Vabariigi Valitsuse 9. detsembri 2022. a määrus nr 121
„Võrgu- ja infosüsteemide küberturvalisuse nõuded“
Lisa

Esmased turvameetmed

- Käesolevas lisas sätestatakse määruse § 5[1] lõikes 1 loetletud turbevaldkondades alaliselt rakendatavad esmased turvameetmed.
- Käesolevas lisas esitatud meetmed on ette nähtud kõigile küberturvalisuse seaduses loetletud teenuseosutajatele, kui määruses ei ole sätestatud teisiti.
- Teenuseosutaja võib käesolevas lisas sätestatud meetme asendada muu samaväärse meetmega või jätta meetme rakendamata, kui kaitsetarve on täidetud ja teenuseosutaja on riski aktsepteerinud.

1. Infoturbe korralduse valdkonnas peab teenuseosutaja:
1.1. määrama küberturvalisuse seaduse §-s 6[1] nimetatud juhatuse liikme ja infoturbe eest vastutava isiku;
1.2. välja töötama võrgu- ja infosüsteemide turvareeglid, sealhulgas infoturbe- ja riskijuhtimispõhimõtted, ning tutvustama neid personalile;
1.3. kontrollima regulaarselt, kas valitud turvameetmed vastavad tegelikule vajadusele ja kas turvameetmed on rakendatud. Turvameetmeid tuleb kontrolli tulemuste põhjal korrigeerida;
1.4. tagama oma tegevuse kriisihalduse ja toimepidevuse, sealhulgas oma varundus- ja taasteprotseduuride toimimise;
1.5. tagama võrgu- ja infosüsteemide hankimise, arendamise ja hooldamise turvalisuse, sealhulgas turvahaavatavuste käsitlemise ja avaldamise;
1.6. pidama infotehnoloogiavarade arvestust ja uuendama seda regulaarselt;
1.7. määrama kasutusel olevale infotehnoloogiaseadmele vastutava kasutaja.

2. Kasutajate teadlikkuse, koolituse ja kasutajaõiguste valdkonnas peab teenuseosutaja:
2.1. tutvustama personalile küberhügieeni- ja infoturbereegleid, hindama teadmisi ja tagama neile vastava koolituse, vajaduse korral perioodiliselt;
2.2. juhendama personali infotehnoloogiaseadmete kasutamisel;
2.3. kasutama võrgu- ja infosüsteemides personaalseid pääsuõigusi;
2.4. sulgema pääsuõigused või kontod, mille järele puudub vajadus või mida ei kasutata;
2.5. eelistama mitmeastmelist autentimist;
2.6. hoidma pääsuks vajalikke vahendeid, sealhulgas salasõnu ja räsisid, volitamata isikutele kättesaamatuna;
2.7. kasutama võrgu- ja infosüsteemis ainult selleks mõeldud ning heaks kiidetud seadmeid, teenuseid ja süsteeme;
2.8. kasutama infotehnoloogiaseadmeid ja andmekandjaid heaperemehelikult ning mitte jätma neid järelevalveta.

3. Andmete turbe valdkonnas peab teenuseosutaja:
3.1. hindama, millised andmed ning võrgu- ja infosüsteemid on vajalikud igapäevaseks kasutamiseks, ning kavandama asendusprotseduurid süsteemide tõrgete ja katkestuste korral;
3.2. välja töötama tööks vajalike andmete kasutamise reeglid, sealhulgas teiste isikutega andmete jagamise kohta;
3.3. tagama kasutatava teabe või teiste isikute edastatud teabe, sealhulgas ärisaladuse ja isikuandmete kaitse ning vajaduse korral kasutama ajakohast krüpteerimist;
3.4. eelistama digitaalset lahendust, mis kinnitab oluliste elektrooniliste andmete päritolu ja terviklust, sealhulgas digitaalset allkirjastamist;
3.5. rakendama andmetele juurdepääsu võimaldamisel teadmisvajaduspõhist juurdepääsuhaldust;
3.6. varundama regulaarselt tööks vajalikke andmeid, hoidma varundatud andmeid töösüsteemist eraldi ja testima varukoopiast andmete taastamist;
3.7. tagama andmete kustutamise enne andmekandja kasutamise lõpetamist või edasiandmist.

4. Väliste partnerite halduse valdkonnas peab teenuseosutaja:
4.1. teadma oma väliseid partnereid, sealhulgas oma otseseid tarnijaid, ja nende tausta. Selle teabe põhjal tuleb rakendada asjakohaseid turvameetmeid, lähtudes riigi koostatud avalikest ohuhinnangutest ja riskianalüüsidest;
4.2. võtma turvameetmete asjakohasust kaaludes arvesse välistele partneritele eriomaseid turvahaavatavusi, nende toote üldist kvaliteeti ja küberturvalisusega seotud tavasid, sealhulgas toote turvalise arendamise korda ning Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega muudetakse määrust (EL) nr 910/2014 ja direktiivi (EL) 2018/1972 ning tunnistatakse kehtetuks direktiiv (EL) 2016/1148 (küberturvalisuse 2. direktiiv) (ELT L 333, 27.12.2022, lk 80–152), artikli 22 lõike 1 kohaselt korraldatud kriitilise tähtsusega tarneahelate turvariskide koordineeritud hindamise tulemusi;
4.3. kokku leppima väliste partneritega kirjalikult taasesitatavas vormis andmete vahetamiseks vajalikud turvanõuded ja kasutatava teenuse tingimused.

5. Küberintsidentide halduse valdkonnas peab teenuseosutaja:
5.1. koolitama personali, kuidas ära tunda intsidente, kuidas tuvastada nende mõju ja ulatust ning kuidas neid vältida ja kuidas intsidentide puhul toimida;
5.2. määrama isiku, kes koordineerib intsidentide lahendamist, asjaomaste asutuste ja koostööpartnerite teavitamist ning on nende kontaktisik;
5.3. kokku leppima alternatiivsed teavituskanalid juhuks, kui tavapärane teabevahetus ei toimi;
5.4. võtma kasutusele abinõud intsidendi mõju vähendamiseks ja leviku piiramiseks.

6. Pilvteenuste ja veebirakenduste kaitse valdkonnas peab teenuseosutaja:
6.1. kasutama turvalist ja ajakohastatud veebibrauserit;
6.2. jälgima, et pilvteenuste vahendusel jagataks teavet vaid teadmisvajaduspõhiselt;
6.3. järgima turvalise e-kirjavahetuse põhimõtteid ja vältima tundmatute manuste või hüperlinkide avamist;
6.4. tutvustama personalile turvaliste telefoni- ja videokõnede tegemise põhimõtteid;
6.5. eristama ja vältima ebaturvaliste veebilehtede ja rakendusliideste kasutamist;
6.6. pidama arvestust kasutatavate pilvteenuste ja nendega seotud riskide üle.

7. Infotehnoloogiaseadmete kaitse valdkonnas peab teenuseosutaja:
7.1. kasutama ajakohast viirusetõrjet ja tulemüüri;
7.2. uuendama regulaarselt kasutatavaid operatsioonisüsteeme ja rakendusi;
7.3. pidama arvestust kasutatava tarkvara, selle turvahaavatavuste ja litsentside üle ning uuendama litsentse õigel ajal;
7.4. kasutama turvalist, usaldusväärset ja kehtiva toega tarkvara, sealhulgas eemaldama infotehnoloogiaseadmetest ja telefonidest tarkvara, mis on aegunud või mida ei kasutata;
7.5. eristama seadmetes kasutaja- ja süsteemi haldusõigusi ning kasutama tavapärases tegevuses vähem privilegeeritud kasutajatunnuseid;
7.6. tagama võrgu- ja infosüsteemide ning rakenduste turvasündmuste logimise ja logide kättesaadavuse;
7.7. krüpteerima olulist teavet töötleva seadme kõvaketta ja teavet sisaldavad välised kõvakettad ajakohast krüptograafilist meedet kasutades;
7.8. paigutama võimaluse korral seadmed nii, et need ei oleks kõrvalistele isikutele ligipääsetavad;
7.9. kasutama tööks vajalikes seadmetes, sealhulgas mobiilseadmes pääsukoodi või ekraanilukku;
7.10. kavandama meetmed juhuks, kui seade läheb kaotsi, varastatakse või läheb katki;
7.11. kustutama seadmest kogu teabe enne selle kasutusest kõrvaldamist ja utiliseerimist;
7.12. rakendama asjakohaseid lisaturvameetmeid oma serveri kaitsmiseks;
7.13. rakendama automaatikaseadme või muu andmesideühendusega seadme kasutamise korral lisaturvameetmeid või keelama seadmes andmeside kasutamise, sealhulgas kaughalduse;
7.14. hindama uute seadmete ning info- ja võrgusüsteemide soetamisel võimalikke riske ja rakendama juba plaanimise etapis asjakohaseid turvameetmeid.

8. Sideühenduste ja võrgu kaitse valdkonnas peab teenuseosutaja:
8.1. koostama arvutivõrgu skeemi, sealhulgas pidama võrguseadmete ning võrgule tuge pakkuvate isikute ja nende kontaktandmete arvestust;
8.2. piirama volitamata juurdepääsu infosüsteemidele ja seadmetele väliste võrkude kaudu, kasutades tulemüüri või samaväärset turvalahendust;

8.3. vältima volitamata isikule kaugjuurdepääsu andmist sisevõrgus või pilvteenustes töödeldavale teabele;
8.4. kasutama traadita kohtvõrgu ühenduste korral tugevat salasõna ja turvaprotokolli.

9. Füüsilise turbe valdkonnas peab teenuseosutaja:
9.1. järgima võrgu- ja infosüsteemide kasutusele võtmisel ja kasutamisel tuleohutusnõudeid;
9.2. jälgima, et ruumi sissepääsud, sealhulgas aknad, hoitakse suletuna, kui ruumis ei viibi personali;
9.3. vältima ruumides kõrvaliste isikute liikumist saatjata, eelkõige ruumides, kus hoitakse seadmeid või töödeldakse andmeid;
9.4. pidama arvestust ruumidele, sõidukitele, hoonetele ja muule varale juurdepääsu võimaldavate vahendite üle, sealhulgas kaardid, koodid ja võtmed;
9.5. rakendama meetmeid hoonesse või ruumidesse loata sisenemise takistamiseks;
9.6. piirama juurdepääsu võrguseadmete, hooneautomaatika ja serveri asukohale, sealhulgas hoidma vastavaid tehnilisi ruume ja seadmeid lukustatuna.