lähtutakse eelkõige spetsiifilisest moodulist ja alles seejärel käesolevast moodulist.

Täiendavalt rakendatakse serverile meetmeid moodulitest [ORP.4 Identiteedi ja õiguste haldus](#), [DER.4 Avariiahaldus](#), [OPS.1.1.2 IT-haldus](#), [OPS.1.1.3 Paiga- ja muudatusehaldus](#) ja [OPS.1.1.4 Kaitse kahjurprogrammide eest](#).

Serveri turvaline paigutamist võrku käsitletakse moodulis [NET.1.1 Võrgu arhitektuur ja lahendus](#).

2 Ohud

Sisukord

[2.1 Andmekadu](#)

[2.2 Teenusetõkestusründed](#)

[2.3 Tarbetud operatsioonisüsteemi komponendid ja rakendused](#)

[2.4 Serveri ülekoormus](#)

2.1 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 püsijäämise.

2.2 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.

2.3 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.

2.4 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 andmebaasserver 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

Sisukord

[3.1 Elutsükel](#)

[3.2 Põhimeetmed](#)

[SYS.1.1.M1 Serveri turvaline asukoht \[tehnikatalitus\]](#)

[SYS.1.1.M2 Kasutajate autentimine](#)

[SYS.1.1.M5 Haldusliideste kaitse](#)

[SYS.1.1.M6 Tarbetute teenuste desaktiveerimine](#)

[SYS.1.1.M9 Kahjurvaratõrje rakenduste kasutamine serveril](#)

[SYS.1.1.M10 Serveri logimine](#)

3.3 Standardmeetmed

[SYS.1.1.M11 Serveri turvapoliitika kehtestamine \[infoturbejuht\]](#)

[SYS.1.1.M12 Serveri kasutuselevõtu kava](#)

[SYS.1.1.M13 Serveri hankimine \[hankeosakond\]](#)

[SYS.1.1.M15 Katkestusteta ja stabiilne toide \[tehnikatalitus\]](#)

[SYS.1.1.M16 Serveri turvaline aluskonfiguratsioon](#)

[SYS.1.1.M19 Lokaalsed paketifiltrid](#)

[SYS.1.1.M21 Serveri käidudokumentatsiooni koostamine](#)

[SYS.1.1.M22 Integreerimine avariivalmendusega](#)

[SYS.1.1.M23 Serverisüsteemi seire](#)

[SYS.1.1.M24 Regulaarne turbe testimine](#)

[SYS.1.1.M25 Serveri kasutuselt kõrvaldamise kord](#)

[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](#)

3.4 Kõrgmeetmed

[SYS.1.1.M27 Hostipõhine sissetungituvastus \(I-A\)](#)

[SYS.1.1.M28 Liiasus \(A\)](#)

[SYS.1.1.M30 Üks teenus serveri kohta \(C-I-A\)](#)

[SYS.1.1.M31 Rakenduste käitamise tõkestamine \(C-I\)](#)

[SYS.1.1.M33 Juursertifikaadi aktiivne haldus \(C-I\)](#)

[SYS.1.1.M38 Serveri süsteemifailide tugevdatud kaitse \(I\)](#)

3.1 Elutsükkel

Kavandamine

SYS.1.1.M11 Serveri turvapoliitika 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 Serveri turvaline asukoht

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 aluskonfiguratsioon

Käitus

SYS.1.1.M9 Kahjurvaratõrje rakenduste kasutamine serveril

SYS.1.1.M10 Serveri logimine

SYS.1.1.M19 Lokaalsed paketilfrid

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

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 Serveri turvaline asukoht [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. Serverit ei kasutata tööjaamana.

d. 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. Kaughalduseks on rajatud muust võrgust eraldatud spetsiaalne haldusvõrk. Selle puudumisel kasutatakse kaughalduseks üksnes turvalisi protokolle (SSH, HTTPS).
- d. Kõik tarbetud liidesed serveris on desaktiveeritud.

SYS.1.1.M6 Tarbetute teenuste desaktiveerimine

- a. Kõik tarbetud teenused (eriti võrguteenused) ja rakendused 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 reaajas 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 kesket 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 turvapoliitika kehtestamine [infoturbejuht]

- a. Organisatsiooni üldisest turvapoliitikast lähtuvalt on dokumenteeritud ja kehtestatud serveri turvapoliitika. Turvapoliitika arvestab serverite erinevat kaitsetarvet.
- b. Kõik serveri hankimise, halduse ja käitusega seotud töötajad tunnevad seda poliitikat.
- c. Serveri turvapoliitika 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. Poliitika nõuete rakendamist 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 [hankeosakond]

- 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 aluskonfiguratsioon

- a. Serveri süsteemi- ja rakendustarkvara hangitakse ainult autentsetest ja usaldusväärsetest allikatest.
- b. Installimiseks on kehtestatud protseduur ja aluskonfiguratsioon.
- c. Serveri aluskonfiguratsioon vastab turvapoliitikale. Turvaseadeid kontrollitakse enne serveri käikuandmist ja pärast iga serveris tehtavat muudatust.
- d. Installitakse ainult serveri otstarbe täitmiseks vajalikud teenused.
- e. 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. Paketifiltriga 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 avariivalmendumusega

- a. Organisatsiooni talitluspidevuse (ingl *business continuity*) kontseptsioon hõlmab ka serverite varundust ja taastet. (vt [DER.4 Avariiahaldus](#))
- 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 kasutatavaid 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.

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;

- põhimõlul töödeldavate protsesside lubatavust.

c. Kasutatavad sisetungituvastuse/sisetungitõrje 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 hoolduslepingud 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“
--------	---

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetusskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

SYS. IT-süsteemid

SYS.1: Server

SYS.1.2: Windows Server

SYS.1.2.2: Windows Server 2012

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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. Piiratud ulatuses on moodul kasutatav ka uuemate Windowsi serveri operatsioonisüsteemide puhul.

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

Sisukord

[2.1 Windows Server 2012 rakendamise puudulik kavandamine](#)

[2.2 Pilvteenuste läbimõtle mata kasutamine](#)

[2.3 Windowsi serveri puudulik haldus](#)

[2.4 Rühmapoliitika puudulik rakendamine](#)

[2.5 Kaitset vajava teabe või protsessi tervikluse kadumine](#)

[2.6 Haldusõiguste lubamatu omandamine või kuritarvitamine](#)

[2.7 Sissemurdmine kaugjuurdepääsu kaudu](#)

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 läbimõtle mata kasutamine

Windows Server 2012 kasutab pilvteenuseid (nt *Microsoft Azure Online Backup*) ka ilma spetsiaalse eritarkvarata. Pilvteenused võivad küll anda eeliseid (näiteks käideldavuses), kuid läbimõtle mata kasutamisel kujutab see endast siiski ohtu konfidentsiaalsusele ja 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 parooli 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

Sisukord

[3.1 Elutsükel](#)

[3.2 Põhimeetmed](#)

[SYS.1.2.2.M1 Windows Server 2012 kasutuselevõtu kava](#)

[SYS.1.2.2.M2 Windows Server 2012 turvaline installimine](#)

[SYS.1.2.2.M3 Windows Server 2012 turvaline haldus](#)

[3.3 Standardmeetmed](#)

[SYS.1.2.2.M4 Windows Server 2012 turvaline konfiguratsioon](#)

[SYS.1.2.2.M5 Kahjurvara tõrje](#)

[SYS.1.2.2.M6 Windows Server 2012 turvaline õiguste haldus ja turvaline autentimine](#)

[SYS.1.2.2.M8 Süsteemi tervikluse kaitse](#)

[3.4 Kõrgmeetmed](#)

[SYS.1.2.2.M11 Sissetungituvastus \(C-I-A\)](#)

[SYS.1.2.2.M12 Liiasus ja kõrgkäideldavuse vahendid \(A\)](#)

[SYS.1.2.2.M14 Krüpteeritud serveri ja virtuaalmasina turvaline sulgemine \(C-I\)](#)

3.1 Elutsükel

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 seadistustsmalle.
- 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 instantsti 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);
- avari-i-ümlerlilitust võimaldava klatri (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.

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

SYS. IT-süsteemid

SYS.1: Server

SYS.1.3: Linuxi ja Unixi server

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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

Sisukord

- [2.1 Süsteemi- ja kasutajateabe luure](#)
 - [2.2 Skriptikeskkonna ärakasutamine](#)
 - [2.3 Teekide dünaamiline laadimine](#)
 - [2.4 Valideerimata allikatest pärit tarkvara](#)
-

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 tüüpteeke 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

Sisukord

- [3.1 Elutsükk](#)
- [3.2 Põhimeetmed](#)
 - [SYS.1.3.M2 Korrektne identifikaatorite määramine](#)
 - [SYS.1.3.M3 Irdmäluseadmete automaatse failisüsteemiga sidumise vältimine](#)
 - [SYS.1.3.M4 Rakenduste kaitsmine](#)
 - [SYS.1.3.M5 Tarkvarapakettide turvaline installimine](#)
- [3.3 Standardmeetmed](#)
 - [SYS.1.3.M6 Kasutajate ja rühmade haldus](#)
 - [SYS.1.3.M8 SSH-ga krüpteeritud andmevahetus](#)
 - [SYS.1.3.M10 Volitamata õiguste laiendamise takistamine](#)
- [3.4 Kõrgmeetmed](#)
 - [SYS.1.3.M14 Süsteemi- ja kasutajateabe luure takistamine \(C\)](#)
 - [SYS.1.3.M16 Volitamata õiguste laiendamise täiendav takistamine \(C-I\)](#)

[SYS.1.3.M17 Tuuma lisaturve \(C-I\)](#)

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 rühmanime 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 privilegieerimata 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 tüüprofiilid 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. Tüüprofiile 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.

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

SYS. IT-süsteemid

SYS.1: Server

SYS.1.5: Virtualiseerimissüsteem

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

1.1 Eesmärk

Esitada meetmed virtualiseerimiskeskonna 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 virtualiseerimiskeskond. Virtualiseerimiskeskonna 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 etalon turbe moodulile rakendatakse virtuaalserverite puhul operatsioonisüsteemi põhiseid serveri- või kliendimoduleid 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).

Virtualiseerimiskeskonnaga 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

Sisukord

[2.1 Vead virtualiseerimise kavandamisel](#)

[2.2 Virtualiseerimise konfigureerimisvead](#)

[2.3 Ressursside piisamatus virtuaalse IT-süsteemi tarbeks](#)

[2.4 Hetktõmmisega seonduv andmeleke või ressursipuudus](#)

[2.5 Virtualiseerimissüsteemi haldusserveri tõrge](#)

[2.6 Valideerimata rakenduste väärkasutamine](#)

[2.7 Virtualiseerimisserveri turvarike](#)

2.1 Vead virtualiseerimise kavandamisel

Virtualiseerimissüsteemi tehnilise ja korraldusliku kavandamise puudumine võib põhjustada vigu virtualiseerimiskeskonna 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 virtualiseerimiskeskonnas 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

Virtualiseerimissüsteemi 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 hetktõmmiselt 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 virtualiseerimiskeskonnas võimalik analüüsida 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 teenusetökestusrünnete 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

Sisukord

[3.1 Elutsükel](#)

[3.2 Põhimeetmed](#)

[SYS.1.5.M2 Virtualiseerimissüsteemi turvaline rakendamine](#)

[SYS.1.5.M3 Virtualiseerimiskeskonna turvaline konfiguratsioon](#)

[SYS.1.5.M4 Virtualiseerimistaristu turvaline võrgukonfiguratsioon](#)

[SYS.1.5.M5 Virtualiseerimiskeskonna haldusliideste turve](#)

[SYS.1.5.M6 Virtualiseerimissüsteemi logimine](#)

[SYS.1.5.M7 Aja sünkroonimine virtualiseerimissüsteemis](#)

[3.3 Standardmeetmed](#)

[SYS.1.5.M8 Virtualiseerimissüsteemi kavandamine \[arhitekt\]](#)

[SYS.1.5.M9 Virtualiseerimissüsteemi võrguarhitektuuri kavandamine \[arhitekt\]](#)

[SYS.1.5.M10 Virtualiseerimissüsteemi halduse eeskiri \[IT-juht\]](#)

[SYS.1.5.M11 Virtualiseerimissüsteemi haldusvõrk](#)

[SYS.1.5.M12 Virtualiseerimistaristu halduse õigused ja rollid](#)

[SYS.1.5.M13 Virtualiseerimissüsteemi jaoks sobiv riistvara](#)

[SYS.1.5.M14 Virtualiseerimistaristu ühtsed konfiguratsiooninõuded](#)

[SYS.1.5.M15 Erineva kaitsetarbega külalissüsteemide lahusus](#)

[SYS.1.5.M16 Virtuaalmasinate isoleerimine](#)

[SYS.1.5.M17 Virtualiseerimisserveri konfiguratsiooni kontrollimine ja seire](#)

[SYS.1.5.M19 Virtualiseerimissüsteemi regulaarsed läbivaatused](#)

[3.4 Kõrgmeetmed](#)

[SYS.1.5.M20 Kõrgkäideldav arhitektuur \[arhitekt\] \(A\)](#)

[SYS.1.5.M21 Külalissüsteemide turvaline konfigureerimine \(I-A\)](#)

[SYS.1.5.M22 Virtualiseerimisserveri tugevdamine \(C-I\)](#)
[SYS.1.5.M23 Virtuaalserveri õiguste piiramine \(C-I\)](#)
[SYS.1.5.M24 Virtuaalserverite hetktõmmiste desaktiveerimine \(C-I-A\)](#)
[SYS.1.5.M25 Virtuaalserveri konsoolpääsu minimaalne kasutamine \(A\)](#)
[SYS.1.5.M26 Avaliku võtme taristu kasutamine \[arhitekt\] \(C-I-A\)](#)
[SYS.1.5.M27 Sertifitseeritud virtualiseerimistarkvara \(C-I-A\)](#)
[SYS.1.5.M28 Virtualiseeritud IT-süsteemide krüpteerimine \(C\)](#)

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 Virtualiseerimiskeskonna 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 Virtualiseerimiskeskonna 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 Kõrgkaideldav 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 eraldi 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 [IT-juht]

- 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 eraldi 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“
--------	--

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetusskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

SYS. IT-süsteemid

SYS.1: Server

SYS.1.8: Salvestilahendused

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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 salvestisüsteemis 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.2.1 Väljastellimine](#).

2 Ohud

Sisukord

[2.1 Salvestikomponentide ebaturvaline vaikeseadistus](#)

[2.2 Andmete manipuleerimine salvestisüsteemi kaudu](#)

[2.3 Andmepüük salvestipõhisel andmete dubleerimisel](#)

[2.4 WWN-identifikaatori võltsimise rünne](#)

[2.5 Võrkude loogilise lahususe rikkumine](#)

[2.6 Salvestilahenduse komponendi tõrge](#)

[2.7 Lubamatu füüsiline juurdepääs salvestusvõrgu kommutaatoritele](#)

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 *Simple Network Management Protocol*, SNMP) protokolle 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 salvestusvõrgu 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 reaajas 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

Sisukord

[3.1 Elutsükel](#)

[3.2 Põhimeetmed](#)

[SYS.1.8.M1 Salvestisüsteemi sobiv paigalduskoht \[tehnikatalitus\]](#)

[SYS.1.8.M2 Salvestilahenduse turvaline aluskonfiguratsioon](#)

[SYS.1.8.M4 Haldusliideste turve](#)

[3.3 Standardmeetmed](#)

[SYS.1.8.M6 Salvestilahenduse turvajuhend \[infoturbejuht\]](#)

[SYS.1.8.M7 Salvestilahenduse kavandamine](#)

[SYS.1.8.M8 Sobiva salvestilahenduse valimine](#)

[SYS.1.8.M9 Salvestilahenduse hoolduspartneri valimine](#)

[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.M14 Salvestusvõrgu \(SAN\) segmentimine](#)

[SYS.1.8.M15 Salvestilahenduse tarbijate turvaline lahusus](#)

[SYS.1.8.M16 Andmete turvaline kustutamine](#)

[SYS.1.8.M17 Salvestisüsteemi konfiguratsiooni dokumenteerimine](#)

[SYS.1.8.M18 Salvestisüsteemide läbivaatused ja aruandlus \[infoturbejuht\]](#)

[SYS.1.8.M19 Salvestisüsteemi kasutuselt kõrvaldamine](#)

[SYS.1.8.M20 Salvestilahenduse avariivalmendus ja -toimingud](#)

[3.4 Kõrgmeetmed](#)

[SYS.1.8.M21 Salvestipuuli \(*storage pool*\) kasutamine tarbijate lahutamiseks \(C-I\)](#)

[SYS.1.8.M22 Kõrgkäideldav salvestusvõrk \(A\)](#)

[SYS.1.8.M23 Krüpteerimine salvestilahendustes \(C-I\)](#)

[SYS.1.8.M24 Salvestusvõrgukanga \(*SAN fabric*\) tervikluse tagamine \(I\)](#)

[SYS.1.8.M25 Andmete mitmekordne ülekirjutamine kustutamisel \(C\)](#)

[SYS.1.8.M26 Salvestusvõrgu „tugev“ tsoonimine](#)

3.1 Elutsükel

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 hoolduspartneri 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]

- Salvestisüsteemi komponendid on paigaldatud lukustatud ruumidesse. Juurdepääs ruumidesse on ainult pääsuõigusega isikutel.
- Ruumides on tagatud katkematu elektritoide.
- Keskkonna temperatuur ja õhuniiskus vastab salvestisüsteemi tootja soovitatule.

SYS.1.8.M2 Salvestilahenduse turvaline aluskonfiguratsioon

- Enne salvestilahenduse käidukeskkonda paigaldamist on paigaldatud tarkvarakomponentide uuendid ja ajakohastatud riistvarakomponentide püsivara.
- Aluskonfiguratsioonis on kõik vaikeparoolid muudetud ja tarbetud kasutajakontod desaktiveeritud.
- Salvestisüsteemi tarbetud liidesed on desaktiveeritud.
- Vaikekonfiguratsiooni, aluskonfiguratsiooni ja hetkekonfiguratsiooni failid on varundatud ja kaitstud.

SYS.1.8.M4 Haldusliideste turve

- Salvestisüsteemide halduse pääsuõigused on piiratud.
- Haldusliidestele puudub juurdepääs ebausaldatavatest võrkudest.
- Salvestisüsteemi kaughaldusel kasutatakse turvalisi protokolle. Ebaturvaliste protokollide puhul on halduseks loodud eraldi haldusvõrk.

3.3 Standardmeetmed

SYS.1.8.M6 Salvestilahenduse turvajuhend [infoturbejuht]

- Organisatsiooni üldise turvapoliitika alusel on koostatud salvestilahenduste turvajuhend, mis sisaldab nõudeid salvestilahenduse turvaliseks kavandamiseks, rakendamiseks, halduseks, käituseks ja kõrvaldamiseks.
- Turvajuhendit on töötajatele tutvustatud. Kõik salvestisüsteemi haldurid järgivad turvajuhendit.
- Salvestilahenduse turvajuhendi muudatused kooskõlastatakse infoturbejuhiga ja dokumenteeritakse.
- Turvajuhendi rakendamist kontrollitakse regulaarselt. Kontrolli tulemused dokumenteeritakse.

SYS.1.8.M7 Salvestilahenduse kavandamine

- Salvestilahenduse kavandamise etapis on läbi viidud salvestilahenduse vajaduste, jõudluse ja mahu analüüs.
- Nõuete spetsifikatsiooni alusel on koostatud salvestilahenduse rakendamise kava, mis määratleb:
 - sobiva riistvaraspetsifikatsiooni;
 - valmistaja ja tarnija valimise kriteeriumid;
 - hangitava lahenduse arhitektuuri (tsentraliseeritud või hajutatud);
 - võrgühenduste 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 (ingl *Fibre 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 avariilukorras.

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 (*storage 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 turvaparametritega 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

- 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“

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetusskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

APP. Rakendused

APP.1: Klientrakendused

APP.1.1: Kontoritarkvara

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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 Andmebaasisüsteemid](#).

2 Ohud

Sisukord

[2.1 Organisatsiooni vajadustega mittearvestamine](#)

[2.2 Dokumendi manipuleerimine](#)

[2.3 Dokumendi tervikluse kadu](#)

[2.4 Dokumendi puudulik tõendatavus](#)

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

Sisukord

[3.1 Elutsükel](#)

[3.2 Põhimeetmed](#)

[APP.1.1.M2 Aktiivsisu piiramine](#)

[APP.1.1.M3 Välisallikatest pärit dokumentide turvaline avamine \[kasutaja\]](#)

[APP.1.1.M17 Kontoritarkvara turvafunktsioonide rakendamise koolitus](#)

[3.3 Standardmeetmed](#)

[APP.1.1.M6 Kontoritarkvara uute versioonide testimine](#)

[APP.1.1.M10 Kontoritarkvara kasutajapoolsete lisaarenduste reguleerimine](#)

[APP.1.1.M11 Kontoritarkvara lisandprogrammide nõuetekohane kasutuselevõtt](#)

[APP.1.1.M12 Pilvtalletusest loobumine \[kasutaja\]](#)

[APP.1.1.M13 Vaatefunktsioonide kasutamine \[kasutaja\]](#)

[APP.1.1.M14 Andmete kaitsmine tagantjärele muutmise eest \[kasutaja\]](#)

[3.4 Kõrgmeetmed](#)

[APP.1.1.M15 Kripteerimine ja digisignatuurid \(C-I\)](#)

[APP.1.1.M16 Dokumentide tervikluse kontroll \(I\)](#)

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 töötajatele 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 krüptomehhanismile 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.

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

APP. Rakendused

APP.1: Klientrakendused

APP.1.2: Veebibrauser

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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 Interneti 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

Sisukord

[2.1 Veebibrauseri kaudu leviv kahjurkood](#)

[2.2 Eksploidipakid](#)

[2.3 Andmevahetuse pealtkuulamine](#)

[2.4 Tervikluskadu veebibrauseris](#)

[2.5 Privaatsusriike](#)

2.1 Veebibrauseri kaudu leviv kahjurkood

Veebibrauseriga ebausaldusväärsest allikast kahjursisu (ingl malicious content) allalaadimisel on oht kasutaja seade märkamatuks 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 Privaatsusriike

Brauseri turvalise seadistusega 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

Sisukord

[3.1 Elutsükel](#)

[3.2 Põhimeetmed](#)

[APP.1.2.M1 Veebibrauseri turvamehhanismide kasutamine](#)

[APP.1.2.M2 Side krüpteerimine](#)

[APP.1.2.M3 Turvalised sertifikaadid](#)

[APP.1.2.M6 Paroolihalduri kasutamine veebibrauseris](#)

[APP.1.2.M13 DNS-over-HTTPS protokollide kasutamine](#)

3.3 Standardmeetmed

[APP.1.2.M7 Andmete kaitse veebibrauseris \[kasutaja\]](#)

3.4 Kõrgmeetmed

[APP.1.2.M9 Isoleeritud brauserikeskkond \(C-I\)](#)

[APP.1.2.M10 Brauseri privaatrežiim \[kasutaja\] \(C-I\)](#)

[APP.1.2.M11 Kahjursisu olemasolu kontroll \(C\)](#)

[APP.1.2.M12 Kahe brauseri strateegia \(A\)](#)

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 protokoll kasutamise

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 kasutatakse üksteisest isoleeritud aladel.
- c. Brauseris on rakendatud ajakohasele W3C spetsifikatsioonidele vastav sisuturbe (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 turvaprotokollil 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 protokoll kasutamine

a. Klientseadmetes kasutatavad brauserid toetavad DNS-over-HTTPS (DoH) protokoll kasutamist. Klientseadmete veebibrauserites on DoH kasutamine sisse lülitatud.

b. Kasutatav DNS-server toetab DNS-over-HTTPS protokoll.

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 mikrofoni 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 spetsialiseeritud IT-süsteemis.

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.

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetusskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

APP. Rakendused

APP.1: Klientrakendused

APP.1.4: Mobiilirakendused (äpid)

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

1.1 Eesmärk

Esitada meetmed äriprotsessi toetavates mobiilirakendustes ehk äppides töödeldavate andmete kaitseks. Äppe käsitletakse päritolust (iseehitatud või mobiilirakenduste 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

Sisukord

[2.1 Ebasobiva mobiilirakenduse valimine](#)

[2.2 Liiga suured õigused](#)

[2.3 Soovimatud funktsioonid mobiilirakendustes](#)

[2.4 Tarkvara nõrkused ja vead mobiilirakendustes](#)

[2.5 Rakenduse andmete ebaturvaline lokaalne talletamine](#)

[2.6 Konfidentsiaalse teabe tuletamine metaandmetest](#)

[2.7 Konfidentsiaalsete andmete leke mobiilirakendusest](#)

[2.8 Ebaturvaline ühendus tagasüsteemidega](#)

[2.9 Suhtlused väljaspool organisatsiooni taristut](#)

[2.14 Sõltuvus taga- või välissüsteemidest ja -teenustest](#)

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 osutada 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 Suhtlused väljaspool organisatsiooni taristut

Mobiilirakendustega on võimalik luua suhtlusi 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.

2.14 Sõltuvus taga- või välissüsteemidest ja -teenustest

Paljude mobiilirakenduste töö sõltub otseselt välissüsteemidest ja -teenustest. Ilma andmesideühenduseta töötavad paljud mobiilirakendused üksnes piiratud või ei saa neid üldse kasutada. Kui välisteenusega seotud andmesideühendus või teenus ise on kättesaamatu, on mobiilirakenduse käideldavus häiritud.

3 Meetmed

Sisukord

[3.1 Elutsükel](#)

[3.2 Põhimeetmed](#)

[APP.1.4.M1 Mobiilirakenduse nõuete analüüs \[vastutav spetsialist\]](#)

[APP.1.4.M5 Mobiilirakenduste pääsuõiguste piiramine ja kontroll \[vastutav spetsialist\]](#)

[APP.1.4.M7 Mobiilirakenduste lokaalsete andmete turve](#)

[APP.1.4.M8 Andmelekete avastamine ja takistamine](#)

[3.3 Standardmeetmed](#)

[APP.1.4.M3 Mobiilirakenduste turvaline levitamine](#)

[APP.1.4.M12 Mobiilirakenduste turvaline desinstallimine](#)

[3.4 Kõrgmeetmed](#)

[APP.1.4.M14 Mitmikautentimine mobiilirakendustes \(C-I\)](#)

[APP.1.4.M15 Mobiilirakenduste läbistustestimised \(C-I-A\)](#)
[APP.1.4.M16 Mobiilirakenduste haldus \(C-I-A\)](#)

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 vajalike ni.

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 organisatsioonisisesse 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.

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

APP. Rakendused

APP.2: Kataloogiteenused

APP.2.1: Kataloogiteenus üldiselt

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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

Andmekaitespetsialist, vastutav spetsialist.

1.3 Piirangud

Moodul käsitleb kataloogiteenuste üldisi turvaaspekte. Meetmed tuntuimate kataloogiteenuste kaitseks on esitatud moodulites [APP.2.2 Active Directory](#) ja [APP.2.3 OpenLDAP](#).

Kataloogiteenust jagava serveri moodulid on esitatud mooduligrupis SYS.1 *Server*. Täiendavalt tuleb arvestada meetmeid mooduligrupist OPS.1.1 *IT põhitööd*.

2 Ohud

Sisukord

- [2.1 Kataloogiteenuse rakendamise puuduv või piisamatu kavandamine](#)
 - [2.2 Sektsioonimise ja dubleerimise väär või piisamatu rakendamine](#)
 - [2.3 Kataloogiteenuse pääsuõiguste väär või piisamatu kavandamine](#)
 - [2.4 Pääsuõiguste puudulik haldus](#)
 - [2.5 Kataloogiteenuse juurdepääsu väär konfiguratsioon](#)
 - [2.6 Kataloogiteenuse komponentide tõrked](#)
 - [2.7 Kataloogiteenuse kahjustamine volitamata juurdepääsu kaudu](#)
 - [2.8 Kataloogiteenuse väär programmeerimine](#)
-

2.1 Kataloogiteenuse rakendamise puuduv või piisamatu kavandamine

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 andmekao, vea andmetalletuses, kataloogiteenuse halva sooritusvõime või kataloogiteenuse tõrked.

2.3 Kataloogiteenuse pääsuõiguste väär või piisamatu kavandamine

Kataloogiteenuste pääsuõiguste haldamine sisaldab palju käsitsi tehtavaid tegevusi, mille käigus on võimalik teha vigu. Piisamatu kavandamine (näiteks siis kui ei ole selge, kas ja milliseid andmeid võib avateksti kujul edastada) võib olla vastuolus organisatsiooni üldise infoturvapoliitikaga. Kataloogiteenuse konfidentsiaalsete andmete kaitseks ettenähtud turvameetmete puudulik kavandamine võib kaasa tuua krüpteerimismehhanismide ühildamatuse või isegi krüpteerimise puudumise, mistõttu on oht teabe konfidentsiaalsusele ja terviklusele.

2.4 Pääsuõiguste puudulik haldus

Kataloogiteenuse kaudu hallatavatele kasutajatele 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. Eksimused kataloogiteenuse haldamise õiguste määramisel võib ohustada kogu kataloogisüsteemi toimimist.

2.5 Kataloogiteenuse juurdepääsu väär konfiguratsioon

Kataloogiteenuse rakendamisel antakse juurdepääs kataloogiteenusele ka tavarakendustele (nt Interneti- või sisevõrgurakendused). Väär konfiguratsiooni tulemusena võimaldatakse kataloogiteenusele volitamata juurdepääs.

Kui autentimisandmeid edastatakse krüpteerimatult avatekstina, on võimalik andmeid luurata.

2.6 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.

2.7 Kataloogiteenuse kahjustamine volitamata juurdepääsu kaudu

<https://eits.ria.ee/et/versioon/2021/etalonturbe-kataloog/app-rakendused/app2-kataloogiteenused/app21-kataloogiteenus-ueldisel/>

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.

2.8 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

Sisukord

[3.1 Elutsükkel](#)

[3.2 Põhimeetmed](#)

[APP.2.1.M1 Kataloogiteenuse turvaeeskiiri](#)

[APP.2.1.M2 Kataloogiteenuse rakenduskava \[andmekaitse spetsialist, vastutav spetsialist\]](#)

[APP.2.1.M3 Kataloogiteenuse pääsuõiguste korraldus \[vastutav spetsialist\]](#)

[APP.2.1.M4 Kataloogiteenuse turvaline installimine](#)

[APP.2.1.M5 Kataloogiteenuse turvaline konfigureerimine](#)

[APP.2.1.M6 Kataloogiteenuse turvaline käitus](#)

[3.3 Standardmeetmed](#)

[APP.2.1.M7 Kataloogiteenuse turvapoliitika](#)

[APP.2.1.M8 Kataloogiteenuse sektsioonimise ja dubleerimise kava](#)

[APP.2.1.M9 Sobivate kataloogiteenuse komponentide valimine \[vastutav spetsialist\]](#)

[APP.2.1.M11 Kataloogiteenuse juurdepääsu reguleerimine](#)

[APP.2.1.M12 Kataloogiteenuse seire](#)

[APP.2.1.M13 Kataloogiteenuse andmevahetuse turve](#)

[APP.2.1.M14 Kataloogiteenuse kõrvaldamise kord \[vastutav töötaja\]](#)

[APP.2.1.M15 Kataloogiteenuse migratsiooni turve](#)

[3.4 Kõrgmeetmed](#)

[APP.2.1.M16 Kataloogiteenuse avariikava \(C-I-A\)](#)

3.1 Elutsükkel

Kavandamine

APP.2.1.M1 Kataloogiteenuse turvaeeskiiri

APP.2.1.M2 Kataloogiteenuse rakenduskava

APP.2.1.M7 Kataloogiteenuse turvapoliitika

APP.2.1.M8 Kataloogiteenuse sektsioonimise ja dubleerimise kava

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.M4 Kataloogiteenuse turvaline installimine

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

Kõrvaldamine

APP.2.1.M14 Kataloogiteenuse kõrvaldamise kord

Lisanduvad kõrgmeetmed

APP.2.1.M16 Eriolukorra tegevuskava koostamine kataloogiteenuse tõrgete puhuks

3.2 Põhimeetmed**APP.2.1.M1 Kataloogiteenuse turvaeeskiri**

a. On koostatud üldisele infoturvapoliitikale vastav kataloogiteenuse turvaeeskiri.

APP.2.1.M2 Kataloogiteenuse rakenduskava [andmekaitse spetsialist, vastutav spetsialist]

a. On koostatud kataloogiteenuse rakenduskava, milles on esitatud:

- ettenähtud kasutusviisidega sobiv objektiklasside ja atribuutitüüpide mudel;
- vajadustel põhinev pääsuõiguste haldusmudel;
- meetmed, mis takistavad andmete volitamata kogumist kataloogiteenusest.

b. Kataloogiteenuse rakenduskava koostamisse on kaasatud personalitöötajad ja andmekaitse spetsialist.

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.M4 Kataloogiteenuse turvaline installimine

a. Pääsu- ja haldusõigused konfigureeritakse installikava kohaselt juba teenuse installimise käigus.

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.

3.3 Standardmeetmed

APP.2.1.M7 Kataloogiteenuse turvapoliitika

- a. On koostatud ja dokumenteeritud kataloogiteenuse turvaaspekte käsitlev kataloogiteenuse turvapoliitika.
- b. Kataloogiteenuse turvapoliitika, eeskirjad ja korrad on kataloogiteenuse kasutajatele vajalikus ulatuses teatavaks tehtud.

APP.2.1.M8 Kataloogiteenuse sektsioonimise ja dubleerimise kava

- a. Sektsioonimise kavandamisel on arvestatud kataloogiteenuse käideldavust ja kaitsetarvet.
- b. Kataloogiteenuse sektsioonimiskava dokumenteeritakse arvestusega, et võimaldada taastet sektsioonhaaval.
- c. Dubleerimise rakendamisel on arvestatud piisava jõudlusega.

APP.2.1.M9 Sobivate kataloogiteenuse komponentide valimine [vastutav spetsialist]

- a. Kataloogiteenuse rakendamiseks on kehtestatud kataloogiteenuse komponentide valikukriteeriumid.
- b. Valikukriteeriumide hulka kuuluvad kataloogiteenuse otstarbest tulenevad turvanõuded.

APP.2.1.M11 Kataloogiteenuse juurdepääsu reguleerimine

- a. Kataloogiteenuse juurdepääs on konfigureeritud kataloogiteenuse turvapoliitika kohaselt.
- b. Kataloogiteenuse kasutamisel üle Interneti on server kaitstud turvalüüsiga.
- c. 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.
- d. Kataloogiteenuse otsingufunktsioon on piiratud, et vältida tundlike kataloogiandmete leket.

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 informeeritakse 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.

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.

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetusskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

APP. Rakendused

APP.2: Kataloogiteenused

APP.2.2: Active Directory

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

1.1 Eesmärk

Esitada meetmed *Active Directory* (AD) tavakasutuse turbeks olukorras, kus AD teenust kasutatakse Microsoft Windowsi süsteemidest (kliendid ja serverid) koosneva taristu haldamiseks.

1.2 Vastutus

Active Directory meetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Vastutav spetsialist.

1.3 Piirangud

Kataloogiteenuse üldised turbesoovitused on esitatud moodulis [APP.2.1 Kataloogiteenus üldiselt](#). Moodulis ei käsitleta Windows serverite ja klientide operatsioonisüsteemide turvameetmeid (nt [SYS.1.2.2 Windows Server 2012](#) või [SYS.2.2.3 Windows 10 klient](#)) ning võrgutaristu haldust.

Haldusprotsesse (nt andmete varundamine, logimine ja paigahaldus) käsitletakse üksnes ulatuses kuivõrd need on seotud *Active Directory* valdkonna erisustega.

2 Ohud

Sisukord

[2.1 Turvapiiride puudulik kavandamine](#)

[2.2 Usaldusseoste rohkus või lõtvus](#)

[2.3 Turvafunktsioonide puudumine pärandüsteemides](#)

[2.4 Liigsed rollid ja liigsete teenuste käitus domeenikontrolleris](#)

[2.5 Delegeeritud õiguste puudulik järelevalve ning dokumenteerimine](#)

[2.6 Ebaturvaline autentimine](#)

[2.7 Liigsete õigustega või ebaturvalised halduskontod](#)

[2.8 Korduvkasutatavad administraatori paroolid](#)

2.1 Turvapiiride puudulik kavandamine

Kui AD metsa (ingl *AD forest*) struktuuri ja selle turvapiire teadlikult ja hoolikalt ei kavandata, võivad andmed tahtmatult lekkida.

Taristu komponentidele kehtivatest turvanõuetest tulenevalt luuakse täiendavaid AD metsi. See muudab AD kasutuselevõtu ja halduse veelgi keerukamaks.

2.2 Usaldusseoste rohkus või lõtvus

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 nõrkused. Sama kehtib valikautentimisest (ingl *selective authentication*) loobumise korral AD metsade vahelistes usaldusseostes.

2.3 Turvafunktsioonide puudumine pärandüsteemides

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 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 nende 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. Ründaja saab 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.

3 Meetmed

Sisukord

[3.1 Elutsükk](#)

[3.2 Põhimeetmed](#)

[APP.2.2.M1 Active Directory kavandamine \[vastutav spetsialist\]](#)

[APP.2.2.M2 Active Directory halduse kord \[vastutav spetsialist\]](#)

[APP.2.2.M3 Rühmapoliitikad tööks Windowsiga](#)

[APP.2.2.M5 Active Directory turvalisuse tõstmine](#)

[APP.2.2.M6 Active Directory käituse turve](#)

[APP.2.2.M7 Active Directory turvaline haldus \[vastutav spetsialist\]](#)

[3.3 Standardmeetmed](#)

[APP.2.2.M8 Turvalise kanali konfigureerimine Windowsis](#)

[APP.2.2.M9 Turvaline autentimine Active Directory keskkonnas](#)

[APP.2.2.M10 DNS-teenuse turvaline kasutamine](#)

[APP.2.2.M11 Active Directory taristu seire](#)

[APP.2.2.M12 Domeenikontrolleri andmete varundamine](#)

[3.4 Kõrgmeetmed](#)

[APP.2.2.M14 Spetsialiseeritud haldussüsteem \(C-I-A\)](#)

[APP.2.2.M15 Haldus- ja töökeskkonna lahusus \(C-I-A\)](#)

3.1 Elutsükk

Kavandamine

APP.2.2.M1 *Active Directory* kavandamine

APP.2.2.M2 *Active Directory* halduse kord

APP.2.2.M3 Rühmapoliitikad tööks Windowsiga

Evitus

APP.2.2.M5 Active Directory turvalisuse tõstmine

APP.2.2.M8 Turvalise kanali konfigureerimine Windowsis

APP.2.2.M9 Turvaline autentimine *Active Directory* keskkonnas

APP.2.2.M10 DNS-teenuse turvaline kasutamine

Käitus

APP.2.2.M6 *Active Directory* käituse turve

APP.2.2.M7 *Active Directory* turvaline haldus

APP.2.2.M11 *Active Directory* taristu järelevalve

Avariivalmendus

APP.2.2.M12 Domeenikontrollerite andmete varundamine

Lisanduvad kõrgmeetmed

APP.2.2.M14 Spetsialiseeritud haldussüsteem

APP.2.2.M15 Haldus- ja töökeskkonna lahusus

3.2 Põhimeetmed

APP.2.2.M1 *Active Directory* kavandamine [vastutav spetsialist]

a. AD kavandamisel on arvestatud järgmiste aspektidega ja dokumenteeritud:

- millist domeeni funktsionaaltaset (ingl *Domain Functional Level* - DFL) ja AD versiooni kasutatakse;
- 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.

b. Iga domeeni kohta on otsustatud:

- vajalikud AD objektid ja nende hierarhia;
- arvuti- ja kasutajatüüpidest sõltuvad turvasätted;
- rühmapoliitikad (ingl *Group Policy*);
- AD andmete juurdepääsu subjektid ja liidesed;
- automaatselt genereeritavad ja muud usaldusseosed.

c. Iga AD-objekti kohta dokumenteeritakse järgmised andmed:

- nimetus ja asukoht AD puus;
- otstarve;
- AD-objektile kehtestatud halduspääsuõigused;
- õiguste pärilikkuse konfiguratsioon;
- seos rühmapoliitikaga.

d. On kehtestatud vajaduse- ja rollipõhine AD õiguste kontseptsioon ja õiguste delegerimise kord.

APP.2.2.M2 Active Directory halduse kord [vastutav spetsialist]

- a. Haldusega seotud valdkonnad ja õigused on dokumenteeritud lähtudes AD kavandamisel koostatud rollipõhisest AD õiguste kontseptsioonist.
- b. Suurtes domeenides jaotatakse haldusülesanded mitme halduri vahel. AD teenuse- ja andmehaldurite rollid on lahutatud.
- c. AD haldusülesanded on jaotatud delegeerimismudeli kohaselt. Delegeeritakse ainult konkreetse haldusülesande täitmiseks vajalikke õigusi, ülesannete kattuvusi välditakse.

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. Igasse organisatsiooniüksuse (ingl *Organizational Unit* – OU) objektide rühmitusse kuuluvad ainult ühesuguse poliitikaga objektid.
- d. Juurdepääs rühmapoliitikate konfigureerimisele on vajaduspõhiselt piiratud.
- e. Rühmapoliitika konfiguratsiooniga (vt lisamaterjalidest „Rühmapoliitika turvasätete näidis“) on määratud:
- paroolipoliitika;
 - konto blokeerimise poliitika;
 - Kerberose poliitika;
 - seirepoliitika;
 - kasutajaõiguste andmine;
 - turvamehhanismide konfiguratsioon;
 - vastavushalduri (ingl *Security Compliance Manager*, SCM) kasutamine.

APP.2.2.M5 Active Directory turvalisuse tõstmine

- a. Sisseehitatud kontod on kaitstud piisavalt tugevate paroolidega ja neid kasutatakse üksnes avariikontodena.
- b. Eeliskontod on kaitstud kasutajate rühma (ingl *Protected Users*) liikmetel. Selle rühma kontodele on lubatud üksnes Kerberosel põhinev autentimine (alates domeeni funktsionaaltasemest 2012).
- c. Serverirakendustele eriõiguste andmisel kasutatakse võimalusel kaitstud kasutajate rühma hallatavaid halduskontosid või kaitstakse halduskontod vähemalt 20-kohaliste paroolidega.
- d. Domeenikontrollerid (ingl *Domain Controller* – DC) on turvameetmetega kaitstud nii operatsioonisüsteemi kui AD tasemel.
- e. Domeenikontrollerisse tohivad lokaalselt sisse logida vaid domeenihaldurid. Tavakasutajate tegevused domeenikontrolleris on blokeeritud.
- f. Domeenikontroller ei anna peale domeenikontrolleri jaoks vajalike standardteenuste (nt *Active Directory*, *Kerberos* ja DNS) lisaks rakendusteenuseid (nt DFS, DHCP).
- g. Domeenikontroller ei jaga faile ühiskasutusse.

h. Domeenikontrollerit ei kasutata arvutitöökohana (Interneti ja väliste andmekandjate kasutamine on keelatud).

i. Muude operatsioonisüsteemide käivitamine domeenikontrolleris on blokeeritud.

j. AD taasterežiim on kaitstud sobiva parooliga. Sellel režiimil tohib toiminguid teha ainult nelja silma põhimõtte kohaselt.

k. Domeenikontrollerist tehakse regulaarselt varukoopiaid.

l. AD „Igaüks“ (ingl *Everyone*) rühmale mõeldud pääsuõigused on domeenikontrolleris piiratud.

m. Domeenikontrollerit kaitstakse volitamata taaskäivituse eest.

n. Domeenide ja domeenikontrollerite juhised hõlmavad paroolide, kontolukustuse, Kerberose autentimisprotokolli, kasutajaõiguste ja järelevalve turvaseadeid.

o. Domeenidevahelistes usaldusseostes filtreeritakse ja anonüümitakse õiguste andmed.

APP.2.2.M6 Active Directory käituse turve

a. AD domeenide ja AD metsade (ingl *AD forest*) usaldusseoseid analüüsitakse regulaarselt.

b. Teenusehaldurite andmepääsuõigused on vähendatud nende tööks vajaliku miinimumini. Pääsuõigusi kontrollitakse regulaarselt.

c. Domeenihaldurite rühm on kas tühi või võimalikult väike. Mittekasutatavad kontod desaktiveeritakse AD-s ja pärast ettenähtud säilitustähtaega need kustutatakse.

d. 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. Iga kontot on võimalik seostada konkreetse töötajaga.

b. Serverihalduri kontosid ei kasutata tööjaamades. Domeenihalduri kontosid ei kasutata tööjaamades ega serverites.

c. Igapäevaste AD haldusega mitteseotud ülesannete täitmisel kasutatakse standardset kasutajakontot.

d. Lokaalsetele halduskontodele on määratud turvalised ja kordumatud paroolid.

e. Teenusehalduskontosid haldavad üksnes teenusehaldurite rühma liikmed.

f. Teenusehaldurite rühma kuuluvad isikud peavad olema usaldusväärsed ja neil peavad olema piisavad teadmised AD haldamise kohta.

g. Skeemihaldurite rühma lisatakse haldurid üksnes ajutiselt, skeemimuudatuste ajaks. Pärast skeemi muutmist liikmed eemaldatakse rühmast.

h. AD juurdomeeni domeenihalduride rühma kasutajakontode kasutamiseks on vajalik kahe süsteemiülema kohalolu, kellest kumbki teab üht poolt paroolist.

i. AD haldusega tegelevate süsteemiülemate arvutitöökohti kaitstakse, kasutades vähemalt järgmisi meetmeid:

- kasutajakontod luuakse selliselt, et neid saab kasutada ainult kindlates tööjaamades;
- pärast viieminutulist kasutuspausi rakendub automaatne lukustus, avamiseks autentitakse ennast domeenikontrolleris uuesti;
- tööjaama protsesse ei käivitata domeenihalduri õigustega, selle asemel kasutatakse tööjaama lokaalsete administraatorite rühma kuuluvat kontot.
- domeenikontrolleri kaughalduseks kasutatakse vaid krüpteeritud andmesideühendust.

j. Andmepääsude reguleerimiseks globaalses kataloogis ei kasutata domeenipõhiseid rühmi, vaid globaalseid või universaalseid rühmi.

k. Kustutatud AD objektide taastamiseks on aktiveeritud AD prügikast (alates Windows Server 2008 R2).

3.3 Standardmeetmed

APP.2.2.M8 Turvalise kanali konfigureerimine Windowsis

a. Windowsis on tundlike andmete edastuseks konfigureeritud turvanõuetele ja rühmapoliitika parameetritele vastav turvaline kanal (ingl *Secure Channel*).

b. Turvalise kanali kasutamine on aktiveeritud kõikides domeeni klientsüsteemides.

APP.2.2.M9 Turvaline autentimine Active Directory keskkonnas

a. AD keskkonnas kasutatakse võimalusel Kerberose autentimisprotokolli.

b. Ebaturvaline autentimine LM-i ja NTLMv1-i kaudu on blokeeritud. Kui pärandsisüsteemide 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.

d. Anonüümne juurdepääs domeenikontrolleritele on blokeeritud.

APP.2.2.M10 DNS-teenuse turvaline kasutamine

a. Mittesoovitavate DNS-kliendipäringute vältimiseks kasutatakse integreeritud DNS-tsoone ja DNS-i andmete turvalist dunaamilist uuendamist.

b. Juurdepääs DNS-serveri konfiguratsioonandmetele on lubatud üksnes halduskontodelt.

c. Serveri vahemälus olevad DNS-andmed on kaitstud lubamatute muudatuste eest.

d. Domeenikontrollerite juurdepääs DNS-i teenusele on võimalikult palju piiratud.

e. DNS-i päringutega seotud võrgutoimingute seire on võimeline avastama DNS-serveri ummistusründeid.

f. Kasutatakse hajutatud DNS-i, milles iga DNS-server haldab ainult ühte tsooni ja suunab teistelt serveritelt tulevad kliendipäringud vastutavale DNS-serverile. Sekundaarseid DNS-tsoone ei kasutata.

g. DNS-i andmevahetuse kaitseks kasutatakse IPsec protokoll, kui selleks on tagatud piisav andmeside jõudlus.

APP.2.2.M11 *Active Directory* taristu seire

a. AD taristu süsteemisündmused (ingl *System Events*) logitakse. Logisid analüüsitakse regulaarselt.

b. Jälgitakse domeenikontrollerite käideldavust (reaktsiooniaega, LDAP-ühenduste loomise kestust), taaskäivituste esinemist ja süsteemiressursside kasutamist.

c. Muudatusi domeenitasemel ja AD üldstruktuuris (rolli – ja rühmaliikmete muudatused, usaldusseoste muudatused, rühmapoliitika muutmine, AD skeemi muudatused, oluliste failide muutumine) jälgitakse, logitakse ja analüüsitakse.

APP.2.2.M12 Domeenikontrolleri andmete varundamine

a. Organisatsiooni andmevarunduskontseptsiooni osana on koostatud domeenikontrolleri andmevarunduse ja -taaste eeskiri.

b. Varundustarkvaral on tarkvaratootja heakskiit domeenikontrollerite andmevarunduse sobivuse osas.

c. Domeenikontrolleri andmevarunduseks on loodud eraldi teenusehalduskontod, mille õigused kehtivad ainult ühes domeenis. Varundushaldurite rühma liikmete arv on piiratud miinimumini.

d. Pääsuõigusi *AdminSDHolder*-objektile (konteinerobjekt õiguste salvestamiseks) reguleeritakse võimalikult rangelt (vt APP.2.2.M7 *Active Directory turvaline haldus*).

e. Domeenikontrollerite andmeid varundatakse regulaarselt.

f. Domeenikontrollerite andmete varundamise ja taaste protseduuride toimimist kontrollitakse regulaarselt. Domeenikontrollerite taastamisel eelistatakse varukoopia teise domeenikontrollerist andmete dubleerimist.

3.4 Kõrgmeetmed

APP.2.2.M14 Spetsialiseeritud haldussüsteem (C-I-A)

a. AD halduseks on kasutusel tugevalt kaitstud spetsialiseeritud haldussüsteem (*Secure Admin Workstations*, SAW).

APP.2.2.M15 Haldus- ja töökeskkonna lahusus (C-I-A)

a. Domeenikontrollerid ja domeeni haldussüsteemid on paigaldatud eraldiseisvasse AD metsa (ingl *AD forest*), millel on AD töömetsaga ühepoolne usaldusseos (töökeskkond usaldab halduskeskkonda).

b. Eelisõiguste täpseks haldamiseks ja eelistoimingute logimiseks kasutatakse täiendavaid tehnoloogiaid (nt *Privileged Access Management*, PAM).

4 Lisateave

4.1 Rühmapoliitika turvasätete näidis

Allpool on esitatud turvasätteid, 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: igäüks, administraator, autenditud kasutaja, varunduse operaator
- läbiotsitava kontrollimise vahelejätmine: igäüks
- 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 juhitud 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 sisselogimisdioloogis: 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 turvakontrollle 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: määratama
- süsteemi väljalülitamine turvalogi maksimaalse mahu saavutamise korral: desaktiveeritud (märkus: aktiveerida suure kaitsetarbega süsteemides)
- süsteemilogi säilitamine: määratama

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

APP. Rakendused

APP.2: Kataloogiteenused

APP.2.3: OpenLDAP

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

1.1 Eesmärk

Esitada meetmed *OpenLDAP*-il põhineva kataloogiteenuse turvaliseks kasutamiseks ja töödeldava teabe nõuetekohaseks kaitseks.

1.2 Vastutus

OpenLDAP-i meetmete täitmise eest vastutab IT-talitus.

1.3 Piirangud

Moodulis lähtutakse *OpenLDAP*-i versioonist 2.4. Üldised turbesoovitused kataloogiteenuse jaoks on esitatud moodulis [APP.2.1 Kataloogiteenus üldiselt](#).

Haldusprotsesse (nt andmete varundamine, logimine ja paigaldus) käsitletakse üksnes ulatuses kuivõrd need on seotud *OpenLDAP*-i erisustega.

2 Ohud

Sisukord

[2.1 OpenLDAP-i kavandamise puudumine või puudulikkus](#)

[2.4 OpenLDAP-i autonoomse ja online-juurdepääsu puudulik lahusus](#)

2.1 OpenLDAP-i kavandamise puudumine või puudulikkus

Kui tagasüsteemid või seotud parameetrid valitakse väärtalt, mõjutavad need soovimatult *OpenLDAP*-i võimaldatavaid funktsioone.

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 ja *BerkeleyDB* failifunktsioone (nt lukustusfunktsiooni) 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-juurdepääs toimub protokolliga LDAP, autonoomse süsteemi korral ühendutakse andmebaasifailidega otse. Autonoomse ja online juurdepääsu töörežiimide väär kasutamine tekitab erinevaid veaolukordi. Näiteks võib andmebaas taastamisel osutada *OpenLDAP*-i jaoks seostamatuks ja seda ei saa enam kasutada.

3 Meetmed

Sisukord

[3.1 Elutsükel](#)

[3.2 Põhimeetmed](#)

[APP.2.3.M1 OpenLDAP-i rakendamise kavandamine](#)

[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.M6 Turvaline autentimine OpenLDAP-is](#)

[3.3 Standardmeetmed](#)

[APP.2.3.M8 OpenLDAP-i atribuutide piiramine](#)

[APP.2.3.M9 OpenLDAP-i sektsioonimine ja dubleerimine](#)

[APP.2.3.M10 OpenLDAP-i turvaline ajakohastamine](#)

[APP.2.3.M11 OpenLDAP-i käituskeskonna kitsendamine](#)

[3.4 Kõrgmeetmed](#)

3.1 Elutsükel

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 käituskeskonna 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 *OpenLDAP*-i 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);
- ülevaate piirangud ja ülevaate õige järjekorra tagamine.

APP.2.3.M3 *OpenLDAP*-i 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 konfigureerimiseadete (direktiivide) väärtusi kontrollitakse ja vajadusel kohandatakse enne nende esmast jõustumist.

c. Konfigureerimisel on arvestatud *OpenLDAP*-i tagasüsteeme ja ülevaateid.

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 *OpenLDAP*-i 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 *OpenLDAP*-i pääsuõiguste turvaline haldus

a. Pääsuloendis on kasutaja iga tegevus hõlmatud asjakohase direktiiviga, mis seob kasutaja, talle lubatud sihtobjektid ja kasutamisoiguse ulatuse.

b. Pääsuloendite määramisel on arvesse võetud, et *OpenLDAP*-i andmebaasidirektiivid (ingl database directives) kirjutavad üldised direktiivid (ingl global directives) üle.

APP.2.3.M6 Turvaline autentimine *OpenLDAP*-is

- 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. *OpenLDAP*-i paroolide miinimumpikkus, minimaalne ja maksimaalne eluiga ning muutmise nõuded on määratud ülekatega.
- d. Serverid ja klientarvutid salvestavad paroole üksnes räsikujul, kasutades piisavalt murdmiskindlat algoritmi.

3.3 Standardmeetmed

APP.2.3.M8 *OpenLDAP*-i 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 *OpenLDAP*-i sektsioonimine ja dubleerimine

- a. Kataloogiteenuse sektsioonimine alampuudeks on kavandatud ja ellu viidud vastavalt meetmele APP.2.1. M8 *Kataloogiteenuse sektsioonimise ja dubleerimise kava*.
- b. *OpenLDAP* on mitme serveri vahel jaotatud osapuudeks (sektsioonideks).
- c. Andmete sünkroniseerimine serverite vahel tehakse dubleerimisega. Dubleerimisrežiim on valitud vastavalt võrguühendusele ja käideldavusnõuetele.

APP.2.3.M10 *OpenLDAP*-i turvaline ajakohastamine

- a. Enne uue versiooni paigaldamist analüüsitakse, kas ja kuidas uus versioon mõjutab kasutusele võetud tagasüsteemide, tarkvarasõltuvuste ja ülekatete toimimist.
- b. Haldurite endi koostatud skriptide toimimist kontrollitakse enne uue versiooni paigaldamist tootmiskeskonda.
- c. Pärast *OpenLDAP* ajakohastamist kontrollitakse konfiguratsiooni ja pääsuõigusi.

APP.2.3.M11 *OpenLDAP*-i käituskeskkonna kitsendamine

- a. *Slapd*-serveri tööks vajalikud konfiguratsioonifailid ja andmebaasid on piiratud käituskataloogiga.

3.4 Kõrgmeetmed

Selles moodulis kõrgmeetmed puuduvad

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

APP. Rakendused

APP.3: Võrguteenused

APP.3.1: Veebirakendused

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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

Sisukord

[2.1 Turvasündmuste logimise puudulikkus](#)[2.2 Liigse taustainfo avaldamine veebirakendustes](#)[2.3 Veebirakenduse väärkasutus automatiseeritud lahendustega](#)[2.4 Veebirakenduse autentimise ja seansihalduse puudulikkus](#)

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

Sisukord

[3.1 Elutsükel](#)[3.2 Põhimeetmed](#)[APP.3.1.M1 Veebirakenduste autentimine](#)[APP.3.1.M4 Andmete ja sisu kasutamise piiramine](#)[APP.3.1.M7 Kaitse veebirakenduste automatiseeritud kasutamise eest](#)[APP.3.1.M14 Konfidentsiaalsete andmete kaitse](#)[3.3 Standardmeetmed](#)[APP.3.1.M8 Veebirakenduse turvaline arhitektuur \[hankeosakond, infoturbejuht\]](#)[APP.3.1.M9 Veebirakenduste hankimise kord \[hankeosakond\]](#)[APP.3.1.M11 Turvaline ühendus tagasüsteemidega](#)[APP.3.1.M12 Veebirakenduste turvaline konfigureerimine](#)

[APP.3.1.M21 Veebirakenduste turvaline HTTP-konfiguratsioon](#)

[APP.3.1.M22 Veebirakenduste läbivaatus ja läbistustestimine \[infoturbejuht\]](#)

[3.4 Kõrgmeetmed](#)

[APP.3.1.M20 Veebitulemüürid \(C-I-A\)](#)

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 informeeritakse.

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 turvalüüsidesega.
- c. Välisühenduse andmeliiklus on krüpteeritud ja toimub ainult autentitud 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. Konfigureerimisel on võimalik seadistada ja piirata järgmisi veebirakenduse omadusi:
- märgikoodide (ingl *character encoding*) ja automaattõlke kasutamine;
 - ülevõtte 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).
- c. HTTP-päis on seadistatud nii piiravaks kui võimalik.
- d. Küpsistele (ingl *cookie*) on seatud atribuudid *secure*, *SameSite*, ja *httponly*.

APP.3.1.M22 Veebirakenduste läbivaatus ja läbistustestimine [infoturbejuht]

- a. Veebirakenduste turvalisust kontrollitakse ja testitakse regulaarselt.
- b. Läbivaatuste ja läbistustestimiste tulemused dokumenteeritakse. Neid käsitletakse konfidentsiaalsena 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

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

APP. Rakendused

APP.3: Võrguteenused

APP.3.2: Veebiserver

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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](#).

<https://eits.ria.ee/et/versioon/2021/etalonturbe-kataloog/app-rakendused/app3-voorguteenused/app32-veebiserver/>

Kui veebiserveri puhul kasutatakse väliseid teenuseid, rakendatakse lisaks meetmeid moodulist [OPS 2.1 Väljasttellimine](#).

Veebiserveri sündmuste logimist käsitletakse moodulis [OPS.1.1.5 Logimine](#).

2 Ohud

Sisukord

[2.1 Mainekaotus](#)

[2.2 Veebiserveri manipuleerimine](#)

[2.3 Hajus ummistusrünne](#)

[2.4 Konfidentsiaalsete andmete leke](#)

[2.5 Õigusaktide nõuete rikkumine](#)

[2.6 Veebiserveri tõrgete kõrvaldamise puudulikkus](#)

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

Sisukord

[3.1 Elutsükkel](#)

[3.2 Põhimeetmed](#)

[APP.3.2.M1 Veebiserveri turvaline konfigureerimine](#)

[APP.3.2.M2 Veebiserveri failide kaitse](#)

[APP.3.2.M3 Failide üles- ja allalaadimise turve](#)

[APP.3.2.M4 Sündmuste logimine](#)

[APP.3.2.M5 Autentimine](#)

[APP.3.2.M7 Veebisisu avaldamise õiguspärasus \[vastutav spetsialist, vastavushaldur\]](#)

[APP.3.2.M11 Krüpteerimine TLS abil](#)

[3.3 Standardmeetmed](#)

[APP.3.2.M8 Veebiserveri rakendamise kava](#)

[APP.3.2.M9 Veebiserveri turvapoliitika](#)

[APP.3.2.M10 Sobiv veebimajutaja](#)

[APP.3.2.M12 Vigade ja veateadete käsitlemise kord](#)

[APP.3.2.M13 Veebirobotite juurdepääsu piiramine](#)

[APP.3.2.M14 Tervikluse kontroll ja kaitse kahjurvara eest](#)

[APP.3.2.M16 Läbistustestimine ja läbivaatus](#)

[APP.3.2.M20 Kontaktisiku määramine \[haldusosakond\]](#)

[3.4 Kõrgmeetmed](#)

[APP.3.2.M15 Liiasus \(A\)](#)

[APP.3.2.M18 Kaitse ummistusrünnete eest \(A\)](#)

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 käsitus

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 avaldatatud 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 protokollu 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 käsitlemise 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 käsitlese kord

- a. HTTP-teabest ja veateadetest ei ilmne veebiserveri tarkvarakomponentide nime, versiooni ega konfiguratsiooni.
- b. Veebiserver edastab üksnes kasutaja informeerimiseks vajalikke rakendusekohaseid veateateid.
- c. Vigade ja tõrgete korral lülitub veebiserver turvalisele ohutusrežiimile.

APP.3.2.M13 Veebirobotite juurdepääsu piiramine

- a. Otsingurobotite juurdepääs veebisile 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.

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetusskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

APP. Rakendused

APP.3: Võrguteenused

APP.3.3: Failiserver

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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

Sisukord

[2.1 Failiserveri tõrge](#)[2.2 Failiserveri aladimensioneeritus](#)[2.3 Salvestatud failide puudulik kontroll](#)[2.4 Pääsuõiguste kontseptsiooni puudumine või puudulikkus](#)[2.5 Struktureerimata andmehaldus](#)[2.6 Failiserveris talletatud andmete kaotus](#)[2.7 Lunavara](#)

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 märkamatu 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

Sisukord

[3.1 Elutsükkel](#)

[3.2 Põhimeetmed](#)

[APP.3.3.M2 RAID-süsteem](#)

[APP.3.3.M3 Viirusetõrjeprogrammid](#)

[APP.3.3.M15 Failiserveri eelanalüüs](#)

[3.3 Standardmeetmed](#)

[APP.3.3.M6 Failiserveri hankimise kord](#)

[APP.3.3.M7 Sobiva failisüsteemi valimine](#)

[APP.3.3.M8 Struktureeritud andmehaldus \[kasutaja\]](#)

[APP.3.3.M9 Turvaline salvestihaldus](#)

[APP.3.3.M11 Kvootide rakendamine](#)

[APP.3.3.M14 Veaparanduskoodide kasutamine](#)

[3.4 Kõrgmeetmed](#)

[APP.3.3.M12 Andmestiku krüpteerimine \(C-I-A\)](#)

[APP.3.3.M13 Dubleerimine teises asukohas \(A\)](#)

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

<https://eits.ria.ee/et/versioon/2021/etalonturbe-kataloog/app-rakendused/app3-voorguteenusused/app33-failiserver/>

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 kontrollid 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 andmevahetuskiiirus 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 kasutatavad 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.

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

APP. Rakendused

APP.3: Võrguteenused

APP.3.4: Samba

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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

Sisukord

[2.1 Samba turvamata ühenduste pealtkuulamine](#)[2.2 Samba ebaturvalised vaikeseaded](#)[2.3 Samba lubamatu kasutamine või haldamine](#)[2.4 Samba väär haldus](#)[2.5 Andmekadu Sambas](#)[2.6 Andmete tervikluse kadu Sambas](#)

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

Sisukord

[3.1 Elutsükel](#)[3.2 Põhimeetmed](#)[APP.3.4.M1 Samba serveri rakendamise kava](#)[APP.3.4.M2 Samba serveri turvaline aluskonfiguratsioon](#)

3.3 Standardmeetmed

[APP.3.4.M3 Samba serveri operatsioonisüsteemi turvaline konfiguratsioon](#)

[APP.3.4.M4 NTFSi funktsioonide vältimine Samba serveris](#)

[APP.3.4.M5 Samba serveri juurdepääsu turvaline seadistus](#)

[APP.3.4.M6 Winbindi turvaline konfiguratsioon Samba keskkonnas](#)

[APP.3.4.M7 DNS turvaline konfiguratsioon Samba keskkonnas](#)

[APP.3.4.M8 LDAP turvaline konfiguratsioon Samba keskkonnas](#)

[APP.3.4.M9 Kerberose turvaline konfiguratsioon Samba keskkonnas](#)

[APP.3.4.M10 Väliste programmide turvaline rakendamine Samba serveris](#)

[APP.3.4.M12 Samba serveri haldurite koolitus](#)

[APP.3.4.M13 Samba serveri oluliste süsteemikomponentide regulaarne varundus](#)

3.4 Kõrgmeetmed

[APP.3.4.M15 Samba andmepakettide krüpteerimine \(C-I\)](#)

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 protokollis SMB uuemates versioonides (alates SMB v3) sisalduvate meetoditega.

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

APP. Rakendused

APP.3: Võrguteenused

APP.3.6: DNS-server

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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

Sisukord

[2.1 DNS-serveri tõrge](#)

[2.2 DNS-serveri piisamatu suutlikkus](#)

[2.3 DNSi rakendamise puudulik kavandamine](#)[2.4 Vigane domeeniinfo](#)[2.5 DNS-serveri väär konfiguratsioon](#)[2.6 DNSi manipuleerimine](#)[2.7 DNSi kaaperdamine](#)[2.8 DNSi ummistusrünne](#)[2.9 DNSi peegeldusrünne \(DNS-dublee\)](#)

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 puudulikkust 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 ummistusrünne 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

Sisukord

[3.1 Elutsükel](#)

[3.2 Põhimeetmed](#)

[APP.3.6.M1 DNSi rakendamise kava](#)

[APP.3.6.M2 DNS-serveri dubleerimine](#)

[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.M7 DNS-serveri seire](#)

[APP.3.6.M8 Domeeninimede haldus \[haldusosakond\]](#)

[APP.3.6.M9 DNS-serveri avariikava](#)

[3.3 Standardmeetmed](#)

[APP.3.6.M10 DNS-serveriks sobiv server](#)

[APP.3.6.M11 DNS-serveri piisav dimensioneerimine](#)

[APP.3.6.M13 Domeeniteabe nähtavuse piiramine](#)

[APP.3.6.M14 DNS-serverite eraldamine](#)

[APP.3.6.M15 Logiandmete analüüs](#)

[APP.3.6.M16 DNS-serveri õige paigutus P-A-P arhitektuuris](#)

[APP.3.6.M17 Protokollilaienduse DNSSEC rakendamine](#)

[APP.3.6.M18 Tsoonitransaktsiooni turbe tugevdamine](#)

[APP.3.6.M19 DNS-serveri turvaline kasutusel kõrvaldamine](#)

[3.4 Kõrgmeetmed](#)

[APP.3.6.M20 Avariikava teostatavuse kontroll \(A\)](#)

[APP.3.6.M21 DNS-primaarserveri peitmine \(C-I-A\)](#)

[APP.3.6.M22 DNS-teenuste sidumine mitme tarnijaga \(I-A\)](#)

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 töötleva 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 põhisel.

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 anomaaliade 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 Avariiahaldus](#))
- 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 arhitektuuri (*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-tsoonandmetes 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“

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

APP. Rakendused

APP.4: Ärirakendused

APP.4.3: Andmebaasisüsteemid

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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 käsitlen mitterelatsiooniliste andmebaasisüsteemide turvameetmeid. Moodul ei käsitlen 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-haldus](#) ja [OPS.1.1.5 Logimine](#).

2 Ohud

Sisukord

[2.1 Süsteemiressursside ebapiisavus](#)

[2.2 Vaikekontode kasutuselejätt](#)

[2.3 Krüpteerimata andmevahetus](#)

[2.4 Andmekadu andmebaasis](#)

[2.5 Andmete tervikluse kadu](#)

[2.6 SQL-süst](#)

[2.7 Andmebaasihalduse süsteemi ebaturvaline konfiguratsioon](#)

[2.8 Kahjurvara ja ebaturvalised skriptid](#)

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 tiptundidel 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 süsteemiülmana 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 väärtalt 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-käsk, 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

Sisukord

[3.1 Elutsükkel](#)

[3.2 Põhimeetmed](#)

[APP.4.3.M1 Andmebaasisüsteemi turvaeeskiri](#)

[APP.4.3.M3 Andmebaasihalduse süsteemi turvalisuse tõstmine](#)

[APP.4.3.M4 Uute andmebaaside kasutuselevõtu reguleerimine](#)

[APP.4.3.M9 Andmebaasisüsteemi varundamine](#)

[3.3 Standardmeetmed](#)

[APP.4.3.M11 Riistvara dimensioneerimine \[vastutav spetsialist\]](#)

[APP.4.3.M12 Andmebaasihalduse süsteemi tüüpkonfiguratsioon](#)

[APP.4.3.M13 Lingitud andmebaaside piirangud](#)

[APP.4.3.M16 Andmebaasiühenduste krüpteerimine](#)

[APP.4.3.M17 Andmete laadimise ja migratsiooni korraldus \[vastutav spetsialist\]](#)

[APP.4.3.M18 Andmebaasisüsteemi seire](#)

[APP.4.3.M19 Mittekvaliteetsete skriptide vältimine \[arendaja\]](#)

[APP.4.3.M20 Regulaarne läbivaatus](#)

[3.4 Kõrgmeetmed](#)

[APP.4.3.M21 Andmebaasi turbe instrumendid \(C-I\)](#)

[APP.4.3.M22 Avariivalmendus \(C-I-A\)](#)

[APP.4.3.M23 Arhiveerimine \(I-A\)](#)

[APP.4.3.M24 Krüpteerimine andmebaasis \(C\)](#)

[APP.4.3.M25 Andmebaasisüsteemi turvaaudit \(C-I-A\)](#)

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 informeeritakse 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 kasutusele võtmise 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. Ülevaatus 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 teavitusaajad, 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.

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

APP. Rakendused

APP.5: Rühmatarkvara

APP.5.2: Microsoft Exchange ja Outlook

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

1.1 Eesmärk

Esitada meetmed keskmiste ja suurte organisatsioonide jaoks ette nähtud rühmatarkvaralahenduste *Microsoft Exchange*'i ja *Outlook*i turvaliseks kasutamiseks.

1.2 Vastutus

Microsoft Exchange'i ja *Outlook*i 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 operatsioonisüsteemi käsitlevates moodulites.

2 Ohud

Sisukord

[2.1 Microsoft Exchange'i ja Outlooki puuduv või puudulik rakendamise kord](#)

[2.2 Microsoft Exchange'i väär migreerimine](#)

[2.3 Microsoft Exchange'i lubamatu brauseripääs](#)[2.4 Muude süsteemide lubamatu sidumine Microsoft Exchange'iga](#)[2.5 Microsoft Exchange'i ja Outlooki pääsuõiguste väär haldus](#)[2.6 Microsoft Exchange'i väär konfiguratsioon](#)[2.7 Outlooki väär konfiguratsioon](#)[2.8 Outlookile lisatud makrode ja programmiliideste tõrked ja väärkasutus](#)

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 ilmned 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 osutada 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 turvaparametreite 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

*Outlook*i konfigureerimisvead, näiteks kasutajale liigsete juurdepääsuõiguste andmine, tekitavad erinevaid turvaprobleeme. Vääralt valitud suhtlusprotokoll võib põhjustada spetsiifilisi turvanõrkusi. Samuti on võimalik *Outlook*i e-kirjade krüpteerimiseks ja allkirjastamiseks kasutatava privaativõtme kompromiteerimine. Kui krüpteerimist kasutatakse võrgutasemel (nt IPSeci või TLS-i kaudu), võivad krüpteerimismehhanismid vääralt konfigureeritud kliendi korral osutada mittetoimivaks.

2.8 Outlookile lisatud makrode ja programmiliideste tõrked ja väärkasutus

*Outlook*i kui tuntud grupidöövahendit saab kuritarvitada kahjurtarkvara levitamiseks. *Outlook*i 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 väärraid ja ebamajanduslikke juhtimisotsuseid. Halvasti koostatud makro võib automaatselt andmeid lekitada ja neid volitamata kasutajatele kättesaadavaks teha.

3 Meetmed

Sisukord

[3.1 Elutsükkel](#)

[3.2 Põhimeetmed](#)

[APP.5.2.M1 Microsoft Exchange'i ja Outlooki rakendamise kava](#)

[APP.5.2.M2 Microsoft Exchange'iga sobiv taristu](#)

[APP.5.2.M3 Microsoft Exchange'i pääsuõiguste haldus](#)

[APP.5.2.M5 Microsoft Exchange'i varundus](#)

[3.3 Standardmeetmed](#)

[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](#)

[APP.5.2.M11 Microsoft Exchange'i ühenduste turve](#)

[APP.5.2.M12 Outlook Anywhere, MAPI over HTTP ja Outlook Web App kasutamise turve](#)

[3.4 Kõrgmeetmed](#)

[APP.5.2.M17 Microsoft Exchange'i süsteemi andmebaaside krüpteerimine \(C\)](#)

3.1 Elutsükkel

Kavandamine

APP.5.2.M1 *Microsoft Exchange*'i ja *Outlook*i 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 *Outlook*i 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 *Outlook*i rakendamise kava**

a. *Microsoft Exchange*'i ja *Outlook*i 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 *Outlook*i 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 *Outlook*i turvaline konfiguratsioon

a. Igale kasutajale on loodud oma *Outlook*i profiil koos kasutajaspetsiifiliste seadetega.

b. Kasutaja saab muuta vaid selleks spetsiaalselt lubatud seadeid (nt kirja jaluse seadmine, eemaloleku funktsiooni aktiveerimine).

c. Suhtluse teisele osapoolle 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 *Outlook*i 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*).

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

APP. Rakendused

APP.5: Rühmatarkvara

APP.5.3: E-posti server ja klient üldiselt

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

1.1 Eesmärk

Esitada üldised meetmed e-posti serveri ja e-posti klientide turvaliseks kasutamiseks.

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

Sisukord

[2.1 E-posti kasutamise puudulik kavandamine](#)

[2.2 E-posti serveri ja klientide väär seadistamine](#)

[2.3 E-posti ebausaldusväärsus](#)

[2.4 Kahjurvara levitamine](#)

[2.5 Suhtlusrünned](#)

[2.6 E-kirjade volitamata lugemine ja manipuleerimine](#)

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 aadressaadressile. 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 Suhtlusrünned

E-posti teel läbiviidav suhtlusrünned (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 suhtlusrünned 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 suhtlusrünned 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

Sisukord

[3.1 Elutsükkel](#)

[3.2 Põhimeetmed](#)

[APP.5.3.M1 E-posti kliendi turvaline konfiguratsioon](#)

[APP.5.3.M2 E-posti serveri turvaline käitus](#)

[APP.5.3.M3 E-kirjade andmevarundus ja arhiveerimine](#)

[APP.5.3.M4 E-posti serveri spämmi- ja viirusetõrje](#)

[3.3 Standardmeetmed](#)

[APP.5.3.M5 E-kirjade vastuvõtja asendamise kord \[ülemus\]](#)

[APP.5.3.M6 E-posti turvaeeskiri](#)

[APP.5.3.M7 Kasutajate koolitus rühmatarkvara kliendi turbe alal](#)

[APP.5.3.M8 Kasutajate spämmikäsitletus \[kasutaja\]](#)

[APP.5.3.M9 Laiendatud turvameetmed e-posti serveril](#)

[3.4 Kõrgmeetmed](#)

[APP.5.3.M10 Otspunktkrüpteerimine \(C\)](#)

[APP.5.3.M11 E-posti serveri liiasus \(A\)](#)

[APP.5.3.M12 Mustade nimekirjade seire \(A\)](#)

[APP.5.3.M13 TLS-raportid \(C-I-A\)](#)

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 spämmikäsitletus

Lisanduvad kõrgmeetmed

APP.5.3.M10 Otpunktkrüpteerimine

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. On koostatud kirjalik loend konkreetsetes e-posti serveris lubatud protokollidest ja teenustest.
- d. Meiliserveri kasutus spämmi vahendamiseks on välistatud.
- e. 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. Kesksele 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 andmekaitsejuhti.

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:

- kuidas kaitstakse meili- ja veebisuhtluse andmevahetust;
- 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.

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 informeeritud ohtudest seoses e-posti teenuse kasutamisega, sealhulgas õngitsuskirjade ja võltsitud saatjaadressiga 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 Soft File („~“) parameetrit kasutatakse ainult testimisotstarbel.
- c. DMARC ründetuvastusraporteid vaadatakse üle regulaarselt.
- d. E-posti serverite vahelise andmeside kaitseks on rakendatud MTA-STS ja/või DANE turvamehhanismid.

3.4 Kõrgmeetmed**APP.5.3.M10 Otpunktkrüpteerimine (C)**

- a. Organisatsioon kasutab andmevahetuse kaitseks otpunktkrüpteerimist (ingl *end-to-end encryption*).
- b. Krüpteerimiseks 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.

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

APP. Rakendused

APP.6: Tarkvara üldiselt

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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

Sisukord

- [2.1 Sobimatu tarkvara valimine](#)
 - [2.2 Konfiguratsiooniveast põhjustatud andmekaotus](#)
 - [2.3 Tarkvara soetamine ebausaldusväärsest allikast](#)
 - [2.4 Puudulikust hooldusest tingitud turvanõrkused](#)
 - [2.5 Tarkvara väärkasutamisest tulenev andmekaotus](#)
 - [2.6 Ressursipuudus tarkvara kasutamisel](#)
 - [2.7 Tarkvara sobimatus kasutajate vajadustega](#)
-

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 väärtalt konfigureeritud, võidakse tahtmatult paljastada tundlikku teavet. Näiteks sünkronitakse 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 ilmned 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 hoolduslepingut, võib ründaja tarkvaras olevaid turvanõrkusi ära kasutada võrku tungimiseks või andmete varastamiseks.

2.5 Tarkvara väärkasutamisest tulenev andmekaotus

Tarkvaras sisalduvate funktsioonide väär 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

Sisukord

[3.1 Elutsükkel](#)

[3.2 Põhimeetmed](#)

[APP.6.M1 Tarkvara kasutuselevõtu kavandamine \[vastutav spetsialist\]](#)

[APP.6.M2 Tarkvarale esitatavate nõuete loend \[vastutav spetsialist\]](#)

[APP.6.M3 Tarkvara turvaline hankimine \[hankeosakond\]](#)

[APP.6.M4 Tarkvara installimise ja seadistamise kord \[vastutav spetsialist\]](#)

[APP.6.M5 Tarkvara turvaline installimine](#)

[3.3 Standardmeetmed](#)

[APP.6.M6 Täiendavad tarkvara turvafunktsioonid](#)

[APP.6.M7 Sobiva tarkvara valimine \[vastutav spetsialist, hankeosakond\]](#)

[APP.6.M8 Installimeedia turvaline kasutamine](#)

[APP.6.M9 Tarkvara inventuur](#)

[APP.6.M10 Tarkvara turvajuhend](#)

[APP.6.M11 Tarkvara lisandmoodulite ja pluginite haldus](#)

[APP.6.M12 Tarkvara kasutusest kõrvaldamine \[vastutav spetsialist\]](#)

[APP.6.M13 Tarkvara turvaline desinstallimine](#)

[3.4 Kõrgmeetmed](#)

[APP.6.M14 Sertifitseeritud tarkvara kasutamine \(C-I-A\)](#)

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. Tüüp tarkvara 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 esitatavate 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;
- logimisinõuded;

- 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 organisatsioonisiselt 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 ülevõetavaid 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. Tüüp tarkvara 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 võrdluskalaat.

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 äpipoeist) 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. Tüüp-tarkvarast 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 süsteemuudatused 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.

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

APP. Rakendused

APP.7: Tellimustarkvara arendus

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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

Sisukord

[2.1 Puudulikud sätted lepingus välise teenuseandjaga](#)

[2.2 Ebaturvaline tarkvaraarhitektuur](#)

[2.3 Dokumenteerimata funktsioonid](#)

[2.4 Turvameetmete puudumine või puudulikkus rakenduses](#)

[2.5 Puudulik kontroll tarkvara arenduse üle](#)

[2.6 Ebapädev tarkvaraarendaja](#)

2.1 Puudulikud sätted lepingus välise teenuseandjaga

Kui välise teenuseandjaga sõlmitud lepingus on osapoolte tegevused kirjeldatud puudulikult või ebaselgelt, võivad turvameetmed kas isikute teadmatusel, 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 vältitavad.

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

Sisukord

[3.1 Elutsükkel](#)

[3.2 Põhimeetmed](#)

[APP.7.M1 Tellimustarkvara arendusprojekti kavandamine](#)

[APP.7.M2 Tarkvaraarenduse turvanõuete määramine](#)

[APP.7.M3 Tarkvara käidunõuete määramine \[IT-talitus\]](#)

[APP.7.M4 Tellimustarkvara nõuete määramine \[hankeosakond\]](#)

[3.3 Standardmeetmed](#)

[APP.7.M5 Tarkvaraarendusprojekti seire](#)

[APP.7.M6 Tellimustarkvara nõuete põhjalik dokumenteerimine](#)

[APP.7.M7 Tellimustarkvara turvaline hankimine](#)

[APP.7.M8 Töötajate kaasamine tarkvara varajasse testimisse](#)

[3.4 Kõrgmeetmed](#)

[APP.7.M9 Usaldatav deponeerimine \(A\)](#)

[APP.7.M10 Sertifitseeritud tarkvaraarendaja kasutamine \(C-I-A\)](#)

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 teostamisaeg.

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 ilmnenu vigade kõrvaldamiseks ja parendusettepanekute realiseerimiseks piisava ajavaru.

3.4 Kõrgmeetmed

APP.7.M9 Usaldatav deponeerimine (A)

a. Äri kriitilise 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.

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

IND. Tööstuse IT

IND.1: Käidu- ja protsessijuhtimissüsteemid

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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

Sisukord

- [2.1 Keskkonnamõjust tingitud kahjustused](#)
 - [2.2 Käidutehnoloogia puudulik integreerimine turbekorraldusse](#)
 - [2.3 Puudulik käidu- ja protsessijuhtimissüsteemide haldus](#)
 - [2.4 Puudulik juurdepääsu turve](#)
 - [2.5 Ebaturvaline rakenduste areendusprotsess](#)
 - [2.6 Ebaturvaline kaugadministreerimine](#)
 - [2.7 Puudulikud seire- ja avastusprotseduurid](#)
 - [2.8 Puudulik testimine](#)
 - [2.9 Puudulik elutsükli kontseptsioon](#)
 - [2.10 Ebaturvaline hankimine](#)
 - [2.11 Ebaturvaliste protokollide kasutamine](#)
 - [2.12 Ebaturvaline konfiguratsioon](#)
 - [2.13 Käidutehnoloogia sõltuvus IT-võrkudest](#)
-

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 talitusohutuse 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 eripärade, 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 areendusprotsess

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 piiratud 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

Sisukord

[3.1 Elutsükk](#)

[3.2 Põhimeetmed](#)

[IND.1.M1 Integreerimine turbekorraldusse \[infoturbejuht\]](#)

[IND.1.M3 Kahjurprogrammide tõrje](#)

[IND.1.M4 Käidutehnoloogia taristu dokumenteerimine](#)

[IND.1.M18 Käidu- ja protsessijuhtimissüsteemide logimine](#)

[IND.1.M19 Varukoopiate tegemine \[töötaja\]](#)

[3.3 Standardmeetmed](#)

[IND.1.M5 Tsoonimis põhimõtete väljatöötamine \[arhitekt\]](#)

[IND.1.M6 Käidu- ja protsessijuhtimissüsteemide muudatuste haldus](#)

[IND.1.M7 Keskne õiguste haldus \[infoturbejuht\]](#)

[IND.1.M8 Käidutehnoloogia komponentide turvaline haldus \[IT-talitus\]](#)

[IND.1.M9 Ird-andmekandjate ja mobiilseadmete kasutamise kitsendamine](#)

[IND.1.M10 Sündmuste seire, logimine ja avastamine](#)

[IND.1.M11 Turvaline hankimine ja süsteemiarendus \[infoturbejuht\]](#)

[IND.1.M12 Nõrkuste halduse korra kehtestamine](#)

[IND.1.M20 Laiendatud süsteemidokumentatsioon](#)

[IND.1.M21 Suhtluste dokumenteerimine](#)

[IND.1.M22 Keskne logimine ja seire](#)

[IND.1.M23 Käidutehnoloogia komponentide kõrvaldamine](#)

[3.4 Kõrgmeetmed](#)

[IND.1.M13 Käidu- ja protsessijuhtimissüsteemide avariivalmendus \(A\)](#)

[IND.1.M14 Käidutehnoloogia komponentide tugev autentimine \(C-I-A\)](#)

[IND.1.M15 Õiguste kontroll ja seire \(C-I-A\)](#)

[IND.1.M16 Tsoonide tugev isoleerimine \(I-A\)](#)

[IND.1.M17 Regulaarne turbe läbivaatus \[infoturbejuht\] \(I\)](#)

[IND.1.M24 Kommunikatsioon rikke korral \[töötaja\] \(A\)](#)

3.1 Elutsükk

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 protsessijuhtimissüsteemide 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 Tsoonimis põhimõtete väljatöötamine [arhitekt]

- a. Turvatsoonide loomisel on arvestatud käidutehnoloogia ja protsessjuhtimissüsteemide objekte ja funktsioone ning nende erinevat kaitsetarvet võrreldes kontorivõrguga.
- b. Käidutehnoloogia ja protsessjuhtimissüsteemide võrgud on projekteeritud tõrke- ja ründe kindlatena.
- 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 ühenduste avastamiseks ja kõrvaldamiseks.

IND.1.M6 Käidu- ja protsessjuhtimissüsteemide muudatuste haldus

- a. Organisatsioonis on määratletud, dokumenteeritud ja rakendatud käidu- ja protsessjuhtimissüsteemide muudatuste läbiviimise protsess.
- b. Käidu- ja protsessjuhtimissüsteemide muudatuste halduses järgitakse üldisi muudatusehalduse meetmeid (vt [OPS.1.1.3 Paiga- ja muudatusehaldus](#)).

IND.1.M7 Keskne õiguste haldus [infoturbejuht]

- a. Käidu- ja protsessjuhtimissüsteemide 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 protsessjuhtimissüsteemide 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 kontroll-loend, mis sõltuvalt komponendist määrab:
- tarbetute või ebaturvaliste funktsioonide, liideste jm elementide desaktiveerimise;

- turvafunktsioonide aktiveerimise;
- pääsu reguleerimise ja autentimise;
- algaroolide 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 liideses 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 käsitus](#)). Intsidentide käsitlemise plaan hõlmab sündmuste liigitamist, teatamisteid, asjasepuutuvaid struktuuriüksusi, sündmuste analüüsi ning dokumenteerimist, süsteemide taastet ja intsidenti 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 käivitused;
- sisselogimised ja sisselogimiskatsed;
- haldus- ja hooldustoimingud;
- kahjurvaratõrje tulemused;
- võrgusündmused (ühenduse katkemised, sõnumite blokeerimised, ummistused);
- turvalisust puudutavad vea- ja tõrketead.

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.2.1 Väljastellimine](#)).

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 töötajaid 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 protsessijuhtimissüsteemide avariivalmendus (A)

a. Iga turvatsooni kohta on kehtestatud ja dokumenteeritud avariikäsitluse plaan (vt moodul [DER.4 Avariiahaldus](#)), 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 avariiahalduse 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, haldusteel) 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”

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

IND. Tööstuse IT

IND.2: Tööstusautomaatika

IND.2.1: Tööstusautomaatika komponendid üldiselt

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

1.1 Eesmärk

Esitada meetmed tööstusautomaatika süsteemide (ingl *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

Sisukord

[2.1 Süsteemi ebaturvaline konfiguratsioon](#)

[2.2 Puudulik kasutajate ja õiguste haldus](#)

[2.3 Puudulik logimine](#)

[2.4 Automaatikakomponentide manipuleerimine ja sabotaaž](#)

[2.5 Ebaturvalised protokollid](#)

[2.6 Ummistusründed \(DoS\)](#)

[2.7 Kahjurprogrammid](#)

[2.8 Teabe luure](#)

[2.9 Manipuleeritud püsivara](#)

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 seadme 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 mõtetulemusi. Manipuleeritud mõtetulemused 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 kasutajani jõuda juba kompromiteeritud püsivaraga komponent. Ründaja saab võimaluse protsesside ja protseduuride muutmiseks ja võltsimiseks.

3 Meetmed

Sisukord

[3.1 Elutsükel](#)

[3.2 Põhimeetmed](#)

[IND.2.1.M1 Konfigureerimis- ja hooldeliideste juurdepääsu kitsendamine](#)

[IND.2.1.M2 Turvaliste protokollide kasutamine konfigureerimiseks ja hoolduseks \[hooldepersonal\]](#)

[IND.2.1.M4 Tarbetute teenuste, funktsioonide ja liideste desaktiveerimine või desinstallimine \[hooldepersonal\]](#)

[IND.2.1.M6 Võrgu segmentimine \[arhitekt\]](#)

[3.3 Standardmeetmed](#)

[IND.2.1.M7 Andmete varundamine](#)

[IND.2.1.M8 Kahjurvara tõrje](#)

[IND.2.1.M11 Automaatikakomponentide hooldus \[hooldepersonal\]](#)

[IND.2.1.M13 Automaatikakomponentide käikuandmise kord](#)

[IND.2.1.M16 Välisliideste turve](#)

[IND.2.1.M17 Turvalised andmesideprotokollid](#)

[3.4 Kõrgmeetmed](#)

[IND.2.1.M18 Avariiside \[töötaja\] \(A\)](#)

[IND.2.1.M19 Turvatestimine \(C-I-A\)](#)

[IND.2.1.M20 Usaldusväärne programmikood \(I-A\)](#)

3.1 Elutsükel

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 reaalanõuete 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“
--------	--

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

IND. Tööstuse IT

IND.2: Tööstusautomaatika

IND.2.2: Programmeeritavad kontrollid

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

1.1 Eesmärk

Tagada programmeeritavate kontrollide (ingl *programmable logic controller*, PLC) turve olenemata nende valmistajast, otstarbest, arhitektuurist või asukohast.

1.2 Vastutus

Programmeeritavate kontrollide meetmete täitmise eest vastutab käidutehnoloogia talitus.

1.3 Piirangud

Tööstusautomaatika komponentide turbe üldised meetmed on esitatud moodulis [IND.2.1 Tööstusautomaatika komponendid üldiselt](#). Talitusohutuse (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

Sisukord

[2.1 Puudulik dokumentatsioon](#)

2.1 Puudulik dokumentatsioon

Kui programmeeritavate kontrollrite 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 kontrollritega tegeleva töötaja lahkumisel.

3 Meetmed

Sisukord

[3.1 Elutsükel](#)

[3.2 Põhimeetmed](#)

[3.3 Standardmeetmed](#)

[IND.2.2.M1 Programmeeritavate kontrollrite \(PLC\) täielik dokumentatsioon](#)

[IND.2.2.M3 Aja sünkroniseerimine](#)

[3.4 Kõrgmeetmed](#)

3.1 Elutsükel

Käitus

IND.2.2.M1 Programmeeritavate kontrollrite (PLC) täielik dokumentatsioon

IND.2.2.M3 Aja sünkroniseerimine

3.2 Põhimeetmed

Antud moodulis põhimeetmed puuduvad.

3.3 Standardmeetmed

IND.2.2.M1 Programmeeritavate kontrollrite (PLC) täielik dokumentatsioon

- Juhtimisprogrammid ja kontrolleri konfiguratsioon arhiveeritakse pärast iga muudatust.
- Konfiguratsioonimuudatused ja komponentide väljavahetamine dokumenteeritakse.

IND.2.2.M3 Aja sünkroniseerimine

- Süsteemiaegade sünkroniseerimine on tsentraliseeritud ja automaatne.

3.4 Kõrgmeetmed

Antud moodulis kõrgmeetmed puuduvad.

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetusskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

IND. Tööstuse IT

IND.2: Tööstusautomaatika

IND.2.3: Andurid ja täiturid

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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 täituri (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

Sisukord

[2.1 Puudulikud turvanõuded toodete hankimisel](#)[2.2 Väär kalibreerimine](#)

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 väärtalt või kui andurite kalibreerimisele on lubamatu juurdepääs, ei pruugi andurite näidud olla usaldusväärsed ja anda ebaõigeid mõõtetulemusi.

3 Meetmed**Sisukord**[3.1 Elutsükkel](#)[3.2 Põhimeetmed](#)[IND.2.3.M1 Andurite õige valimine ja paigaldamine \[hooldepersonal\]](#)[3.3 Standardmeetmed](#)[IND.2.3.M2 Andurite kalibreerimine \[hooldepersonal\]](#)[3.4 Kõrgmeetmed](#)[IND.2.3.M3 Traadita side vältimine \(C\)](#)

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, tolmu, 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.

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

IND. Tööstuse IT

IND.2: Tööstusautomaatika

IND.2.4: Robotseadmed

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

1.1 Eesmärk

Esitada elektrooniliselt juhitud 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 komponentide üldiselt](#). Käidutehnoloogia üldised korralduslikud turvameetmed esitatakse moodulis [IND.1 Käidu- ja protsessijuhtimissüsteemid](#).

2 Ohud

Sisukord

[2.1 Puudulikust hooldusest põhjustatud tõrge või häiring](#)

[2.2 Sihilikud manipulatsioonid](#)

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

Sisukord

[3.1 Elutsükel](#)[3.2 Põhimeetmed](#)[IND.2.4.M1 Valmistaja tehtava kaughoolduse turve](#)[IND.2.4.M2 Protseduur käituseks pärast garantiiaja lõppu](#)[3.3 Standardmeetmed](#)[3.4 Kõrgmeetmed](#)

3.1 Elutsükel

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 kooskõlastatud.

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.

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

IND. Tööstuse IT

IND.2: Tööstusautomaatika

IND.2.7: Ohutusautomaatika

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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

Sisukord

[2.1 Loogikasüsteemi manipuleerimine](#)

[2.2 Puudulikud seire- ja tuvastusprotseduurid](#)

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 näitused, 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

Sisukord

[3.1 Elutsükel](#)

[3.2 Põhimeetmed](#)

[IND.2.7.M1 Arvelevõtt ja dokumenteerimine \[arhitekt, hooldepersonal\]](#)

[IND.2.7.M2 Riistvara- ja tarkvarakomponentide sihtotstarbeline kasutamine \[hooldepersonal\]](#)

[IND.2.7.M3 Loogikasüsteemi turve \[hooldepersonal\]](#)

[3.3 Standardmeetmed](#)

[IND.2.7.M4 Infoturbe sidumine talitlusohutuse haldusega \[käidutehnoloogia talitus\]](#)

[IND.2.7.M5 Ohutusautomaatika intsidendihaldus \[infoturbejuht\]](#)

[IND.2.7.M6 Ohutusautomaatika tervikluse turve \[arhitekt, hooldepersonal\]](#)

[IND.2.7.M7 Ohutusautomaatika eraldamine ja sõltumatus keskkonnast \[arhitekt, hooldepersonal\]](#)

[IND.2.7.M8 Tehniliste andmete turvaline edastus ohutusautomaatikale \[arhitekt, infoturbejuht, hooldepersonal\]](#)

[IND.2.7.M9 Andme- ja signaaliühenduste turve \[arhitekt, infoturbejuht, hooldepersonal\]](#)

[IND.2.7.M10 Simuleeritud või sillatud muutujate esitus ja alarmeerimine \[arhitekt\]](#)

[IND.2.7.M11 Integreeritud süsteemide ohutuse haldus \[arhitekt, hooldepersonal\]](#)

[3.4 Kõrgmeetmed](#)

[IND.2.7.M12 Rakendusprogrammide ja konfiguratsioonandmete tervikluse ja autentsuse tagamine \[arhitekt\] \(I\)](#)

3.1 Elutsükel

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]

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 talitusohutuse haldusega [käidutehnoloogia talitus]

a. Ohutusautomaatika infoturbega seotud protsessid, õigused ja kohustused on selgelt määratletud ja integreeritud talitusohutuse halduse protsessiga.

b. Ohutusautomaatika seadmeid hallatakse vastavalt õigusnormidele ja ohutusstandarditele.

IND.2.7.M5 Ohutusautomaatika intsidendihaldus [infoturbejuht]

a. On kehtestatud ohutusautomaatika intsidendikäsitusplaan, mis määrab vajalikud rollid ja kohustused;

b. Intsidendikäsitusplaanis 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 talitusohutuse halduse kaudu.

IND.2.7.M8 Tehniliste andmete turvaline edastus ohutusautomaatikale [arhitekt, infoturbejuht, hooldepersonal]

a. Rakendatakse tehnilisi ja korralduslikke meetmeid ohutusautomaatikale 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 suundlülis).

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 alatakse alati ohutusautomaatika keskkonnast;
- andmeliiklus on piiratud määratud portide ja aadressidega;
- edastatavate sõnumite sisu seire võimalike anomaaliade 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“

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetusskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

ISMS. Turbehaldus

ISMS.1: Turbehaldus

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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 etalon turbe meetodikal ja Eesti Infoturbestandardi nõuete dokumendil ([Eesti Infoturbestandard. Nõuded](#)). Infoturbega seotud personalimeetmeid käsitletakse mooduligrupis [ORP.2 Personal](#).

2 Ohud

Sisukord

[2.1 Isikliku vastutuse puudumine turbeprotsessis](#)

[2.2 Puudulik toetus organisatsiooni juhtkonnalt](#)

[2.3 Ebapiisav kava infoturbe strateegia elluviimiseks](#)[2.4 Ebaoptimaalsed investeeringud](#)[2.5 Turvameetmete rakendamata jätmine](#)[2.6 Turbeprotsessi ajakohastamata jätmine](#)[2.7 Seaduste ja lepingute mittetäitmine](#)[2.8 Äriprotsesside häirivad turvaintsidendid](#)[2.9 Ebamajanduslik ressursikasutus puuduliku turbehalduse tõttu](#)

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 üleinvesteermist 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 turvaintsidenti, 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 investeringuta.

3 Meetmed

Sisukord

[3.1 Elutsükkel](#)

[3.2 Põhimeetmed](#)

[ISMS.1.M1 Infoturbe üldvastutuse võtmine juhtkonnatasemel \[organisatsiooni juhtkond\]](#)

[ISMS.1.M2 Turvaeesmärgid ja turbe strateegia \[organisatsiooni juhtkond\]](#)

[ISMS.1.M3 Infoturvapoliitika \[organisatsiooni juhtkond\]](#)

[ISMS.1.M4 Infoturbejuhi määramine \[organisatsiooni juhtkond\]](#)

[ISMS.1.M5 Leping välise infoturbejuhi kasutamiseks \[organisatsiooni juhtkond\]](#)

[ISMS.1.M6 Infoturbekorralduse rajamine \[organisatsiooni juhtkond\]](#)

[ISMS.1.M7 Turvameetmete määramine](#)

[ISMS.1.M8 Töötajate lõimimine turbeprotsessi \[ülemus\]](#)

[ISMS.1.M9 Infoturbe lõimimine organisatsiooniülestes protsessidesse \[organisatsiooni juhtkond\]](#)

[ISMS.1.M10 Turbekontseptsioon](#)

[ISMS.1.M11 Infoturbe käigushoid](#)

[ISMS.1.M12 Infoturbearuanded juhtkonnale \[organisatsiooni juhtkond\]](#)

[ISMS.1.M13 Turbeprotsessi dokumenteerimine](#)

[ISMS.1.M15 Infoturberessursside ökonoomne kasutus \[organisatsiooni juhtkond\]](#)

[3.4 Standardmeetmed](#)

[ISMS.1.M16 Täpsustavate turvapoliitikate väljatöötamine](#)

[3.4 Kõrgmeetmed](#)

[ISMS.1.M17 Kindlustuslepingute sõlmimine \(A\)](#)

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 kohustus 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 eesmärgi, 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 andmekaitsejuhi ning väliste regulaatoritega.

f. Infoturbejuht on kaasatud IT projektidesse ning IT-süsteemide arendusprotsessi.

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

Kui infoturbejuhi rolli ei saa täita oma töötajaga, siis hangitakse infoturbejuht teenusena väljastpoolt organisatsiooni.

a. Välisel infoturbejuhil on vajalik kvalifikatsioon.

b. Infoturbejuhi teenuseleping sisaldab infoturbejuhi tööülesandeid ning nendega seotud õigusi ja kohustusi. Sätestatud on vähemalt järgmised aspektid:

<https://eits.ria.ee/et/version/2021/etalonturbe-kataloog/isms-turbehaldus/isms1-turbehaldus/>

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

c. Välise infoturbejuhiga on sõlmitud konfidentsiaalsusleping.

d. Infoturbejuhi teenuselepingus kajastatakse lepingulise suhte kogu elutsüklil, sealhulgas:

- töid teostavate isikute asendamise kord;
- huvide konflikti määramine 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;
- andmekaitse juht.

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

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

e. Infoturbekorralduse suhtlused 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 tagasi jälgitav;
- 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. Infoturbe 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. 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 väljastellimine.

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
[RIA]	IT-halduse raamdokumentide näidised, https://www.ria.ee/et/kuberturvalisus/iske/juhendid-ja-materjalid.html

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetusskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

ORP. Organisatsioon ja personal

ORP.1: Infoturbe korraldus

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

1.1 Eesmärk

Esitada meetmed infoturbe korralduse sobitamiseks organisatsiooniga, infoturbe juhtimiseks ja käigushoiuks.

1.2 Vastutus

„Infoturbe korraldus“ meetmete täitmise eest vastutab haldusosakond.

Lisavastutajad

Kasutaja, tehnikatalitus, IT-talitus, organisatsiooni juhtkond, töötaja.

1.3 Piirangud

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

2 Ohud

Sisukord

[2.1 Puuduvad või puudulikud eeskirjad](#)

[2.2 Eeskirjade rikkumine](#)

[2.3 Puuduvad, ebasobivad või ühildamatud töövahendid](#)

2.4 Ohud abi- ja välispersonalile tõttu

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 andmetöötleses 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. Töövahendi hankimisel võib uus töövahend osutuda olemasoleva vanema tehnoloogilise keskkonnaga ühildamatuks.

2.4 Ohud abi- ja välispersonalile tõttu

Organisatsioonivälistelt isikutelt ei saa vaikumisi 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

Sisukord

3.1 Elutsükel

3.2 Põhimeetmed

[ORP.1.M1 Kohustuste ja eeskirjade kehtestamine \[organisatsiooni juhtkond\]](#)

[ORP.1.M2 Teabe, rakenduste ja IT-komponentide eest vastutajate määramine \[organisatsiooni juhtkond\]](#)

[ORP.1.M3 Organisatsiooniväliste isikute järelevalve või saatmine \[töötaja\]](#)

[ORP.1.M4 Tegevus- ja kontrollikohustuste lahusus](#)

[ORP.1.M15 Infoturbe kontaktisik](#)

3.3 Standardmeetmed

[ORP.1.M8 Töövahendite ja seadmete haldus \[IT-talitus\]](#)

[ORP.1.M13 Kolimise turve \[IT-haldus, tehnikatalitus\]](#)

[ORP.1.M16 IT-vahendite turvalise kasutamise eeskiri \[kasutaja\]](#)

3.4 Kõrgmeetmed

3.1 Elutsükel

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 Organisatsiooniväliste isikute järelevalve või saatmine

ORP.1.M13 Kolimise turve

ORP.1.M15 Infoturbe kontaktisik

3.2 Põhimeetmed

ORP.1.M1 Kohustuste ja eeskirjade kehtestamine [organisatsiooni juhtkond]

a. Määratakse infoturbeülesannete täitmise kohustused ja õigused.

b. Eeskirjadega kehtestatakse turbe korraldus vähemalt järgmistes valdkondades:

- varundus ja arhiveerimine;
- andmekandjate käitus;
- hoolde- ja remonditööd;
- andmekaitse;
- avariivalmendus.

c. Teabe kaitsetarbest lähtudes määratakse andmete vahetuse kord ja vajalikud kaitsemeetmed.

d. Eeskirjad tehakse teatavaks kõigile töötajale ning neid vaadatakse regulaarselt üle.

ORP.1.M2 Teabe, rakenduste ja IT-komponentide eest vastutajate määramine [organisatsiooni juhtkond]

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 Organisatsiooniväliste isikute järelevalve või saatmine [töötaja]

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 jätta väliseid isikuid organisatsiooni ruumidesse ilma järelevalveta.

ORP.1.M4 Tegevus- ja kontrollikohustuste lahusus

- a. Organisatsioonis tagatakse infoturbe toimingute sooritaja ning toimingute kontrollija rollide lahusus.
- b. Tegevus- ja kontrollikohustuste lahusus kehtib ka töötaja asendamise korral.

ORP.1.M15 Infoturbe kontaktisik

- 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]

- 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 kasutuseks 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]

- a. Enne plaanitud kolimist töötatakse välja või ajakohastatakse kolimisplaan, kus muuhulgas määratletakse töötajate kohustused.
- b. Töötajaid informeeritakse turvameetmetest, mida on vaja järgida kolimise eel, ajal ja järel.
- c. Enne kolimist varundatakse andmed ja märgistatakse üheselt kolitav materjal.
- d. Kolimise käigus rakendatakse juurdepääsu kontrollile, väline personal liigub lähtekohas ja sihtkohas ainult oma töötaja saatel.
- e. Pärast kolimist kontrollitakse, kas kolimisel transporditud esemed on täielikult ja 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 [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

Moodulis kõrgmeetmed puuduvad.

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetusskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

ORP. Organisatsioon ja personal

ORP.2: Personal

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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 käsitletavat meetmed on üldised. Konkreetse funktsiooniga seotud personalimeetmed esitatakse asjakohastes moodulites.

2 Ohud

Sisukord

[2.1 Personali piisamatus](#)

[2.2 Nõuete puudulik tundmine](#)

[2.3 Hooletus andmete kasutamisel](#)

2.4 Ebapiisav töötajate kvalifikatsioon

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 turvameetmeid 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

Sisukord

3.1 Elutsükkel

3.2 Põhimeetmed

[ORP.2.M1 Uue töötaja sisseelamise kord \[ülemus\]](#)

[ORP.2.M2 Töötaja lahkumise protseduur \[ülemus, IT-talitus\]](#)

[ORP.2.M3 Töötaja asendamise kord \[ülemus\]](#)

[ORP.2.M4 Asendamise kord välise töötaja puhul](#)

[ORP.2.M5 Konfidentsiaalsusleping väliste töötajate kasutamisel](#)

[ORP.2.M14 Tööülesannete ja kohustuste kehtestamine \[ülemus\]](#)

[ORP.2.M15 Piisava kvalifikatsiooniga töötajad \[ülemus\]](#)

3.3 Standardmeetmed

[ORP.2.M7 Kandidaadi usaldusväarsuse kontrollimine](#)

3.4 Kõrgmeetmed

[ORP.2.M11 Turvakultuuri analüüs \(C-I-A\)](#)

[ORP.2.M13 Töötaja taustakontroll \(C-I-A\)](#)

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 usaldusväarsuse 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. Soovitavalt 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 informeeritakse 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 usaldusvärsuse 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.

4 Lisateave

Siin lisainfot ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

ORP. Organisatsioon ja personal

ORP.3: Infoturbe teadlikkuse tõstmine ja koolitus

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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

Sisukord

[2.1 Turvanõuete puudulik tundmine](#)

[2.2 Puudulik infoturvateadlikkus](#)

[2.3 Teadvustuse ja koolituse vähene tulemuslikkus](#)

[2.4 Puudlik koolitus turvafunktsioonide alal](#)[2.5 Avastamata jäänud turvasündmused](#)[2.6 Turvameetmete eiramine](#)[2.7 Hooletus teabe töötlemisel](#)[2.8 Infoturbe puudulik omaksvõtmine](#)[2.9 Suhtlusrinne](#)

2.1 Turvanõuete puudulik tundmine

Turvaintsidenti 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 oskamatusel 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, ukseid 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 igäüks 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

Suhtlusrünne (ingl *social engineering*) tulemusel võib ründaja saada teabele või IT-süsteemidele lubamatu juurdepääsu, luues kontakte telefoni, e-posti või sotsiaalsõrgu kaudu ning kasutades ära inimeste abivalmidust. Kui töötaja sellist ründeviisi piisaval määral ei tunne, siis osavalt suheldes suunatakse töötaja toimima lubamatul viisil. Suhtlusrünne tulemusena võib ründaja hankida konfidentsiaalset teavet, levitada kahjurtarkvara või koguni sundida töötajat väidetavale äripartnerile raha üle kandma.

3 Meetmed

Sisukord

[3.1 Elutsükel](#)

[3.2 Põhimeetmed](#)

[ORP.3.M1 Juhtkonna teadlikkuse suurendamine infoturbe alal \[ülemus, organisatsiooni juhtkond\]](#)

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

[3.3 Standardmeetmed](#)

[ORP.3.M4 Infoturbe teadvustus- ja koolitusplaan](#)

[ORP.3.M6 Infoturbe teadvustus- ja koolitusmeetmete kavandamine ja rakendamine](#)

[ORP.3.M7 Infoturbe halduse meetodeid käsitlevad koolitused](#)

[ORP.3.M8 Õpitulemuste mõõtmine ja hindamine \[personaliosakond\]](#)

[3.4 Kõrgmeetmed](#)

[ORP.3.M9 Ohustatud isikute ja organisatsioonide erikoolitus \(C-I-A\)](#)

3.1 Elutsükel

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 informeeritakse 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. Töötajatele ja organisatsioonivälistele kasutajatele on selgitatud, kuidas IT-, tööstusautomaatika- ja esemevõrgu komponente turvaliselt kasutada ja millised on kasutamisega seotud õigused ja kohustused.
- b. Organisatsioon on koostanud eeskirjad IT-, tööstusautomaatika ja esemevõrgu komponentide turvaliseks kasutamiseks. Eeskirjad on arusaadavad ja ajakohased, kohustuste selgeks määratlemiseks on need kinnitatud juhtkonnas.
- c. 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 kontrole.

c. Personaliosakond teeb koolituse sisu ja efektiivsuse hindamisel koostööd infoturbejuhi, andmekaitse spetsialisti, 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. Infoturbe 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 äriplaneerimine

Moodul 13. Taristu turve

Funktsioon	Moodul 1	Moodul 2	Moodul 3	Moodul 4	Moodul 5	Moodul 6	Moodul 7	Moodul 8	Moodul 9
Ülemus	X	X	X	X					
Turbehaldus	X	X	X	X	X	X	X	X	X
Andmekaitse spetsialist	X	X	X	X					
Taristu eest vastutav isik	X	X	X	X	X	O			
Kasutaja	X	X							
Süsteemiülem	X	X		X	X		X	X	X

Tabel. Soovitavad 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.

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetusskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

ORP. Organisatsioon ja personal

ORP.4: Identiteedi- ja õiguste haldus

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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 infoturbejuht.

Lisavastutajad

Kasutaja, IT-talitus.

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

Sisukord

[2.1 Identiteedihalduse protsesside puudumine või puudulikkus](#)

[2.2 Kasutaja õiguste keskse peatamise võimaluse puudumine](#)

2.3 Pääsuõiguste puudulik haldamine

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

3 Meetmed

Sisukord

3.1 Elutsükel

3.2 Põhimeetmed

[ORP.4.M1 Kasutajakontode halduse eeskiri \[IT-talitus\]](#)

[ORP.4.M2 Õiguste andmine, muutmine ja tühistamine \[IT-talitus\]](#)

[ORP.4.M3 Kasutajate õiguste dokumenteerimine \[IT-talitus\]](#)

[ORP.4.M4 Kohustuste jaotamine ja kohustuste lahusus \[IT-talitus\]](#)

[ORP.4.M5 Füüsilise ligipääsu haldamine \[IT-talitus\]](#)

[ORP.4.M6 IT-vahenditele juurdepääsu haldamine \[IT-talitus\]](#)

[ORP.4.M7 Andmete juurdepääsu haldamine \[IT-talitus\]](#)

[ORP.4.M8 Paroolide kasutamise kord \[kasutaja, IT-talitus\]](#)

[ORP.4.M9 Tuvastamine ja autentimine \[IT-talitus\]](#)

[ORP.4.M22 Parooli kvaliteedinõuete kehtestamine \[IT-talitus\]](#)

[ORP.4.M23 Nõuded paroolide töötlevatele IT-süsteemidele \[IT-talitus\]](#)

3.3 Standardmeetmed

[ORP.4.M10 Eeliskontode kaitsmine \[IT-talitus\]](#)

[ORP.4.M11 Paroolide lähtestamine ja muutmine \[IT-talitus\]](#)

[ORP.4.M12 IT-süsteemide ja rakenduste autentimiskord \[IT-talitus\]](#)

[ORP.4.M13 Sobivate autentismehhanismide valimine \[IT-talitus\]](#)

[ORP.4.M14 Kasutajakontode kasutuse kontrollimine \[IT-talitus\]](#)

[ORP.4.M15 Identiteedi- ja õiguste halduse protseduurid \[IT-talitus\]](#)

[ORP.4.M16 IT-süsteemidele juurdepääsu reguleerimine \[IT-talitus\]](#)

[ORP.4.M17 Sobiv identiteedi- ja õiguste halduse süsteem \[IT-talitus\]](#)

[ORP.4.M18 Keskse autentimisteenuse kasutamine \[IT-talitus\]](#)

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

3.4 Kõrgmeetmed

[ORP.4.M20 Identiteedi- ja õiguste halduse süsteemi avariivalmendus \(C-I-A\) \[IT-talitus\]](#)

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

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

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 paroolide 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 [IT-talitus]

- a. Organisatsioon on koostanud ja kinnitanud kasutajakontode halduse eeskirja.
- b. Kasutajakonto määratakse identiteedipõhiselt, 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 [IT-talitus]

- 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 [IT-talitus]

- 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 [IT-talitus]

- 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 [IT-talitus]

- 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 [IT-talitus]

- 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 [IT-talitus]

- 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, IT-talitus]

- 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 [IT-talitus]

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 [IT-talitus]

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. Soovitav 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 [IT-talitus]

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 [IT-talitus]

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 [IT-talitus]

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 [IT-talitus]

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 [IT-talitus]

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 [IT-talitus]

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 [IT-talitus]

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 [IT-talitus]

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 [IT-talitus]

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.

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

ORP.4.M18 Keskse autentimisteenuse kasutamine [IT-talitus]

a. Ühtse identiteedi- ja õiguste halduse rakendamiseks kasutatakse kesket 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 (C-I-A) [IT-talitus]

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 kasutatakse 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.

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetusskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

ORP. Organisatsioon ja personal

ORP.5: Vastavusehaldus (nõuete haldus)

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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

Sisukord

[2.1 Seaduse- või lepingusätete rikkumine](#)

[2.2 Teabe lubamatu avaldamine](#)

[2.3 Suhtluspartneri identiteedi puudulik kontrollimine](#)

2.4 Siseteabe kogemata avaldamine

2.1 Seaduse- või lepingusätete rikkumine

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

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 kättesse.

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

Sisukord

3.1 Elutsükkel

3.2 Põhimeetmed

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

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

3.3 Standardmeetmed

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

ORP.5.M5 Erandite haldus [infoturbejuht]

ORP.5.M8 Vastavusehalduse regulaarne läbivaatus

3.4 Kõrgmeetmed

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;
 - tegutsemise 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.

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

CON. Kontseptsioonid ja meetodikad

CON.1: Krüptokontseptsioon

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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, ülemus.

1.3 Piirangud

Krüptomoodulite 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

Sisukord

[2.1 Puudulik võtmehaldus](#)

[2.2 Õiguslike raamtingimuste rikkumine krüptovahendite rakendamisel](#)

[2.3 Andmete konfidentsiaalsuse või tervikluse kadu kasutamisvigade tõttu](#)

[2.4 Tarkvaravead või -defektid krüptograafilises vahendis](#)

[2.5 Krüptomooduli tõrge](#)

[2.6 Ebaturvalised krüptograafilised vahendid](#)

[2.7 Viga krüpteeritud andmetes või krüptovõtmes](#)

[2.8 Krüptomooduli volitamatu kasutamine](#)

[2.9 Krüptovõtme paljastamine](#)

[2.10 Võltsitud sertifikaat](#)

2.1 Puudulik võtmehaldus

Kui krüpteeritud andmed ja krüptovõtmed asuvad samal andmekandjal, saavad sümmeetrilise krüptoprotseduuri korral kõik andmekandjale või sidekanalile juurdepääsu omavad isikud andmeid dekrüpteerida.

2.2 Õiguslike raamtingimuste rikkumine krüptovahendite rakendamisel

Õiguslikud raamtingimused krüptovahendite rakendamisel võivad riigiti erineda. Mõnes riigis ei tohi krüptovahendeid ilma riikliku loata kasutusele võtta või on riigis piiratud suure murdmiskindlusega krüptograafiaga toodete eksport. Andmekaitseseadus võib sätestada, et isikuandmete kaitseks tuleb rakendada kindlaksmääratud krüptograafilisi protseduure.

2.3 Andmete konfidentsiaalsuse või tervikluse kadu kasutamisvigade tõttu

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

2.4 Tarkvaravead või -defektid krüptograafilises vahendis

Krüptomehhanismide turvalisust võivad vähendada nõrkused või vead krüptograafiliste vahendite tarkvaras.

2.5 Krüptomooduli tõrge

Tehniliste defektide, elektrikatkestuste või tahtliku hävitamise tõttu võib tekkida tõrge krüptomoodulis.

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 organisatsiooniväline 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. Üksnes ühe biti muutmine krüptovõtmes ei lase sellega krüpteeritud andmeid enam dekrüpteerida.

2.8 Krüptomooduli volitamatu kasutamine

Kui ründajal õnnestub krüptomoodulit lubamatult kasutada, saab ta manipuleerida elutähtsaid IT-süsteeme.

2.9 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.

Krüpteeritud kõvaketta korral võib ründaja kõvaketta dekrüpteerimiseks paigaldada klaviatuuri ja arvuti vahele paroolile juurdepääsu saamiseks klahvilogeri (ingl *keylogger*).

2.10 Võltsitud sertifikaat

Sertifikaate kasutatakse avaliku krüptovõtme konkreetse isiku privaativõtme 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

Sisukord

[3.1 Elutsükkel](#)

[3.2 Põhimeetmed](#)

[CON.1.M1 Krüptovahendi valimise kord \[vastutav spetsialist\]](#)

[CON.1.M2 Andmevarundus krüptovahendi kasutamisel \[IT-talitus\]](#)

[3.3 Standardmeetmed](#)

[CON.1.M3 Side krüpteerimine](#)

[CON.1.M4 Korrektne võtmehaldus](#)

[CON.1.M5 Krüptovõtmete kustutus ja hävitamine \[IT-talitus\]](#)

[CON.1.M6 Krüptoprotsesside ja -toodete vajaduse uuring \[IT-talitus, vastutav spetsialist\]](#)

[3.4 Kõrgmeetmed](#)

[CON.1.M7 Krüptoprotsesside ja -toodete turvapoliitika \(C-I-A\)](#)

[CON.1.M8 Krüptoprotsesside mõjurite uuring \(C-I-A\)](#)

[CON.1.M9 Sobivate krüptovahendite valimine \(C-I\) \[IT-talitus, vastutav spetsialist\]](#)

[CON.1.M10 Krüptokontseptsioon \(C-I\)](#)

[CON.1.M11 Krüptomooduli turvaline konfiguratsioon \(C-I\) \[IT-talitus\]](#)

[CON.1.M12 Turvaline rollijaotus krüptomooduli kasutamisel \(C-I\) \[IT-talitus\]](#)

[CON.1.M13 Krüptomooduli turvaline koostöö operatsioonisüsteemiga \(C-I\)](#)

[CON.1.M14 Kasutajate ja haldurite koolitus \(C-I-A\) \[organisatsiooni juhtkond, IT-talitus, vastutav spetsialist\]](#)

[CON.1.M15 Reageerimine krüptoprotsessi nõrgenemisele \(C-I\)](#)

[CON.1.M16 Krüptomooduli füüsiline turve \(C-I\) \[IT-talitus\]](#)

[CON.1.M17 Kiirguseturve \(C\) \[IT-talitus\]](#)

[CON.1.M18 Varu-krüptomoodul \(C-I-A\) \[IT-talitus\]](#)

3.1 Elutsükkel

Kavandamine

CON.1.M6 Krüptoprotsesside ja -toodete vajaduse uuring

CON.1.M1 Krüptovahendi valimise kord

Käitus

CON.1.M3 Side krüpteerimine

CON.1.M4 Korrektne võtmehaldus

CON.1.M5 Krüptovõtmete kustutus ja hävitamine

Avariivalmendus

CON.1.M2 Andmevarundus krüptovahendi kasutamisel

Lisanduvad kõrgmeetmed

CON.1.M7 Krüptoprotsesside ja -toodete turvapoliitika

CON.1.M8 Krüptoprotsesside mõjurite uuring

CON.1.M9 Sobivate krüptotoodete valimine

CON.1.M10 Krüptokontseptsioon

CON.1.M11 Krüptomooduli turvaline konfiguratsioon

CON.1.M12 Turvaline rollijaotus krüptomooduli kasutamisel

CON.1.M13 Krüptomooduli turvaline koostöö operatsioonisüsteemiga

CON.1.M14 Kasutajate ja haldurite koolitus

CON.1.M15 Reageerimine krüptoprotsessi nõrgenemisele

CON.1.M16 Krüptomooduli füüsiline turve

CON.1.M17 Kiirguseturve

CON.1.M18 Varu-krüptomoodul

3.2 Põhimeetmed

CON.1.M1 Krüptovahendi valimise kord [vastutav spetsialist]

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

b. Krüptovahendis kasutatakse hetkel soovitatavaid võtmepikkusi.

CON.1.M2 Andmevarundus krüptovahendi kasutamisel [IT-talitus]

a. Krüpteeritud andmete varundamisel on krüptovõtmed kaitstud lubamatu juurdepääsu eest. Pika kasutuskestusega krüptovõtmeid hoitakse väljaspool kasutatavat IT-süsteemi.

b. Andmete krüpteerimiseks kasutatud krüptoalgoritmide ja võtmepikkuste vastavust hetkel soovitavatele väärtustele kontrollitakse regulaarselt.

c. Krüpteeritud kujul salvestatud andmete loetavus on tagatud pikaajaliselt.

d. Kasutusest võetud krüptovahendid on archiveeritud ja konfiguratsioon on varundatud.

3.3 Standardmeetmed

CON.1.M3 Side krüpteerimine

Side krüpteeritakse, kui see on võimalik ja teostatav mõistlike pingutustega.

CON.1.M4 Korrektnel võtmehaldus

- a. Krüptovõtmeloomisel on kasutatud sobivat võtmegeneraatorit ja turvalist keskkonda.
- b. Krüptovõtit kasutatakse ainult üheks kasutusotstarbeks. Krüpteerimiseks ja signatuuride moodustamiseks kasutatakse erinevaid võtmeid.
- c. Krüptovõtmel transpordil kasutatakse turvalisi edastuskanaleid.
- d. Krüptovõtme kasutamisel kontrollitakse võtmeandmel päritolu ja terviklust.
- e. Krüptovõtmeid muudetakse vastavalt IT-süsteemi nõuetele ja fikseeritud sagedusega.
- f. Krüptovõtmel haldamiseks on loodud turvaline keskkond.

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

- a. Kasutusest võetud krüptovõtmed ja sertifikaadid kustutatakse turvaliselt ja hävitatakse.
- b. Kontrollimatu võtmehoidlaga krüptograafilisi tooteid ei kasutata.

CON.1.M6 Krüptoprotsesside ja -toodel vajaduse uuring [IT-talitus, vastutav spetsialist]

- a. Krüptograafia kasutamise vajadusuuringuga on määratud, mis toimingutel krüptoprotsesse ja -tooteid kasutatakse.
- b. On määratud krüptograafiliselt kaitstavad IT-süsteemid ja sideühendused.

3.4 Kõrgmeetmed

CON.1.M7 Krüptoprotsesside ja -toodel turvapoliitika (C-I-A)

- a. Organisatsiooni üldise turvapoliitika alusel on välja töötatud krüptoprotsesside ja -toodel turvapoliitika ning protseduurid krüptotoodel kasutuselevõtuks ning asendamiseks.
- b. Krüptoprotsesside ja -toodel turvapoliitikaga on määratud:
 - kes vastutab krüptoprotsesside ja -toodel eest;
 - kuidas tagatakse krüptomoodulite turvaline konfigureerimine;
 - kuidas krüptotooteid kasutatakse ja hooldatakse.
- c. Krüptoprotsesside ja -toodel kasutajatele on koostatud õppematerjalid, tegevusjuhised ning loodud teavitused probleemidest ja turvasündmustest teavitamiseks. Asjassepuutuvad töötajad järgivad tegevusjuhiseid.
- d. Krüptoprotsesside ja -toodel turvapoliitika täitmist kontrollitakse regulaarselt. Kontrollitulemused dokumenteeritakse.

CON.1.M8 Krüptoprotsesside mõjurite uuring (C-I-A)

- a. Suure kaitsetarbe korral arvestatakse enne krüptoprotsesside rakendamist järgmiseid mõjureid:
 - turvaaspektid (vt CON.1.M6 Krüptoprotsesside ja -toodel vajaduse uuring);

- tehnilised aspektid;
- personali- ja korralduslikud aspektid;
- majanduslikud aspektid;
- krüptomehhanismide ja võtmepikkuste kasutusiga;
- krüptotoodete kinnitamine;
- õiguslikud raamtingimused.

CON.1.M9 Sobivate krüptovahendite valimine (C-I) [IT-talitus, vastutav spetsialist]

a. Enne krüptovahendi valimist määratakse, millistele nõuetele peab toode vastama. Seejuures pööratakse tähelepanu järgmistele aspektidele:

- funktsionaalsus;
- koostalitlusvõime;
- majanduslik otstarbekus;
- töö- ja tõrkekindlus.

b. Kasutusotstarbe ja käituskoha alusel otsustatakse, kas on vajalik kasutada ainult sertifitseeritud krüptovahendeid.

CON.1.M10 Krüptokontseptsioon (C-I)

a. Organisatsiooni krüptokontseptsioonis on kirjeldatud kasutatavate krüptograafiliste vahendite tehnilised ja korralduslikud nõuded.

b. Krüptokontseptsioonis on loetletud asjassepuutuvad IT-süsteemid ja sideühendused.

c. Krüptokontseptsiooni ajakohastatakse regulaarselt.

CON.1.M11 Krüptomooduli turvaline konfiguratsioon (C-I) [IT-talitus]

a. Krüptomooduli installimisel ja konfigureerimisel luuakse uued krüptovõtmed ning kontrollitakse krüptomooduli toimivust.

b. Krüptomooduli kasutuselevõtule eelnevalt on määratud nõuded rakenduskeskkonnale.

c. IT-süsteemi muudatuste järgselt testitakse kasutatavate krüptoprotsesside toimivust.

d. Krüptomooduli konfiguratsioon dokumenteeritakse, dokumentatsiooni kontrollitakse regulaarselt.

CON.1.M12 Turvaline rollijaotus krüptomooduli kasutamisel (C-I) [IT-talitus]

a. Krüptomooduli konfigureerimisel on määratud kasutajarollid. Pääsu reguleerimisega võimaldatakse teenuse kasutamine ainult selleks volitatud töötajatele.

b. Krüptomoodul on konfigureeritud nii, et iga kasutajavahetuse või seansi aegumise korral sisestatakse autentimisandmed uuesti.

CON.1.M13 Krüptomooduli turvaline koostöö operatsioonisüsteemiga (C-I)

a. Operatsioonisüsteemi ja krüptomoodulite koostalitlus tagab, et installitud krüptomoduleid ei saa märkamatuks välja lülitada ega ignoreerida.

b. Kasutusel või arhiveeritud võtmeid ei saa väärkasutada.

c. Kaitstavaid andmeid ei saa andmekandjatele salvestada või neid infotöötlussüsteemist välja viia krüpteerimata kujul.

d. Krüptomooduli manipuleerimiskatsed tuvastatakse.

CON.1.M14 Kasutajate ja haldurite koolitus (C-I-A) [organisatsiooni juhtkond, IT-talitus, vastutav spetsialist]

a. Kasutajate ja haldurite koolitusel selgitatakse, kuidas krüptomoduleid tööülesannete täitmiseks kasutatakse ja mida tähendavad krüptomoodulite konkreetsed turvasätted.

b. Koolitusel juhitakse tähelepanu ohtudele, mis kaasnevad turvasätetest mugavuse tõttu möödahiilimisel või turvasätete desaktiveerimisel. Koolituse sisu on vastavuses reaalse rakendusstsenaariumiga.

c. Halduritele selgitatakse krüptograafiliste sätete seadistamist ning antakse ülevaade krüptograafia põhimõistetest.

CON.1.M15 Reageerimine krüptoprotsessi nõrgenemisele (C-I)

Organisatsiooni infoturbe tagamiseks krüptoprotsessi nõrgenemisel rakendub protseduur, mis taastab krüptoprotsessi turvaseme või asendab nõrgenenud krüptoprotsessi sobiva alternatiiviga.

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

a. Rakendatakse meetmeid krüptomoodulile volitamata füüsilise juurdepääsu tõkestamiseks.

b. Krüptomooduliteks valitakse sellised riist- ja tarkvaratooted, mis võimaldavad teha eneseteste.

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

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

CON.1.M18 Varu-krüptomoodul (C-I-A) [IT-talitus]

a. Tagatakse varu-krüptomooduli olemasolu.

4 Lisateave

Lühend	Publikatsioon
[RIA]	Cybernetica. Krüptograafiliste algoritmide elutsükli uuring, 2017., https://www.ria.ee/sites/default/files/content-editors/publikatsioonid/kryptograafiliste_algoritmide_elutsykli_uuring_2017.pdf

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetusskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

CON. Kontseptsioonid ja metoodikad

CON.2: Isikuandmete kaitse

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.2 Piirangud](#)

1.1 Eesmärk

Esitada isikuandmete kaitse seos etalonturbega. Mooduli eesmärk on kaitsta füüsiliste isikute põhiõiguste teostamist isikuandmete töötlemisel organisatsioonis.

1.2 Vastutus

Isikuandmete kaitse nõuete täitmise eest vastutab andmekaitse spetsialist.

Lisavastutajad

Organisatsiooni juhtkond.

1.2 Piirangud

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

2 Ohud

Sisukord

[2.1 Andmekaitse seaduste eiramine](#)

[2.2 Puudulikud andmetöötlusprotseduurid](#)

[2.3 Puudulik privaatsus](#)[2.4 Liiga madala kaitsetarbe määramine](#)

2.1 Andmekaitseaduste eiramine

Euroopa Liidu isikuandmete kaitse üldmäärusest tulenevalt peab isikuandmete töötlemiseks olema õiguslik alus. Oht isikutele tekib, kui organisatsioon ei töötle andmeid eesmärgipäraselt, töötleb andmeid läbipaistmatult, turvameetmeid rakendamata ja ilma andmesubjektide sekkumisvõimaluseta.

2.2 Puudulikud andmetöötlusprotseduurid

Andmete väärkasutamise oht kasvab, kui organisatsioonis puuduvad protseduurid IT-süsteemidele ja andmetele õiguspärase juurdepääsu tagamiseks või kui andmete kasutamine ei ole logide ega dokumentatsiooni abil tõendatav.

2.3 Puudulik privaatsus

Privaatsuse riive võib tekkida juhtudel kui töödeldakse eriliiki isikuandmeid, mis paljastavad rassilist ja etnilist päritolu, poliitilisi vaateid, religioosseid või maailmavaatelisi tõekspidamisi ning ametiühingusse kuulumist, samuti geneetilisi andmeid, andmeid tervise, seksuaalelu ning süüdimõistvate kohtuotsuste kohta.

2.4 Liiga madala kaitsetarbe määramine

Liiga madala kaitsetarbe määramine ei pruugi tagada piisavat isikuandmete kaitset, andmekaitseõiguslikud nõuded jäävad täitmata.

3 Meetmed

Sisukord

[3.1 Põhimeetmed](#)[CON.2.M1 Vastavus isikuandmete kaitse üldmääruse ja isikuandmete kaitse seadusega \[organisatsiooni juhtkond\]](#)

3.1 Põhimeetmed

CON.2.M1 Vastavus isikuandmete kaitse üldmääruse ja isikuandmete kaitse seadusega [organisatsiooni juhtkond]

- Organisatsioon tagab vastavuse isikuandmete kaitse üldmäärusega ning järgib isikuandmete kaitse seaduse nõudeid.
- Organisatsioon rakendab isikuandmete kaitseks kehtestatud ja rakendatud korralduslike ja tehnilisi meetmeid ning kontrollib andmekaitse meetmete rakendamist. Meetme mittejärgimine on põhjendatud.

4 Lisateave

Lühend	Publikatsioon
[GDPR]	Isikuandmete kaitse üldmäärus, https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32016R0679&from=ET
[RT]	Isikuandmete kaitse seadus, 15.01.2019, https://www.riigiteataja.ee/akt/104012019011
[ISO27701]	ISO/IEC 27701:2019 „Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines“

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

CON. Kontseptsioonid ja metoodikad

CON.3: Andmevarunduse kontseptsioon

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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

Sisukord

- [2.1 Andmevarunduse puudumine](#)
 - [2.2 Taaste testimise puudumine](#)
 - [2.3 Varukoopiate andmekandjate ebaturvaline säilitus](#)
 - [2.4 Dokumentatsiooni puudumine või puudulikkus](#)
 - [2.5 Õigusaktide nõuete eiramine](#)
 - [2.6 Ebaturvaline pilvteenusetarnija](#)
 - [2.7 Andmekandja salvestusmahu piisamatus](#)
 - [2.8 Andmevarunduse kontseptsiooni puudulikkus](#)
 - [2.9 Andmete salvestuskiiruse piisamatus](#)
 - [2.10 Lunavara rünne](#)
-

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 pilvteenusetarnija

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 ohvrit 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

Sisukord

[3.1 Elutsükel](#)

[3.2 Põhimeetmed](#)

[CON.3.M1 Andmevarunduse mõjurite piiritlemine \[vastutav spetsialist, IT-talitus\]](#)

[CON.3.M2 Andmevarunduseeskiri \[vastutav spetsialist, IT-talitus\]](#)

[CON.3.M4 Andmevarundusplaanid](#)

[CON.3.M5 Regulaarne andmevarundus \[IT-talitus, töötaja\]](#)

[CON.3.M12 Varunduseks kasutatavate andmekandjate turvaline säilitus \[IT-talitus\]](#)

[CON.3.M14 Varukoopiate turve \[IT-talitus\]](#)

[CON.3.M15 Varunduse regulaarne testimine \[IT-talitus\]](#)

[3.3 Standardmeetmed](#)

[CON.3.M6 Andmevarunduse kontseptsioon \[vastutav spetsialist, IT-talitus\]](#)

[CON.3.M7 Sobiva andmevarundussüsteemi soetamine \[IT-talitus\]](#)

[CON.3.M9 Tingimuste tagamine kaugvarunduseks \[IT-talitus\]](#)

[3.4 Kõrgmeetmed](#)

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

3.1 Elutsükel

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 äripool omanikud.

b. Andmevarunduse mõjuritena on määratud vähemalt järgnev:

- varundatavate andmete koosseis;
- varundatavate andmete käideldavus-, terviklus-, ja konfidentsiaalsusnõuded;
- seadusandlusest tulenevad nõuded;
- vajalik andmemahut;
- 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. Varundatavate andmete lubatav taasteaeg määratakse tuginedes IT-süsteemi maksimaalselt talutavale seisuaajale (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.M1 *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 põlvna;
- süsteemiandmed varundatakse vähemalt kord kuus ühe andmete põlvna;
- 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 ärijätkevusplaaniga (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

- Rakendusandmed, süsteemiandmed, tarkvara, logiandmed
- 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)
- Varundustsüklid
- Andmete kataloog
- Varuandmete kustutus
- Tarbetute andmekandjate hävitamine
- Lugemisseadmete töövõime tagamine

5. Varunduse minimaalkontseptsioon

6. Töötajate kohustumus andmevarunduse alal

7. Taasteharjutused

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetusskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

CON. Kontseptsioonid ja metoodikad

CON.6: Andmete kustutus ja hävitamine

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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

Andmekaitse spetsialist, 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

Sisukord

[2.1 Kustutuse ja hävitamise eeskirja puudumine või puudulik dokumenteerimine](#)

[2.2 Konfidentsiaalsuse kadu andmekandjate jääkteabe tõttu](#)

[2.3 Ebausaldusväärse kõrvaldusteenuse kasutamine](#)

2.4 Defektsete andmekandjate väär käsitlemine

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 andmelekkede 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 jääkteabe 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 terveniisti taastada.

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

3 Meetmed

Sisukord

[3.1 Elutsükel](#)

[3.2 Põhimeetmed](#)

[CON.6.M1 Andmete kustutuse ja hävitamise kord \[haldusosakond, vastutav spetsialist, andmekaitse spetsialist, IT-talitus\]](#)

[CON.6.M2 Kaitset vajavate töövahendite ja andmekandjate turvaline kasutuselt kõrvaldamine](#)

[CON.6.M11 Andmekandjate hävitamise tellimine väliselt teenuseandjalt \[hankeosakond\]](#)

[CON.6.M12 Protseduurid andmete turvaliseks kustutuseks](#)

[3.3 Standardmeetmed](#)

[CON.6.M4 Protseduurid andmekandjate turvaliseks hävitamiseks](#)

[CON.6.M8 Andmete kustutuse juhised töötajatele \[töötaja, IT-talitus, andmekaitespetsialist\]](#)

[CON.6.M13 Defektsete andmekandjate hävitamise juhised](#)

[3.4 Kõrgmeetmed](#)

[CON.6.M14 Andmekandjate turvalise hävitamise täiendavad juhised \(C\)](#)

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, andmekaitespetsialist, 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 andmekaitespetsialistiga.

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.2.1 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 protseduureeglite 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, andmekaitse spetsialist]

- 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. Optilised andmekandjad hävitatakse vastavalt ISO/IEC 21964-2 turvatase O-3 juhistele.
- b. Paberkandjad hävitatakse vastavalt ISO/IEC 21964-2 turvatase P-3 juhistele.
- c. Kui IT-seadmetesse integreeritud andmekandjate sisu kustutamiseks ei ole seadme vastavat funktsionaalsust, eraldatakse andmekandja seadmest ja hävitatakse vastavalt ISO/IEC 21964-2 turvatasemete E-3 või H-3 juhistele.

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“

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

CON. Kontseptsioonid ja metoodikad

CON.7: Välislähetuste infoturve

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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

Sisukord

[2.1 Teabe pealtkuulamine ja luuramine / Majandusspionaaž](#)[2.2 Kaitset vajava teabe avaldamine ja väärkasutus \(elektrooniline ja füüsiline\)](#)[2.3 Identiteedi teesklus](#)[2.4 Turvateadlikkuse puudumine ja hooletus teabega tegelemisel](#)[2.5 Kohalike õigusaktide või eeskirjade rikkumine](#)[2.6 Sundimine, väljapressimine, inimrööv ja korruptsioon](#)[2.7 Teave lubamatust allikast / väljamõeldis](#)[2.8 Seadmete, andmekandjate ja dokumentide vargus või kaotamine](#)

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 märkamatuks 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, inimrööv 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

Sisukord

[3.1 Elutsükkel](#)

[3.2 Põhimeetmed](#)

[CON.7.M1 Välislähetuste infoturbe eeskiri](#)

[CON.7.M2 Töötajate teadlikkuse suurendamine](#)

[CON.7.M3 Riigispetsiifiliste õigusaktide, reisi- ja keskkonnatingimuste väljaselgitamine \[personaliosakond\]](#)

[CON.7.M4 Ekraanifiltri kasutamine \[kasutaja\]](#)

[CON.7.M5 Ekraaniluku kasutamine \[kasutaja\]](#)

[CON.7.M6 Õigeaegne intsidendist teatamine \[kasutaja\]](#)

[CON.7.M7 Turvaline kaugjuurdepääs \[IT-talitus, kasutaja\]](#)

[CON.7.M8 Avalike raadiokohtvõrkude turvaline kasutamine \[kasutaja\]](#)

[CON.7.M9 Andmekandjate turvaline käitlus \[kasutaja\]](#)

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

[CON.7.M12 Kaitset vajavate materjalide ja dokumentide turvaline hävitamine \[kasutaja\]](#)

[3.3 Standardmeetmed](#)

[CON.7.M11 Varguskaitsevahendid \[kasutaja\]](#)

[CON.7.M13 Andmete ja andmekandjate turvaline kaasavõtmine \[kasutaja\]](#)

[CON.7.M14 E-posti turve \[kasutaja, IT-talitus\]](#)

[3.4 Kõrgmeetmed](#)

[CON.7.M15 Mobiilsete IT-seadmete kiirguseturve \(C\)](#)

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

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

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

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 käsitusala;
- juhtkonna, infoturbejuhi ja reisiva töötaja vastutus;
- IT-süsteemi kaotuse, varguse või teabelekke käsitus;
- 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

<https://eits.ria.ee/et/versioon/2021/etalonturbe-kataloog/con-kontseptsioonid-ja-metoodikad/con7-vaelislahetuste-infoturbe/>

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

CON.7.M4 Ekraanifiltri kasutamine [kasutaja]

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 organisatsiooni 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 privaativõrku (ingl *virtual private network*, VPN) või sellega võrreldavaid turvamehhanisme (vt [NET.3.3 Virtuaalne privaativõrk \(VPN\)](#), 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 veendunud, 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;
 - mälu pulgal 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. Vältitakse 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).

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

CON. Kontseptsioonid ja metoodikad

CON.8: Tarkvaraarendus

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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

Sisukord

[2.1 Ebasobiv tarkvaraarendusmetoodika](#)

[2.2 Ebasobiva tarkvaraarenduskeskkonna valimine](#)

[2.3 Ebapiisav kvaliteedihaldus](#)

[2.4 Puuduv või puudulik dokumentatsioon](#)

[2.5 Ebapiisav arenduskeskkonna turve](#)

[2.6 Tarkvara kavandamise vead](#)

[2.7 Puudulikud tarkvara testimis- ja vastuvõtuprotseduurid](#)

[2.8 Tootmiskeskonna andmete kasutamine tarkvara testimisel](#)

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 värskest 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 töötamiseks 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 tarkvaratööde 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 Tootmiskeskonna andmete kasutamine tarkvara testimisel

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

Kui testimist tehakse otse tootmiskeskonnas, 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

Sisukord

[3.1 Elutsükel](#)

[3.2 Põhimeetmed](#)

[CON.8.M2 Sobiva tarkvaraarendusmetoodika valimine](#)

[CON.8.M3 Sobiva tarkvaraarenduskeskkonna valimine](#)

[CON.8.M5 Turvaline süsteemi kavandamine](#)

[CON.8.M6 Usaldusväärsetest allikatest pärinevate tarkvarateekide kasutamine](#)

[CON.8.M7 Tarkvara testimine tarkvaraarenduse käigus \[testija, arendaja\]](#)

[CON.8.M8 Tarkvaramuudatuste, paikade ja uuendite turvaline paigaldamine \[arendaja\]](#)

[CON.8.M10 Lähtekoodi versioonihaldus](#)

[CON.8.M20 Välise tarkvarakomponentide kontrollimine](#)

[3.3 Standardmeetmed](#)

[CON.8.M1 Tarkvaraarenduse rollide ja vastutuste määramine \[haldusosakond\]](#)

[CON.8.M11 Tarkvaraarenduste läbiviimise korra koostamine](#)

[CON.8.M12 Detailne tarkvara dokumentatsioon](#)

[CON.8.M14 Tarkvaraarendajate infoturbealane koolitus](#)

[CON.8.M16 Tarkvaraarenduse järelevalve](#)

[CON.8.M21 Tarkvara riskide kaalutlemine](#)

[CON.8.M22 Turvaline tarkvaarahitektuur](#)

3.4 Kõrgmeetmed

[CON.8.M17 Usalduväärsete arendusvahendite valimine \(C-I-A\)](#)

[CON.8.M18 Regulaarsed arenduskeskkonna turvaauditid \(C-I-A\)](#)

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

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 tarkvaarahitektuur

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 *production 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 viivitusega.
- 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 digitaalsete 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, nõuete haldus ja muudatuste haldus;
 - tarkvara kavandamine ja tarkvara arhitektuur;
 - tarkvaraarenduse infoturbe;
 - 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 ründemetoditele.
- 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“

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

CON. Kontseptsioonid ja metoodikad

CON.9: Teabevahetus

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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

Sisukord

[2.1 Teabe puudumine ettenähtud ajal](#)

[2.2 Teabe volitamata avalikustamine](#)

[2.3 Väära või sisemise teabe edastamine](#)

[2.4 Andmete lubamatu kopeerimine või muutmine](#)

2.5 Ebapiisavate krüptovahendite kasutamine

2.1 Teabe puudumine ettenähtud ajal

Teabe puudumine ettenähtud ajal võib oluliselt kahjustada äriprotsesse või põhjustada väärte 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. Andmeliidestest ja riistvara tõrked võivad põhjustada andmevahetuse täieliku katkemise.

2.2 Teabe volitamata avalikustamine

Teabevahetusel võivad andmed ja seeläbi ja konfidentsiaalne teave sattuda valedesse kättesse 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 märkamatuks 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 Meetmed

Sisukord

3.1 Elutsükel

3.2 Põhimeetmed

[CON.9.M1 Lubatavate teabevahetuspartnerite määramine \[haldusosakond, kasutaja\]](#)

[CON.9.M2 Teabevahetuse kord \[haldusosakond, kasutaja\]](#)

[CON.9.M3 Teabevahetuse koolitus töötajatele \[vastutav spetsialist\]](#)

3.3 Standardmeetmed

[CON.9.M4 Välise teabevahetuse lepped \[haldusosakond\]](#)

[CON.9.M5 Jäaketeabe kõrvaldamine failidest enne edasiandmist \[kasutaja\]](#)

[CON.9.M6 Saatja ja saaja IT-süsteemide ühilduvuse kontroll](#)

[CON.9.M7 Edasiantavate andmete varundamine \[kasutaja\]](#)

[CON.9.M8 Krüpteerimine ja digitaalsignatuurid \[kasutaja\]](#)

[3.4 Kõrgmeetmed](#)

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

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 Jäakteabe 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 konfidentsiaalselt 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;
- tegutsemise 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 turvaparametrid.

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.

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

CON. Kontseptsioonid ja metoodikad

CON.10: Veebirakenduste arendus

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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

Sisukord

[2.1 Puudulik autentimine ja kasutusõiguste andmine](#)

[2.2 Puudulik sisendite ja väljundite valideerimine](#)

[2.3 Veebirakenduse puuduv või puudulik tõrkehaldus](#)

[2.4 Puudulik turvasündmuste logimine](#)[2.5 Tundliku taustainfo avaldamine veebirakenduses](#)[2.6 Automaatsete ründe vahendite kasutamine](#)[2.7 Puudulik seansihaldus](#)

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 veebirakendusesse 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 tõrkehalvus

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 rünale 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 ründe vahendite 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 kasutajatele kättesaamatuks. Ründe vahendi 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

Sisukord

[3.1 Elutsükel](#)

[3.2 Põhimeetmed](#)

[CON.10.M1 Turvaline autentimine veebirakenduses](#)

[CON.10.M2 Veebirakenduse juurdepääsu reguleerimine](#)

[CON.10.M3 Turvaline seansihaldus](#)

[CON.10.M4 Veebirakenduse sisu kasutamise piiramine](#)

[CON.10.M5 Andmete üleslaadimise piiramine](#)

[CON.10.M6 Kaitse veebirakenduste volitamata automaatse kasutamise eest](#)

[CON.10.M7 Konfidentsiaalsete andmete kaitse](#)

[CON.10.M8 Sisendite valideerimine ja väljundite kodeerimine](#)

[CON.10.M9 Kaitse SQL-süsti eest](#)

[CON.10.M10 Tundliku taustainfo avaldamise piiramine](#)

[3.3 Standardmeetmed](#)

[CON.10.M11 Veebirakenduse turvaline tarkvaraarhitektuur](#)

[CON.10.M12 Oluliste muutuste kinnitamine](#)

[CON.10.M13 Veebirakenduse tõrketöötlus](#)

[CON.10.M14 Veebirakenduste turvaline HTTP-konfiguratsioon](#)

[CON.10.M15 Päringuvõltsingu takistamine](#)

[CON.10.M16 Mitmikautentimise kasutamine](#)

[3.4 Kõrgmeetmed](#)

[CON.10.M17 Ressursside blokeerimise takistamine \(A\)](#)

[CON.10.M18 Tundlike andmete krüptograafiline turve \(C-I\)](#)

3.1 Elutsükel

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 kavatsed ja korralisi veebilehepäringuid soovimatutest päringutest või volitusetä käskudest.

b. Kontrollitakse, kas kaitstud ressurssidele ja funktsioonidele juurde pääsemiseks on lisaks seansiidentifikaatorile vaja mingit lisanduvat volitustõendit.

c. Kasutaja kavatsed 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.

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

OPS. Käidutööd

OPS.1: Oma käidutööd

OPS.1.1: IT-põhitööd

OPS.1.1.2: IT-haldus

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

1.1 Eesmärk

Esitada meetmed IT-süsteemide ja võrkude turvaliseks halduseks.

1.2 Vastutus

IT-halduse meetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Personaliosakond.

1.3 Piirangud

Moodulis on esitatud IT-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](#).

Kolmandate poolte haldusülesannete täitmist käsitlevad moodulid [OPS.2.1 Väljasttellimine](#) ja [OPS.3.1 Teenuseandja infoturve](#). IT-haldust veaolukorras käsitletakse mooduligrupis *DER.2 Turvaintsidentide haldus*.

2 Ohud

Sisukord

[2.1 Kohustuste reguleerimatusest tingitud probleemid](#)

[2.2 Pädeva personali puudumine](#)

[2.3 Haldusõiguste kuritarvitus](#)

[2.4 Rünnete hõlbustamine](#)

[2.5 Töö häirimine](#)

[2.6 Intsidende analüüsi võimaluse puudumine](#)

2.1 Kohustuste reguleerimatusest tingitud probleemid

Kui IT-halduse ülesanded (nt kavandamise, installimise, dokumenteerimise, paigahalduse või järelevalve osas) pole selgelt määratud või kui IT-halduse kord ei ole töötajatele teada või arusaadav, võivad turbe jaoks olulised tegevused jääda ellu viimata.

2.2 Pädeva personali 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.

2.3 Haldusõiguste kuritarvitus

Dokumentidele ja andmebaasis asuvatele andmetele juurdepääsu omavad isikud võivad oma suuremaid õigusi enda või kõrvaliste isikute huvides ära kasutada. IT-haldurit võidakse andmetele juurdepääsu saamise nimel survestada või muul viisil mõjutada.

2.4 Rünnete hõlbustamine

Rünnet IT-süsteemile lihtsustavad IT-halduri poolt IT-süsteemi konfigureerimisel tehtud hooletusvead. Ka IT-süsteemi kaitseks mõeldud turvameetmeid alati ei rakendata (nt mugavuse või mõne muu põhjuse tõttu).

Vähene turvateadlikkus, haldurite ajanappus ja protseduuride puudumine loovad nõrkusi, mida ründaja saab kergelt ära kasutada.

2.5 Töö häirimine

Haldustoimingute läbiviimine mõjutab tavaliselt IT-süsteemide tööd. Kui IT-halduse toiminguid tehes ei arvestata nende mõju samaaegsele IT-süsteemide kasutamisele ja toiminguid ei ajastata töövälisele ajale, võidakse äriprotsessi olulisel määral häirida.

2.6 Intsidende analüüsi võimaluse puudumine

Turvaintsidenti korral on ründe toimumist ja selle ulatust keeruline kindlaks teha. Kui IT-intsidenti ei suudeta kiiresti tuvastada või süsteemis plaanitud muudatust lubamatust muudatusest eristada, võib ründaja võrgus segamatult tegutseda.

3 Meetmed

Sisukord

[3.1 Elutsükel](#)

3.2 Põhimeetmed[OPS.1.1.2.M2 Asendamise kord ja avariivalmendus](#)[OPS.1.1.2.M3 IT-halduri ettevalmistus tööks](#)[OPS.1.1.2.M4 IT-haldurina töötamise lõpetamine \[personaliosakond\]](#)[OPS.1.1.2.M5 Halduskonto tegevuste kontrollimine](#)[OPS.1.1.2.M6 Halduskontode turve](#)**3.3 Standardmeetmed**[OPS.1.1.2.M7 IT-halduri kohustuste määramine](#)[OPS.1.1.2.M8 Rakenduste haldus](#)[OPS.1.1.2.M9 Piisavate ressursside eraldamine IT-talitusele](#)[OPS.1.1.2.M10 Enesetäiendus ja turvateabe hankimine](#)[OPS.1.1.2.M11 Haldustegevuste dokumenteerimine](#)[OPS.1.1.2.M12 Hoolde- ja remonditööde kord](#)[OPS.1.1.2.M20 Seadmete korra kohane kasutuselevõtt](#)**3.4 Kõrgmeetmed**[OPS.1.1.2.M14 IT-haldurite taustakontroll \[personaliosakond\] \(C-I-A\)](#)[OPS.1.1.2.M15 Halduskohustuste jagamine \(C-I\)](#)[OPS.1.1.2.M16 Halduspääsu tehniline eraldamine \(C-I-A\)](#)[OPS.1.1.2.M17 IT-süsteemiülemate nelja silma põhimõte \(C-I\)](#)[OPS.1.1.2.M18 Haldustoimingute täielik logimine \(C-I\)](#)[OPS.1.1.2.M19 Kõrgkäideldavusnõuete arvestamine \(A\)](#)

3.1 Elutsükkel**Kavandamine**

OPS.1.1.2.M3 IT-halduri ettevalmistus tööks

OPS.1.1.2.M4 IT-haldurina töötamise lõpetamine

OPS.1.1.2.M7 IT-halduri kohustuste määramine

OPS.1.1.2.M12 Hoolde- ja remonditööde kord

Evitus

OPS.1.1.2.M5 Halduskontode kitsendused

OPS.1.1.2.M6 Halduskontode turve

OPS.1.1.2.M8 Rakenduste haldus

OPS.1.1.2.M9 Piisavate ressursside eraldamine

Käitus

OPS.1.1.2.M10 Enesetäiendus ja turvateabe hankimine

OPS.1.1.2.M11 Haldustegevuste dokumenteerimine

OPS.1.1.2.M20 Seadmete korra kohane kasutuselevõtt

Avariivalmendus

OPS.1.1.2.M2 Asendamise kord ja avariivalmendus

Lisanduvad kõrgmeetmed

OPS.1.1.2.M14 IT-haldurite taustakontroll

OPS.1.1.2.M15 Halduskohustuste jagamine

OPS.1.1.2.M16 Halduspääsu tehniline eraldamine

OPS.1.1.2.M17 IT-haldurite nelja silma põhimõte

OPS.1.1.2.M18 Haldustoimingute täielik logimine

OPS.1.1.2.M19 Kõrgkäideldavusnõuete arvestamine

3.2 Põhimeetmed**OPS.1.1.2.M2 Asendamise kord ja avariivalmendus**

a. IT-süsteemide halduritele on määratud asendajad, kellel on IT-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.M3 IT-halduri ettevalmistus tööks

a. IT-halduri ülesanded ja vastutus on dokumenteeritud ametijuhendis.

b. IT-haldurit on juhendatud hallatavate IT-süsteemide, rakenduste ja võrkude osas.

c. IT-haldurile on tutvustatud organisatsiooni poliitikaid, eeskirju ja töökorraldust.

d. IT-süsteemiülemale on selgitatud organisatsioonis kehtivaid turvanõudeid, samuti infoturbe halduse süsteemi ülesehitust ja protseduure.

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 Halduskonto tegevuste kontrollimine

a. Igal IT-süsteemiülemal ja igal IT-süsteemiülemas asendajal on personaalne eeliskonto (ingl *privileged account*), mida ta kasutab üksnes haldustoiminguteks.

b. Kõik halduskontoga tehtud tegevused ja pääsukatsed logitakse. Logitud andmete terviklust kaitstakse.

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 authentication*).

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 halduseks ei kasutata lokaalset konsooli, on halduskontode kasutamine kaitstud turvaliste võrguprotokollide (nt SSH, TLS) ja piisava tugevusega krüpteerimisega.

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 käitamis (nt versioonivahetusel), kooskõlastatakse see eelnevalt rakenduse kasutajatega, arvestades kasutajate vajadusi.

OPS.1.1.2.M9 Piisavate ressursside eraldamine IT-talitusele

a. Jooksvate haldusülesannete täitmiseks on olemas piisavalt personali ja muid ressursse.

b. On olemas piisavad reservid ettenägematute asjaoludega toimetulekuks, eelkõige turvaintsidentide käsitlemiseks ja lahendamiseks.

c. Ressursside piisavust kontrollitakse regulaarselt (vähemalt kord aastas) ja kohandatakse vastavalt vajadusele.

OPS.1.1.2.M10 Enesetäiendus ja turvateabe hankimine

a. IT-halduritele võimaldatakse infotehnoloogia arengule vastavaid täiendkoolitusi.

b. Koolitusplaanis arvestatakse, et vajalikud IT-halduse pädevused oleksid mitmel töötajal, et võimaldada töötajate asendamine.

c. IT-haldurid täiendavad ennast pidevalt hallatavate süsteemide, teenuste ja protokollide turvalisusega seotud teemadel (nt CERTi nõuanded, kasutajafoorumid, tootja uudiskirjad, meililistid jms).

OPS.1.1.2.M11 Haldustegevuste dokumenteerimine

a. Kõik IT-süsteemi haldusega seotud 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.M12 Hoolde- ja remonditööde kord

a. IT-süsteeme hooldatakse regulaarselt.

b. Kõikide hoolde- ja remonditööde kohta on olemas dokumentatsioon, millest nähtub, mis tegevused on tehtud ja millal.

c. Seadmete hoolduse ja remondi eest on vastutama määratud konkreetset isikud.

d. IT-seadmete hooldamisel täidetakse tootja nõudeid nii toimingute kui ka vajaliku hooldussageduse kohta.

e. Hoolde- ja remonditööde planeerimisel pööratakse tähelepanu turvaaspektidele. Mujale hooldusse või remonti andmisel eemaldatakse seadmetest tundlik teave.

f. Töötajaid teavitatakse hoolde- ja remonditöödest aegsasti.

g. Töötajad on teadlikud, et välise remonditööde läbiviija tegevust tuleb jälgida ja töö tulemust kontrollida.

OPS.1.1.2.M20 Seadmete korrahakohane kasutuselevõtt

a. Organisatsioonis on ülevaade kõigist seadmetest, mis võivad infoturbe olukorda mõjutada. Seadmete register vastab tegelikule olukorrale.

b. Lisaks IT-süsteemide ja tööstusautomaatika komponentidele on registrisse kantud ka esemevõrgu (ingl *Internet of Things*, IoT) seadmed.

c. Seadmete hankimisel arvestatakse nende ühilduvust ja turvalisust. Võimalusel testitakse uusi seadmeid enne nende soetamist.

d. Enne kasutuselevõttu läbivad seadmed kooskõlastusprotseduuri, mille käigus seadmed märgistatakse ja registreeritakse (nt varade registris).

3.4 Kõrgmeetmed

OPS.1.1.2.M14 IT-haldurite taustakontroll [personaliosakond] (C-I-A)

a. IT-haldurite usaldusväarsuse tagamiseks viiakse läbi tavatöötajaga võrreldes laiendatud taustakontroll, kui selle teostamiseks eksisteerib seaduslik alus.

b. Töötaja esitatud akadeemilise ja erialase kvalifikatsiooni tõesust kontrollitakse päringutega ülikoolile ja varasematele tööandjatele.

OPS.1.1.2.M15 Halduskohustuste jagamine (C-I)

a. IT-haldurite liigse volitatus riski leevendatakse haldusülesannete jagamisega mitme halduri vahel nii, et üks isik ei saaks kontrollimatult tegutseda.

- b. Haldusrollid on loodud andmete liiki ja süsteemiarhitektuuri arvestades ega kattu.
- c. Automaatseid, piiramisvõimaluseta halduskontosid (juurkasutaja, peakasutaja) kasutatakse võimalikult vähe, nendele kontodele juurdepääsuks kasutatakse mitmikautentimist (ingl *multifactor authentication*).

OPS.1.1.2.M16 Halduspääsu tehniline eraldamine (C-I-A)

- a. Haldusliidestele juurdepääs on eraldatud tehniliste meetmetega (nt lubatud ühest konkreetsest võrgusegmentist).
- 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.M17 IT-süsteemiülemate nelja silma põhimõte (C-I)

- a. Juurdepääs turvakriitilistele süsteemidele on reguleeritud nii, et selleks on alati vaja kahte töötajat (nt süsteemiülemade parooli jaotamisega kaheks osaks, millest kumbki pool on teada ainult ühele süsteemiülemalest).
- b. Haldusprotseduuride läbiviimisel täidab üks süsteemiülem ettenähtud haldusülesandeid ja teine kontrollib tema tegevust.

OPS.1.1.2.M18 Haldustoimingute täielik logimine (C-I)

- a. Turvakriitilistes süsteemides logitakse lisaks süsteemi sisselogimistele ka kõik süsteemiülemade 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 Kõrgkäideldavusnõuete arvestamine (A)

- a. Kõrgkäideldavusnõuete täitmiseks on välja töötatud sobivad kontseptsioonid ja meetmed.
- b. Kasutusele võetud IT-komponendid, IT-arhitektuur ning tööprotsessid toetavad kõrgkäideldavusnõuete täitmist.
- c. Kõrgkäideldavusnõuetele vastavust kontrollitakse testimiste (nt koormustestimine), auditite ja läbivaatuste käigus.

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

OPS. Käidutööd

OPS.1: Oma käidutööd

OPS.1.1: IT-põhitööd

OPS.1.1.3: Paiga- ja muudatusehaldus

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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 üldiselt. 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](#).

2 Ohud

Sisukord

[2.1 Puudulikult kehtestatud kohustused](#)

[2.2 Puudulik teabevahetus muudatuste haldamisel](#)

[2.3 Äriprotsessidega mitteamvestamine](#)

[2.4 Piiratud ressursid paiga- ja muudatusehalduses](#)

[2.5 Probleemid paikade ja muudatuste automaatse paigaldamisega](#)

[2.6 Puudulikud taastevõimalused paiga- ja muudatusehalduses](#)

[2.7 Paikade ja muudatuste prioriteetsuse väär hindamine](#)

[2.8 Andmete ja tööriistade manipuleerimine muudatuste haldamisel](#)

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 mitteamvestamine

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 äri vajadustele.

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

Paigaldustarkvara 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

Sisukord

[3.1 Elutsükkel](#)

[3.2 Põhimeetmed](#)

[OPS.1.1.3.M1 Paiga- ja muudatusehalduse kord \[vastutav spetsialist\]](#)

[OPS.1.1.3.M2 Vastutuse määramine](#)

[OPS.1.1.3.M3 Automaatuuenduste turvaline seadistus](#)

[OPS.1.1.3.M15 IT-süsteemide regulaarne uuendamine](#)

[OPS.1.1.3.M16 Turvanõrkuste ja turvauuendite teabe seire](#)

[3.3 Standardmeetmed](#)

[OPS.1.1.3.M5 Muutmistaotluste käsitlemine \[vastutav spetsialist\]](#)

[OPS.1.1.3.M6 Muudatuste kooskõlastamine](#)

[OPS.1.1.3.M7 Muudatusehalduse sobitamine äriprotsessidega](#)

[OPS.1.1.3.M8 Paiga- ja muudatusehalduse tööriistade turvaline rakendamine](#)

[OPS.1.1.3.M9 Uue riistvara testimise ja kasutuselevõtu protseduurid](#)

[OPS.1.1.3.M10 Tarkvaratoodete tervikluse ja autentsuse tagamine](#)

[OPS.1.1.3.M11 Infotöötluse pidev dokumenteerimine](#)

[3.4 Kõrgmeetmed](#)

[OPS.1.1.3.M12 Muudatusehalduse tööriistade kasutamine \(A\)](#)

[OPS.1.1.3.M13 Muudatuste tulemuslikkuse hindamine \[vastutav spetsialist\] \(I-A\)](#)

[OPS.1.1.3.M14 Muudatuste sünkroniseerimine \(C-I-A\)](#)

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 käsitlemine

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

OPS.1.1.3.M16 Turvanõrkuste ja turvauuendite teabe seire

Lisanduvad kõrgmeetmed

OPS.1.1.3.M12 Muudatusehalduse tööriistade kasutamine

OPS.1.1.3.M13 Muudatuste tulemuslikkuse hindamine

OPS.1.1.3.M14 Muudatuste sünkroniseerimine

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 paigaldamise nõuetele.

b. Vajadusel tõkestatakse uuendite päringud avalikust uuendusserverist ja blokeeritakse uuendite installimise automaatne käivitus.

c. Võimalusel võetakse kasutusele organisatsioonisene 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.

OPS.1.1.3.M16 Turvanõrkuste ja turvauuendite teabe seire

a. IT-haldurid jälgivad regulaarselt infot kasutatava tarkvara ja riistvara teadaolevate nõrkuste ning põhi- ja tarkvaravara uuendite väljalaske kohta.

b. Teadaolevad riistvara, operatsioonisüsteemide ja rakenduste nõrkused parandatakse esimesel võimalusel. Kui nõrkuse parandamiseks ei ole tootja väljastanud turvapaika, kasutatakse IT-süsteemi kaitseks täiendavaid turvameetmeid.

c. Ilma tootjapoolse toeta ja teadaolevate turvanõrkustega riistvara, operatsioonisüsteemid, rakendused ja teenused eemaldatakse kasutusest.

3.3 Standardmeetmed

OPS.1.1.3.M5 Muutmistaotluste käsitlemine [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 infoturbe.

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 Infotöötamise 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.

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetusskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

OPS. Käidutööd

OPS.1: Oma käidutööd

OPS.1.1: IT-põhitööd

OPS.1.1.4: Kaitse kahjurprogrammide eest

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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 käsitlemine](#) ja [DER.2.3 Ulatuslike turvaintsidentide lahendamine](#).

Kasutajate koolitust käsitletakse moodulis [ORP.3 Infoturbe teadlikkuse tõstmine ja koolitus](#).

2 Ohud

Sisukord

[2.1 Tarkvara nõrkused ja kahjurkoodi allalaadimine](#)[2.2 Väljapressimine lunavaraga](#)[2.3 Siht- ja suhtlusründed](#)[2.4 Bottnetid](#)[2.5 Tootmissüsteemide ja esemevõrgu seadmete nakatamine](#)

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

Sisukord

[3.1 Elutsükkel](#)

[Kavandamine](#)[Soetamine](#)[Evitus](#)[Käitus](#)[Lisanduvad kõrgmeetmed](#)

3.2 Põhimeetmed

[OPS.1.1.4.M1 Kahjurprogrammide tõrje kontseptsioon](#)[OPS.1.1.4.M2 Süsteemikohaste turvamehhanismide kasutamine](#)[OPS.1.1.4.M3 Kahjurvaratõrje tarkvara valimine lõppseadmetele](#)[OPS.1.1.4.M5 Kahjurvaratõrje tarkvara rakendamine](#)[OPS.1.1.4.M6 Viirusetõrjeprogrammide ja viiruse käe kirja andmestike ajakohastamine](#)[OPS.1.1.4.M7 Kasutajate teadlikkuse suurendamine \[kasutaja\]](#)

3.3 Standardmeetmed

[OPS.1.1.4.M9 Kahjurprogrammiga nakatumisest teatamine](#)

3.4 Kõrgmeetmed

[OPS.1.1.4.M10 Spetsiaalse analüüsikeskkonna kasutamine \(C-I-A\)](#)[OPS.1.1.4.M11 Mitme skaneerimismootori rakendamine \(C-I-A\)](#)[OPS.1.1.4.M12 Andmekandjalüüside rakendamine \(C-I-A\)](#)[OPS.1.1.4.M13 Ebausaldusväärsete failide käitlus \(C-I-A\)](#)[OPS.1.1.4.M14 Infoturbe toodete valimine ja kasutuselevõtt sihtrünnete tõrjeks \(C-I-A\)](#)

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 käe kirja 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 kasutuskeskonnale.
- 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 soovitudele.
- 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 poolt 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 käsitlemiseks.

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 töötamiseks 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.

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetusskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

OPS. Käidutööd

OPS.1: Oma käidutööd

OPS.1.1: IT-põhitööd

OPS.1.1.5: Logimine

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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 moodulis [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

Sisukord

[2.1 Puuduv või piisamatu logimine](#)

[2.2 Asjassepuutuvate logiandmete puudulik valimine](#)

[2.3 Sünkroniseerimata aeg logimisel](#)

[2.4 Logimise halb plaanimine](#)

[2.5 Logiandmete konfidentsiaalsuse ja tervikluse kadu](#)

[2.6 Valesti konfigureeritud logimine](#)

[2.7 Andmeallikate tõrge](#)

[2.8 Liiga väike logitaristu](#)

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 reaajas 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 kasutajanimedid, 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

Sisukord

[3.1 Elutsükkel](#)

[3.2 Põhimeetmed](#)

[OPS.1.1.5.M1 Logimise eeskiri \[vastutav spetsialist\]](#)

[OPS.1.1.5.M3 Sündmuste logimise konfigureerimine](#)

[OPS.1.1.5.M4 Aja sünkroniseerimine](#)

[OPS.1.1.5.M5 Õiguslike raamtingimuste täitmine \[infoturbejuht\]](#)

[3.3 Standardmeetmed](#)

[OPS.1.1.5.M6 Keskse logitaristu rajamine](#)

[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](#)

[3.4 Kõrgmeetmed](#)

[OPS.1.1.5.M11 Logimisjõudluse suurendamine \(C-I-A\)](#)

[OPS.1.1.5.M12 Logiandmete krüpteerimine \(C-I\)](#)

[OPS.1.1.5.M13 Kõrgkäideldav logimissüsteem \[infoturbejuht\] \(A\)](#)

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

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 soovitudele.

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 võrgusegmentidele 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 logimisarendus 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 andmetötluse 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.

4 Lisateave

Lühend	Publikatsioon
--------	---------------

[NIST]	NIST, Special Publication 800-92 „Guide to Computer Security Log Management“
--------	--

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetusskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

OPS. Käidutööd

OPS.1: Oma käidutööd

OPS.1.1: IT-põhitööd

OPS.1.1.6: Tarkvara testimine ja kasutuselevõtt

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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, andmekaitespetsialist, 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

Sisukord

[2.1 Tarkvara testimine tööandmetega](#)

[2.2 Puuduv või piisamatu testimisprotseduur](#)

[2.3 Puuduv või piisamatu kinnitusprotseduur](#)

[2.4 Testide ja testimistulemuste puudulik dokumenteerimine](#)

[2.5 Kinnituskriteeriumide puudulik dokumenteerimine](#)

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 ilmnedas alles käidukeskkonnas ning põhjustada tarkvaraprojekti valmimisega hilinemise ja rahalise kahju.

3 Meetmed

Sisukord

[3.1 Elutsükel](#)

[3.2 Põhimeetmed](#)

[OPS.1.1.6.M1 Tarkvara testimise kavandamine](#)

[OPS.1.1.6.M2 Tarkvara funktsionaaltestimine \[testija\]](#)

[OPS.1.1.6.M3 Testimistulemuste analüüsimine \[testija\]](#)

[OPS.1.1.6.M4 Tarkvara kinnitamine \[vastutav spetsialist\]](#)

[OPS.1.1.6.M5 Mittefunktsionaalsete testide tegemine \[testija\]](#)

[OPS.1.1.6.M11 Testandmete anonüümimine või pseudonüümimine \[andmekaitespetsialist, testija\]](#)

[3.3 Standardmeetmed](#)

[OPS.1.1.6.M6 Tarkvara testija juhendamine \[vastutav spetsialist\]](#)

[OPS.1.1.6.M7 Personali valimine tarkvara testijaks \[vastutav spetsialist, personaliosakond\]](#)

[OPS.1.1.6.M10 Testimise vastuvõtu kord](#)

[OPS.1.1.6.M12 Regressioontestimine \[testija\]](#)

[OPS.1.1.6.M13 Testkeskkonna lahutamine käidukeskkonnast](#)

[OPS.1.1.6.M15 Paigaldamise ja seadistamise juhendi järgimine \[testija\]](#)

3.4 Kõrgmeetmed

[OPS.1.1.6.M14 Läbistustestide sooritamine \[testija\] \(C-I-A\)](#)

[OPS.1.1.6.M16 Testija taustakontroll \[testija\] \(C\)](#)

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 testimiskeskonnast 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 [andmekaitse spetsialist, 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 personalijuhiga ja andmekaitse spetsialistiga.

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 ülevaatus 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 [testija] (C)

<https://eits.ria.ee/et/versioon/2021/etalonturbe-kataloog/ops-kaeidutoeod/ops1-oma-kaeidutoeod/ops11-itpoohitoeod/ops116-tarkvara-testimine-ja-kasutuselevootu/>

- 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.

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

OPS. Käidutööd

OPS.1: Oma käidutööd

OPS.1.2.2: Arhiveerimine

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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

Sisukord

- [2.1 Andmekandjate sobimatus pikaajaliseks säilitamiseks](#)
 - [2.2 Arhiivisüsteemi puudulikud liigituskriteeriumid](#)
 - [2.3 Arhiivipääsude puudulik dokumenteerimine](#)
 - [2.4 Paberandmete puudulik ülekandmine elektroonilisse arhiivi](#)
 - [2.5 Krüpteerimisprotseduuride puudulik uuendamine arhiveerimisel](#)
 - [2.6 Puudulik järelevalve arhiveerimise üle](#)
 - [2.7 Õiguslike raamtingimuste rikkumine arhiveerimisel](#)
-

2.1 Andmekandjate sobimatus pikaajaliseks säilitamiseks

Aja möödudes võivad andmekandjad füüsiliselt ja tehnoloogiliselt vananeda ning seetõttu kasutuskõlbatuteks 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 märkamatuks 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

Sisukord

3.1 Elutsükkel**3.2 Põhimeetmed**

[OPS.1.2.2.M1 Elektroonilise arhiveerimise mõjurite väljaselgitamine](#)

[OPS.1.2.2.M2 Arhiveerimiskontseptsiooni väljatöötamine](#)

[OPS.1.2.2.M3 Arhiivisüsteemi ja arhiivimeediumite hoiu sobiv korraldus \[IT-talitus\]](#)

[OPS.1.2.2.M4 Andmete ühtne indekseerimine arhiveerimisel \[IT-talitus, kasutaja\]](#)

[OPS.1.2.2.M5 Arhiveeritavate andmetike asjakohane valmendus \[IT-talitus\]](#)

[OPS.1.2.2.M6 Arhiivisüsteemi indeksiandmebaasi tervikluse kaitse \[IT-talitus\]](#)

[OPS.1.2.2.M7 Süsteemi- ja arhiivandmete regulaarne varundamine \[IT-talitus\]](#)

[OPS.1.2.2.M8 Arhiivipöörduste logimine \[IT-talitus\]](#)

[OPS.1.2.2.M9 Arhiveerimiseks sobiva andmevormingu valimine \[IT-talitus\]](#)

3.3 Standardmeetmed

[OPS.1.2.2.M10 Arhiivisüsteemi kasutamise eeskiri \[IT-talitus\]](#)

[OPS.1.2.2.M11 Arhiivisüsteemi haldajate koolitus \[IT-talitus\]](#)

[OPS.1.2.2.M12 Arhiivimeediumi salvestusressursside seire \[IT-talitus\]](#)

[OPS.1.2.2.M13 Arhiveerimisprotsessi regulaarne läbivaatus](#)

[OPS.1.2.2.M14 Arhiivisüsteemide turu regulaarne jälgimine \[IT-talitus\]](#)

[OPS.1.2.2.M15 Krüptomehhanismide ajakohastus arhiveerimisel \[IT-talitus\]](#)

[OPS.1.2.2.M16 Arhiivisüsteemi tehniliste komponentide uuendamine \[IT-talitus\]](#)

[OPS.1.2.2.M17 Sobiva arhiivisüsteemi valimine \[IT-talitus\]](#)

[OPS.1.2.2.M18 Sobivad arhiivimeediumid \[IT-talitus\]](#)

[OPS.1.2.2.M19 Arhiveerimise ja taaste regulaarne kontroll \[IT-talitus\]](#)

3.4 Kõrgmeetmed

[OPS.1.2.2.M20 Krüptoprotseduuride dubleerimine \[IT-talitus\] \(C-I\)](#)

[OPS.1.2.2.M21 Dokumentide turvaline üleviimine elektroonilisse arhiivi \(C-I\)](#)

3.1 Elutsükkel**Kavandamine**

OPS.1.2.2.M1 Elektroonilise arhiveerimise mõjurite väljaselgitamine

OPS.1.2.2.M2 Arhiveerimise kontseptsiooni väljatöötamine

Soetamine

OPS.1.2.2.M18 Sobivad arhiivimeediumid

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

Käitus

OPS.1.2.2.M4 Andmete ühtne indekseerimine arhiveerimisel

OPS.1.2.2.M5 Arhiveeritavate andmetike 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 arhiivandmete 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 organisatsiooni juhtkonna poolt kinnitatud.

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 suuruselt 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 indekseerimise 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 indeksandmebaasi tervikluse kaitse [IT-talitus]

a. Indeksandmebaasi terviklust kontrollitakse regulaarselt. Tervikluse kahjustumine kõrvaldatakse viivitamata, sellekohased andmed dokumenteeritakse.

b. Indeksandmebaasi varundatakse regulaarselt, varunduse taastatavust kontrollitakse pärast igat varundust.

c. Suurte arhiivibaaside puhul indeksandmebaasid dubleeritakse.

OPS.1.2.2.M7 Süsteemi- ja arhiivandmete regulaarne varundamine [IT-talitus]

a. Kõiki arhiivandmeid, indeksandmebaase 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 algatakse 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 salvestusmaht 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 arhiivandmed 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 ilmnunud tõrgete käsitlemiseks 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

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

OPS. Käidutööd

OPS.1: Oma käidutööd

OPS.1.2.4: Kaugtöö

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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

Sisukord

[2.1 Kaugtöökoha eeskirja puudumine või puudulikkus](#)

[2.2 Teenistusliku kaugtööarvuti lubamatu privaatsus](#)

[2.3 Viivitused kaugtöötaja kättesaamatuse tõttu](#)[2.4 Teabe mittejäudmine töötajani](#)[2.7 Turvameetmete eiramine](#)

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 kätte.

2.2 Teenistusliku kaugtöövutit lubamatu privaatkasutus

Töötaja 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 osutada vajalikul hetkel kättesaamatuks. See võib tuua kaasa viivitusi tööprotsessis. Sõltuvalt organisatsioonist võib see oluliselt mõjutada tervet äriprotsessi.

2.4 Teabe mittejäudmine 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

Sisukord

[3.1 Elutsükkel](#)[3.2 Põhimeetmed](#)[OPS.1.2.4.M1 Kaugtöö eeskiri \[ülemus, personaliosakond\]](#)[OPS.1.2.4.M2 Kaugtöövutit turve](#)[OPS.1.2.4.M5 Kaugtöötajate teadlikkuse tõstmine ja koolitus](#)[3.3 Standardmeetmed](#)[OPS.1.2.4.M6 Kaugtöö turbekontseptsioon](#)[OPS.1.2.4.M7 Sidevahendite kasutamise kord \[IT-talitus, töötaja\]](#)[OPS.1.2.4.M8 Regulaarne teabevahetus organisatsiooniga \[ülemus, töötaja\]](#)[OPS.1.2.4.M9 Kaugtöökoha kasutajatugi ja hooldus \[IT-talitus, töötaja\]](#)[OPS.1.2.4.M10 Kaugtöökoha nõuete analüüs \[IT-talitus\]](#)[3.4 Kõrgmeetmed](#)

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 Kaugtöövutit 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]

a. Töötajatele järgimiseks on koostatud ja tehtud töötajatele kättesaadavaks kaugtöö korraldust reguleeriv eeskiri.

b. Kaugtöö eeskirjas on arvestatud järgmisi turvaaspekte:

- konfidentsiaalse teabe käitlus;
- andmekaitseõud;
- andmevarundus ja andmete sünkroniseerimine;
- andmeside kasutamine;
- kaugpääsuõigused;
- dokumentide ja andmekandjate transport ja säilitamine;
- turvasündmustest teatamise kord.

c. On koostatud töökaitse õiguslikke aspekte arvestavad, tööandja ja töötaja vahelised kaugtöö kokkulepped, milles on määratletud vähemalt järgmine:

- kaugtöö vabatahtlikkus;
- töövahendid;
- tööaeg ja kättesaadavus;
- reageerimisajad, näiteks e-kirjade lugemise sagedus;
- ületunnitöö, lisatasud ja täiendavate kulude tasumine;
- materiaalne vastutus;
- kaugtöö lõpetamine.

d. Kaugtöö eeskirja vaadatakse üle ja seda ajakohastatakse regulaarselt.

OPS.1.2.4.M2 Kaugtöövutit turve

a. Kaugtöövutit kasutatakse ainult määratud otstarbeks (nt ei tohi kasutaja installida kaugtöövutisse heakskiitmata tarkvara).

b. Kaugtöövõrki kasutatakse ainult selleks volitatud isik. Volitatud isikuteks on kaugtöötaja ja kaugtöövõrkide haldur.

c. Kaugtöövõrki 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

a. Kaugtöötajad on läbinud kaugtöö turvameetmete alase koolituse.

b. Kaugtöötaja koolitusel on käsitletud järgmisi aspekte:

- kaugtöö ohud;
- tööalaste dokumentide turvaline hoidmine;
- kaugtöökoha füüsiline turve;
- võrguturve;
- andmekandjate turvaline kasutamine;
- lihtsamad hooldetööd ja probleemilahendused.

c. Kaugtöötajate koolitamisel järgitakse meetmeid moodulist [ORP.3 Infoturbe teadlikkuse tõstmine ja koolitus](#).

d. 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:

- teabevahetuseks kasutatavad sidevõimalused (sh sõnumiside, telefon, e-post);
- andmete edastamiseks kasutatavad teenused;
- videokonverentsiteenuste kasutamine;
- teabevahetuse turvameetmed;
- digiallkirjastamise kasutamine;
- 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. Töölased 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 hoolduseks.

OPS.1.2.4.M10 Kaugtöökoha nõuete analüüs [IT-talitus]

a. 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;
- nõuded dokumentide ja andmekandjate transportimisele;
- kaugtöökoha riist- ja tarkvarakomponentide vajadus ja valik (kooskõlastatakse IT-haldusega).

b. Konkreetse kaugtöökoha nõuded dokumenteeritakse ja kooskõlastatakse IT-juhiga.

3.4 Kõrgmeetmed

Antud moodulis kõrgmeetmed puuduvad

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

OPS. Käidutööd

OPS.1: Oma käidutööd

OPS.1.2.5 Kaughooldus

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

1.1 Eesmärk

Esitada meetmed aktiivse ja passiivse kaughoolduse käigus salvestatava, töödeldava ja edastatava teabe 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](#).

2 Ohud

Sisukord

[2.1 Kaughoolduse eeskirjade puudulik järgimine](#)

[2.2 Kaughoolduse kavandamise ja reguleerimise puudumine või puudulikkus](#)

[2.3 Väär autentimine kaughoolduses](#)

[2.4 Tegemata või väär kaughooldus](#)

[2.5 Ebaturvaliste protokollide kasutamine kaughoolduses](#)

[2.6 Kaughooldusfunktsioonide kontrollimatu kasutamine](#)

[2.7 Võrgustatud kaughooldusteenuse lubamatu kasutamine](#)

[2.8 Integreeritud kaughoolduskomponentide lubamatu kasutamine](#)

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 tähelepanematusel või mugavusest tingitud eksimus kaasa tuua olulise kahju. Turvameetmete eiramine kaughoolduse käigus on raskesti tuvastatav ning sellest tingitud turvanõrkuste ära kasutamisel 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, paigalduse 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 väärtalt, 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

Sisukord

[3.1 Elutsükkel](#)

[3.2 Põhimeetmed](#)

[OPS.1.2.5.M1 Kaughoolduse rakendamise kava](#)

[OPS.1.2.5.M2 Turvaline ühenduse loomine kaughooldusel \[kasutaja\]](#)

[OPS.1.2.5.M3 Sideühenduste turve kaughooldusel](#)

[3.3 Standardmeetmed](#)

[OPS.1.2.5.M5 Võrgustatud hooldusteenuste turvaline rakendamine \[kasutaja\]](#)

[OPS.1.2.5.M6 Kaughoolduse eeskiri](#)

[OPS.1.2.5.M7 Kaughoolduse dokumentatsioon](#)

[OPS.1.2.5.M8 Turvalised kaughoolduse protokollid](#)

[OPS.1.2.5.M9 Sobivate kaughooldustööriistade valimine](#)

[OPS.1.2.5.M10 Kaughooldustööriistade haldus \[kasutaja\]](#)

[OPS.1.2.5.M17 Kaughoolduse autentimismehhanismid](#)

[OPS.1.2.5.M19 Kaughooldus välisteenusena](#)

[OPS.1.2.5.M20 Kaughoolduse turvaline läbiviimine](#)

[OPS.1.2.5.M21 Avariiplaan kaughoolduse tõrke puhuks](#)

[OPS.1.2.5.M24 Integreeritud kaughooldusfunktsioonide turve](#)

[OPS.1.2.5.M25 Väljaspoolt haldusvõrku tehtava kaughoolduse piiramine](#)

[3.4 Kõrgmeetmed](#)

[OPS.1.2.5.M14 Kaughoolduskliendi turvaline seadistus \(C\)](#)

[OPS.1.2.5.M22 Kaughoolduse sidevõrkude liiasus \(A\)](#)

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 haldus

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 Kaughoolduskliendi 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 andmekaitsevenõuetel 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 haldus [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. Kaughooldusessiooni 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 algatakse 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.2.1 Väljastellimine](#) 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.
- . 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 Avariiahaldus](#).

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.

OPS.1.2.5.M22 Kaughoolduse sidevõrkude liiasus (A)

a. Kaughoolduse tegemiseks avariiolukorras on võimalik IT-süsteemile juurdepääsuks kasutada varusideühendust (nt. 4G mobiilsidevõrku).

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetusskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

OPS. Käidutööd

OPS.2: Käidutööd teenusena

OPS.2.1: Väljasttellimine

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

1.1 Eesmärk

Esitada meetmed organisatsiooni turvaeesmärkide saavutamiseks, turvalisuse hoidmiseks ja parendamiseks pärast IT protsesside või teenuste väljasttellimist teenuseandjalt.

1.2 Vastutus

Väljasttellimise meetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Hankeosakond, vastutav spetsialist, avariitölem, personaliosakond, haldusosakond.

1.3 Piirangud

Moodul ei käsitle teenuseandjaga suhtlemiseks kasutatavate 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

Sisukord

- [2.1 Infoturbe eeskirjade puudumine või puudulikkus](#)
 - [2.2 Pääsuõiguste halduse puudulikkus](#)
 - [2.3 Testimis- ja kinnitusprotseduuride puudumine või puudulikkus](#)
 - [2.4 Teenuse tarnelepingu puudulikkus](#)
 - [2.5 Väljasttellimise lõpetamise reguleerimise puudulikkus](#)
 - [2.6 Sõltuvus teenuseandjast](#)
 - [2.7 Tööõhkkonna halvenemine väljasttellimise kavandamisel](#)
 - [2.8 Puudulik infoturbe väljasttellimiskava evitusjärgus](#)
 - [2.9 Teenuseandja süsteemi tõrge](#)
 - [2.10 Väljasttellitava teenusega liidestuse nõrkused](#)
 - [2.11 Simultaantöö võime puudumine teenuseandjal](#)
-

2.1 Infoturbe eeskirjade puudumine või puudulikkus

Kui eeskirjades on töötaja vastutus, kohustused ning kontroll nende täitmise üle üheselt määratlemata, võivad olulised turvalisust tõstvad tegevused jääda tegemata. Kui teenuseandja jätab pärast tehnilisi või korralduslikke teenusemuudatusi juhendi ajakohastamata, võib hiljem tekkida probleeme teenuse migreerimisega. Kui eeskirjad ei ole üheselt mõistetavad, võidakse need jätta täitmata.

2.2 Pääsuõiguste halduse puudulikkus

Kui pääsuõiguste andmine, haldamine ja kontrollimine on teenuseandja poolelt halvasti korraldatud, võivad ohtu sattuda välisteenus klientide andmed. Teenuseandja töötajatele kontrollimatu haldusõiguste andmine soodustab pääsuõiguste ära kasutamist teabe kopeerimise või manipuleerimise eesmärgil.

2.3 Testimis- ja kinnitusprotseduuride puudumine või puudulikkus

Kui teenuse klient ei ole teenuseandjale kehtestanud tarkvara testimise ja kasutuseks kinnitamise nõudeid, võivad tarkvaravead või konfiguratsiooni nõrkused jääda märkamata. Alles kasutamisel võib selguda, et uued komponendid või paigaldatud uuendid muudavad olulisel määral tarkvara toimimist või et sobiva jõudluse saavutamiseks on vaja rohkem ressursse. Klientide õigeaegselt teavitamata jätmine võib kaasa tuua mõlemale poolele täiendavaid kulusid.

2.4 Teenuse tarnelepingu puudulikkus

Teenuseandjaga sõlmitud tarneleping ei pruugi sisaldada kõiki teenuseandja kohustusi ja kõiki rakendamisele kuuluvaid turvameetmeid. Näiteks, kui tarneleping seda ei reguleeri, ei pruugi teenuseandja kinni pidada kliendi teavitamiskohustusest. Rakendamata turvameetmed võivad kaasa tuua ka õigusaktide nõuete eiramise.

2.5 Väljasttellimise lõpetamise reguleerimise puudulikkus

Kui välisteenus tarnelepingu lõpetamise korras 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 tarnija kasuks. Samuti võivad teenuse lõpetamisega kaasneda erinevad turvaprobleemid. Puudulik andmete (sh varundatud andmete) kustutamise kord võib põhjustada konfidentsiaalsete andmete lekke.

2.6 Sõltuvus teenuseandjast

Otsus kasutada väljasttellimist võib viia organisatsiooni teenuseandjast täielikku sõltuvusse, põhjustades oskusteabe kaotust ja äriprotsessi üle kontrolli kadumist. Klient ei pruugi puudujääke teenuseandja infoturbes ise märgata. Teenuseandja võib tekkinud olukorda oma huvides ära kasutada (nt tõsta märkimisväärselt teenuse hinda).

2.7 Tööõhkkonna halvenemine väljasttellimise kavandamisel

Kliendi organisatsiooni töötajad peavad väljasttellimist tihti negatiivseks muudatuseks, mis põhjustab tööõhkkonna halvenemist. Negatiivse suhtumise korral väljasttellimisse võivad töötajad tahtmata või tahtlikult jätta turvameetmed rakendamata või isegi neile põhjustatud ebamugavuste eest kätte maksta. Väljasttellimisele üleminek võib põhjustada oskusteabega töötajate lahkumise juba väljasttellimise kavandamisjärgus, mistõttu projekti ei õnnestugi edukalt ellu viia.

2.8 Puudulik infoturbe väljasttellimiskava evitusjärgus

Välisteenuale üleminek on piiratud sageli rangete tähtaegade ja rahastusnõuetega. Seetõttu võidakse evitusjärgus keskenduda ainult funktsionaalsetele nõuetele. Turvakontrollid, auditid, läbivaatused ja muud kvaliteeditagamise meetmed jäetakse aja ja raha kokkuhoiu eesmärgil ära. Näiteks võimaldatakse arendajal töötada reaalse isikuandmetega, sest isikuandmete anonüümimiseks ei jätku aega.

2.9 Teenuseandja süsteemi tõrge

Kui teenuseandja IT-süsteemides on rike, siis on sellest mõjutatud ka välisteenu kliendid. Raskemal juhul tähendab see seda, et väljasttellitava teenuse kliendid ei saa teenust kasutada. Sarnased probleemid tekivad ka liidestuse tõrgete korral.

2.10 Väljasttellitava teenusega liidestuse nõrkused

Kui väljasttellitava teenuse kliendi ja tarnija vaheline IT-liidestus ei ole piisavalt turvatud, eksisteerib oht edastatavate andmete konfidentsiaalsusele ja terviklusele.

2.11 Simultaantöö võime puudumine teenuseandjal

Kui erinevate klientide IT-süsteemid ja andmed ei ole üksteisest piisavalt turvaliselt lahutatud, võib klient pääseda juurde teise kliendi andmetikele, sealhulgas konfidentsiaalsetele andmetele. Kui samaaegselt tuleb täita mitme kliendi ressursimahukaid päringuid, võib teenuseandja IT-süsteemis tekkida ressursikonflikt.

3 Meetmed

Sisukord

[3.1 Elutsükel](#)

[3.2 Põhimeetmed](#)

[OPS.2.1.M1 Turvanõuded väljasttellitavale teenusele](#)

[3.3 Standardmeetmed](#)

[OPS.2.1.M2 Töötajate õigeaegne kaasamine \[haldusosakond\]](#)

[OPS.2.1.M3 Teenuseandja valimise kriteeriumid](#)

[OPS.2.1.M4 Teenuselepingu vastavus kliendi nõuetele](#)

[OPS.2.1.M5 Väljasttellimise strateegia](#)

[OPS.2.1.M6 Välisteenu turbe põhimõtted \[vastutav spetsialist\]](#)

[OPS.2.1.M7 Lubatavate suhtluspartnerite määramine \[haldusosakond\]](#)

[OPS.2.1.M8 Teenuseandja personali kasutamise kord \[personaliosakond\]](#)

[OPS.2.1.M9 Teenuseandja ja kliendi võrguühenduse kokkulepe](#)

[OPS.2.1.M10 Teenuseandja ja kliendi andmevahetuse kokkulepe](#)

[OPS.2.1.M11 Välisteenu infoturbe korraldus](#)

[OPS.2.1.M12 Muudatuste haldus \[vastutav spetsialist\]](#)

[OPS.2.1.M13 Turvaline migratsioon välisteenu kasutamisel](#)

[OPS.2.1.M14 Avariivalmendus väljasttellimisel \[avariiulem\]](#)

[OPS.2.1.M15 Välisteenulepingu korra kohane lõpetamine \[hankeosakond\]](#)

[3.4 Kõrgmeetmed](#)

[OPS.2.1.M16 Teenuseandja töötajate taustakontroll \(C-I\)](#)

3.1 Elutsükkel

Kavandamine

OPS.2.1.M1 Turvanõuded väljasttellitavale teenusele

OPS.2.1.M2 Töötajate õigeaegne kaasamine

OPS.2.1.M5 Väljasttellimise strateegia

OPS.2.1.M8 Teenuseandja personali kasutamise kord

Evitus

OPS.2.1.M3 Teenuseandja valimise kriteeriumid

OPS.2.1.M4 Teenuselepingu vastavus kliendi nõuetele

OPS.2.1.M6 Välisteenuse turbe põhimõtted

OPS.2.1.M7 Lubatavate suhtluspartnerite määramine

OPS.2.1.M9 Teenuseandja ja kliendi võrguühenduse kokkulepe

OPS.2.1.M10 Teenuseandja ja kliendi andmevahetuse kokkulepe

OPS.2.1.M13 Turvaline migratsioon välisteenuse kasutamisel

Käitus

OPS.2.1.M11 Välisteenuse infoturbe korraldus

OPS.2.1.M12 Muudatuste haldus

OPS.2.1.M15 Välisteenuselepingu korrakohane lõpetamine

Avariivalmendus

OPS.2.1.M14 Avariivalmendus väljasttellimisel

Lisanduvad kõrgmeetmed

OPS.2.1.M16 Teenuseandja töötajate taustakontroll

3.2 Põhimeetmed

OPS.2.1.M1 Turvanõuded väljasttellitavale teenusele

a. Välisteenustele on kehtestatud turvanõuded, väljasttellimise turbe põhimõtete olemasolul lähtutakse nõuete kehtestamisel nendest (vt OPS.2.1.M6 *Välisteenuse turbe põhimõtted*).

b. Teenusepooled on kokku leppinud oma kaitsealad ja nende vajaliku kaitsetarbe.

c. Kõikidele teenuse liidestele on määratud turvanõuded, andmevahetusprotseduurid ja vajalikud juurdepääsuõigused.

d. Teenuselepingus on määratud nõutav teenuse kvaliteet ja kvaliteedikontrolli (nt sõltumatu kolmanda poole auditi) läbimise kohustus.

3.3 Standardmeetmed

OPS.2.1.M2 Töötajate õigeaegne kaasamine [haldusosakond]

a. Töötajaid teavitatakse väljasttellimise kavast hanke võimalikult varajases staadiumis.

OPS.2.1.M3 Teenuseandja valimise kriteeriumid

a. Teenuseandja valimiseks on koostatud turvanõudeid sisaldav nõuete profiil.

b. On kehtestatud järgmised teenuseandja valimise ja hindamise kriteeriumid:

- teenuste sobivus ja läbipaistvus;
- vastavus kliendi turvanõuetele;
- maine ja soovitusel;
- ärikultuur (välismaise teenuseandja korral);
- personali kvalifikatsioon.

OPS.2.1.M4 Teenuselepingu vastavus kliendi nõuetele

a. Kõik välisteenuse aspektid lepitakse teenuseandjaga kirjalikult kokku teenuselepingus.

b. Teenuselepingus määratletakse lepingupartnerite infoturbealased õigused ja kohustused.

c. Teenuselepingus lepitakse kokku välisteenuse korraldamisega seotud üksikasjades, näiteks taristu kasutustingimustes, alltöövõtu lubamises või mittelubamises, töötajatele püstitatud nõuetes, isikuandmete kaitses, huvide konflikti vältimises ning tõrgete ja intsidentide käsitleluses.

d. Teenuseandja tagab nõuete täitmise kontrollimiseks vajalikud teabe saamise ja juurdepääsu õigused ning kui lepingus on nii sätestatud, siis ka auditeerimisvõimalused.

OPS.2.1.M5 Väljasttellimise strateegia

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.2.1.M6 Välisteenuste turbe põhimõtted [vastutav spetsialist]

a. Välisteenustele on välisteenuse tellija ja teenuseandja poolt kokku lepitud mõlema poole vajadusi rahuldavad turbe põhimõtted (nt teenuslepingu lisana).

b. Turbe põhimõtete määratlemisel lähtutakse välisteenuse olemusest ja kaitsetarbest.

c. Välisteenuse turbe põhimõtted käsitlevad järgmisi valdkondi:

- teenuse töökorraldus;
- vajalik riistvara ja tarkvara;
- side ja andmevahetus;
- andmete ja vahendite migratsioon;
- teenuse seire ja kvaliteedi tagamine;
- avariivalmendus ja intsidendikäsitus.

d. Välisteenuse turbe põhimõtete järgimist kontrollitakse teenuse kliendi või sõltumatu kolmanda poole osavõtul regulaarselt.

OPS.2.1.M7 Lubatavate suhtluspartnerite määramine [haldusosakond]

a. Iga välisteenuse jaoks on määratud organisatsioonisiseseid ja -väliseid suhtluspartnerid, nende õigused ja edastatava teabe sisu.

b. Mõlemad pooled kontrollivad suhtluspartneri volituste olemasolu ja kehtivust.

c. Suhtluspartnerite andmeid hoitakse dokumenteeritult ja ajakohasena.

OPS.2.1.M8 Teenuseandja personali kasutamise kord [personaliosakond]

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.2.1.M9 Teenuseandja ja kliendi võrguühenduse kokkulepe

a. Võrguühenduse kokkuleppega on määratud, millistele objektidele ja võrguteenustele tohib teenuseandja kliendi võrgus juurde pääseda.

b. Enne teenuseandja kliendi võrku lubamist on kokku lepitud:

- ühenduse kasutamise korralduslikud ja tehnilised tingimused;
- ühenduse kaitsetarve ja turvameetmed;
- poolte konfidentsiaalsuskohustused;
- eritingimused välismaise teenuseandja puhul.

c. Teenuseandja ja klient on määranud võrguühendusega seotud organisatoorse ja tehniliste küsimuste lahendamiseks kontaktisikud.

d. Teenuseandja ja klient on leppinud kokku võrguühenduse intsidentidest teavitusteed ning intsidentide käsitlemise korra.

OPS.2.1.M10 Teenuseandja ja kliendi andmevahetuse kokkulepe

a. Andmevahetuse kokkuleppega on määratud andmete koosseis, andmete kasutamise otstarve ja andmevahetuse protseduurid.

b. Enne andmevahetuse alustamist on teenuseandja ja klient kokku leppinud järgnevas:

- andmevahetuse viisid;

- kasutatavad andmevormingud;
- andmete käideldavuskriteeriumid (näiteks päringutele reageerimise aeg);
- kohustus järgida asjakohaseid õigusakte;
- andmete kaitsetarve ja turvameetmed;
- poolte konfidentsiaalsuskohustused;
- eritingimused välismaise teenuseandja puhul.

c. Teenuseandja ja klient on leppinud kokku andmekaitse intsidentide teavitusteedes, kontaktisikutes ning intsidentide lahendamise korras.

OPS.2.1.M11 Välisteenuse infoturbe korraldus

- a. Kokku lepitud turvameetmete rakendatust ja ajakohasust kontrollitakse regulaarselt.
- b. Teenusepooled vahetavad regulaarselt teavet riskide, probleemide ja olukorra muutuste kohta.
- c. Teenusepooled teevad regulaarselt ühiseid infoturbe õppuseid ja testimisi.

OPS.2.1.M12 Muudatuste haldus [vastutav spetsialist]

- a. Eelseisvatest muudatustest teavitatakse välisteenuse klienti aegsasti.
- b. Kõik teenuse muudatused dokumenteeritakse.
- c. Enne muudatuse tegemist lepivad pooled kokku muudatuse tagasivõtu lahenduses.
- d. Teenusepooled selgitavad välja muudatuse mõju turvalisusele. Vajadusel muudetakse turbekontseptsiooni.

OPS.2.1.M13 Turvaline migratsioon välisteenuse kasutamisel

- a. Migratsiooni kavandamiseks ja läbiviimiseks moodustatakse teenusepoolte ülene tööühm, määratakse vastutusalad ja kontaktisikud.
- b. Teenuseandjale tehakse väljaõpe kliendi tööprotsesside ja IT süsteemide kohta.
- c. Migratsiooni tulemust testitakse enne selle kasutuselevõttu. Migratsiooni testimisel ei kasutata testandmetena tegelikke andmeid.
- d. Teenuse kliendi töötajaid juhendatakse toimima migratsiooni ajal ja pärast seda.
- e. Kõik migratsiooni tulemusena toimunud muudatused dokumenteeritakse, vajadusel ajakohastatakse teenusedokumentatsioon ning turbe põhimõtted.

OPS.2.1.M14 Avariivalmendus väljasttellimisel [avariülem]

- a. Välisteenuse jaoks töötatakse välja avariivalmenduse plaan, mis hõlmab teenusepoolte IT-komponentide, liidestuste ja sidekanalite taastet.
- b. Välisteenuse avariivalmenduse plaanis dokumenteeritakse teenusepoolte vastutus, kontaktisikud ja protseduurid.
- c. Välisteenuse klient kontrollib teenuseandja avariimeetmete rakendamist, selleks korraldavad teenusepooled ühiseid intsidentikäsitluse õppuseid.

OPS.2.1.M15 Välisteenuselepingu korrakohane lõpetamine [hankeosakond]

- a. Välisteenuselepingus lepitakse kokku lepingu korralise lõpetamise tingimused (nt etteteatamise tähtaeg). Tingimustekohane teenuse lõpetamine ei mõjuta kliendi tööprotsesside jätkuvust.
- b. Välisteenuselepingus lepitakse kokku lepingu erakorralise lõpetamise tingimused.
- c. Välisteenuseleping määrab poolte õigused ja kohustused lepingu lõppemisel, sealhulgas teenuseandja kohustuse tema valduses olevad kliendi andmed turvaliselt üle anda või kustutada.

3.4 Kõrgmeetmed

OPS.2.1.M16 Teenuseandja töötajate taustakontroll (C-I)

- a. Välisteenuselepingus kehtestavad teenusepooled teenuseandja töötajate turvakontrolli läbiviimise kriteeriumid.
- b. Teenusepooled lepivad kokku, milliseid turvakontrolle tehakse ja kumb pool taustakontrolli läbi viib.

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetusskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

OPS. Käidutööd

OPS.2: Käidutööd teenusena

OPS.2.2: Pilvteenuste kasutamine

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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 väljastellimist (vt [OPS.2.1 Väljastellimine](#)) pilvteenustele omaste erisustega (sama infrastruktuuri kasutatakse paljude klientide teenindamiseks). Teenuseandjapoolsed meetmed on kirjeldatud moodulis [OPS.3.1 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

Sisukord

- [2.1 Pilvteenuste strateegia puudumine või puudulikkus](#)
 - [2.2 Sõltuvus pilvteenuseandjast \(kontrolli kaotamine\)](#)
 - [2.3 Puudulik nõuete haldus pilvteenuste kasutamisel](#)
 - [2.4 Õigusaktide nõuete rikkumine](#)
 - [2.5 Simultaanteninduse võime puudumine pilvteenuse andjal](#)
 - [2.6 Pilvteenuse andjaga sõlmitud lepingu puudulikkus](#)
 - [2.7 Pilvteenustele migreerimise puudulik kavandamine](#)
 - [2.8 Pilvteenuste puudulik integreerimine omaenda IT-süsteemidega](#)
 - [2.9 Pilvteenuse kasutamise lõpetamise puudulik reguleerimine](#)
 - [2.10 Pilvteenuste halduse raamistiku puudulikkus](#)
 - [2.11 Avariivalmenduse kontseptsiooni puudulikkus](#)
 - [2.12 Pilvteenuse andja süsteemi tõrge](#)
-

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 välis teenuse teabe turvalisust.

2.5 Simultaanteninduse 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 märkimisväärsed 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 töötajale 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 pilvtöötluste platvormi vastu sooritatakse tulemuslik rünne.

3 Meetmed

Sisukord

[3.1 Elutsükk](#)

[3.2 Põhimeetmed](#)

[OPS.2.2.M1 Pilvteenuste strateegia \[vastutav spetsialist, organisatsiooni juhtkond, andmekaitse spetsialist\]](#)

[OPS.2.2.M2 Pilvteenuste turvapoliitika \[vastutav spetsialist\]](#)

[OPS.2.2.M3 Pilvteenuste loendi koostamine \[vastutav spetsialist\]](#)

[OPS.2.2.M4 Vastutusalade ja liidestuste määramine \[vastutav spetsialist\]](#)

[3.3 Standardmeetmed](#)

[OPS.2.2.M5 Pilvteenusele migreerimise kava \[vastutav spetsialist\]](#)

[OPS.2.2.M6 Pilvteenusega liitumise tegevusplaan](#)

[OPS.2.2.M7 Pilvteenuste turbe programm](#)

[OPS.2.2.M8 Pilvteenuse andja valimise kriteeriumid \[organisatsiooni juhtkond\]](#)

[OPS.2.2.M9 Kliendi vajadustele vastav pilvteenuse leping \[organisatsiooni juhtkond\]](#)

[OPS.2.2.M10 Turvaline migratsioon pilvteenusele \[vastutav spetsialist\]](#)

[OPS.2.2.M11 Pilvteenuse avariivalmenduse programm](#)

[OPS.2.2.M12 Infoturbe pilvteenuste kasutamisel](#)

[OPS.2.2.M13 Pilvteenuste turbe piisavuse tõendamine](#)

[OPS.2.2.M14 Pilvteenuselepingu korra kohane lõpetamine \[vastutav spetsialist, organisatsiooni juhtkond\]](#)

3.4 Kõrgmeetmed

[OPS.2.2.M15 Pilvteenuse ülekantavuse tagamine \[vastutav spetsialist\] \(A\)](#)

[OPS.2.2.M16 Andmete täiendav varundamine \[vastutav spetsialist\] \(I-A\)](#)

[OPS.2.2.M17 Krüpteerimine pilvteenuse kasutamisel \(I-A\)](#)

[OPS.2.2.M18 Liidendusteenuste korra kohane kasutamine \[vastutav spetsialist\] \(C-I-A\)](#)

[OPS.2.2.M19 Pilvteenuse andja töötajate taustakontroll \[personaliosakond\] \(C-I-A\)](#)

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 Infoturbe pilvteenuste kasutamisel

OPS.2.2.M13 Pilvteenuste turbe piisavuse tõendamine

Kõrvaldamine

OPS.2.2.M14 Pilvteenuselepingu korra kohane 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 strateegiaga 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;
- suhtlused 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 Infoturbe pilvteenuste kasutamisel

a. Pilvteenuste dokumentatsiooni ja kasutusjuhiseid ajakohastatakse regulaarselt.

b. Pilvteenuse vastavust teenuslepingus 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-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 korra kohane lõpetamine [vastutav spetsialist, organisatsiooni juhtkond]

a. Pilvteenuselepingu lõppemise puhuks on kehtestatud protseduurid üleminekuks sisemisele teenusele või teisele pilvteenuseandjale, täites kõiki seniseid teenusenõudeid.

b. Pilvteenuselepingu 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 töötuskohas 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“
[RIA]	RIA juhend „Juhend avalike pilveteenuste turvaliseks kasutamiseks avalikus sektoris“, 2019, https://www.ria.ee/sites/default/files/content-editors/ISKE/avalike-pilvede-kasutamise-juhend.pdf

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

OPS. Käidutööd

OPS.3: Teenuseandja käidutööd

OPS.3.1: Teenuseandja infoturve

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

1.1 Eesmärk

Esitada meetmed teenuseandja infoturbe kavandamiseks, rakendamiseks, juhtimiseks ja kontrollimiseks ning nõutava turbetaseme hoidmiseks teenuseandja vaatest.

1.2 Vastutus

Teenuseandja infoturbe meetmete täitmise eest vastutab IT-talitus.

Lisavastutajad

Andmekaitespetsialist, organisatsiooni juhtkond, avariülem, personaliosakond, haldusosakond.

1.3 Piirangud

Moodul sisaldab teenuseandjale kohalduvaid turvameetmeid. Teenusesaaja vaadet käsitletakse moodulis [OPS.2.1 Väljasttellimine](#). Moodulis ei käsitleta teenuseandja ja väljasttellitava teenuse kliendi vaheliste sidekanalite turvet.

2 Ohud

Sisukord

- [2.1 Laivõrgu tõrge](#)
 - [2.2 Puuduv või piisamatu infoturbe regulatsioon](#)
 - [2.3 Pääsuõiguste puudulik haldamine](#)
 - [2.4 Puuduvad või piisamatud testimis- ja kinnitusprotseduurid](#)
 - [2.5 Andmete ja andmekandjate eaturvaline transportimine](#)
 - [2.6 Teenuseandja puudulik infoturbe haldus](#)
 - [2.7 Teenuse saajaga puudulikult sõlmitud teenusleping](#)
 - [2.8 Teenuslepingu lõpetamise puudulik kord](#)
 - [2.9 Puudulik avariivalmenduse kontseptsioon](#)
 - [2.10 Teenuseandja IT-süsteemi tõrge](#)
 - [2.11 Teenuseandja IT-süsteemidega liidestuse nõrkused](#)
 - [2.12 Suhtlusrünne](#)
 - [2.13 Simultaanteeninduse võime puudumine teenuseandjal](#)
-

2.1 Laivõrgu tõrge

Teenuseandja, kes ei osuta oma teenust kliendi juures kohapeal, sõltub suurel määral laivõrkude käideldavusest (ingl *Wide Area Network*, WAN). Laivõrgu tõrge võib kaasa tuua teenuseandja teenuse katkestuse.

2.2 Puuduv või piisamatu infoturbe regulatsioon

Kui infoturbe regulatsioon ei määratle selgelt vastutusalasid ja kontrollifunktsioone, võivad vajalikud infoturbe meetmed teenuseandja juures jääda rakendamata. Infoturbe eeskirjad ja korrad võivad jääda pärast tehnilisi ja korralduslikke muudatusi ajakohastamata.

2.3 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.

2.4 Puuduvad või piisamatud testimis- ja kinnitusprotseduurid

Kui teenuseandja ei ole riist- ja tarkvara jaoks kehtestanud piisavaid testimis- ja kinnitusprotseduure, võivad teenuse tark- ja riistvaravead või konfiguratsiooni nõrkused jääda märkamata. Kui teenuseandja käidukeskkonnas võetakse kasutusele uued komponendid ilma neid eelnevalt testimata, võivad sellega kaasnevad turvanõrkused mõjutada ka kliendile antavat teenust.

2.5 Andmete ja andmekandjate eaturvaline transportimine

Kui andmete, dokumentide ja andmekandjate transport ei ole korraldatud vastavalt nõutud kaitsetarbele, võib andmekao, volitamata juurdepääsu või manipulatsiooni tõttu tekkida märkimisväärne kahju nii väljasttellivale organisatsioonile kui ka teenuseandjale.

2.6 Teenuseandja puudulik infoturbe haldus

Puudulikult kehtestatud või nõuetele mittevastav teenuseandja infoturbe haldus väljendub infoturbe valdkonna eest vastutuse puudumises, puudulikus juhtkonnapoolses toetuses ja turbeotsuste läbipaistmatuses. Puuduliku infoturbe halduse korral ei suuda teenuseandja teenust tarbiva organisatsiooni infoturbe nõudeid täita.

2.7 Teenuse saajaga puudulikult sõlmitud teenusleping

Kui kaitsetarve ja sellel põhinevad andmete ja süsteemide turvanõuded ei ole kliendi ja teenuseandja vahel kokku lepitud, võivad kliendi andmed jääda vajaliku kaitseta.

2.8 Teenuslepingu lõpetamise puudulik kord

Kui teenuslepingu lõpetamise kord on puudulik, võivad tekkida probleemid andmete kliendile üleandmisega. Teenuseandja võib kliendi andmed taastamatult kustutada ning andmed jäävad kliendile terviklikult ja nõuetekohaselt üleandmata.

2.9 Puudulik avariivalmenduse kontseptsioon

Kui teenuseandja avariivalmenduse kontseptsioon on puudulik, võib teenuste taastamine võtta kauem aega ja kliendi äriprotsessid olla häiritud suuremal määral, kui teenuslepingus kokku lepitud.

2.10 Teenuseandja IT-süsteemi tõrge

Teenuseandja IT-süsteemide katkestused mõjutavad teenuse käideldavust. Sarnased probleemid tekivad ka liidestuse tõrgete korral teenuseandja ja kliendi vahel. Kui lepingus on nii kokku lepitud, võib see teenuseandja jaoks tähendada ka rahalist kulu teenuse kliendi kahjunõude rahuldamiseks.

2.11 Teenuseandja IT-süsteemidega liidestuse nõrkused

Kui väljasttellitava teenuse kliendi ja teenuseandja vaheline IT-liidestus ei ole piisavalt kaitstud, võivad edastatavate andmete konfidentsiaalsus ja terviklus ohtu sattuda. Kaitseta või halvasti kaitstud liidestega võib kaasned ka kõrvaliste isikute volitamata juurdepääs andmetele.

2.12 Suhtlusrünne

Suhtlusrünne (ingl *social engineering*) abil on võimalik panna inimesi lubamatul viisil toimima. Kui suhtlusrünne sihtmärgiks on teenuseandja töötajad, võib ründaja saada niimoodi juurdepääsu mitme ettevõtte paljudele andmetele.

2.13 Simultaanteninduse 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.

3 Meetmed

Sisukord

[3.1 Elutsükel](#)

[3.2 Põhimeetmed](#)

[OPS.3.1.M1 Teenuseosutamise põhimõtted](#)

[3.3 Standardmeetmed](#)

[OPS.3.1.M2 Teenuse tarneleping kliendiga](#)

[OPS.3.1.M3 Väljasttellitava teenuse turbe programm](#)

[OPS.3.1.M4 Lubatavate teabevahetuspartnerite määramine \[haldusosakond, andmekaitse spetsialist\]](#)

[OPS.3.1.M5 Teenuseandja personali kasutamise kord \[personaliosakond\]](#)

[OPS.3.1.M6 Teenuseandja välispersonal kasutamise kord \[personaliosakond\]](#)

[OPS.3.1.M7 Simultaanteninduse kord](#)

[OPS.3.1.M8 Kliendi võrgu kasutamise kokkulepe](#)

[OPS.3.1.M9 Teenusepartnerite vahelise andmevahetuse kokkulepe](#)
[OPS.3.1.M10 Väljasttellitava teenuse infoturve](#)
[OPS.3.1.M11 Pääsu reguleerimine \[haldusosakond\]](#)
[OPS.3.1.M12 Muudatuste haldus \[organisatsiooni juhtkond\]](#)
[OPS.3.1.M13 Turvaline migratsioon välisteenusele](#)
[OPS.3.1.M14 Välisteenuse avariivalmendus \[avariiuülem\]](#)
[OPS.3.1.M15 Teenuse tarnelepingu lõpetamise kord \[organisatsiooni juhtkond\]](#)
[3.4 Kõrgmeetmed](#)
[OPS.3.1.M16 Teenuseandja töötajate taustakontroll \[personaliosakond\] \(C-I\)](#)

3.1 Elutsükkel

Kavandamine

OPS.3.1.M1 Teenuseosutamise põhimõtted

OPS.3.1.M7 Simultaanteninduse kontseptsioon

Evitus

OPS.3.1.M2 Teenuse tarneleping kliendiga

OPS.3.1.M3 Väljasttellitava teenuse turbe programm

OPS.3.1.M4 Lubatavate teabevahetuspartnerite määramine

OPS.3.1.M5 Teenuseandja personali kasutamise kord

OPS.3.1.M6 Teenuseandja välispersonali kasutamise kord

OPS.3.1.M8 Kliendi võrgu kasutamise kokkulepe

OPS.3.1.M9 Teenusepartnerite vahelise andmevahetuse kokkulepe

OPS.3.1.M13 Turvaline migratsioon välisteenusele

Käitus

OPS.3.1.M10 Väljasttellitava teenuse infoturve

OPS.3.1.M11 Pääsu reguleerimine

OPS.3.1.M12 Muudatuste haldus

Avariivalmendus

OPS.3.1.M14 Avariivalmendus väljasttellimisel

OPS.3.1.M15 Teenuse tarnelepingu lõpetamise kord

Lisanduvad kõrgmeetmed

OPS.3.1.M16 Teenuseandja töötajate turvakontroll

3.2 Põhimeetmed

OPS.3.1.M1 Teenuseosutamise põhimõtted

a. On koostatud teenuseosutamise põhimõtted, milles esitatakse teenuse raamtingimused ja teenuse kliendile vajalik teave teenuste turvaseme ja turvanõuete kohta.

b. Teenuseosutamise põhimõtted määratlevad vähemalt järgmist:

- teenuse eesmärgid ja soorituse hindamise indikaatorid;
- teenuse- ja turvaseme;
- teenuseandja ja kliendi koostöö korralduse;
- sõltuvused välistest teenuseandjatest;
- teenuseandja töö- ja turvakultuuri.

3.3 Standardmeetmed

OPS.3.1.M2 Teenuse tarneleping kliendiga

a. Teenuse kliendiga lepitakse kirjalikult kokku teenuse väljatöötamise, arenduse, kvaliteedikontrolli ja muutmisega seotud koostöökohustused.

b. Leping kliendiga määrab piisavalt täpselt järgmised aspektid:

- teenuse sisu;
- õigused ja kohustused;
- teenustase;
- ühine taristu, selle turve ja omandiõigused;
- töökorraldus;
- personali kasutamine;
- avariihaldus;
- õiguslikud raamtingimused;
- alltöövõtjate kasutamine;
- simultaanteenindus, vt ka OPS.3.1.M10 *Teenuse kasutamise infoturve*;
- muudatuste haldus ja testimine;
- teenuse seire;
- kvaliteedikontrollid ja läbivaatused.

OPS.3.1.M3 Väljasttellitava teenuse turbe programm

a. Väljasttellitavate teenuste turvalisuse tagamiseks on koostatud üldine turbekontseptsioon.

b. Iga kliendi tarbeks kehtestatakse teenuse turbe programm, tuginedes kliendilt saadud nõuetele.

c. Teenuse turbe programmis määratakse:

- koostöökohustused ja vastutusalad;
- teenuseandja ja kliendi vaheline liidestus;
- kliendi kaitseala piirid.

d. Turbekontseptsiooni rakendamist kontrollitakse regulaarselt.

OPS.3.1.M4 Lubatavate teabevahetuspartnerite määramine [haldusosakond, andmekaitse spetsialist]

a. Teenuseandja ja klient määravad teabevahetuseks:

- kontaktisikud;

- välisteenuse toimimiseks vajaliku teabe;
- teabe lubatavad kasutusviisid.

b. Partnerite teabevahetuse asja- ja ajakohasust kontrollitakse juhtumipõhiselt, vajadusel muudetakse teabevahetuse partnereid.

OPS.3.1.M5 Teenuseandja personali kasutamise kord [personaliosakond]

a. Teenuseandja töötajatele on selgitatud nende tööülesandeid, teenuse kliendi infoturbepoliitikat ja turvanõudeid.

b. Töötajate kohustused on sätestatud teenuselepingus. Teenuseandja tagab teenuselepingu täitmiseks vajalike töötajate väljaõppe ja korrakohase asendamise.

c. Teenuseandja kõik töötajad, kes saavad tööülesannete täitmise käigus juurdepääsu teenuse kliendi konfidentsiaalsetele dokumentidele ja andmetele, kohustuvad kirjalikult (nt konfidentsiaalsusleppe vormis) täitma asjakohaseid õigusakte ja teenuse kliendi nõudeid.

d. Teenuse kliendil võimaldatakse kontrollida teenusega seotud töötajate tausta ja kvalifikatsiooni vastavust.

OPS.3.1.M6 Teenuseandja välispersonali kasutamise kord [personaliosakond]

a. Välispersonali kasutamisest teavitab teenuseandja teenuse klienti.

b. Välised töötajad teavad oma ülesandeid, turvaeeskirju, teenuseandja ja kliendi turvanõudeid ning kohustuvad kirjalikult neid järgima. Teenuse kliendil võimaldatakse kontrollida teenuseandja töötajate vastavust.

c. Lühiajaliselt kliendi juures viibivaid teenuseandja väliseid töötajaid käsitletakse kliendi vaates kui külalisi.

d. Teenuseandjal on olemas protseduur väliste töötajatega töösuhte lõpetamiseks.

OPS.3.1.M7 Simultaanteninduse kord

a. Teenuse turbe programmi osana on kehtestatud simultaanteninduse kord, mis tagab klientide käitlus- ja andmekontekstide lahususe.

b. Simultaanteninduse kord sisaldab vähemalt järgmist:

- simultaantöö õiguslikud alused;
- klientide tehniline lahusus;
- klientide prioriseerimine;
- simultaanteninduse halduse ja kliendikonteksti halduse lahusus;
- andmebaaside lahusus andmebaasisüsteemis;
- võrgutaristu virtualiseerimine (VLAN, VPN).

OPS.3.1.M8 Kliendi võrgu kasutamise kokkulepe

a. Võrgu kasutamise kokkuleppega on määratud, millistele objektidele ja võrguteenustele tohib teenuseandja kliendi võrgus juurde pääseda.

b. Enne teenuseandja kliendi võrku lubamist lepitakse kokku:

- ühenduse kasutamise korralduslikud ja tehnilised tingimused;
- ühenduse kaitsetarve ja turvameetmed;

- võrguühenduse eest vastutajad;
- kontaktisikud;
- sidepartnerid, nende õigused ja kohustused;
- lubatavad teenused;
- võrguühenduse turvameetmed ja nende seire;
- logimisõigused ja -kohustused;
- intsidentide lahendamise kord ja kulude korvamine.

OPS.3.1.M9 Teenusepartnerite vahelise andmevahetuse kokkulepe

a. Andmevahetuse kokkuleppega on määratud andmete koosseis, andmete kasutamise otstarve ja andmevahetuse protseduurid.

b. Enne andmevahetuse alustamist lepitakse kokku:

- kasutatavad rakendused;
- kasutatavad andmevormingud;
- andmete käideldavuskriteeriumid (siinhulgas päringutele reageerimise aeg);
- andmete kasutusotstarve;
- teabevahetuse turbe meetmed (vt [CON.9 Teabevahetus](#));
- kohustus järgida asjakohaseid õigusakte;
- turvamehhanismid (viirusetõrje, krüpteerimine, signeerimine, võtmehaldus jms);
- poolte konfidentsiaalsuskohustused.

c. Teenuseandja ja klient on leppinud kokku andmekaitse intsidentide teavitusteedes, kontaktisikutes ning intsidentide lahendamise korras.

OPS.3.1.M10 Väljasttellitava teenuse infoturve

a. Teenusepartnerid kontrollivad vastastikku turbeprogrammide ajakohasust ja piisavust.

b. Teenusepartnerid ajakohastavad regulaarselt oma poliitikaid ja dokumentatsiooni.

c. Teenusepartnerid vahetavad regulaarselt teavet ohtude, riskide, keskkonna ning muudatuste kohta.

d. On kehtestatud infoturbe intsidentide ühise käsitlemise kord.

e. Teenusepartnerid korraldavad turvaseme kontrolliks regulaarselt ühiseid läbivaatusi, harjutusi ja testimisi.

f. Väljasttellitava teenuse turvameetmete rakendamist teenuseandja juures on hinnanud sõltumatu audiitor. Kehtiva turvalisust tõendava sertifikaadi või audiitori koondhinnangu puudumisel korraldab väljasttellitava teenuse turvameetmete auditeerimise klient.

OPS.3.1.M11 Pääsu reguleerimine [haldusosakond]

a. Sisepääsu ruumidesse, süsteemidesse ja võrkudesse ning juurdepääsu andmetele ja tarkvarale reguleeritakse korralduslike ja tehniliste vahenditega.

b. Pääsuõigused on jagatud minimaalsuse põhimõttel vastavalt tööalastele vajadustele.

c. Pääsuõigusi saab kasutada ainult turvalise autentimise kaudu.

OPS.3.1.M12 Muudatuste haldus [organisatsiooni juhtkond]

a. On koostatud eeskiri IT-komponentide ja konfiguratsiooniandmete muudatuste läbiviimiseks.

- b. Kõik muudatused kavandatakse, testitakse, kinnitatakse ja dokumenteeritakse.
- c. Muudatuste dokumenteerimise viis ja maht kooskõlastatakse teenuse kliendiga.
- d. Suured turvalisust puudutavad muudatused kooskõlastatakse kliendi infoturbejuhiga.
- e. On kehtestatud protseduur muudatuste tagasivõtuks.

OPS.3.1.M13 Turvaline migratsioon välisteenusele

- a. Välisteenusele migreerimise ajaks moodustatakse teenusepoolte ühine turbehalduse rühm.
- b. Migratsiooni ajaks on koostatud turbekontseptsioon ja seda ajakohastatakse pärast migratsiooni.
- c. Dokumenteeritakse poolte kontaktandmed migratsiooni küsimustes. Üleviidavad objektid ja nende konfiguratsioon on piisavalt dokumenteeritud.
- d. Migratsiooni alustatakse pärast välisteenuselepingu sõlmimist, välisteenuse testimist ja kliendi personali koolitust välisteenuse alal.
- e. Kõik migratsiooni ajaks tehtud erandid kõrvaldatakse pärast migratsiooni.

OPS.3.1.M14 Välisteenuse avariivalmendus [avariiuülem]

- a. On koostatud välisteenuse avariivalmenduse kava, mis hõlmab mõlema teenusepoolte asjakohaseid komponente ja teenuseliideseid.
- b. Välisteenuse avariivalmenduse kava on määratud järgnev:
 - kohustused, kontaktisikud ja protseduurid;
 - andmevarunduse üksikasjad;
 - juhised tüüpolukordade puhuks.
- c. Avariivalmenduse plaan on kooskõlastatud teenuse kliendiga ja seda kontrollitakse regulaarsete ühisõppustega.

OPS.3.1.M15 Teenuse tarnelepingu lõpetamise kord [organisatsiooni juhtkond]

- a. Teenuse tarnelepingus on kokku lepitud lepingu korralise lõpetamise tingimused. Lepingu tingimustekohane lõpetamine ei mõjuta negatiivselt kliendi ega tarnija äriprotsesse.
- b. Teenuse tarnelepingus on kokku lepitud lepingu erakorralise lõpetamise tingimused.
- c. Teenuse tarnelepingus on sätestatud teenuse andmisel kasutatud riist-ja tarkvara omandiõigus ja nende kasutamise jätkumise tingimused.
- d. Lepingu lõpetamisel vahendite kasutamine ja tehtavad protseduurid dokumenteeritakse.
- e. Lepingu lõppemisel antakse teenuseandja juures hoitud kliendi andmed kliendile üle.
- f. Kliendiga seotud meta-ja haldusandmed kustutatakse turvaliselt teenuseandja poolel.
- g. Lepingu lõppemisel vaadatakse üle teenuseandja töötajate pääsuõigused ja vajaduse korral need tühistatakse.

3.4 Kõrgmeetmed

OPS.3.1.M16 Teenuseandja töötajate taustakontroll [personaliosakond] (C-I)

- a. Teenuseandja kontrollib enne töölepingu sõlmimist uute töötajate ja välispersonali usaldusväärsust.
- b. Teenusepooled lepivad kokku teenuseandja töötajate taustakontrolli läbiviimise kriteeriumid.

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

DER. Avastamine ja reageerimine

DER.1: Turvaintsidentide avastamine

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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

Sisukord

[2.1 Õigusaktide sätete eiramine](#)

[2.2 Vastutajate puudulik kvalifikatsioon](#)[2.3 Sissetungituvastuse süsteemide puudulik seadistus](#)[2.4 Teabe puudumine kaitstava IT-süsteemi kohta](#)[2.5 Avastussüsteemide vähene kasutamine](#)[2.6 Ebapiisav inimressurss](#)

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 turvaintsidentid jääda märkamata.

2.3 Sissetungituvastuse süsteemide puudulik seadistus

Kui sissetungituvastuse süsteemid on valesti seadistatud, võib see tekitada rohkelt ebaolulisi hoiatusteateid. Turvaintsidentidele 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

Sisukord

[3.1 Elutsükel](#)[3.2 Põhimeetmed](#)[DER.1.M1 Turvaintsidentide avastamise eeskiri](#)[DER.1.M2 Logiandmete analüüsi õiguspärasus](#)[DER.1.M3 Turvasündmustest teavitamise kord](#)[DER.1.M4 Töötajate teadlikkuse tõstmine \[ülemus, kasutaja, töötaja\]](#)[DER.1.M5 IT-süsteemi avastusfunktsioonide rakendamine \[vastutav spetsialist\]](#)[3.3 Standardmeetmed](#)[DER.1.M6 Logiandmete pidev jälgimine ja analüüs](#)

[DER.1.M7 Vastutajate koolitus \[ülemus\]](#)

[DER.1.M9 Täiendavad avastussüsteemid \[vastutav spetsialist\]](#)

[DER.1.M11 Keskne logimistaristu turvasündmuste analüüsiks \[vastutav spetsialist\]](#)

[DER.1.M12 Välisallikate teabe analüüs \[vastutav spetsialist\]](#)

[DER.1.M13 Regulaarne avastussüsteemide läbivaatus](#)

3.4 Kõrgmeetmed

[DER.1.M10 TLS- ja SSH-proksid \[vastutav spetsialist\] \(C\)](#)

[DER.1.M14 Logiandmete analüüsile spetsialiseerunud töötajad \(C-I\)](#)

[DER.1.M15 Reaalajas toimuv sündmuseteadete keskhalldus \(C-I-A\)](#)

[DER.1.M16 Avastussüsteemide rakendamine kaitsetarbe alusel \(C-I-A\)](#)

[DER.1.M17 Automaatne reageerimine turvasündmustele \(C-I\)](#)

[DER.1.M18 Regulaarne tervikluse kontroll \(C-I\)](#)

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 keskhalldus

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 aadressaadid eri liiki intsidentide puhuks, teavitatavad isikud, isikute kättesaadavus ja intsidenti kiireloomulisusest sõltuv sidekanali valik.
- b. Töötajad on teadlikud oma ülesannetest ja kohustustest. Turvasündmuse kahtluse korral teavitatakse sellest kohehelt 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 käsitus](#)).

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 sündmuseteade edastatakse 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. Sündmuseteade 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 sündmuseteateid 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 turvasündmuse 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 käsitlemise protsessi (vt ka [DER.2.1. Turvaintsidentide käsitlemine](#)).

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-I)

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:

- tuvastama ründeid, väärkasutusi ja rikkumisi;
- teatama turvasündmustest automaatselt;
- 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.

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetusskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

DER. Avastamine ja reageerimine

DER.2: Turvaintsidentide haldus

DER.2.1: Turvaintsidentide käsitus

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

1.1 Eesmärk

Esitada juhised turvaintsidentide süstemaatiliseks käsitlemiseks.

1.2 Vastutus

Turvaintsidentide käsitlemise meetmete täitmise eest vastutab infoturbejuht.

Lisavastutajad

Andmekaitespetsialist, vastutav spetsialist, IT-talitus, organisatsiooni juhtkond, avariijuh.

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 lahendamise](#). Intsidenti tulemusena tekkinud avariiolukorras tegutsemist käsitletakse moodulis [DER.4 Avariiahaldus](#).

2 Ohud

Sisukord

[2.1 Turvaintsidentide puudulik käsitus](#)

[2.2 Tõendusjälgede hävitamine turvaintsidentide käsitusel](#)

2.1 Turvaintsidentide puudulik käsitus

Kui turvaintsidentidele reageeritakse ebasobival viisil või meetmeid kiiresti ei rakendata, võib ründaja turvanõrkust ära kasutada pikema perioodi jooksul. Väärad otsused turvaintsidentide käsitusel võivad tekitada väga suurt kahju, sealhulgas ka asjatuid kahjusid kolmandatele osapooltele. Näited juhtumitest, mis viitavad turvaintsidentide puudulikule käsitlemisele:

- tulemüüri logifailid sisaldavad kahtlasi kirjeid;
- intsidentist teavitamisega venitatakse;
- kontoris toimunud varguse käsitlemisel ei arvestata, et varastatud sülearvutis võis olla konfidentsiaalseid andmeid.

2.2 Tõendusjälgede hävitamine turvaintsidentide käsitusel

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 intsidentide avastamist installida serverisse puuduvad turvapaigad ja uuendid.

3 Meetmed

Sisukord

[3.1 Elutsükel](#)

[3.2 Põhimeetmed](#)

[DER.2.1.M1 Turvaintsidentide määratlemine](#)

[DER.2.1.M2 Turvaintsidentide käsitluse juhend](#)

[DER.2.1.M3 Vastutuste ja kontaktisikute määramine](#)

[DER.2.1.M4 Turvaintsidentist teavitamise kord \[organisatsiooni juhtkond, IT-talitus, andmekaitse spetsialist, avariitöök\]](#)

[DER.2.1.M5 Turvaintsidentide lahendamise kord \[IT-talitus\]](#)

[DER.2.1.M6 Tõukeskonnaga taastamine pärast turvaintsidentide \[IT-talitus\]](#)

[3.3 Standardmeetmed](#)

[DER.2.1.M7 Turvaintsidentide käsitluse meetodika \[organisatsiooni juhtkond\]](#)

[DER.2.1.M8 Turvaintsidentide käsitluse tööriist](#)

[DER.2.1.M9 Turvaintsidentist teavitamise juhend](#)

[DER.2.1.M10 Turvaintsidentide toime piiramine \[avariitöök, IT-talitus\]](#)

[DER.2.1.M11 Turvaintsidentide hindamine \[IT-talitus\]](#)

[DER.2.1.M12 Turvaintsidentide ja IT-intsidentide käsitluse ühendamine \[avariitöök\]](#)

[DER.2.1.M13 Turbe- ja avariitöökude integreerimine \[avariitöök\]](#)

[DER.2.1.M14 Turvaintsidentist teavitamise eskalatsiooniplaan \[IT-talitus\]](#)

[DER.2.1.M15 IT-talituse töötajate valmidus turvaintsidentide käsitluseks \[IT-talitus\]](#)

[DER.2.1.M16 Turvaintsidentide käsitluse dokumenteerimine](#)

[DER.2.1.M17 Turvaintsidentide järeltoimingud](#)

[DER.2.1.M18 Protsessi täiustamine kogemuste ja välisarengute põhjal \[vastutav spetsialist\]](#)

[3.4 Kõrgmeetmed](#)

[DER.2.1.M19 Turvaintsidentide käsitlemise prioriteetid \[organisatsiooni juhtkond\] \(C-I-A\)](#)

[DER.2.1.M20 Organisatsiooni turvaintsidentidest teatamise keskus \(C-I-A\)](#)

[DER.2.1.M21 Ekspertrühm turvaintsidentide käsitlemiseks \(C-I-A\)](#)

[DER.2.1.M22 Turvaintsidentide käsitlemise korralduse läbivaatus \(C-I-A\)](#)

3.1 Elutsükkel

Kavandamine

DER.2.1.M1 Turvaintsidentide määratlemine

DER.2.1.M2 Turvaintsidentide käsitlemise juhend

DER.2.1.M3 Vastutuste ja kontaktisikute määramine

DER.2.1.M7 Turvaintsidentide käsitlemise metoodika

DER.2.1.M8 Turvaintsidentide käsitlemise tööühm

DER.2.1.M9 Turvaintsidentidest teavitamise juhend

DER.2.1.M11 Turvaintsidentide hindamine

DER.2.1.M14 Turvaintsidentide eskalatsiooniplaan

Käitus

DER.2.1.M4 Turvaintsidentidest teavitamise kord

DER.2.1.M5 Turvaintsidentide lahendamise kord

DER.2.1.M10 Turvaintsidentide toime piiramine

DER.2.1.M12 Turvaintsidentide ning IT-intsidentide käsitlemise ühendamine

DER.2.1.M13 Turbe- ja avariihalduse integreerimine

DER.2.1.M15 IT-talituse töötajate valmidus turvaintsidentide käsitlemiseks

DER.2.1.M16 Turvaintsidentide käsitlemise 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 käsitlemisprioriteetid

DER.2.1.M20 Organisatsiooni turvaintsidentide teatamiskeskus

DER.2.1.M21 Ekspertühm turvaintsidentide käsitlemiseks

DER.2.1.M22 Turvaintsidentide käsitlemise korralduse läbivaatus

3.2 Põhimeetmed

DER.2.1.M1 Turvaintsidentide määramine

- a. Organisatsioon on määratud, millised intsendid on turvaintsendid. Turvaintsident on IT-tõrgetest selgesti eristatav.
- b. Turvaintsidentide käsitlemise kaasatud töötajad teavad turvaintsidentide määramist.
- c. Turvaintsidentide määramise ja käsitlemise aluseks võetakse konkreetsete äriprotsesside, IT-süsteemide ja rakenduste kaitsetarve.

DER.2.1.M2 Turvaintsidentide käsitlemise juhend

- a. Turvaintsidentide käsitlemiseks on koostatud protseduurijuhend. Juhendis on määratud käsitlemisala, millele juhend laieneb.
- b. Juhend sisaldab praktilisi ja sihtühmakohaseid tegevusjuhiseid käitumiseks turvaintsidentide 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 käsitlemisega 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 Turvaintsidentide teavitamise kord [organisatsiooni juhtkond, IT-talitus, andmekaitse spetsialist, avariijuhend]

- a. Turvaintsidentide ilmnemisel teavitatakse sellest organisatsioonisiseseid ja -väliseid asjaosalisi viivitamata ning turvaintsidentide käsitlemise juhendi kohaselt.
- b. Igakordselt otsustatakse, kas intsidentide lahendamiseks kaasatakse lisaks ka andmekaitse spetsialist, jurist või organisatsiooni juhtkond.
- c. Kui turvaintsidentidest tuleb teavitada väliseid ametiasutusi (CERT-EE, politsei, Andmekaitse Inspeksioon), tehakse seda teavitamiskohustustes määratud perioodi jooksul, teavitamiseks kasutatakse turvalisi suhtlusi.

DER.2.1.M5 Turvaintsidentide lahendamise kord [IT-talitus]

- a. Turvaintsidentide lahendamiseks isoleeritakse mõjutatud komponendid, intsident dokumenteeritakse ja selgitatakse välja selle põhjus.

b. Vajadusel kaasatakse turvaintsidentide eri teemavaldkondadega seotud küsimuste lahendamiseks organisatsioonisiseseid või -väliseid spetsialiste. Selleks on loodud turvalised suhtlused.

c. Intsidentide lahendamise käigus taastatakse võimalikult kiiresti intsidentidele eelnenud normaalolukord (vt DER.2.1.M6 *Töökeskkonna taastamine pärast turvaintsidenti*).

DER.2.1.M6 Töökeskkonna taastamine pärast turvaintsidenti [IT-talitus]

a. Turvaintsidentide analüüsimiseks eraldatakse intsidentidest mõjutatud seadmed võrgust.

b. Intsidentide 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. Intsidentijärgsel andmete ennistamisel kontrollitakse andmete õigsust ja terviklust. Varundatud andmete taastamisel veendutakse, et need ei ole turvaintsidentidest mõjutatud.

e. Enne mõjutatud seadmete taaskasutuselevõttu muudetakse kõik seadmes kasutatud paroolid, viiakse läbi turvatestimine ja kontrollitakse koos kasutajaga komponendi funktsioneerimist.

f. Uute või korduvate anomaaliade avastamiseks seiratakse pärast töökeskkonna taastamist mõjutatud ja ennistatud seadmete võrguliiklust

3.3 Standardmeetmed

DER.2.1.M7 Turvaintsidentide käsitlemise meetodika [organisatsiooni juhtkond]

a. Turvaintsidentide käsitlemise juhendis (vt DER.2.1.M2 *Turvaintsidentide käsitlemise juhend*) on dokumenteeritud meetodika ja protseduurid eri liiki turvaintsidentide käsitlemiseks.

b. Organisatsiooni juhtkond on turvaintsidentide käsitlemise meetodika kinnitanud ja kasutajatele teatavaks teinud.

c. Turvaintsidentide käsitlemise meetodikat kontrollitakse ja ajakohastatakse regulaarselt.

DER.2.1.M8 Turvaintsidentide käsitlemise tööühik

a. Turvaintsidentide käsitlemiseks moodustatakse tööühik, tööühiku koosseisu võidakse olenevalt intsidentide liigist muuta.

b. Tööühiku liikmetele on eelnevalt määratud konkreetne roll ja ülesanded, mida nad on valmis vajadusel täitma.

c. Turvaintsidentide käsitlemise tööühiku koosseisu muudetakse vastavalt vajadusele.

DER.2.1.M9 Turvaintsidentide teavitamise juhend

a. Intsidentide 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 [avariitöö, 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 käsitle ühendamine [avariülem]

- 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 käsitle erisusi.
- c. Turbehalduse töötajatel on IT-intsidentide haldusvahendile lugemisõigusega ligipääs.

DER.2.1.M13 Turbe- ja avariihalduse integreerimine [avariülem]

- a. Kui turvaintsidendi tulemusel on käivitatud avariihalduse protsess, koordineerib intsidendi lahendamist avariülem.
- 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 käsitlemiseks [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 käsitle juhendiga ning läbinud vajalike vahendite kasutamise koolituse.

DER.2.1.M16 Turvaintsidentide käsitlemise dokumenteerimine

- a. Turvaintsidentid dokumenteeritakse ühtse tüüpprotseduuri kohaselt.
- b. Turvaintsidendi dokumenteerimisel fikseeritakse kõik käsitle käigus tehtud tegevused koos läbiviimise ajaga ning talletatakse mõjutatud komponentide logiandmed.

c. Turvaintsidentide käsitlemise raport arhiveeritakse viisil, mis tagab selle tervikluse ja konfidentsiaalsuse.

DER.2.1.M17 Turvaintsidentide järeltoimingud

a. Turvaintsidentide käsitlemise järgselt hinnatakse:

- kui kiiresti turvaintsident tuvastati ja lahendati;
- kas teavitusteed toimusid;
- kas oli piisavalt andmeid mõjuhinna läbiviimiseks;
- kas avastamismeetmed ja käsitusmeetmed olid tõhusad.

b. Varasemate turvaintsidentide kogemusi kasutatakse sarnaste turvaintsidentide käsitlemise tegevuskava koostamiseks. Tegevuskava muudatused tehakse sihtrühmadele teatavaks.

c. Juhtkonda teavitatakse toimunud turvaintsidentist ja selle käsitlemise tulemustest.

DER.2.1.M18 Protsessi täiustamine kogemuste ja välisarengute põhjal [vastutav spetsialist]

a. Turvaintsidentide käsitlemise täiustamiseks küsitakse turvaintsidentide lahendamisel kaasatud olnud isikute arvamusi ja vastutajate tagasisidet.

b. Pärast IT-süsteemides ja intsidentihalduses toimunud muudatusi ajakohastatakse intsidentide avastamis- ja haldusvahendeid ning juhendeid.

3.4 Kõrgmeetmed

DER.2.1.M19 Turvaintsidentide käsitlemise prioriteedid [organisatsiooni juhtkond] (C-I-A)

a. Äriprotsesside erinevast kaalukusest tulenevalt määratakse intsidentide käsitlemise prioriteedid.

b. Turvaintsidentide käsitlemise prioriteedid kinnitab organisatsiooni juhtkond. Sarnasel alusel prioriteete kasutatakse ka IT- intsidentihalduses.

c. Turvaintsidentide käsitlemisega seotud otsustajad tunnevad ja kasutavad prioriteete, arvestades ka turvaintsidentidele 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 intsidentide teadele tavapärasel tööajal ilma viivitusega.

c. Turvaintsidentidest teatamise keskuse töötajad on saanud piisava infoturbe koolituse.

d. Kogu turvaintsidentidega seotud teavet käsitletakse turvaintsidentidest teatamise keskuses konfidentsiaalsena.

DER.2.1.M21 Ekspertühm turvaintsidentide käsitlemiseks (C-I-A)

a. Turvaintsidentide käsitlemiseks on moodustatud kogunud ja usaldusväärsetest töötajatest koosnev ekspertühm. Ekspertühm on varustatud piisavate tehniliste ja rahaliste ressurssidega.

b. Ekspertühma liikmetel on organisatsiooni süsteemide analüüsimiseks hea ettevalmistus. Ühema liikmed tegelevad pideva teadmiste täiendamisega nii kasutusele võetud süsteemide kui ka turvaintsidentide avastamise ja nendele reageerimise valdkonnas.

c. Ekspertühma liikmete usaldusvärsust kontrollitakse ning rühma koosseisu uuendatakse vastavalt vajadusele.

d. Ekspertühma liikmed on kaasatud intsidentide eskalatsiooni- ja teavituskanalitesse.

e. Ekspertühm on lõimitud intsidentide halduse korraldusse (vt DER.2.1.M8 *Turvaintsidentide käsitlemise töörühm*), ekspertühma vastutus on määratud ja kooskõlastatud (vt DER.2.1.M3 *Vastutuste ja kontaktisikute määramine*).

DER.2.1.M22 Turvaintsidentide käsitlemise korralduse läbivaatus (C-I-A)

a. Turvaintsidentide käsitlemise korraldust ning sellega seotud mõõdetavaid näitajaid (nt turvaintsidentide avastamisel, intsidentidest teavitamisel ja intsidentide eskaleerimisel) hinnatakse regulaarselt.

b. Turvaintsidentide käsitlemise toimivust kontrollitakse nii plaanitud läbivaatuste kui etteteatamiseta läbivaatuste teel. Kontrollimine on eelnevalt juhtkonnaga kooskõlastatud.

c. Praktilise kogemuse saamiseks harjutatakse intsidendikäsitlemist simuleeritud turvaintsidentidega.

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

DER. Avastamine ja reageerimine

DER.2: Turvaintsidentide haldus

DER.2.2: IT-kriminalistika võimaldamine

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

1.1 Eesmärk

Esitada meetmed infoturvaintsidentide 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

Andmekaitse spetsialist, vastutav spetsialist, organisatsiooni juhtkond.

1.3 Piirangud

Moodul ei sisalda ründetuvastuse meetmeid (vt [DER.1 Turvaintsidentide avastamine](#)). Samuti ei selgitata kriteeriume ja protsesse otsustamiseks kriminalistikauuringu vajalikkust, see tehakse turvaintsidentide käsitlemise ajal (vt [DER.2.1 Turvaintsidentide käsitlemine](#)).

Samuti ei hõlma moodul õigusrikkumistega seotud õiguskaitseorganite poolt läbiviidavaid turvakriminalistika ekspertiise.

2 Ohud

Sisukord

[2.1 Õiguslike raamtingimuste rikkumine](#)

[2.2 Asitõendite kaotus puuduliku turbe tõttu](#)

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

Sisukord

[3.1 Elutsükkel](#)

[Kavandamine](#)

[3.2 Põhimeetmed](#)

[DER.2.2.M1 Andmekäitluse õiguslike raamtingimuste järgimine \[andmekaitespetsialist, organisatsiooni juhtkond\]](#)

[DER.2.2.M2 Esmameetmete juhend infoturvaintsidendi puhuks](#)

[3.3 Standardmeetmed](#)

[DER.2.2.M3 Kriminalistikateenuse tarnijate kaardistamine](#)

[DER.2.2.M4 Kriminalistikauuringu seotus kriisi- ja intsidendihaldusega](#)

[DER.2.2.M5 Infoturvaintsidendi asitõendite turbe juhend](#)

[DER.2.2.M6 Personali koolitus IT-kriminalistika alal](#)

[DER.2.2.M7 IT-kriminalistika töövahendite õige valimine](#)

[DER.2.2.M8 Asitõendite õige valimine ja järjestamine \[vastutav spetsialist\]](#)

[DER.2.2.M9 Analüüsitavate andmete õige valimine \[vastutav spetsialist\]](#)

[DER.2.2.M10 Asitõendite IT-kriminalistikaturve \[vastutav spetsialist\]](#)

[DER.2.2.M11 Asitõendite turbe dokumenteerimine \[vastutav spetsialist\]](#)

[DER.2.2.M12 Originaal-andmekandjate ja asitõendite turvaline säilitus \[vastutav spetsialist\]](#)

[3.4 Kõrgmeetmed](#)

[DER.2.2.M13 Raamlepingud kriminalistikateenuse tarnijatega \(C-I-A\)](#)

[DER.2.2.M14 Tüüpprotseduurid asitõendite turbeks \(C-I-A\)](#)

[DER.2.2.M15 Asitõendite turbe õppused \(C-I-A\)](#)

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 [andmekaitse spetsialist, organisatsiooni juhtkond]**

- a. Kriminalistikauuringu tarbeks andmete kogumine ja analüüs viiakse läbi õigusaktidega lubatud piires (vt [ORP.5 Vastavushaldus \(nõuetehaldus\)](#)).
- b. Andmete töötlemine kooskõlastatakse andmekaitse spetsialistiga. 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 valdkonnaüleised teavitusteed ja vastutajad, kontaktisikud on vajadusel kättesaadavad.

DER.2.2.M5 Infoturvaintsidentide asitõendite turbe juhend

a. On koostatud asitõendite turbe juhend, mis sisaldab meetodeid, tehnilisi vahendeid, õiguslikke raamtingimusi ja dokumenteerimise nõuded 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 originaalasiitõendeid 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. Protseduurid 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)

- a. Kriminalistikauuringu ja analüüsiga seotud töötajad harjutavad regulaarselt infoturvaintsidentide asitõendite turbe rakendamist.

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetusskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

DER. Avastamine ja reageerimine

DER.2: Turvaintsidentide haldus

DER.2.3: Ulatuslike turvaintsidentide lahendamine

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

1.1 Eesmärk

Esitada meetmed ulatuslike turvaintsidentide lahendamiseks.

Käesolevas moodulis käsitletakse ulatusliku turvaintsidentide näitena kinnisrünnet. Moodul kirjeldab, kuidas taastada kinnisrünnete 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 kinnisrünnete intsidentide käsitlemist, üldine turvaintsidentide haldus on esitatud moodulites [DER.1 Turvaintsidentide avastamine](#) ja [DER.2.1 Turvaintsidentide käsitlemine](#).

Moodul ei hõlma kinnisründe sissetungijälgede avastamist turvarikkemärkide (ingl *indicator of compromise*) abil ega tagauste (ingl *backdoor*) tuvastamist.

2 Ohud

Sisukord

[2.1 Lahendamise puudulikkus](#)

[2.2 Jälgede hävitamine](#)

[2.3 Ründaja enneaegne alarmeerimine](#)

[2.4 Andmete kaotus ja IT-süsteemi tõrge](#)

[2.5 Võrguteabe muutmata jätmise pärast kinnisrünnet](#)

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 intsidendi 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 võrgusegmentid. IT-süsteemide seiskamine mõjutab teenuste käideldavust. Kui intsidendi lahendamine kestab kaua, võib see põhjustada märkimisväärseid kahjusid.

2.5 Võrguteabe muutmata jätmise 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

Sisukord

[3.1 Elutsükel](#)

3.2 Põhimeetmed[DER.2.3.M1 Juhtrühma rajamine](#)[DER.2.3.M2 Lahendusstrateegia valimine](#)[DER.2.3.M3 Mõjutatud võrguosade isoleerimine](#)[DER.2.3.M4 Pääsuandmete ja krüptovõtmete blokeerimine ja muutmine](#)[DER.2.3.M5 Algse sissetungitee sulgemine](#)[DER.2.3.M6 Tööseisundi taastamine](#)**3.3 Standardmeetmed**[DER.2.3.M7 IT-süsteemi sihipärane tugevdamine](#)[DER.2.3.M8 Ründekäsitluse sidekanalite turve](#)[DER.2.3.M9 Mõjutatud IT-süsteemide asendamine](#)**3.4 Kõrgmeetmed**[DER.2.3.M10 Ümberkujundused sama ründaja uue ründe takistamiseks \(C-I\)](#)

3.1 Elutsükkel**Kavandamine ja algatamine**

DER.2.3.M1 Juhtrühma rajamine

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 rajamine**

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 märkamatuks.

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 värskest 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 kinnisründe 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. Vältitakse 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 Ründekäsitle 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

- a. Suure kaitsetarbega IT-süsteemide korral vahetatakse riistvara pärast kinnisründe intsidenti täielikult välja.
- b. 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 ebanormaalse tegevusmuustrite 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 privilegieeritud kontode haldusvahendeid.
- **Välise 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.

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

DER. Avastamine ja reageerimine

DER.3: Infoturbe hindamine

DER.3.1: Auditid ja läbivaatused

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

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 soovitude 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

Sisukord

- [2.1 Turvameetmete puudulik või plaanimata rakendamine](#)
 - [2.2 Turvameetmete toimetu või ebamajanduslik rakendamine](#)
 - [2.3 Infoturbe halduse süsteemi puudulik rakendamine](#)
 - [2.4 Kontrollija puudulik kvalifikatsioon](#)
 - [2.5 Keskpika perioodi plaanimise puudumine](#)
 - [2.6 Puudulik auditi plaanimine ja kooskõlastamine](#)
 - [2.7 Isikuandmete kasutamise kooskõlastamatus](#)
 - [2.8 Sihilik turvaprobleemide varjamine](#)
-

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 auditiplan 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 andmekaitse spetsialisti 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 tegematajätmissi. Seetõttu võib infoturbe hetkeseisust jääda ebatäpne ülevaade.

3 Meetmed

Sisukord

[3.1 Elutsükkel](#)

[3.2 Põhimeetmed](#)

[DER.3.1.M1 Vastutaja määramine \[organisatsiooni juhtkond\]](#)

[DER.3.1.M2 Auditi ettevalmistamine](#)

[DER.3.1.M3 Auditi läbiviimine \[auditirühm\]](#)

[DER.3.1.M4 Infoturbe läbivaatuse sooritamine \[infoturbe läbivaatuse rühm\]](#)

[3.3 Standardmeetmed](#)

[DER.3.1.M5 Lõimimine infoturbeprotsessi](#)

[DER.3.1.M6 Kontrollimisaluse ja ühtse hindamissüsteemi kehtestamine](#)

[DER.3.1.M7 Auditikava](#)

[DER.3.1.M8 Läbivaatuste objektide loend](#)

[DER.3.1.M9 Sobiv auditi- või läbivaatusrühm \[auditirühm, infoturbe läbivaatuse rühm\]](#)

[DER.3.1.M10 Auditiplaani või läbivaatuse plaani koostamine \[auditirühm, infoturbe läbivaatuse rühm\]](#)

[DER.3.1.M11 Teavevahetuse ja kontrollide läbiviimise kord \[auditirühm, infoturbe läbivaatuse rühm\]](#)

[DER.3.1.M12 Auditi avakoosolek \[auditirühm\]](#)

[DER.3.1.M13 Dokumentide ülevaatus ja kontroll \[auditirühm, infoturbe läbivaatuse rühm\]](#)

[DER.3.1.M14 Pistelised kontrollid \[auditirühm, infoturbe läbivaatuse rühm\]](#)

[DER.3.1.M15 Sobivad kontrollimeetodid \[auditirühm, infoturbe läbivaatuse rühm\]](#)

[DER.3.1.M16 Kohapealse kontrolli tegevuskava \[auditirühm\]](#)

[DER.3.1.M17 Kohapealse kontrolli kord \[auditirühm, infoturbe läbivaatuse rühm\]](#)

[DER.3.1.M18 Intervjuude läbiviimine \[auditirühm\]](#)

[DER.3.1.M19 Riskikäsitusplaani läbivaatus \[auditirühm\]](#)

[DER.3.1.M20 Lõpukoosolek \[auditirühm\]](#)

[DER.3.1.M21 Tulemuste hindamine \[auditirühm\]](#)

[DER.3.1.M22 Auditi aruanne \[auditirühm\]](#)

[DER.3.1.M23 Läbivaatuse tulemuste dokumenteerimine \[infoturbe läbivaatuse rühm\]](#)

[DER.3.1.M24 Auditi või läbivaatuse lõpetamine \[auditirühm, infoturbe läbivaatuse rühm\]](#)

[DER.3.1.M25 Järeldoimingud ja järelkontroll](#)

[DER.3.1.M26 Auditikava jälgimine ja kohandamine](#)

[DER.3.1.M27 Auditite ja läbivaatuste dokumentide säilitamine ja arhiveerimine](#)

[3.4 Kõrgmeetmed](#)

[DER.3.1.M28 Audiitorite taustakontroll \(C-I\)](#)

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 Teavevahetuse 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 Riskikäsitusplaani 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 Järeldoimingud 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 käsitusala 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 ülevaatus, testimisi ja kohapealseid kontrole.
- c. Kohapealsete kontrollide käigus ei tohi audiitorid sekkuda iseseisvalt IT-süsteemide töösse ega anda otseseid tegevusjuhiseid kontrolliobjekti muutmiseks.
- d. Audititulemused dokumenteeritakse ja vormistatakse kirjaliku auditiaruandena.
- e. Auditiaruanne esitatakse määratud kontaktsikule kokkulepitud tähtajal.

DER.3.1.M4 Infoturbe läbivaatuse sooritamise [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 juhtlähivaataja 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 auditiplaani.

DER.3.1.M13 Dokumentide ülevaatus ja kontroll [auditirühm, infoturbe läbivaatuse rühm]

- a. Dokumente vaadatakse üle vastavalt kontrolliraamistikus ettenähtud korrale.
- b. Dokumentide ülevaatus käigus kontrollitakse, kas dokumendid on ajakohased, terviklikud ja arusaadavad.
- c. Dokumentide ülevaatus 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 intervjuueringimist (vt DER.3.1.M18 *Intervjuude läbiviimine*) või dokumentide ülevaatus (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 Riskikäsitusplaani 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 riskikäsitusplaanis ettenähtud meetmed rakendatud.

DER.3.1.M20 Lõpukoosolek [auditirühm]

- a. Auditi lõpetamisel korraldab auditirühm koos auditeeritava organisatsiooni asjaomaste vastutajatega lõpukoosoleku.
- b. Lõpukoosolekul esitletakse esialgseid audititulemusi 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 tähtjaks 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 audititulemusi 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 lepatakse kokku tulemuste avaldamise õigused ja piirangud, kaasaarvatud selle, et audititulemusi ei edastataks ilma kontrollitud organisatsiooni nõusolekuta muudele organisatsioonidele.

DER.3.1.M25 Järeloimingud 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 käsitusala 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 arhiveerimistähtaaja 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

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetusskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

DER. Avastamine ja reageerimine

DER.3: Infoturbe hindamine

DER.3.2: Infoturbe vastavusauditid

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

1.1 Eesmärk

Esitada juhised auditeeritavale organisatsioonile infoturbe vastavusauditite korraldamiseks. Infoturbe vastavusauditi eesmärk on tagada vastavus õigusaktidega ja organisatsioonisisesel 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 relevantssed muude vastavusauditite puhul.

Moodul ei ole piisav sõltumatute sertifitseerimisauditite (nt ISO27001 sertifitseerimisauditi) läbiviimiseks.

2 Ohud

Sisukord

- [2.1 Väliste turbesuuniste rikkumine](#)
 - [2.2 Turvameetmete puudulik või plaanimata rakendamine](#)
 - [2.3 Turvameetmete toimetu või ebamajanduslik rakendamine](#)
 - [2.4 Infoturbe halduse süsteemi puudulik rakendamine](#)
 - [2.5 Audiitori puudulik kvalifikatsioon](#)
 - [2.6 Huvide konflikt organisatsioonisiseses auditirühmas](#)
 - [2.7 Keskpika perioodi plaanimise puudumine](#)
 - [2.8 Puudulik auditi plaanimine ja kooskõlastamine](#)
 - [2.9 Personaliesindusega kooskõlastamatus](#)
 - [2.10 Sihilik lahknemuste ja probleemide varjamine](#)
 - [2.11 Kaitset vajava teabe leke](#)
-

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 külguksiga). 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 igapäevatoos, 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 tegematajätmissi. 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

Sisukord

[3.1 Elutsükk](#)

[3.2 Põhimeetmed](#)

[DER.3.2.M1 Infoturbe auditite vastutaja määramine \[organisatsiooni juhtkond\]](#)

[DER.3.2.M2 Auditite läbiviimise juhend](#)

[DER.3.2.M3 Kontrollimisaluse määramine](#)

[DER.3.2.M4 Infoturbe vastavusauditite kavandamine](#)

[DER.3.2.M6 Infoturbe auditi ettevalmistamine \[auditirühm\]](#)

[DER.3.2.M8 Auditiaruannete säilitamine](#)

[3.3 Standardmeetmed](#)

[DER.3.2.M9 Infoturbe vastavusauditite lõimimine infoturbeprotsessi](#)

[DER.3.2.M10 Teabevahetus](#)

[DER.3.2.M22 Infoturbe auditi järeletegevused](#)

[3.4 Kõrgmeetmed](#)

3.1 Elutsükk

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 käsitusala 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 audititsükli 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 seis.

d. Parandusmeetmete rakendamise põhjal otsustatakse täiendava infoturbe järelauditi vajadus, sellisel juhul kohandatakse auditikava.

3.4 Kõrgmeetmed

Antud moodulis kõrgmeetmed puuduvad.

4 Lisateave

Lühend	Publikatsioon
[E-ITS-J3]	Eesti infoturbestandard. Auditeerimisjuhend, 2021
[EISAÜ]	Eesti Infosüsteemide Audiitorite Ühing, Infosüsteemide audiitorkontrolli eeskirjad, 1997, https://eisay.ee/infosusteemide-auditorkontrolli-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

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetusskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

DER. Avastamine ja reageerimine

DER.4: Avariiahaldus

1 Kirjeldus

Sisukord

[1.1 Eesmärk](#)

[1.2 Vastutus](#)

[1.3 Piirangud](#)

1.1 Eesmärk

Esitada meetmed infoturbe ja jätkuvuse halduse tagamiseks avariiolukordades.

1.2 Vastutus

Avariiahalduse meetmete täitmise eest vastutab avariijuht.

Lisavastutajad

Infoturbejuht, organisatsiooni juhtkond, personaliosakond, ülemus.

1.3 Piirangud

Selles moodulis ei esitata avariiahalduse käivitamise kriteeriume, asjakohane otsus tehakse turvaintsidendi käsitlemise ajal (vt [DER.2.1 Turvaintsidentide käsitlemine](#)).

Kriise käsitletakse eraldi kriisihalduse raames, millel on antud mooduliga üksnes kokkupuutepunktid (nt avariiolukordade edasise laiendamise raames).

2 Ohud

Sisukord

[2.1 Personali väljalangemine](#)

[2.2 IT-süsteemi tõrge](#)[2.3 Laivõrgu \(WAN\) tõrge](#)[2.4 Hoone avarii](#)[2.5 Tarnija või teenuseandja teenuse katkemine](#)

2.1 Personali väljalangemine

Personali väljalangemine laiemalt (nt epideemia või streigi tõttu) või oluliste võtmeisikute lahkumine võib organisatsiooni 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

Sisukord

[3.1 Elutsükel](#)[3.1 Põhimeetmed](#)[3.2 Standardmeetmed](#)[DER.4.M1 Avariiteatmik](#)[DER.4.M2 Avariihalduse lõimimine üleorganisatsioonilistesse protsessidesse \[infoturbejuht\]](#)[3.3 Kõrgmeetmed](#)[DER.4.M3 Avariihalduse käsitusala ja strateegia \[organisatsiooni juhtkond\] \(C-I-A\)](#)[DER.4.M4 Avariihalduse poliitika ja juhtkonna vastutus \[organisatsiooni juhtkond\] \(C-I-A\)](#)[DER.4.M5 Avariihalduse korraldus \[organisatsiooni juhtkond\] \(C-I-A\)](#)[DER.4.M6 Vajalike ressursside olemasolu \[organisatsiooni juhtkond\] \(C-I-A\)](#)[DER.4.M7 Avariikontseptsioon \[organisatsiooni juhtkond\] \(C-I-A\)](#)[DER.4.M8 Töötajate kaasamine avariihalduse protsessi \[ülemus, personaliosakond\] \(C-I-A\)](#)[DER.4.M9 Avariihalduse lõimimine üleorganisatsioonilistesse protsessidesse \[organisatsiooni juhtkond\] \(C-I-A\)](#)[DER.4.M10 Testid ja avariioppused \[organisatsiooni juhtkond\] \(C-I-A\)](#)[DER.4.M12 Avariihalduse protsessi dokumenteerimine \(C-I-A\)](#)[DER.4.M13 Avariihalduse süsteemi läbivaatus ja juhtimine \[organisatsiooni juhtkond\] \(C-I-A\)](#)[DER.4.M14 Avariimeetmete regulaarne läbivaatus ja täiustamine \[organisatsiooni juhtkond\] \(C-I-A\)](#)

[DER.4.M15 Avariiahalduse süsteemi toimivuse hindamine \[organisatsiooni juhtkond\] \(C-I-A\)](#)

[DER.4.M16 Väljasttellitavate komponentide avariivalmendus \[organisatsiooni juhtkond\] \(C-I-A\)](#)

3.1 Elutsükkel

Kavandamine ja algatamine

DER.4.M1 Avariiteatmik

DER.4.M2 Avariiahalduse lõimimine üleorganisatsioonilistesse protsessidesse

Lisanduvad kõrgmeetmed

DER.4.M3 Avariiahalduse käsitusala ja strateegia

DER.4.M4 Avariiahalduse poliitika ja juhtkonna vastutus

DER.4.M5 Avariiahalduse korraldus

DER.4.M6 Vajalike ressursside olemasolu

DER.4.M7 Avariikontseptsioon

DER.4.M8 Töötajate kaasamine avariiahalduse protsessi

DER.4.M9 Avariiahalduse lõimimine üleorganisatsioonilistesse protsessidesse

DER.4.M10 Testid ja avariioõppused

DER.4.M12 Avariiahalduse protsessi dokumenteerimine

DER.4.M13 Avariiahalduse süsteemi läbivaatus ja juhtimine

DER.4.M14 Avariimeetmete regulaarne läbivaatus ja täiustamine

DER.4.M15 Avariiahalduse 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. Avariolukorras 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 tüüpvariide (nt tulekahju) tegutsemisjuhistega, muudatused avariiteatmikus tehakse avariihaldusesse kaasatud töötajatele teatavaks.

e. Avariiteatmik on avariihaldusesse kaasatud töötajatele avariolukorras 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 avariioõppused [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 Avariiahalduse süsteemi toimivuse hindamine [organisatsiooni juhtkond] (C-I-A)

a. Avariiahalduse süsteemi toimivust ja tõhusust hinnatakse regulaarselt vastavalt määratud mõõtmis- ja hindamiskriteeriumitele, tulemust võrreldakse eelmiste hindamiste tulemustega.

b. Hindamistulemustest teavitatakse juhtkonda, kes otsustab avariiahalduse täiustamise. Juhtkonna otsused dokumenteeritakse.

DER.4.M16 Väljasttellitavate komponentide avariivalmendus [organisatsiooni juhtkond] (C-I-A)

a. Väljasttellitavate komponentide avariivalmenduse kavandamisel hindab juhtkonna määratud vastutaja tarnija või teenuseandja avariiahalduse küpsustaset.

b. Avariitestid ja -õppused kooskõlastatakse tarnija või teenuseandjaga, vajaduse korral korraldatakse ühisõppusi.

c. Teavet testitulemuste, kontrollide ja täiustusmeetmete kohta vahetatakse tarnija või teenuseandjaga regulaarselt.

4 Lisateave

Siin lisateavet ei ole

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetuskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

Auditeerimisjuhend

Märkus: Tegemist on Eesti Infoturbestandardi "Auditeerimisjuhendi" 2021 aasta uuendatud DRAFT versiooniga.

Sisukord

- [1. Sissejuhatus](#)
- [2. Mõisted ja lühendid](#)
- [3. E-ITS auditi eesmärk](#)
- [4. Auditi kohustus](#)
- [5. E-ITS auditi eeldused](#)
- [6. Audititsükli üldine korraldus](#)
- [7. E-ITS auditi tellimine](#)
- [8. Nõuded E-ITS audiitorile](#)
- [9. E-ITS eelaudit](#)
- [10. E-ITS põhiaudit](#)
- [11. E-ITS vaheaudit](#)
- [12. Lõpparuanne ja järeldusotsus](#)
- [13. Auditijärgsed tegevused](#)
- [14. Seonduvad dokumendid](#)

1. Sissejuhatus

1.1. Käesolev dokument annab juhiseid Eesti infoturbestandardi (edaspidi E-ITS) põhise sõltumatu auditi (edaspidi E-ITS audit, audit) läbiviimiseks. E-ITS auditite läbiviimise üldised põhimõtted on sätestatud [viide õigusaktile].

1.2. Juhend on mõeldud auditi läbiviijale (E-ITS audiitor, audiitorettevõtte), auditi tellijale ja auditeeritavale organisatsioonile (E-ITS rakendav organisatsioon, asutus, ettevõtte). Auditeeritav organisatsioon saab juhendi põhjal ülevaate auditi läbiviimise eeltingimustest, auditi hanke ettevalmistamisest ja auditi kvaliteedi hindamisest. E-ITS audiitorile annab juhend juhised auditi kavandamiseks, läbiviimiseks ja tulemi vormistamiseks.

2. Mõisted ja lühendid

Nr	Termin või	Lähtekeeles	Lühike definitsioon
		(inglise	

	lühend	/saksa)	
1	Audiitor (E-ITS audiitor)	<i>auditor</i>	E-ITS auditit läbi viiv isik, auditirühma liige
2	Auditeeritav	<i>auditee</i>	Asutus või selle osa, mida auditeeritakse
3	audiitorettevõtte	<i>auditing entity</i>	Auditeerimislepingu alusel E-ITS auditit teostav ettevõtte (vt p 5. <i>Auditeerimise korraldus</i>)
4	auditirühm	<i>audit team</i>	Audiitoritest ja tehnilistest ekspertidest koosnev rühm auditite läbiviimiseks
5	audititsükel	-	Seadusest tulenev E-ITS auditeerimisperiood (pikkusega kolm aastat), pärast mida tuleb läbi viia uus E-ITS põhiaudit.
6	E-ITS	-	Eesti infoturbestandard
7	E-ITS audit, audit	-	Eesti infoturbestandardi põhine sõltumatute pädevate isikute sooritatav süstemaatiline, sõltumatu ja dokumenteeritud protsess infoturbe halduse süsteemi ja infoturbe protsesside läbivaatuseks, asitõendite kogumiseks, asitõendite objektiivseks hindamiseks ja tulemuste teatamiseks auditeeritavale
8	ISMS	<i>ISMS</i>	Infoturbe halduse süsteem (ingl <i>information security management system</i>)
9	juhtaudiitor	<i>lead auditor</i>	E-ITS audiitor, kes juhib auditirühma tööd, vastutab auditi läbiviimise eest ja allkirjastab auditi aruanded. Juhtaudiitoril on olemas auditi läbiviimiseks vajalik kvalifikatsioon (p 8. <i>Nõuded E-ITS audiitorile</i>)
10	kaitseala	<i>Informationsverbund</i> (saksa k.)	Turbekontseptsiooni koostamise ja rakendamise käsitusala. Organisatsioon liigitab kaitsealasse kogumi sihtobjekte, mida turbeprotsess hakkab edaspidi kaitsma.
11	kaitsetarve	<i>Schutzbedarf</i> (saksa k)	Vara väärtusest tulenev vajadus seda kaitsta. ISO/IEC 21964: andmete ja teabe omadus, väljendab vajadust kaitsta teda kahju eest, mille võib tekitada konfidentsiaalsuse, tervikluse ja/või käideldavuse rikkumine. Standard BSI 200 laiendab kaitsetarve ka äriprotsessile
12	käsitusala	<i>scope</i>	Auditi kontekstis: Auditi käsitusalasse kuuluvad äriprotsessid ja sihtobjektid
13	lahknevus	<i>nonconformity</i>	Erinevus standardi meetmes kirjeldatud ja tegeliku olukorra vahel
14	risk	<i>risk</i>	Määramatuse mõju, sh ohu võimekus tekitada organisatsioonile kahju
15	sihtobjekt	<i>Zielobjekt</i> (saksa k)	Kaitsealasse kuuluv kaitsetarbega vara (rakendus, IT komponent, komponendirühm, taristu, personal, allüksus jne)
16	äriprotsess	<i>business process</i>	Organisatsiooni tegevuse element, mingi eesmärgi saavutamisele suunatud tegevuste, toimingute või protseduuride kogum. Äriprotsessi tulemusena luuakse kliendile väärtust ning võivad tekkida tooted või teenused

3. E-ITS auditi eesmärk

3.1. E-ITS auditi eesmärk on hinnata, kas auditeeritava organisatsiooni infoturbe halduse süsteem ning selle raames rakendatud meetmed vastavad organisatsiooni eesmärkidele, on kooskõlas äriprotsessidega, on vastavuses küberturvalisuse seaduse ja Eesti infoturbestandardi ISMS nõuete dokumendiga (E-ITS [ISMS. Nõuded](#)). E-ITS auditi läbiviimisel arvestatakse infoturbe ohtudest tulenevaid riske ja auditeeritava organisatsiooni riskitaluvust.

4. Auditi kohustus

4.1. E-ITS auditi kohustus tuleneb [viide õigusaktile], ning E-ITS-i rakendava organisatsiooni eesmärkidest ja lepingulistest kohustustest.

4.2. E-ITS audit on soovitatav läbi viia ka organisatsioonidel, kellel auditi kohustust ei ole, kuid kes on riigi, kohaliku omavalitsuse või muu avalik-õigusliku isiku või avalikke ülesandeid täitva eraõigusliku isiku andmetöötluspartnerid või kelle äriprotsessid on auditi kohuslasega muul viisil seotud.

4.3. E-ITS auditi kohustus ei rakendu organisatsioonidele, kelle vastavust standardile ISO/IEC 27001 on nõutud kaitseala osas kinnitatud ISO/IEC 27006 kohaselt akrediteeritud sertifitseerija väljastatud ning ajaliselt kehtiva sertifikaadiga.

5. E-ITS auditi eeldused

5.1. Auditi läbiviimise eelduseks on toimiva infoturbe halduse süsteemi olemasolu vastavalt dokumendi - E-ITS [ISMS. Nõuded](#) ja E-ITS etalonturbe meetmete kataloogi viimase 12 kuu jooksul avaldatud versioonile.

5.2. Auditi käsitusala on üheselt arusaadavalt piiritletud ja dokumenteeritud.

5.3. Auditeeritav on sooritanud järgnevad tegevused:

5.3.1. käsitusalasse jäävatele äriprotsesside ja varade kaardistus, sh väliste infoturbealaste nõuete tuvastamine (nt regulatsioonid, lepingud);

5.3.2. kaitsetarbe määramine;

5.3.3. turbeviisi kinnitamine;

5.3.4. etalonturbe meetmete valik ja kinnitamine;

5.3.5. meetmete rakendamise analüüs ja vastutajate määramine;

5.3.6. infoturbe dokumentatsiooni koostamine ja uuendamine;

5.3.7. riskianalüüsi läbi viimine (vajadusel);

5.3.8. infoturbe rakendusplaani koostamine ja täitmine kinnitatud tegevusplaani alusel.

5.4. Kui äriprotsesside kaitsetarve on erinev normaalsest, on organisatsioon läbi viinud IT riskianalüüsi. Soovituslik metoodika riskianalüüsi läbiviimiseks on esitatud dokumendis - E-ITS [Riskihaldusjuhend](#).

5.5. Organisatsiooni infoturbe dokumentatsioon on vastavuses dokumendiga - E-ITS [ISMS. Nõuded](#).

5.6. Infoturbe dokumentatsiooni kuuluvad poliitikad ja eeskirjad on organisatsiooni juhtkonna poolt kinnitatud vähem kui 24 kuud tagasi, alates E-ITS põhiauditi alguskuupäevast.

5.7. E-ITS rakendamise käigus on organisatsioon koostanud infoturbe rakendusplaani. Infoturbe rakendusplaan sisaldab minimaalselt:

5.8.1. rakendatavate E-ITS moodulite loetelu;

5.8.2. iga mooduli E-ITS turvameetmeid koos meetmete rakendatuse määraga. Meetmete rakendatuse hinnang peab andma audiitorile piisava ja tõepärase sisendinfo meetmepõhiste kontrollide läbiviimiseks.

5.8.3. meetmekohaseid viiteid organisatsiooni poliitikatele, eeskirjadele või juhenditele;

5.8.4. meetmete rakendamise eest vastutajaid;

5.8.5. meetme teadliku mitterakendamise puhul juhtkonna vastavat otsust ja põhjendust.

6. Audititsükli üldine korraldus

6.1. Auditeerimiseks sõlmitakse audiitorettevõttega auditeerimisleping.

6.2. Auditeerimislepingu kestvus on üks E-ITS audititsükkel (kolm aastat). E-ITS auditeerimisleping sisaldab järgmiste, ühte E-ITS audititsükklisse jäävate auditite läbiviimist:

6.2.1. E-ITS eelaudit;

6.2.2. E-ITS põhiaudit;

6.2.3. E-ITS järelaudit (vajadusel);

6.2.4. E-ITS vaheaudit(id).

6.3. Auditiriski vähendamiseks ei tohi E-ITS audiitor või audiitorettevõtte viia ühes organisatsioonis E-ITS auditid läbi järjest rohkem kui kahe audititsükli vältel.

6.4. Enne auditiprotseduuridega alustamist sõlmitakse audiitorettevõtte ja auditeeritava organisatsiooni vahel konfidentsiaalsusleping.

6.5. Enne esmakordset E-ITS auditit või audiitorettevõtte vahetumisel viiakse organisatsioonis esmalt läbi E-ITS eelaudit (p 9 [E-ITS Eelaudit](#)). E-ITS põhiauditi läbiviimiseks peab eelaudit lõppema positiivse tulemusega.

6.6. E-ITS eelauditi ja E-ITS põhiauditi vaheline ajavahemik võib olla maksimaalselt kuus kuud. Selle aja jooksul auditeeritav organisatsioon puuduste ilmnemisel kõrvaldab puudused auditi eeldustena käsitletavate tööde osas.

6.7. Auditiprotseduurid viiakse läbi koostöös auditeeritava organisatsiooni kontaktisikuga, kes korraldab organisatsiooni võtmeisikute kättesaadavuse auditi plaanimise ja läbiviimise ajal. Põhjendatud erandjuhtudel tohib auditiprotseduure teostada kaugtöö vormis (sellisel juhul kajastatakse see fakt auditi aruandes).

6.8. Kui E-ITS põhiauditi käigus ilmneb kõrge riskitasemega lahknevusi standardist (p 12.7), viiakse kõrge riskitasemega lahknevuste osas läbi järelaudit (p 13. [Auditijärgsed tegevused](#)).

6.9. Üks aasta pärast E-ITS põhiauditit või pärast olulisi muudatusi infoturbe kaitsealas (nt pärast äriprotsesse oluliselt mõjutavate IT-süsteemide juurutamist või kaitseala laiendamist) viiakse muudatustest mõjutatud käsitusala osas läbi E-ITS vaheaudit (p 11. [E-ITS vaheaudit](#)).

6.10. E-ITS järel- ja vaheauditite kavandamise etapis teavitab auditeeritav organisatsioon E-ITS audiitorit muudatustest organisatsiooni äriprotsessides, süsteemis toimuvatest muudatustest ja toimunud infoturbe intsidentidest.

6.11. Kolmeaastase audititsükli jooksul tehakse vähemalt kaks E-ITS vaheauditit.

6.12. Infoturbe halduse süsteemi toimimine ja jätkusuutlikkus fikseeritakse kirjalikus lõpparuandes ja järelendusotsuses, otsus kehtib kuni järgmise E-ITS põhiauditi järelendusotsuse avaldamiseni.

6.13. Audiitorettevõtte võib järelauditite või vaheauditite järgselt oma hinnangut muuta, esitades organisatsiooni juhtkonnale muudetud ja allkirjastatud järelendusotsuse.

7. E-ITS auditi tellimine

7.1. E-ITS auditi tellija võib tellida E-ITS auditi korraga rohkem kui ühele auditeeritavale organisatsioonile.

7.2. E-ITS auditi läbiviimise vajadusest teatatakse E-ITS audiitorile või audiitorettevõttele üldjuhul vähemalt kaks kuud ette. Järelauditi ja vaheauditite tellimine ja läbiviimine võib pooltevahelisel kokkuleppel toimuda ka lühema etteteatamistähtajaga.

7.3. E-ITS auditi tellimisel kirjeldab tellija üheselt ja arusaadavalt auditi käsitusala, sealhulgas auditeerimisele määratud äriprotsesse ja nende kaitsetarvet ning erisusi.

7.4. Tellija esitab rakendatavate E-ITS etalonturbe moodulite nimekirja, andmetöötluse asukohad ja kasutatavad töökeeled, arvutikasutajate arvu, infoturbe meeskonna ja IT-meeskonna suuruse.

7.5. Kui käsitusalasse kuuluvaid andmeid töödeldakse mitmes erinevas asukohas, peab E-ITS auditi tellija määrama hankekutses ja lepingus minimaalse asukohtade arvu, milles audit läbi viiakse. Asukohtade valik ja asukohtade arv peab tagama kõikide asukohatüüpide proportsionaalse esindatuse. Kui andmeid töödeldakse kolmes või vähemas erinevas asukohas (välja arvatud pilvteenuse tarnija asukohad), viiakse auditiprotseduurid läbi kõigis asukohtades.

7.6. Käsitusala auditi läbiviimise käigus ei muudeta.

7.7. Tellija toob hankekutses eraldi välja, kui asukohas kohapealseid auditiprotseduure pole võimalik läbi viia (nt õigusaktidest või teenuseandjaga sõlmitud kokkulepetest tulenevalt).

7.8. Kui organisatsioon tellib E-ITS auditit mitmendat korda, lisab ta hankekutsele viimase auditi järelalusotsuse.

7.9. Tellija võib hankekutses esitada oma nägemuse auditi töömahule.

7.10. Hankekutse põhjal peab E-ITS audiitoril või audiitorettevõttel olema võimalik adekvaatselt hinnata auditiprotseduuride läbiviimisega seotud tööaega ja kulusid. E-ITS auditi hinnastamisel tugineb audiitorettevõtte auditi tellija poolt punktide 7.3 - 7.7 kohaselt esitatud teabele.

7.11. E-ITS järelauditi ja täiendavate E-ITS vaheauditite tellimine toimub auditeerimislepingus kokkulepitud tingimuste ja kehtiva audiitori tunni- või päevahinna alusel.

7.12. Auditi tellimisel tuleb määratleda auditeeritava(te) organisatsiooni(de) kontaktisikud.

8. Nõuded E-ITS audiitorile

8.1. E-ITS auditi viib läbi vastava kutseoskusega juhtaudiitor, kes juhib auditirühma tööd, vastutab auditi käigus teostatavate tööde eest ja kes allkirjastab auditi lõppraporti.

8.2. Juhtaudiitoril on auditi läbiviimise aja vältel vähemalt üks kehtiv sertifikaat järgnevatest:

8.2.1. Infosüsteemide sertifitseeritud audiitori CISA (*Certified Information Systems Auditor, CISA*) sertifikaat, mille väljaandjaks on ISACA;

8.2.2. ISO 27001 juhtiva audiitori sertifikaat, mille väljaandjaks on IRCA (*International Register of Certificated Auditors*);

8.2.3. ISO 27001 juhtiva audiitori sertifikaat, mille väljaandjaks on PECB (*Professional Evaluation and Certification Board*).

8.3. Juhtaudiitor on auditile eelneva kolme kalendriaasta jooksul osalenud vähemalt kolmes infoturbe halduse süsteemi auditis (sh E-ITS ja ISKE auditid). Juhtaudiitoril on vähemalt nelja-aastane IT auditi, IT juhtimise või infoturbe alane töökogemus.

8.4. Auditi läbiviimisesse võib kokkuleppel tellijaga kaasata teisi audiitoreid ja tehnilisi eksperte. Kaasatud audiitorid ja eksperdid töötavad juhtaudiitori koordineerimisel.

8.5. Auditirühma kaasatud audiitoritel on vähemalt kahe-aastane IT auditi, IT juhtimise või infoturbe alane töökogemus.

8.6. Auditirühma kaasatud tehnilistel ekspertidel on auditeerimisobjekti spetsiifikast tulenev tehniline kvalifikatsioon või vähemalt kahe-aastane IT halduse või infoturbe alane töökogemus.

8.7. Auditirühma liikmed (juhtaudiitor, teised audiitorid ja kaasatud eksperdid) peavad olema auditeeritavast organisatsioonist sõltumatud ja ei tohi olla osalenud auditeeritava organisatsiooni infoturbe halduse süsteemi kavandamises või rakendamises, sh organisatsiooni konsulteerimises auditeeritavas valdkonnas, auditi alguskuupäevale eelneva kolme aasta jooksul.

8.8. Auditirühma liikmete sõltumatus peab olema kinnitatud vastava isiku poolt allkirjastatud deklaratsiooniga.

8.9. Auditirühma liikmed peavad tagama oma kohustuste täitmise käigus teatavaks saanud informatsiooni konfidentsiaalsuse. Organisatsiooni poolt sisendina antud isikuandmete töötlemisel, sh isikuandmeid sisaldavate dokumentide läbivaatusel ja logiandmete ja tuvastussüsteemide andmete kasutamisel, järgib audiitor andmekaitsealaste õigusaktide nõudeid.

8.10. Audiitor peab auditi läbiviimisel järgima tunnustatud auditeerimise standardeid ja suuniseid, infoturbe parimaid tavasid ja audiitori kutse-eetika koodeksit (nt ISACA <https://eisay.ee/kutse-eetika-koodeks>).

8.11. E-ITS audiitor juhendub auditi kavandamisel ja läbiviimisel E-ITS nõuetest ja käesolevast auditeerimisjuhendist. Auditi protseduuride teostamisel järgitakse etalonturbe kataloogi moodulis "[DER.3.2 Infoturbe vastavusauditid](#)" esitatud meetmeid.

8.12. E-ITS auditi kavandamisel ja auditi maksumuse hindamisel peab audiitor pakkumuses eraldi välja tooma auditi ettevalmistamise, dokumentatsiooni läbivaatuse, kohapealsetele auditiprotseduuride läbiviimise, tõendusmaterjalide analüüsimise ning aruannete koostamisega seonduva töömahu hinnangu ja ajaplaani.

9. E-ITS eelaudit

9.1. Eelauditi raames kontrollib audiitor, kas auditeeritav organisatsioon on täitnud auditi eeldustena käsitletavat nõude (p 5 [E-ITS auditi eeldused](#)).

9.2. Eelauditi raames kontrollib audiitor infoturvapoliitika(te) aja- ja asjakohasust, infoturbe rakendusplaani olemasolu ja piisavust.

9.3. Eelauditi aruandes hindab audiitorettevõtte organisatsiooni valmisolekut E-ITS auditi läbiviimiseks ning vajadusel esitab soovitusel auditi eeldustena käsitletavate toimingute sooritamiseks. Eelauditi aruandele ei rakendata lõpparuande sisule ja vormistamisele kehtivaid nõudeid (p 12 [Auditi lõpparuanne](#)).

10. E-ITS põhiaudit

10.1. E-ITS põhiauditi käigus kontrollib audiitor vastavust dokumendile - E-ITS [ISMS. Nõuded](#) ja infoturbe meetmete rakendatust.

10.2. Enne põhiauditi läbiviimist koostatakse ja kooskõlastatakse auditeeritava organisatsiooniga auditi plaan.

10.3. Audiitor tutvub auditeeritava asutuse eelmise audititsükli auditiaruannetega (kui see on olemas), huvipoolte nõuete ja esitatud kaebuste ning toimunud intsidentidega.

10.4. Audiitor valib ja dokumenteerib kontrollitavaid sihtobjekte ja infoturbe meetmeid järgnevalt:

10.4.1. juhtaudiitor määrab äriprotsessi põhiselt auditeeritavad sihtobjektid ning lisab need auditi plaani, lähtudes käsitusala ulatuses tehtud modelleerimise tulemustest ning organisatsiooni ja auditirühma riskihinnangutest;

10.4.2. iga rakendatava mooduli põhimeetmete täitmist kontrollib audiitor täies ulatuses;

10.4.3. moodulisestest standard- ja kõrgmeetmetest valimi moodustamisel lähtub audiitor organisatsiooni valitud turbeviisist ning moodulikohasest riskihinnangust, tuginedes auditeeritava organisatsiooni riskianalüüsi tulemustele ja mooduliga seotud ohtude hindamisele antud organisatsiooni kontekstis;

10.4.4. täiendavalt kontrollib audiitor käsitusalasle kuuluvaid sihtobjekte ja meetmeid, millega seoses varasemate infoturbe auditite käigus oli tuvastatud puudusi.

10.5. Audiitor hindab infoturbe dokumentatsiooni asjakohasust ja täielikkust, dokumentatsioonist tulenevate turvameetmete rakendamist ja dokumendis - E-ITS [ISMS. Nõuded](#) esitatud nõuete täidetust.

10.6. Audiitor hindab riske äriprotsessidele, mis tulenevad meetmete mitterakendamisest või osalisest rakendamisest mooduliga seotud ohtude põhiselt, arvestades organisatsiooni spetsiifikat ja varade kaitsetarvet.

10.7. Audiitor hindab organisatsioonis toimunud intsidente ja organisatsiooni valmisolekut juhuks, kui sarnane intsident korduks.

10.8. Audiitor viib hinnangu kujundamiseks läbi intervjuusid, vaatlusi, ringkäike, meetmete toimimise teste ning dokumentatsiooni läbivaatuseid.

10.9. Auditi tõendusmaterjali võib auditeeritav audiitorile kas väljastada, kohapeal näidata või demonstreerida intervjuu käigus (nt võrguskeem, logide analüsaator, tulemüüri reeglid, õiguste süsteemi selgitamisel reaalsed isikute põhised näited).

10.10. Kui dokumentidega tutvumine toimub kohapeal, tagatakse audiitorile selleks vajalik töökoht ja töötingimused.

10.11. Auditeeritava organisatsiooni teenuseandjate turvalisuse hindamisel võib audiitor oma hinnangu kujundamisel tugineda teenuseandja (nt pilvteenuse tarnija) esitatud auditi käsitusala hõlmavatele turvasertifikaatidele ja vastavusauditite aruannetele.

10.12. E-ITS põhiaudit lõpeb auditi lõpparuande ja järeldusotsuse esitamisega (p 12 [Lõpparuanne ja järeldusotsus](#)).

11. E-ITS vaheaudit

11.1. E-ITSi vaheauditid peavad koos põhiauditiga katma kogu auditi käsitusala nii, et iga äriprotsessi suhtes saaks audititsükli jooksul auditeeritud kõigi asjakohaste moodulite rakendatus.

11.2. E-ITS vaheauditi käigus hindab audiitor:

11.2.1. E-ITS põhiauditi järgselt tehtud muudatuste mõju infoturbele;

11.2.2. E-ITS põhiauditi käigus tuvastatud lahknevuste käsitlemist;

11.2.3. eelmisest põhi- või vaheauditi valimi väljajätte (vt p 11.1);

11.2.4. organisatsiooni toimetulekut uute ja aktuaalsete infoturbe ohtudega.

11.3. E-ITS vaheauditite sisu käsitusala plaanib auditeeritav organisatsioon E-ITS auditi tellimise käigus (p 7 [E-ITS auditi tellimine](#)).

11.4. E-ITS vaheauditi tellib auditeeritav organisatsioon mitte rohkem kui 12 kuu möödumisel eelmisest auditist (arvestades auditi järeldusotsuse või eelmise vaheauditi tulemuste esitamise ajast). Kui organisatsiooni infoturbe kaitsealas on toimunud olulisi muudatusi (nt pärast äriprotsesse oluliselt mõjutavate IT-süsteemide juurutamist või kaitseala laiendamist), tellitakse audit enne plaanitud tähtaega.

11.5. Vaheauditi läbiviimise täpne aeg määratakse pooltevahelisel kokkuleppel.

11.6. E-ITS vaheauditi käigus tehtud tähelepanekud vormistab audiitor vaheauditi aruandena lähtudes lõpparuande ja järeldusotsuse nõuetest (vt p 12).

11.7. Aruandes esitatud tähelepanekute põhjal on audiitoril õigus muuta auditi järeldusotsust.

12. Lõpparuanne ja järeldusotsus

12.1. Lõpparuanne koosneb kahest eraldi digiallkirjastatud elektroonilisest dokumendist: auditi järeldusotsus ja auditi lõpparuanne.

12.2. Auditi järeldusotsus sisaldab:

12.2.1. auditi läbiviimise aega;

12.2.2. käsitusala kirjeldust;

12.2.3. vastavushinnangut valitud E-ITS turbeviisile;

12.2.4. audiitori üldhinnangut riskihaldusele ja meetmete rakendamisele;

12.2.5. audiitori üldhinnangut organisatsiooni infoturbe halduse süsteemi toimimisele.

12.3. Auditi järeldusotsus ei sisalda konfidentsiaalset teavet. Auditeeritav organisatsioon tohib auditi järeldusotsust jagada kolmandatele osapooltele.

12.4. E-ITS põhiauditi lõpparuanne koosneb järgmistest osadest:

12.4.1. auditi kokkuvõte, kus tuuakse välja auditi läbiviimise aeg ja koht, auditi käsitusala (sh loend auditeeritud äriprotsessidest), turbeviis (põhiturve, standardturve või tuumikuturve), võimalikud piirangud auditi läbiviimisel ja audiitori üldhinnang infoturbe halduse süsteemi toimimise kohta. Audiitori üldhinnangust esitatakse ka auditi käigus kinnitust saanud positiivsed aspektid;

12.4.2. auditi ajaplaan ja auditi läbiviimise töömaht;

12.4.3. auditis osalenud auditeeritava organisatsiooni töötajad ja auditirühma liikmed ning nende rolli kirjeldus;

12.4.4. audiitori hinnang infoturbe halduse süsteemi vastavusele dokumendile - E-ITS [ISMS. Nõuded](#) (p 10.5);

12.4.5. audiitori hinnang E-ITS meetmete rakendatuse kohta mooduligruppide (ISMS, ORP, CON jne) lõikes;

12.4.6. auditi lõpparuande lisadena vormistatud tõendusmaterjal.

12.5. Auditi lõpparuandes annab audiitor hinnangu järgmistele infoturbe halduse süsteemi aspektidele:

12.5.1. kas infoturbe eest vastutajad on määratud;

12.5.2. kas kaitseala ja äriprotsessidega seotud varad on määratud piisava detailsuse ja täpsusega;

12.5.3. kas varade kaitsetarve on määratud asjakohaselt, tuginedes organisatsiooni poolt antud sisendile regulatsioonide, lepingute ja äriprotsessidest tulenevate nõuete kohta (sh hinnatakse kaitsetarbe ülevaatamise sagedust ja protseduure);

12.5.4. kas etalonturbe moodulite ja meetmete valik ja dokumenteerimine on läbi viidud korrektselt;

12.5.5. kas riskianalüüsi tulemusena lisandunud meetmed on asjakohased ja vastavad organisatsiooni eesmärkidele;

12.5.6. kas valitud turbeviis, turbekontseptsiooni teostus, sh meetmete rakendamine, vastab organisatsiooni vajadustele ja E-ITS nõuetele.

12.6. Audiitor analüüsib meetmete mitterakendamise põhjendusi ning hindab meetmete mitterakendamisest või osalisest rakendamisest tulenevaid riske järgnevalt:

- **Kõrge risk** - oluline lahknevus meetmes kirjeldatu ja tegeliku olukorra vahel. Meetme mitterakendamisest tulenevate riskide realiseerumisel võib tekkida suur kahju organisatsiooni varadele ja tegevusele. Kahju toime põhjustab lepingute ja regulatsioonide nõuete rikkumisi, võib ähvardada äriprotsesside jätkusuutlikkust või organisatsiooni olemasolu.
- **Madal risk** - osaline lahknevus meetmes kirjeldatu ja tegeliku olukorra vahel. Riskide realiseerumisel võib tekkida piiratud ja ohjatatav kahju organisatsiooni varadele ja tegevusele nagu lühiajalised töökatkestused.
- **Infoks** - potentsiaalne risk. Vähene lahknevus meetmes kirjeldatu ja tegeliku olukorra vahel. Risk kahju tekkeks on väike või puudub. Osaliselt rakendatud meetmete täielik rakendamine aitab ettevõtte infoturbe halduse süsteemi parendada.

12.7. Audiitor toob E-ITS põhiauditi lõpparuandes eraldi välja:

12.7.1. standardist lahknevused, millest auditi käsitusala osas tulenevad äriprotsessile või äriprotsessidele kõrge riskitasemega riskid;

12.7.2. standardist lahknevused, mille riskitase üksikult võttes on madal, kuid mis koosmõju tõttu või ebasoodsatel asjaolude kokkusattumisel võivad põhjustada kõrge riski ühele või mitmele äriprotsessile.

12.8. Et vältida audititsükli jooksul tekkida võivat nõustamise ja auditeerimise konflikti, ei esita audiitor lõpparuandes konkreetseid soovitusi, kuidas tuleks E-ITS meetmeid rakendada.

12.9. Kui E-ITS rakendav organisatsioon on otsustanud etalonturbe kataloogi moodulit või meedet mitte rakendada, siis audiitor hindab selle mooduli või meetme mitterakendamise põhjenduse piisavust ning selle mitterakendamisest tulenevaid riske äriprotsessidele vähemalt alusotude ja meetmete vastavustabeli alusel.

12.10. E-ITS põhiauditi lõpparuandes esitatud tõendusmaterjal on kontrollitav, viited tõendusmaterjalile on piisavad ja testid korratavad.

12.11. E-ITS põhiauditi lõpparuandes esitatakse aruande lisadena tõendusmaterjal järgmiste asjaolude kohta:

12.11.1. põhiauditi käigus tehtud intervjuude, analüüsitud juhendite, protseduurireeglite jms loend, mille alusel audiitor hinnangu andis;

12.11.2. põhiauditi käigus tehtud testimiste ja kontrolliprotseduuride tööpaberid või vaatlustulemused, mis sisaldavad vähemalt tõendusmaterjali:

- varunduse ja taaste toimimise kohta;
- logimise ja logianalüüsi toimimise kohta;
- pääsuõiguste halduse toimimise kohta;
- ründetuvastuse lahenduse toimivuse kohta;
- intsidendihalduse toimimise kohta;
- kasutajakoolituste kohta;
- teenuste väljasttellimise ja partnerasutuste lepingunõuetest tuleneva turbe seire kohta;
- füüsilise turbe meetmete toimimise kohta.

12.12. Kui audiitor on oma töös osaliselt tuginenud varasema E-ITS või ISO27001 auditi tulemustele, tuuakse auditi aruandes selgelt välja, mis osas ning millisele auditi aruandele audiitor on tuginenud.

12.13. Enne lõpparuande kinnitamist esitatakse auditeeritava asutuse esindajale auditi aruande kavand. Audiitori tähelepanekutes esinevate ebatäpsuste korrigeerimiseks ja täiendavate tõendusmaterjalide esitamiseks on auditeeritaval organisatsioonal aega vähemalt viis tööpäeva.

12.14. E-ITS põhiauditi lõpparuanne esitatakse hiljemalt üks kuu pärast audititoimingute lõpetamist.

12.15. Auditeeritav organisatsioon kinnitab kirjalikult auditi tulemuse vastuvõtmise.

12.16. Kokkuleppel tellijaga võib audiitor tutvustada E-ITS põhiauditi lõpparuannet organisatsiooni juhtkonnale, koguda auditi läbiviimise kohta tagasisidet või leppida kokku täiendavate auditite läbiviimise.

12.17. Auditeeritava asutuse esindajal on õigus esitada audiitori hinnangu või järeldusotsuste kohta audiitorile kirjalik protest. Protesti aktsepteerimisel viib audiitor auditiaruandesse või järeldusotsusesse sisse asjakohased parandused. Protesti mitteaktsepteerimisel lisab audiitor auditi aruande juurde protesti ja selle mitteaktsepteerimise põhjenduse.

12.18. Auditi järeldusotsuse huvitatud osapooltele või auditi aruande ja järeldusotsuse järelevalveasutusele esitab auditi tellija.

13. Auditijärgsed tegevused

13.1. Auditeeritav organisatsioon koostab parandusmeetmete rakendamise tegevuskava, määrab vastutajad ja tähtajad. Infoturbe eest vastutav isik teeb parandusmeetmete rakendamise ülevaatus ja vajadusel ajakohastab rakenduskava.

13.2. Raportis esitatud madala riskitasemega lahknevused (kirjeldatud p 12.7) kõrvaldab auditeeritav organisatsioon mõistliku aja jooksul, kuid mitte hiljem kui audititsükli lõpuks.

13.3. Kõrge riskiastmega lahknevused (kirjeldatud p 12.7) on auditeeritav organisatsioon kohustatud kõrvaldama mitte hiljem kui kuue kuu jooksul.

13.4. Kõrge riskiastmega lahknevuste osas tellib auditeeritav organisatsioon järelauditi. E-ITS järelauditi tellimist käsitleb p 7 [E-ITS auditi tellimine](#).

13.5. Kui säilitustähtaja pikkus ei tulene muudest õigusaktidest või eeskirjadest, säilitab auditeeritav organisatsioon (juhul kui tellija ja auditeeritav organisatsioon on erinevad, siis ka tellija) E-ITS auditi aruandeid ja alusdokumente turvaliselt vähemalt seitse aastat.

13.6. Audiitor säilitab auditi aruandeid ja seonduvaid tööpabereid poolte vahelise kokkuleppe kohaselt, tähtaja määramata jätmisel lähtutakse audiitorettevõtte sisekorrast.

13.7. Auditi aruandeid ja seonduvaid alusdokumente hoitakse turvaliselt ning kaitstakse muudatuste eest. Juurdepääs neile on lubatud üksnes vastava pääsuõigusega isikutel.

14. Seonduvad dokumendid

[E-ITS-S1] E-ITS [ISMS. Nõuded](#)

[E-ITS-J1] E-ITS [Rakendusjuhend](#)

[E-ITS-J2] E-ITS [Riskihaldusjuhend](#)

[E-ITS-K2] [ISMS] | Eesti infoturbestandard. Etalonturbe kataloog. ISMS. Turbehaldus

[E-ITS-K2] [DER] Eesti infoturbestandard. Etalonturbe kataloog. DER. Avastamine ja reageerimine