EELNÕU
26.04.2022

VABARIIGI VALITSUS

MÄÄRUS

Võrgu- ja infosüsteemide küberturvalisuse nõuded

Määrus kehtestatakse küberturvalisuse seaduse § 7 lõike 5 alusel.

1. peatükk
Üldsätted

§ 1. Reguleerimisala

Määrusega kehtestatakse küberturvalisuse seaduse §-s 7 sätestatud kohustuste täitmise ja süsteemide küberturvalisuse tagamiseks:

1) volitus üleriigilise küberturvalisuse tagamise korraldamise eest vastutavale ministrile Eesti infoturbestandardi ning süsteemide turvameetmete erinõuete kehtestamiseks;

2) süsteemide turvameetmete üldnõuded;

3) süsteemide turvameetmete erinõuded ja nende kohaldamise ulatus.

§ 2. Terminid

Käesolevas määruses kasutatakse termineid järgmises tähenduses:

1) andmekogu on andmekogu avaliku teabe seaduse § 43^1 lõike 1 tähenduses;

2) infoturve on süsteemile turvameetmete loomise, valimise ja rakendamise protsesside kogum;

3) pilvsüsteem on süsteem või süsteemi osa, mille pidamist teostab teenuse osutaja pilvandmetöötlusteenust kasutades.

2. peatükk
Eesti infoturbestandard

§ 3. Eesti infoturbestandardi kehtestamise volitus

(1) Eesti infoturbestandardi kehtestab üleriigilise küberturvalisuse tagamise korraldamise eest vastutav minister määrusega.

(2) Süsteemi turvalisuse tagamiseks rakendatud meetmete vastavust Eesti infoturbestandardile eeldatakse ka juhul, kui on täidetud kõik järgmised tingimused:

1) teenuse osutaja rakendatud turvameetmed vastavad rahvusvahelise standardiga ISO/IEC 27001 kehtestatud nõuetele;

2) teenuse osutaja on esitanud Riigi Infosüsteemi Ametile kehtiva vastavussertifikaadi, mis kinnitab punktis 1 sätestatud kohustuse täitmist.

§ 4. Eesti infoturbestandardi auditeerimine

(1) Teenuse osutaja viib läbi Eesti infoturbestandardi tingimuste täitmise auditi iga kolme aasta järel.

(2) Teenuse osutaja edastab lõike 1 alusel läbiviidud auditi järeldusotsuse Riigi Infosüsteemi Ametile 30 päeva jooksul selle kättesaamisest.

(3) Lõigetes 1 ja 2 sätestatut ei kohaldata:

1) teenuse osutajale, kellel on majandusaasta jooksul keskmiselt alla 10 töötaja ja kelle aasta bilansimaht või aastakäive ei ületa 2 miljonit eurot, arvestades mikroettevõtjate määratlusi Euroopa Komisjoni soovituses 2003/361/EÜ mikro-, väikeste ja keskmise suurusega ettevõtjate määratlemise kohta (ELT L 124, 20.05.2003, lk 36–41);

2) muuseumile, rahvaraamatukogule, etendusasutusele, kohaliku omavalitsuse üksuse ametiasutuse hallatavale asutusele ja osavalla või linnaosa ametiasutuse hallatavale asutusele, kui tegemist ei ole haridusasutusega, andmekogu vastutava töötlejaga või volitatud töötlejaga.

3. peatükk
Turvameetmete nõuded

1. jagu

Turvameetmete üldnõuded

§ 5. Teenuste kaardistuse ja turvameetmete dokumentatsioon

(1) Teenuse osutaja dokumenteerib enda teenused, teenuste haldamise süsteemid, nendele rakendatavad turvameetmed ja riskianalüüsi.

(2) Teenuse osutaja säilitab lõikes 1 nimetatud dokumentatsiooni vähemalt seitse aastat alates selle koostamisest ning teeb vastava taotluse korral selle Riigi Infosüsteemi Ametile kättesaadavaks.

(3) Teenuse osutaja võib lõikes 1 nimetatud dokumentatsiooni koostada muu õigusakti alusel koostatava dokumendi osana.

§ 6. Riskianalüüsi ajakohastamine

Teenuse osutaja ajakohastab riskianalüüsi:

1) viivitamatult pärast olulise mõjuga küberintsidendi toimumist;

2) viivitamatult pärast teenuse osutamiseks kasutatava süsteemi sellist muutust, mis mõjutab süsteemi turvalisust või

3) hiljemalt kolme aasta möödumisel viimasest ajakohastamisest.

2. jagu
Turvameetmete erinõuded

1. jaotis

Andmekogu

§ 7. Turvameetmete nõuete erisused andmekogu pidamisel

(1) Andmekogu vastutav töötleja korraldab andmekogu turbeastme ja andmete turvaklassi määramise, andmekogu andmete turvaklassi määramiseks andmete tähtsuse hindamise ning andmete turvalisuse puudumisest tuleneva kahjude hindamise.

(2) Andmekogu andmetele määratud turvaklass ja andmekogu turbeaste kooskõlastatakse koos andmekogu registreerimiseks või andmekogu andmete ajakohastamiseks ettevalmistatava tehnilise dokumentatsiooniga avaliku teabe seaduse § 43^9 lõike 1 punkti 6 alusel kehtestatud õigusaktis sätestatud korras.

(3) Andmekogu vastutav töötleja ja andmekogu majutav volitatud töötleja rakendab turvameetmed andmekogu kasutusele võtmise ajaks.

(4) Andmekogu vastutav töötleja ja andmekogu majutav volitatud töötleja rakendab andmekogu pidamisega seotud süsteemide turvameetmeid andmekogu turbeastmest lähtuvalt.

§ 8. Andmekogu turbeastme määramine

(1) Turbeaste võib olla kõrge (H), keskmine (M) või madal (L).

(2) Andmekogu turbeaste määratakse lähtuvalt andmete turvaklassist. Kui andmete turvaklassi vähemalt üks osaklass vastab tasemele 3, siis on andmekogu turbeaste kõrge (H). Kui andmete turvaklassi vähemalt üks osaklass vastab tasemele 2, siis on andmekogu turbeaste vähemalt keskmine (M). Muul juhul on andmekogu turbeaste vähemalt madal (L).

§ 9. Andmete turvaklassi määramine

(1) Andmete turvaklass määratakse vastavalt infoturbe eesmärkidele tervikluse, konfidentsiaalsuse ja käideldavuse parameetrite kaudu.

(2) Andmete käideldavus on eelnevalt kokku lepitud vajalikul ja nõutaval tööajal kasutamiskõlblike andmete õigeaegne ning hõlbus kättesaadavus (st vajalikul ja nõutaval ajahetkel ning vajaliku ning nõutava aja jooksul) selleks volitatud isikule või tehnilisele vahendile.

(3) Andmete terviklus on andmete õigsuse, täielikkuse ja ajakohasuse tagatus ning päritolu autentsus ja volitamatute muutuste puudumine.

(4) Andmete konfidentsiaalsus on andmete kättesaadavus ainult selleks volitatud isikule või tehnilisele vahendile.

(5) Andmete turvaklass on kombinatsioon andmete käideldavuse (K), tervikluse (T) ja konfidentsiaalsuse (S) turvaosaklasside tasemetest. Andmete turvaklassi tähis moodustatakse osaklasside tähistest nende järjestuses KTS (näiteks K2T3S1).

§ 10. Andmete turvaosaklasside määramine

(1) Andmete turvaosaklass on andmete tähtsusest tulenev infoturbe eesmärgi saavutamise nõutav tase.

(2) Andmekogu vastutav töötleja määrab andmete käideldavuse, tervikluse ja konfidentsiaalsuse turvaosaklasside tasemed vastavalt käesolevas paragrahvis sätestatud skaalale. Turvaosaklasside taseme määramisel lähtub andmekogu vastutav töötleja järgnevast:

1) andmetega seotud nõuded tulenevalt õigusaktidest ja lepingulistest kohustustest;

2) andmetega seotud nõuded tulenevalt pakutavate teenuste iseloomust;

3) küberintsidentidest tekkivate kahjude olulisus.

(3) Andmete käideldavuse alusel määratakse turvaosaklass järgmisest skaalast lähtuvalt:

1) K0 – töökindlus – pole oluline, jõudlus – pole oluline;

2) K1 – töökindlus – 90% (lubatud summaarne seisak nädalas ~ ööpäev); lubatav nõutava reaktsiooniaja kasv tippkoormusel – tunnid (1÷10);

3) K2 – töökindlus – 99% (lubatud summaarne seisak nädalas ~ 2 tundi); lubatav nõutava reaktsiooniaja kasv tippkoormusel – minutid (1÷10);

4) K3 – töökindlus – 99,9% (lubatud summaarne seisak nädalas ~ 10 minutit); lubatav nõutava reaktsiooniaja kasv tippkoormusel – sekundid (1÷10).

(4) Andmete tervikluse alusel määratakse turvaosaklass järgmisest skaalast:

1) T0 – info allikas, muutmise ega hävitamise tuvastatavus ei ole olulised; info õigsuse, täielikkuse ja ajakohasuse kontroll pole vajalik;

2) T1 – info allikas, selle muutmise ja hävitamise fakt peavad olema tuvastatavad; info õigsuse, täielikkuse ja ajakohasuse kontroll erijuhtudel ja vastavalt vajadusele;

3) T2 – info allikas, selle muutmise ja hävitamise fakt peavad olema tuvastatavad; vajalik on info õigsuse, täielikkuse ja ajakohasuse perioodiline kontroll;

4) T3 – info allikas, selle muutmise ja hävitamise faktil peab olema tõestusväärtus; vajalik on info õigsuse, täielikkuse ja ajakohasuse kontroll reaalajas.

(5) Andmete konfidentsiaalsuse alusel määratakse turvaosaklass järgmisest skaalast:

1) S0 – avalik info: juurdepääsu teabele ei piirata (st lugemisõigus on kõigil huvitatutel, muutmise õigus on määratud tervikluse nõuetega);

2) S1 – info asutusesiseseks kasutamiseks: juurdepääs teabele on lubatav juurdepääsu taotleva isiku teadmisvajaduse korral;

3) S2 – salajane info: info kasutamine on lubatud ainult teatud kindlatele kasutajate gruppidele, juurdepääs teabele on lubatav juurdepääsu taotleva isiku teadmisvajaduse korral;

4) S3 – ülisalajane info: info kasutamine on lubatud ainult teatud kindlatele kasutajatele, juurdepääs teabele on lubatav juurdepääsu taotleva isiku teadmisvajaduse korral.

(6) Turvaosaklassi määramisel lähtutakse andmestiku enim kaitset vajavate andmete infoturbe tasemest.

§ 11. Turvameetmete rakendamine andmekogu turbeastmest lähtuvalt

(1) Paragrahvi 7 lõikes 4 sätestatud kohustuse täitmiseks peab andmekogu vastutav töötleja ja andmekogu majutav volitatud töötleja Eesti infoturbestandardi järgimisel lähtuma kaitsealast, mis hõlmab vähemalt kõiki andmekogu pidamisega seotud süsteeme, määrama kõikidele andmekogu pidamisega seotud süsteemidele ja teenustele vähemalt andmekogu turbeastmele vastava kaitsetarbe ning rakendama Eesti infoturbestandardi etalonturbe standardturve turbeviisi.

(2) Turbeastmele kõrge (H) vastav Eesti infoturbestandardi kaitsetarve on väga suur (VS), turbeastmele keskmine (M) vastav Eesti infoturbestandardi kaitsetarve on suur (S) ning turbeastmele madal (L) vastav Eesti infoturbestandardi kaitsetarve on normaalne (N).

(3) Paragrahvi 7 lõikes 4 sätestatud kohustus loetakse täidetuks, kui andmekogu vastutav töötleja ja andmekogu majutav volitatud töötleja on täitnud kõik § 3 lõikes 2 sätestatud tingimused.

2. jaotis
Avalike ülesannete täitmist oluliselt mõjutavad süsteemid

§ 12. Avalike ülesannete täitmist oluliselt mõjutavate süsteemide loetelu

Süsteemid, millel on oluline mõju riigi ja kohaliku omavalitsuse üksuse võimele täita avalikke ülesandeid, on:

1) e-toimiku süsteem;

2) elektrooniline kataster;

3) elektrooniline kinnistusraamat;

4) kommertspandiregister;

5) maksukohustuslaste register;

6) mittetulundusühingute ja sihtasutuste register;

7) rahvastikuregister;

8) riigi- ja kohaliku omavalitsuse asutuste riiklik register;

9) Riigi Teataja infosüsteem;

10) riigikassa infosüsteem;

11) sotsiaalkaitse infosüsteem;

12) äriregister.

§ 13. Avalike ülesannete täitmist oluliselt mõjutavate süsteemide pidamise nõuded

Paragrahvis 12 nimetatud süsteemide andmekoosseis, vajadusel koos andmekoosseisu kasutamiseks vajaliku toimiva rakenduskihiga, varundatakse välisriigiga sõlmitud rahvusvahelise lepingu alusel regulaarselt välisriigis asuvasse turvalisse andmekeskusesse.

3. jaotis

Pilvsüsteem

§ 14. Nõuete kohaldamise ulatus

(1) Käesolevas jaotises sätestatud nõudeid kohaldatakse pilvsüsteemide pidamisele. Jaotises sätestatud pilvsüsteemi pidamise nõuete vastuolu korral määruses või selle alusel kehtestatud nõuetega kohaldatakse käesolevas jaotises sätestatud nõudeid.

(2) Jaotises sätestatud nõudeid kohaldatakse üksnes küberturvalisuse seaduse § 3 lõikes 4 loetletud asutusele, kogule või isikule (edaspidi *kasutaja*).

§ 15. Tehniliste suvandite kehtestamise volitus

Küberturvalisuse korraldamise eest vastutav minister võib määrusega kehtestada pilvsüsteemi pidamiseks kasutatava pilvandmetöötlusteenuse kohustuslikud tehnilised suvandid.

§ 16. Pilvsüsteemi pidamiseks kasutatav pilvandmetöötlusteenus

(1) Pilvsüsteemi pidamiseks kasutab kasutaja pilvandmetöötlusteenust, mille pakkujast ei tulene kõrget riski pilvsüsteemi turvalisusele.

(2) Kasutaja hindab enne pilvandmetöötlusteenuse kasutamist, kas pilvandmetöötlusteenuse pakkujast tuleneb kõrge risk pilvsüsteemi turvalisusele.

(3) Pilvandmetöötlusteenuse pakkujast tuleneva riski hindamisel arvestatakse muu hulgas teavet selle kohta, kas pilvandmetöötlusteenuse pakkuja:

1) asukoht või peakontor on riigis (edaspidi *asukohariik*), mis ei ole Euroopa Liidu, Põhja-Atlandi Lepingu Organisatsiooni (edaspidi *NATO*) või Majandusliku Koostöö ja Arengu Organisatsiooni (edaspidi *OECD*) liikmesriik;

2) asukohariigis eiratakse demokraatliku õigusriigi põhimõtteid või ei austata inimõigusi;

3) asukohariigis ei kaitsta muu riigi isikute intellektuaalomandit, isikuandmeid või ärisaladust;

4) asukohariik käitub küberruumis agressiivselt;

5) asukohariigile on Euroopa Liidu, NATO või OECD liikmesriigid omistanud küberrünnakuid;

6) allub sõltumatu kohtuliku kontrollita asukohariigi või muu välisriigi valitsusele või riigiasutusele;

7) asukohariik või muu välisriik võib kohustada teda tegutsema Eesti Vabariigi julgeolekut ohustaval viisil;

8) majandustegevus rikub turupõhise konkurentsi põhimõtteid või puuduvad asukohariigis piisavad tingimused turupõhise konkurentsi põhimõtete järgimiseks;

9) omandistruktuur, organisatsiooniline ülesehitus või juhtimisstruktuur on läbipaistmatu;

10) rahastamine on läbipaistmatu;

11) teenused sisaldavad turvanõrkusi ning nende kõrvaldamiseks on piisavad turvameetmed rakendamata;

12) teenuste toimepidevus on järjepidevalt puudulik, välja arvatud vääramatu jõu tõttu;

13) kasutab oma teenuste pakkumiseks muid pilvandmetöötlusteenuseid, mille pakkuja vastab punktides 1–12 kirjeldatud tingimustele.

§ 17. Pilvsüsteemis töödeldava teabe konfidentsiaalsus

(1) Kasutaja tagab avaliku teabe seaduse § 35 lõike 1 punktides 3^1, 4, 5, 5^1, 5^2, 6, 6^1, 6^2, 9 või 18^1 sätestatud teabe konfidentsiaalsuse pilvandmetöötlusteenuse pakkuja eest pilvsüsteemis, sealhulgas tagab kasutaja loetletud teabe krüpteerimise.

(2) Lõikes 1 sätestatud kohustust ei kohaldata avaliku teabe seaduse § 35 lõike 1 punktis 9 sätestatud teabele ulatuses, milles pilvsüsteemi või selle pidamiseks kasutatavat pilvandmetöötlusteenust kasutatakse kasutaja süsteemide turvalisuse tagamiseks.

(3) Üleriigilise küberturvalisuse tagamise korraldamise eest vastutav minister võib kehtestada määrusega nõuded käesoleva paragrahvi lõikes 1 nimetatud teabe krüpteerimise krüptomaterjalidele.

§ 18. Logimine

(1) Kasutaja edastab või tagab muul moel juurdepääsu Riigi Infosüsteemi Ametile pilvandmetöötlusteenuse kasutamisega kaasnevatele logidele, mis võimaldavad analüüsida peetava pilvsüsteemi turvalisust ohustavaid riske.

(2) Kasutaja kasutab vaid sellist pilvandmetöötlusteenust, mille lõikes 1 nimetatud logidele saab kasutaja juurdepääsu, et pidada pilvsüsteemi:

1) mis töötleb avaliku teabe seaduse § 35 lõike 1 punktides 3^1, 4, 5, 5^1, 5^2, 6, 6^1, 6^2, 9 või 18^1 sätestatud teavet; või

2) mille kaitsetarve on Eesti infoturbestandardi järgi vähemalt suur (S).

§ 19. Pilvsüsteemi terviklus ja käideldavus

(1) Süsteemi, mille kaitsetarve käideldavuse põhikomponendist tulenevalt on Eesti infoturbestandardi järgi vähemalt suur (S), pidamisel pilvsüsteemina peab kasutaja ka alternatiivset süsteemi või meedet. Alternatiivne süsteem või meede peab võimaldama kasutajal jätkata tegevusi, mille toimepidevus tugineb käesolevas lõikes nimetatud pilvsüsteemile.

(2) Lõikes 1 nimetatud alternatiivne süsteem või selle osa võib olla pilvsüsteem, kui see on kasutatav sõltumata lõikes 1 nimetatud pilvsüsteemile pilvandmetöötlusteenuse pakkuja vastava teenuse või selle pakkumiseks kasutatava kolmanda osapoole teenuse osutamisest.

(3) Lõikes 1 nimetatud pilvsüsteemi terviklust või käideldavust mõjutava küberintsidendi korral tagab kasutaja võimekuse rakendada lõikes 1 nimetatud alternatiivset süsteemi või meedet viivitamatult ja kuni küberintsidendi lõppemiseni.

(4) Kui kasutaja ei määra süsteemile kaitsetarvet Eesti infoturbestandardi järgi ning kohaldub § 3 lõige 2, siis loetakse lõikes 1 nimetatud pilvsüsteemiks samaväärse riskitasemega süsteem, mida peetakse pilvsüsteemina.

4. peatükk
Rakendussätted

§ 20. Üleminek Eesti infoturbestandardile

(1) Kui teenuse osutaja haldab riigi või kohaliku omavalitsuse üksuse süsteemi, siis kuni 31. detsembrini 2022. a eeldatakse süsteemi turvalisuse tagamiseks rakendatud meetmete vastavust Eesti infoturbestandardile, kui teenuse osutaja kohaldab nimetatud süsteemi turvalisuse tagamisele avaliku teabe seaduse § 43^9 lõike 1 punkti 4 alusel kehtestatud määruses sätestatud nõudeid.

(2) Kui teenuse osutaja ei halda riigi või kohaliku omavalitsuse üksuse süsteemi, siis kuni 31. detsembrini 2022. a eeldatakse süsteemi turvalisuse tagamiseks rakendatud meetmete vastavust Eesti infoturbestandardile, kui teenuse osutaja rakendab, seirab ja ajakohastab turvameetmeid, millega nähakse ette vähemalt:

1) süsteemide juurdepääsuõiguste haldamine, süsteemi kasutajate identifitseerimine ja autoriseerimine;

2) teenuse osutamiseks vajalikest andmetest regulaarsete varukoopiate tegemine ja protseduurid andmete varukoopiatest taastamiseks;

3) süsteeme käitava ja süsteemides käideldava tarkvara ajakohasus;

4) süsteemides läbiviidavate toimingute logid toimingu teostaja, toimingu liigi ja toimingu teostamise ajaga;

5) tarkvaralised ja riistvaralised lahendused süsteemide turvalisust ohustava tegevuse ning tarkvara tuvastamiseks ja tõrjumiseks ning

6) protseduurid süsteemide turvalisuse või teenuse toimepidevuse taastamiseks.

§ 21. Eesti infoturbestandardi järgimise auditeerimise tähtajad

(1) Teenuse osutaja, kes on Vabariigi Valitsuse 20. detsembri 2007. a määruse nr 252 „Infosüsteemide turvameetmete süsteem“ § 9^1 lõike 1 alusel kohustatud läbi viima turvameetmete süsteemi rakendamise auditeerimist, on kohustatud esmakordse Eesti infoturbestandardi järgimise auditeerimise läbi viima kahe aasta jooksul pärast viimast Vabariigi Valitsuse 20. detsembri 2007. a määruse nr 252 „Infosüsteemide turvameetmete süsteem“ § 9^1 lõike 1 alusel läbi viidud turvameetmete süsteemi auditeerimist.

(2) Teenuse osutaja, kes on Vabariigi Valitsuse 20. detsembri 2007. a määruse nr 252 „Infosüsteemide turvameetmete süsteem“ § 9^1 lõike 2 alusel kohustatud läbi viima turvameetmete süsteemi rakendamise auditeerimist, on kohustatud esmakordse Eesti infoturbestandardi järgimise auditeerimise läbi viima kolme aasta jooksul pärast viimast Vabariigi Valitsuse 20. detsembri 2007. a määruse nr 252 „Infosüsteemide turvameetmete süsteem“ § 9^1 lõike 2 alusel läbi viidud turvameetmete süsteemi auditeerimist, kuid mitte hiljem kui kolme aasta jooksul alates käesoleva määruse jõustumisest.

(3) Teenuse osutaja, kes on Vabariigi Valitsuse 20. detsembri 2007. a määruse nr 252 „Infosüsteemide turvameetmete süsteem“ § 9^1 lõike 3 alusel kohustatud läbi viima turvameetmete süsteemi rakendamise auditeerimist, on kohustatud esmakordse Eesti infoturbestandardi järgimise auditeerimise läbi viima nelja aasta jooksul pärast viimast Vabariigi Valitsuse 20. detsembri 2007. a määruse nr 252 „Infosüsteemide turvameetmete süsteem“ § 9^1 lõike 3 alusel läbi viidud turvameetmete süsteemi auditeerimist, kuid mitte hiljem kui kolme aasta jooksul alates käesoleva määruse jõustumisest.

(4) Käesoleva paragrahvi lõigetes 1–3 nimetamata teenuse osutaja on kohustatud esmakordse Eesti infoturbestandardi järgimise auditeerimise läbi viima hiljemalt kolme aasta jooksul alates Eesti infoturbestandardi järgimise auditeerimise kohustuse tekkimisest.

§ 22. Määruse jõustumine

(1) Käesolev määrus jõustub [*tulevane kuupäev on seotud küberturvalisuse seaduse, avaliku teabe seaduse ja Eesti Rahvusringhäälinud seaduse eelnõu 531 SE jõustumise kuupäevaga, mis jõustub üldises korras*].

(2) Käesoleva määruse §-d 7–11 jõustuvad 1. jaanuaril 2023. a.

(3) Käesoleva määruse §-d 14–19 jõustuvad 1. jaanuaril 2024. a.

Kaja Kallas
Peaminister

Andres Sutt
Ettevõtlus- ja infotehnoloogiaminister

Taimar Peterkop
Riigisekretär