26.09.2017

Küberturvalisuse seaduse eelnõu seletuskiri

1. Sissejuhatus

1.1. Sisukokkuvõte

Euroopa Parlament ja nõukogu võttis vastu 6. juulil 2016. a direktiivi (EL) nr 2016/1148 meetmete kohta, mille eesmärk on tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus (ET 19.07.2016 L 194/1) (edaspidi *NIS direktiiv*). Liikmesriigid on kohustatud vastu võtma ja avaldama direktiivi rakendamiseks vajalikud õigusnormid 9. maiks 2018. NIS direktiiv näeb ette, et riigisiseses õiguses kehtestatakse turvameetmete rakendamise ja teavitamise nõuded olulise teenuse ja digitaalse teenuse osutajatele.

Võrgu- ja infosüsteemide usaldusväärsus ja turvalisus peavad majandus- ja ühiskondlike vajaduste jätkusuutlikuks rahuldamiseks olema tagatud valdkondadeüleselt. NIS direktiivi eesmärk on tagada võrgu- ja infosüsteemide turvalisuse kõrge tase kogu liidus ja NIS direktiiv seab liikmeriikidele ülesandeks täita see sobivate meetmetega, lähtudes riigi eripärast ja kehtivast õiguskorrast.

Eestis on Riigi Infosüsteemi Amet peamine küberintsidentidega tegelev ametiasutus. Praeguses õigusruumis on seaduse tasemel Riigi Infosüsteemi Ameti ülesannetest reguleeritud vaid järelevalvepädevus teatud valdkondade võrgu- ja infosüsteemide turvalisuse üle, mis seisneb kontrollimisfunktsiooni täitmises selle üle, kas ettevõtjad ja asutused järgivad nendes valdkondades sätestatud turvameetmeid. Samal ajal on jäetud seaduse tasandil reguleerimata ohtu ennetavad ja tõrjuvad tegevused, nagu küberintsidentide (sh ka küberrünnakute poolt põhjustatud intsidentide) käsitlemine, hoiatuste ehk ohuteadete andmine küberintsidentide ennetamiseks (näiteks levivate lunavara kampaaniate korral) ning küberturbe seire teostamine. Arvestades, et ülal loetletud tegevused on vajalikud ohtude ennetamiseks ja tõrjumiseks, sätestatakse eelnõus subjektide õigused, kohustused ja vastutus, Riigi Infosüsteemi Ameti kui küberintsidentide ennetamise ja lahendamise eest vastutava asutuse pädevus ja volitused järelevalve teostamisel.

Lisaks eeltoodule sätestatakse käesolevas seaduses kohustus tagada avalike ülesannete täitmisel infosüsteemide turvalisus.

Eelnõu seadusena vastuvõtmiseks on vajalik Riigikogu lihthäälteenamus.

1.2. Eelnõu ettevalmistajad

Eelnõu ja seletuskirja koostasid Majandus- ja Kommunikatsiooniministeeriumi riigi infosüsteemide osakonna nõunik Laura Kask (tel: 639 7645, e-post: laura.kask@mkm.ee) ja küberturbe valdkonna nõunik Madis Raaper (tel: 639 7615, e-post: madis.raaper@mkm.ee), ministeeriumi nõunik Mait Heidelberg (tel: 639 7613, e-post: mait.heidelberg@mkm.ee) ja Riigi Infosüsteemi Ameti õigusnõunik Kristiina Laanest (e-post: kristiina.laanest@ria.ee; tel: 666 8863), õigusvaldkonna peaspetsialist Elsa Neeme (e-post: elsa.neeme@ria.ee; tel: 666 8862) ja juhtivanalüütik Kadri Kaska (e-post: kadri.kaska@ria.ee). Eelnõu juriidilise ekspertiisi tegi Majandus- ja Kommunikatsiooniministeeriumi õigusosakonna nõunik Anne-Ly Normak (tel: 715 3403, e-post: anne-ly.normak@mkm.ee) ja keeletoimetuse Kristiane Liivoja (e-post: kristiane.liivoja@mkm.ee, tel: 625 6370).

1.3. Märkused

Eelnõuga muudetakse elektroonilise side seadust (RT I 2004, 87, 593, RT I 23.03.2017, 6), hädaolukorra seadust (RT I 2009, 39, 262, RT I, 03.03.2017, 6), lennundusseadust (RT I 2003, 23, 143, RT I, 03.03.2017, 16), raudteeseadust (RT I 2004, 18, 131, RT I, 16.05.2017, 3), sadamaseadust (RT I 2009, 37, 251, RT I, 03.03.2017, 24) ja tervishoiuteenuste korraldamise seadust (RT I 2001, 50, 284, RT I, 03.03.2017, 25).

2. Seaduse eesmärk

Küberturvalisuse seaduse eelnõu eesmärgiks on NIS direktiivi ülevõtmine Eesti õigusruumi ning riigisiseste meetmete sätestamine elutähtsa ja ühiskondliku ja majandustegevuse säilitamise seisukohast oluliste võrgu- ja infosüsteemide turvalisuse tagamiseks . NIS direktiivi ülevõtmise otstarbeks on vajalik uue seaduse vastuvõtmine, mis sätestab nii NIS direktiivist tulenevad kohustused kui ka Riigi Infosüsteemi Ameti kui pädeva asutuse õigused teostada järelevalvet ning koordineerida küberintsidentide ennetamist, tuvastamist ja lahendamist. Eelnõuga kehtestatakse küberturvalisuse tagamise põhimõtted, isikute õigused ja kohustused küberturvalisuse tagamisel võrgu- ja infosüsteemides ning järelevalve nende nõuete täitmise üle. NIS direktiivi rakendamisega tugevneb ja ühtlustub küberturbealane koostöö liikmesriikide vahel.

Seaduseelnõu väljatöötamisele eelnes ka väljatöötamiskavatsus (edaspidi *VTK*), mis kooskõlastati erinevate ministeeriumide poolt. Eesti Infotehnoloogia ja Telekommunikatsiooni Liit esitas oma arvamuse ametlikult koos küsimuste ja tähelepanekutega. Kaitseministeerium, Sotsiaalministeerium, Välisministeerium, Siseministeerium ning Justiitsministeerium kooskõlastasid VTK koos märkustega. Kõik ministeeriumid avaldasid toetust uue tervikseaduse loomiseks. Peamiste märkustena toodi välja vajadus selgitada detailsemalt ja põhjendatumalt Riigi Infosüsteemi Ameti kui küberintsidentide ennetamise ja lahendamise eest vastutava asutuse õigusi ja järelevalve sätteid, eelnõu lisandväärtust võrreldes praegu olemasolevate õigusaktidega, kahjude hüvitamise ning vastutuse selgitamise vajadust.

Eelnõu eesmärkideks on:
1. Sätestada elutähtsa ja ühiskondliku ja majandustegevuse säilitamise seisukohast oluliste ning võrgu- ja infosüsteemidest sõltuvate teenuste osutamisel selged ja ühetaolised õigused ja kohustused küberturvalisuse tagamiseks; samuti tagada kooskõlas NIS direktiivis sätestatud nõuetega ühtsed turvalisus- ja teavitamisnõuded ELi siseturul tegutsevatele digitaalsete teenuste osutajatele.
2. Tõhustada olulistest küberintsidentidest ja ohtudest teavitamist, et parandada ühiskonna ja majanduse toimimist mõjutavate küberintsidentide ennetamise, avastamise ning neile reageerimise võimekust. Teavitusmehhanism võimaldab parandada nii riigi kui ka avalikkuse ja erasektori valmisolekut küberintsidentidega toimetulekuks ja suurendada viimaste kaasatust. Samas tagatakse tundliku äriteabe ning isikuandmete kaitse.
3. Parandada teavitamiskohustuse ja intsidentidealase infovahetuse korralduse sätestamise kaudu Euroopa Liidu (edaspidi *EL*) ülest ohuteadlikkust ja reageerimisvõimekust piiriülestele küberintsidentidele.
4. Sätestada alused küberohtude ennetamiseks, väljaselgitamiseks ning tõrjumiseks, sätestades Riigi Infosüsteemi Ameti pädevuse riikliku ja haldusjärelevalve teostamisel.

NIS direktiiv seab eesmärgiks tagada võrgu- ja infosüsteemide turvalisuse kõrge tase kogu EL-is ja seab liikmeriikidele ülesandeks täita see sobivate meetmetega, lähtudes riigi eripärast ja kehtivast õiguskorrast. Laiemaks eesmärgiks on suurendada koostööd EL-i liikmesriikide vahel küberturvalisuse valdkonnas. Eesti jaoks on küberturbe valdkonnas oluline, et vastastikku jagataks rohkem kogemusi, oskusi, tehnoloogiaid ja teavet riiklikus küberruumis toimuva kohta. NIS direktiiv võimaldab üksteise informeerimise, abistamise ning ühiselt reageerimise kaudu parandada usaldust ja turvalisust kogu EL-is.

NIS direktiivi ülevõtmise ajaraami arvestades ei ole seaduseelnõuga võimalik kogu kübervaldkonna normide laiapõhjaline revisjon, mistõttu puudutab eelnõu väljatöötamispakett eelkõige NIS direktiivi ülevõtmise ja järelevalvemeetmetega seonduvat. Järelevalve sätted reguleerivad riikliku järelevalve tegemiseks pädeva asutuse ning tema kasutada olevate riikliku järelevalve erimeetmete loetelu ning mõningaid erisusi. Riikliku järelevalve sätete puhul on arvesse võetud korrakaitseseadust (edaspidi *KorS,* RT I, 02.12.2016, 6). Kuna NIS direktiivi eesmärk on anda järelevalveasutusele piisavad õigused, et NIS direktiivi eesmärke ellu viia, on eelnõus sätestatud järelevalvemeetmed põhjendatud ja kohased, et sekkuda võrgu- ja infosüsteemi turvalisust ähvardava või realiseerunud ohu korral ohu väljaselgitamiseks või tõrjumiseks proportsionaalsel viisil, vältides ohu süvenemist või laienemist teistele süsteemidele. Samuti jätab NIS direktiiv ühemõtteliselt liikmesriikidele võimaluse kehtestada vajalikud meetmed avaliku korra (avaliku turvalisuse) tagamiseks. Seega toetavad ja täiendavad direktiivi turvalisus- ja teavitusnõuded ning järelevalvemeetmed teineteist ning täidavad sama eesmärki: tagada Eesti võrgu- ja infosüsteemide kõrge turvalisus kooskõlas direktiivi eesmärgiga.

Küberturvalisuse valdkonna reguleerimise vajaduse tingib riigi, majanduse ja ühiskonna sõltuvus e-lahenduste ning digitaalse taristu (võrgu- ja infosüsteemide) toimimisest. 2016. a läbiviidud uuringu[1] järelduste kohaselt, milles hinnati missioonikriitiliste ehk riigi toimimiseks vajalike elutähtsate teenuste küberriske, on erandita kõik uuringus osalenud teenuse osutajad[2] teenuse osutamisel sõltuvad võrgu- ja infosüsteemide toimimisest ning ligi pooled loevad oma sõltuvust kriitiliseks. Lisaks sõltub rohkem kui viiendik küsitletud teenuseosutajaist kriitilisel määral kolmandate isikute pakutavast info- ja kommunikatsioonitehnoloogia (edaspidi *IKT*) taristust või teenustest. See tähendab, et viimaste toimepidevust mõjutav küberintsident mõjutab suure tõenäosusega ka teisi olulisi teenuseid.

Ühiskonna suureneva sõltuvuse taustal võrgu- ja infosüsteemidest areneb tehnoloogia ülikiiresti; võrgu- ja infosüsteemide suurenev keerukus ning internetti ühendatud väga erinevate seadmete kasvav arv ning küberruumis tegutsevate erineva motivatsiooni ja oskustasemega toimijate kasvav hulk muudab küberturvalisuse üha suuremaks väljakutseks. Ohukeskkonna muutumine tingib vajaduse tagada senisest parem olukorrateadlikkus ja tagada ohtude ennetamine, väljaselgitamine ja tõrjumine ka juhul, kui süsteemi omanik või valdaja vajalikku hoolsust tahtlikult või teadmatusest ei täida.

[1] https://www.ria.ee/public/Kuberturvalisus/Elutahtsate-teenuste-osutamist-mojutavate-tegurite-uuringu-kokkuvote.pdf.

2 Uuringuga hõlmatud teenused olid järgmised: elektri, maagaasi ja vedelkütusega varustamine; riigimaanteede ja kohalike teede sõidetavus ning raudteeveoteenuste toimimine; telekommunikatsiooniteenused; finants- ja tervishoiuteenused; kommunaalteenused, nagu kaugküttega varustamine, veevarustus ja kanalisatsioon; sadamate ja laevaliikluskorralduse ning aeronavigatsiooniteenuste ja lennuväljade toimimine.

2016. a registreeriti Riigi Infosüsteemi Ameti infoturbe intsidentide käsitlemise osakonna CERT-EE (*Computer Emergency Response Team*)[3] poolt elutähtsate teenuste osutajaid puudutanud juhtumeid 253, mis moodustab registreeritud juhtumite üldarvust alla 3% ning tuvastatud intsidentide üldarvust (st kõigist juhtumeist, millega kaasnes vahetu mõju teabe või süsteemi konfidentsiaalsusele, terviklusele või käideldavusele) veidi üle 11%.[4] Tänavu esimese poolaasta jooksul on CERT-EE registreerinud 325 elutähtsa teenuse osutajaid puudutanud juhtumit, ehk keskmiselt 54 juhtumit kuus.[5] Ehkki need kõik ei ole vahetult mõjutanud elutähtsa teenuse toimimist, vaid on piirdunud mõjuga teenuse osutaja infosüsteemidele, esineb igal kuul ka pikemaid teenusekatkestusi ning kriitilisi intsidente – näiteks registreeriti 2016. a Eestis 12 elutähtsa teenuse osutaja lunavaraga nakatumise juhtu, sh tervishoiuteenuste ning transpordisektoris.[6]

Internetiajastu on loonud pinnase uut laadi käitumiskohuste tekitamise järele ning seega nõuab ühiskond riigi kaitseülesannete laiendamist uute ohupotentsiaalidega toimetulemiseks. Küberturvalisuse tagamiseks peab regulatsioon olema ettenähtav ning sätestama selged õiguslikud alused, millistel juhtudel, viisil ja vahenditega on riigil õigus ja kohustus sekkuda, kui info- ja võrgusüsteemide turvalisus on ohustatud. Avalikkusel ja seaduse rakendajal peab olema võimalik kindlaks teha, milliste avalike ülesannete täitmist seadusandja määratud pädevalt asutuselt eeldatakse ja millised sekkumismehhanismid on pädevale asutusele seaduses sätestatud kohustuste järgimise tagamiseks ette nähtud.

Eelnõu pealkirja ja mõistete sisustasime valikul lähtuti terminoloogilisest järjepidevusest varasemate õigusaktide ja poliitikadokumentidega. Eesliide „küber-" on alusterminina käibel alates 2008. a vastu võetud esimesest küberjulgeoleku strateegiast. Kehtiva „Küberjulgeoleku strateegia 2014–2017"[7] lisa 2 piiritleb kübervaldkonna baasmõisted ja nende omavahelised seosed, mh küberturvalisuse mõiste.[8] Nii varasema kui ka kehtiva hädaolukorra seaduse (edaspidi *HOS,* RT I, 03.03.2017, 1) alusel määratletakse „ulatuslik küberintsident" võimaliku hädaolukorra põhjustava sündmusena[9] ning selle lahendamiseks on kehtestatud ulatusliku küberintsidendi hädaolukorra lahendamise plaan. Küberturvalisuse mõistega opereerib ka Kaitseliidu seadus (RT I, 03.03.2017, 10, mh Kaitseliidu küberturvalisuse tagamisse kaasamist puudutavas) ning riigisaladuse ja salastatud välisteabe seadus. Riigi Infosüsteemi Ameti põhimääruse kohaselt on ametil pädevus küberturvalisuse valdkonnas. Seega on „küberturvalisus" terminina praktikas juurdunud ja kasutusel valdkondade üleselt.

Alljärgnevalt on ülevaade NIS direktiivi sätetest.

Direktiivi art 1 sätestab reguleerimis- ja kohaldamisala, täpsemalt direktiivi eesmärgi, milleks on meetmete sätestamine võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge taseme

[3] *Computer Emergency Response Team.*
[4] Riigi Infosüsteemi Ameti küberturvalisuse teenistuse 2016. a kokkuvõte, lk 23. https://www.ria.ee/public/Kuberturvalisus/RIA-kuberturbe-aastaraport-2016.pdf .
[5] RIA küberturvalisuse kuukokkuvõtted, jaanuar–juuni 2017. https://www.ria.ee/ee/kuberturvalisuse-kokkuvotted.html
[6] Riigi Infosüsteemi Ameti küberturvalisuse teenistuse 2016. a kokkuvõte. https://www.ria.ee/public/Kuberturvalisus/RIA-kuberturbe-aastaraport-2016.pdf
[7] https://www.mkm.ee/sites/default/files/kuberjulgeoleku_strateegia_2014-2017.pdf
[8] https://www.mkm.ee/sites/default/files/lisa_2_valdkondlik_metoodika.doc
[9] Vabariigi Valitsuse 22.06.2017 määrus nr 108 "Loetelu sündmustest, mis võivad põhjustada hädaolukorra ja mille kohta koostatakse riskianalüüs, ning hädaolukorra riskianalüüsi koostamist juhtivad asutused" (RT I, 28.06.2017, 33).

saavutamiseks liidus, parandades seeläbi siseturu toimimist. Samuti sätestatakse meetmed, mis on vajalikud art 1 lõikes 1 välja toodud eesmärgi saavutamiseks.

Direktiivi art 2 kohaselt toimub NIS direktiivis isikuandmete töötlemine kooskõlas direktiiviga 95/46/EÜ (ET 23.11.1995 L 281) ning kooskõlas määrusega (EÜ) nr 45/2001 (ET 12.01.2001 L 008).

Direktiivi art 3 kohaselt võivad liikmesriigid võtta vastu või säilitada sätteid eesmärgiga saavutada võrgu- ja infosüsteemide turvalisuse kõrgem tase.

Direktiivi art 4 seletab lahti direktiivis kasutatavad mõisted.

Direktiivi art 5 seab liikmesriikidele ülesandeks identifitseerida 9. novembriks 2018 oluliste teenuste operaatorid, kelle tegevuskoht on vastava liikmesriigi territooriumil. Artiklis on sätestatud identifitseerimise kriteeriumid, mille peavad kõik liikmesriigid aluseks võtma. Samuti on seal toodud välja nõue, et liikmesriigid peavad korrapäraselt ja vähemalt iga kahe aasta tagant vaatama üle oluliste teenuste operaatorite nimekirja ja vajadusel seda ajakohastama. Liikmesriigid peavad iga kahe aasta tagant esitama komisjonile vajaliku teabe, et komisjon saaks hinnata direktiivi rakendamist, eelkõige liikmesriikide lähenemisviiside järjepidevust seoses oluliste teenuste operaatorite identifitseerimisega.

Direktiivi art 6 kõneleb olulisest häirivast mõjust oluliste teenuste osutamisel ning sätestab sektoritevahelised tegurid, mida liikmesriigid peavad arvesse võtma.

Direktiivi art 7 sätestab riikliku võrgu- ja infosüsteemide turvalisuse strateegia. Iga liikmesriik on kohustatud võtma vastu võrgu- ja infosüsteemide turvalisuse strateegia, milles määratletakse strateegilised eesmärgid ning asjakohased poliitilised ja regulatiivsed meetmed, mille abil saavutada võrgu- ja infosüsteemide turvalisuse kõrge tase ja seda säilitada, ning mis hõlmab direktiivis osutatud sektoreid ja teenuseid. Liikmesriikidel tekib kohustus edastada riiklik võrgu- ja infosüsteemide turvalisuse strateegia komisjoni kolme kuu jooksul pärast selle vastuvõtmist.

Direktiivi art 8 kohustab liikmesriike määrama võrgu- ja infosüsteemide turbe vallas ühe või mitu riiklikku pädevat asutust ning riikliku ühtse kontaktpunkti. Iga liikmesriik peab teavitama pädeva asutuse ja ühtse kontaktpunkti määramisest ning selle avalikustama.

Direktiivi art 9 kohustab liikmesriike määrama direktiivis sätestatud nõuetele vastava Computer Security Incident Response Team'i (edaspidi CSIRT), kes hõlmab direktiivis osutatud sektoreid ja teenuseid ning kes vastutab riskide ja intsidentide käsitlemise eest põhjalikult määratletud protseduuri kohaselt. CSIRT-i võib luua pädeva asutuse osana.

Direktiivi art 10–13 räägivad liikmesriikidevahelisest koostööst. Liikmesriikide vahel luuakse koostöörühm, mille ülesandeks on toetada ja hõlbustada liikmesriikidevahelist strateegilist koostööd ja infovahetust, luua usaldust ja kindlustunnet ning saavutada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase liidus. Samal ajal luuakse ka riiklike CSIRT-ide võrgustik, mis lisaks usalduse ja kindlustunde loomisele aitab edendada ka kiiret ja tõhusat operatiivkoostööd. Art 11 ja 12 sätestavad koostöörühma ja CSIRT-ide võrgustiku ülesanded.

Direktiivi art 14 ja 15 räägivad oluliste teenuste operaatorite võrgu- ja infosüsteemide turvalisusest. Liikmesriigid peavad tagama, et oluliste teenuse operaatorid võtavad kasutusele asjakohased ja proportsionaalsed tehnilised ning korralduslikud meetmed, et hallata riske, mis ohustavad nende töös kasutatavate võrgu- ja infosüsteemide turvalisust. Tehnika taset arvesse võttes tagatakse nende meetmetega olemasolevale ohule vastav võrgu- ja infosüsteemide turvalisuse tase. Liikmesriigid peavad samuti tagama, et oluliste teenuste operaatorid võtavad kasutusele asjakohased meetmed, selleks et ennetada ja minimeerida oluliste teenuste osutamiseks kasutatavate võrgu- ja infosüsteemide turvalisust kahjustavate intsidentide mõju, eesmärgiga tagada kõnealuste teenuste järjepidevus. Liikmesriigid peavad tagama ka selle, et oluliste teenuste operaatorid teatavad põhjendamatu viivituseta pädevale asutusele või CSIRT-ile intsidentidest, millel on oluline mõju nende pakutavate oluliste teenuste järjepidevusele.

Direktiivi art 16–18 kõnelevad digitaalse teenuse osutajate võrgu- ja infosüsteemide turvalisusest ning intsidentide teavitamisest. Liikmesriigid peavad tagama, et digitaalse teenuse osutajad teevad kindlaks riskid, mis ohustavad nende võrgu- ja infosüsteemide turvalisust, mida nad kasutavad direktiivis osutatud teenuste osutamisel liidus, ning võtavad kasutusele asjakohased ja proportsionaalsed tehnilised ning korralduslikud meetmed, et neid riske juhtida. Tehnika taset arvesse võttes tagatakse nende meetmetega olemasolevale ohule vastav võrgu- ja infosüsteemide turvalisuse tase ning võetakse arvesse erinevaid elemente. Liikmesriigid peavad samuti tagama, et digitaalsed teenused võtavad kasutusele meetmed, et vältida ja minimeerida intsidentide mõju, ning tagavad, et digitaalse teenuse osutajad teatavad pädevale asutusele või CSIRT-ile põhjendamatu viivituseta igast intsidendist, millel on oluline mõju nende poolt liidus osutatavale direktiivis sätestatud teenusele.

Direktiivi art 19 ja 20 kõnelevad standardimisest ja vabatahtlikust teavitamisest. Liikmesriigid innustavad võrgu- ja infosüsteemide turvalisust käsitlevate Euroopa või rahvusvaheliselt heaks kiidetud standardite ja spetsifikatsioonide kasutamist, ilma et nad nõuaksid või soosiksid konkreetset tüüpi tehnoloogia kasutamist. Samuti sätestatakse, et üksused, mis ei ole määratletud kui oluliste teenuste operaatorid ega digitaalse teenuse osutajad, võivad vabatahtlikult teavitada intsidentidest, millel on oluline mõju nende osutatavate teenuste järjepidevusele.

Direktiivi art 21–27 on lõppsätted, mis kõnelevad karistustest, komiteemenetlusest, läbivaatamisest, üleminekumeetmetest, ülevõtmisest, jõustumisest ning adressaatidest. Liikmesriigid on kohustatud võtma vastu ja avaldama direktiivi järgimiseks vajalikud õigus- ja haldusnormid 9. maiks 2018 ning kohaldama kõnealuseid meetmeid alates 10. maist 2018.

3. Eelnõu sisu ja võrdlev analüüs

Seaduseelnõu koosneb 6 peatükist ja 27 paragrahvist.

Eelnõu 1. peatükk käsitleb seaduse üldsätteid ning küberturvalisuse tagamise põhimõtteid.

Eelnõu § 1 sätestab seaduse reguleerimisala. Lõikes 1 on sätestatud seaduse mõjupiirkond, milleks on riigi ja ühiskonna toimimise seisukohast oluliste võrgu- ja infosüsteemide pidamise nõuded, küberintsidentide ennetamise ja lahendamise alused ning järelevalve seaduses sätestatud kohustuste täitmise üle.

Arvestades asjaolu, et tänapäeva maailmas on enamik osutatavaid teenuseid vähemal või rohkemal määral võrgu- ja infosüsteemidest sõltuvad, on vaja tagada süsteemide turvalisus ja usaldusväärsus. Võimalike manipulatsioonide või suisa tahtlike rünnakute ennetamiseks ja nende tekitatud kahjude vähendamiseks on vajalik luua ühtne ja selge regulatsioon, mis sätestab kohustused erinevatele osapooltele, eesmärgiga kaitsta avalikku korda, isikute tervist ja vara ning laiemalt ühiskonna elukorraldust.

Eelnõu § 1 lõige 2 sätestab, et käesolev seadus ei kohaldu riigisaladuse või salastatud välisteabe töötlussüsteemide pidamisel. Riigisaladuse ja salastatud välisteabe kaitse seaduse § 10 punkti 2 kohaselt infrastruktuuri ja teabe kaitse riigisaladus on riigisaladuse ja salastatud välisteabe töötlussüsteemi käsitlev teave, välja arvatud teave, mille avalikuks tulek ei kahjusta Eesti Vabariigi julgeolekut. See teave salastatakse täiesti salajasel või madalamal tasemel kuni 50 aastaks.

Lõige 3 sätestab, et juhul, kui võrgu- ja infosüsteemi turvanõuded on reguleeritud välislepingus, mõnes muus seaduses või selle alusel kehtestatud õigusaktis, siis kohaldatakse eriseaduses sätestatud nõudeid. Lõikes 3 on arvestatud näiteks nii finantsvaldkonna (NIS direktiivi põhjenduspunkt 12) kui ka veetranspordi erisustega (NIS direktiivi põhjenduspunkt 10).

Lõige 4 sätestab haldusmenetluse kohaldamise, mille puhul lähtutakse haldusmenetluse seaduse sätetest.

Eelnõu § 2 kirjeldab eelnõus kasutatavaid mõisteid. Eelnõus kasutatavate mõistete selgitused on esitatud seletuskirja terminoloogia peatükis (seletuskirja neljandas peatükis).

Eelnõu §-s 3 sätestatakse seaduse kohaldamisala.

Paragrahvis tuuakse välja need teenuse osutajad, kellele kõnealune seadus kohaldub. Lõike 1 punktis 1 sätestatakse, et seadus kohaldub HOS-i §-s 36 sätestatud elutähtsa teenuse osutajale elutähtsa teenuse osutamiseks kasutatavate infosüsteemide ja nendega seotud infovarade osas. HOS-is on elutähtsate teenuste loetelus elektriga varustamine, maagaasiga varustamine, vedelkütusega varustamine, riigitee sõidetavuse tagamine, telefoniteenus, mobiiltelefoniteenus, andmesideteenus, elektrooniline isikutuvastamine ja digitaalne allkirjastamine, vältimatu abi toimepidevus, makseteenus, sularaharinglus, kaugküttega varustamine, kohaliku tee sõidetavuse tagamine ning veega varustamine ja kanalisatsoon.

Punktis 2 sätestatakse, et seadus kohaldub raudteeseaduses sätestatud raudtee-ettevõtjale, kes majandab avalikku raudteeinfrastruktuuri või kelle kaubaveo või reisijateveo turuosa on vähemalt 20% kaubaveo või reisijateveo turuosast avaliku raudtee majandamise toimimise ja raudteeveo, sealhulgas avaliku reisijateveo toimimise teenuse osutamiseks kasutatavate infosüsteemide ja nendega seotud infovara osas. Tegemist on teenusega, mis oli enne 01.07.2017 kehtinud HOS-i kohaselt elutähtis teenus. Vaatamata sellele, et tegemist pole enam elutähtsa teenusega, on elektroonilise turvalisuse nõuete täitmise kohustus sätestatud valdkondlikus seaduses.

Punktis 3 sätestatakse, et seadus kohaldub lennundusseaduses sätestatud lennuvälja käitajale, kelle käitatav lennuväli on avatud rahvusvaheliseks regulaarseks lennuliikluseks, samuti Tallinna lennuinfopiirkonnas lennuliikluse teenindamist tagav aeronavigatsiooniteenuse osutaja lennuväljade toimimise ja aeronavigatsiooniteenuse toimimise teenuse osutamiseks

kasutatavate infosüsteemide ja nendega seotud infovarade osas. Tegemist on samuti teenusega, mille puhul on võrgu- ja infosüsteemide turvalisuse nõuded sätestatud juba varem ning kavandatava muudatusega lisatakse eriseadusesse viide.

Punktis 4 sätestatakse, et seadus kohaldub sadamaseaduses sätestatud sadamale, mis teenindab rahvusvahelises meresõidus sõitvaid reisilaevu või 500 ja enama kogumahutavusega laevu, ja sadam, mis teenindab meresõiduohutuse seaduse kohaselt määratletud kohalikus rannasõidus sõitvaid I kategooria laevu või A-klassi reisilaevu sadamate toimimise ja laevaliikluse korraldamise süsteemi toimimise teenuse osutamiseks kasutatavate infosüsteemide ja nendega seotud infovara osas. Sarnaselt punktidele 2 ja 3 on samuti tegemist eriseaduse viite lisamisega.

Punktis 5 sätestatakse, et seadus kohaldub elektroonilise side seaduses sätestatud sideettevõtja, kes osutab kaabelleviteenust, mida tarbib vähemalt 10 000 lõppkasutajat, ja ringhäälinguvõrgu teenuse osutaja kaabelleviteenuse või ringhäälinguvõrgu teenuse osutamiseks kasutatava süsteemi ja sellega seotud infovara osas.

Punktis 6 sätestatakse, et seadus kohaldub tervishoiuteenuste korraldamise seaduses sätestatud piirkondlikule haiglale ja keskhaigla pidajale statsionaarse eriarstiabi ja perearstile üldarstiabi teenuse osutamiseks kasutatavate infosüsteemide ja nendega seotud infovara osas. Kui statsionaarne eriarstiabi oli varasemalt elutähtis teenus, siis küberturvalisuse tagamise kohustusi peavad tulevikus järgima ka perearstid üldarstiabi teenuse osutamiseks. Vältimatu arstiabi on siiani elutähtsaks teenuseks ja nemad kohustuvad nõudeid järgima § 2 punkti 1 alusel. Küberturvalisus on meditsiinisektoris olnud terava tähelepanu all üleilmselt juba pikka aega ning sarnaselt paljudele arenenud riikidele on ka Eesti meditsiinisektor küberrünnakutele haavatav.. Rahvusvaheliste küberturvalisuse ettevõtete FireEye[10] ja Symantec[11] ning ENISA[12] raportid on antud sektoris ohtude realiseerumise kohta hulgaliselt näiteid. Näiteks 2017.a. toimunud WannaCry lunavara puhangu ajal oli häiritud ligi 20% Suurbritannia tervishoiu sektorist. Ka Eesti pole jäänud nendest ohtudest puutumata – tervishoiuteenuse osutajad on pidanud maksma küberkurjategijatele rahasummasid, et lunavara poolt krüpteeritud andmeid tagasi saada. Samuti on Eesti tervishoiuteenuse osutajate arvutivõrkudest leitud seadmeid, mis ei tohiks seal olla ja mis võisid võimaldada potentsiaalsetele kurjategijatele ligipääsu tervishoiuteenuse osutajate arvutivõrkudesse.
Perearstide puhul on vajalik ühtlustada nende poolt kasutatavate infosüsteemide turvanõudeid vältimaks näiteks isikuandmete lekkeid või andmete krüpteerimist lunavara rünnakute käigus. Paljudel perearstidel on nimistus sadu kui mitte tuhandeid inimesi ning võimalus sellises mahus isikuandmete lekkimiseks küberrünnaku käigus on tänapäeval täiesti arvestatav. Perearstid (nagu ka ülejäänud tervishoiuteenuste osutajad) kasutavad oma tööülesannete täitmiseks tervise infosüsteemi (*TIS*)[13], mida haldab Tervise ja Heaolu Infosüsteemide Keskus (TEHIK). TIS-ga liidestumisel peab tervishoiuteenuse osutaja oma infosüsteemides juurutama ID-kaardil või muul turvalisel autentimisvahendil põhineva autentimissüsteemi, seadma sisse valmiduse X-teel andmevahetuseks ja teostama oma infosüsteemis liidestumiseks vajalikud täiendused vastavalt TEHIK publitseeritud Tervise Infosüsteemi standardi[14] hetkel kehtivale

[10] https://www2.fireeye.com/what-healthcare-can-do-about-cyber-attacks.html
[11] https://www.symantec.com/content/dam/symantec/docs/other-resources/ha-it-security-2017-study-ebook.pdf
[12] https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals
[13] Tervishoiuteenuste korraldamise seadus §59[1] lõike 1 kohaselt on tervise infosüsteem riigi infosüsteemi kuuluv andmekogu, milles töödeldakse tervis-hoiuvaldkonnaga seotud andmeid tervishoiuteenuse osutamise lepingu sõlmimiseks ja täitmiseks, tervishoiuteenuse kvaliteedi ja patsiendi õiguste tagamiseks ning rahva tervise kaitseks, sealhulgas tervislikku seisundit kasjastavate registrite pidamiseks ja tervishoiu juhtimiseks.
[14] http://pub.e-tervis.ee/

versioonile. Seega kasutavad TISi nii suured haiglad kui ka väiksemad perearstid (s.h. ka perearstid ja perearstikeskused). Seega peavad neile rakenduma ka sarnased küberturvalisuse tagamise kohustused.

Punktis 7 sätestatakse, et seadus kohaldub Eesti maatunnusega seotud tipptaseme domeeninimede registri haldajale registri pidamiseks kasutatava süsteemi infosüsteemide ja nendega seotud infovara osas. Tegemist on lisaks perearsti üldarstiabi teenusele teise teenusega, millel varasemalt pole olnud kohustust rakendada meetmeid küberturvalisuse tagamiseks. Eesti maatunnusega seotud tipptaseme domeeninimede registripidaja (ehk Eesti Interneti SA) ning tema osutatava teenusega seonduv pole reguleeritud üheski seaduses. Kuna tegemist on teenusega, mille sujuv toimimine on kriitilise tähtsusega Eesti internetikeskkonna küberturvalisuse tagamisel, siis on otstarbekas nimetatud teenus hõlmata käesolevas seaduses.

Punkti 8 kohaselt laienevad nõuded ka Eesti Rahvusringhäälingule Eesti Rahvusringhäälingu seaduse § 5 lõike 1 punktis 10 sätestatud ülesande täitmiseks kasutatavate infosüsteemide ja nendega seotud infovarade osas. Rahvusringhäälingu ülesandeks on teiste seas tagada adekvaatse informatsiooni operatiivne edastamine elanikkonda või riiklust ohustavates olukordades. Arvestades info edastamise olulisust elanikkonna teavitamisel kriisidest või tähtsatest ühiskonda puudutavatest sündmustest, on äärmiselt oluline rahvusringhäälingu toimimise järjepidevus ja katkematus. Selle tagamiseks peavad olema ka rahvusringhäälingu infosüsteemid kaitstud ning seda on võimalik saavutada piisavate turvanõuete täitmise kaudu.

Punktis 9 sätestatakse, et hõlmatud on ka riigiside, s.o kriitilise tähtsusega side, mereraadioside ja operatiivraadiosidevõrgu teenuse osutajale elektroonilise side seaduse tähenduses nende teenuste osutamiseks kasutatavate infosüsteemide ja nendega seotud infovara osas.

Lõige 2 sätestab, et käesoleva paragrahvi lõike 1 punktides 1–7 nimetatud teenuse osutajat, kes tegutseb Euroopa parlamendi ja nõukogu direktiivi (EL) nr 2016/1148 meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus (ELT L 194, 19.07.2016, lk 1–30) lisas II esitatud sektorites, loetakse olulise teenuse operaatoriks vastava direktiivi tähenduses. Lähtuvalt kehtivast regulatsioonist on mõistlik jääda seni kasutuses olevate terminite juurde. Eestis on taolised olulised teenused määratletud HOS-is elutähtsate teenustena ja eriseadustes, samas on HOS valdkondade loetelu erinev kui NIS direktiivi lisas esitatud teenuste loetelu. Seetõttu ei ole peetud otstarbekaks lisada olulise teenuse mõistet käesolevasse eelnõusse- NIS direktiivi lisas esitatud teenuste puhul on ka teenuseid, mis ei ole Eesti kontekstis olulised või mida ei osutata (nt tuumaelektrijaama pidamine). NIS direktiivi art 5 lõige 2 identifitseerib olulise teenuse operaatorit kui avaliku või erasektori üksust järgmiste kriteeriumitega: 1) üksus osutab teenust, mis on oluline elutähtsa ühiskondliku ja/või majandustegevuse säilitamise seisukohast, 2) kõnealuse teenuse osutamine sõltub võrgu- ja infosüsteemidest, 3) intsidendil oleks oluliselt häiriv mõju nimetatud teenuse osutamisele. Üksuste liigid sektorite kaupa on järgmised: energeetika (nafta, gaas, elekter), transport (lennu-, raudtee-, maantee- ja veetransport), pangandus, finantsturu taristu, tervishoiusektor (tervishoiuasutused, kaasa arvatud haiglad ja erakliinikud), joogivee varustus ja jaotamine ning digitaalne taristu.

Lõige 3 paneb Riigi Infosüsteemi Ametile kohustuse identifitseerida hiljemalt 9. novembriks 2018. a seaduse kohaldamisalas olevad teenuse osutajad, kes tegutsevad Euroopa parlamendi ja nõukogu direktiivi (EL) nr 2016/1148 II lisas esitatud sektorites.

Eelnõu § 4 sätestab digitaalse teenuse osutaja.

Digitaalse teenuse osutaja puhul lähtutakse NIS direktiivi käsitlusest, mille kohaselt on digitaalse teenuse osutaja infoühiskonna teenuse osutaja infoühiskonna teenuse seaduse tähenduses, kes pakub internetipõhist kauplemiskohta, internetipõhist otsingumootorit või pilvandmetöötlusteenust. Internetipõhised kauplemiskohad on näiteks www.on24.ee või www.osta.ee keskkonnad, internetipõhised otsingumootorid on näiteks www.neti.ee ja www.google.ee ning pilvandmetöötlusteenused on näiteks Dropbox või Microsoft Azure. Digitaalse teenuse osutaja mõistet tuleb eristada teenuse osutaja mõistest ning teenuse osutaja ja digitaalse teenuse osutaja nõuded on seaduses reguleeritud erinevates paragrahvides. NIS direktiivi kontekstis on digitaalse teenuse osutaja regulatsiooni puhul maksimumharmoneerimisega, mis tähendab, et liikmesriigid ei saa siseturu reegleid arvestades sätestada leebemaid ega karmimaid nõudeid kui direktiiv.

Lõige 2 sätestab, et seadus ei kohaldu digitaalse teenuse osutajale, kes on mikro- või väikeettevõtja raamatupidamise seaduse § 3 punktide 14 ja 15 tähenduses. Mikroettevõtja on osaühing, kelle näitajad vastavad aruandeaasta bilansipäeval kõikidele järgmistele tingimustele: varad kokku kuni 175 000 eurot, kohustused ei ole suuremad kui omakapital, üks osanik, kes on ka juhatuse liige, ja kelle müügitulu on aruandeaastal kuni 50 000 eurot. Väikeettevõtja on Eestis registreeritud äriühing, kes ei ole mikroettevõtja ja kelle näitajatest võib aruandeaasta bilansipäeval vaid üks ületada järgmisi tingimusi: varad kokku 4 000 000 eurot, müügitulu 8 000 000 eurot ja keskmine töötajate arv aruandeaasta jooksul 50 inimest.

Eelnõu § 5 sätestab EL-i liikmesriikidevahelise süsteemide turvalisuse tagamisega seotud koostöö ühtse kontaktpunkti ja pädeva asutuse. NIS direktiivi art 8 sätestab nõude, et iga liikmesriik määrab võrgu- ja infosüsteemide turbe vallas ühe või mitu riiklikku pädevat asutust ning ühtse kontaktpunkti. Pädev asutus Eesti kontekstis on asutus, kes täidab järelevalveasutuse rolli ehk teostab järelevalvet eelnõuga pandud kohustuste täitmise üle. Liikmesriigid võivad määrata selle ülesande olemasolevale asutusele. Kui liikmesriik nimetab ainult ühe pädeva asutuse, siis on see pädev asutus ka ühtne kontaktpunkt. Eestis on pädevaks asutuseks ja ühtseks kontaktpunktiks sama asutus ehk Riigi Infosüsteemi Amet. Ühtne kontaktpunkt täidab sidepidamisfunktsiooni, et tagada liikmesriikide asutuste piiriülene koostöö teiste liikmesriikide asjaomaste asutuste, koostöörühma ja CSIRT-ide võrgustikuga. Pädevad asutused ja ühtne kontaktpunkt peavad vajaduse korral ja kooskõlas riigisisese õigusega konsulteerima ja tegema koostööd asjakohaste riiklike õiguskaitse- ja andmekaitseasutustega.

Eelnõu § 6 sisustab seaduse tasandil põhimõtted, mis juhinduvad NIS direktiivi eesmärgist edendada riskihalduse kultuuri[15], täites sellega ka teadlikkuse tõstmise ülesannet. Seaduse adressaatidele põhimõtetest õigusi ja kohustusi ei tulene, viimased on sätestatud konkreetsetes normides.

Põhimõtete määratlemisel on lähtutud küberturvalisuse valdkonna rahvusvahelisest heast tavast, võttes sõnastamisel arvesse OECD soovitust „Digital Security Risk Management for Economic and Social Prosperity“ (*General Principles*).[16] Samadest aluspõhimõtetest on

[15] NIS direktiivi preambuli punktid 4 ja 44.
[16] http://acts.oecd.org/Instruments/ShowInstrumentView.aspx?InstrumentID=328&InstrumentPID=371&Lang=en

järjepidevalt juhindunud ka Eesti 2008. ja 2014. a küberjulgeoleku strateegiad[17]. Põhimõtteid defineerimata järgib ka NIS direktiivi lähenemine.

Paragrahvi 6 punktis 1 määratletud isiklikkuse põhimõte näeb ette, et esmane vastutus oma võrgu- ja infosüsteemi turvalisuse tagamisel lasub selle haldajal. Eesti küberjulgeoleku korraldus tervikuna on 2008. a saati lähtunud eeldusest, et infoühiskonnas vastutab iga osaline tema valduses oleva võrguühendusega tehnilise seadme või süsteemi turvalisuse eest. Hea infoturbe eelduseks on, et infosüsteemi omanik on oma vastutusest teadlik ja rakendab teadvustatud riskidele vastavaid turvameetmeid[18]. OECD eelviidatud soovituse kohaselt oodatakse igalt infosüsteemi omanikult samuti, et ta oleks teadlik tema tegevust mõjutavatest digitaalse keskkonna riskidest ja võtaks vastutuse nende haldamise eest.

Süsteemi (ja sellega seotud infovara) haldaja all, mõistetakse isikut, kes omab asja kasutamise üle tegelikku kontrolli (sh ka rendi-, üüri-, hoiu-, pandi- või muu selletaolise suhte alusel, mis annab isikule õiguse teise isiku asja vallata ning kellel on süsteemile juurdepääsuõigus). Haldaja mõiste on kooskõlas ka vastutava ja volitatud töötleja instituudiga avaliku teabe seaduse (edaspidi *AvTS*) tähenduses.

Fundamentaalselt säilib haldaja vastutus ka juhul, kui ta annab lepinguga teatud tegevused üle. Selles osas kehtib põhimõte, et delegeerida saab ülesandeid, ent mitte vastutust.

Punkt 2 sätestab tervikliku kaitse põhimõtte. Kui isikliku hoolsuse põhimõte selgitab vastutuse paiknemist, siis see põhimõte avab hoolsuskohustuse sisu: aktsepteeritava turvalisuse tagamine eeldab süsteemi ohustavate konkreetsete riskide kindlakstegemist ning süsteemi kaitseks asjakohaste korralduslike ja tehniliste abinõude rakendamist. Riski haldamine võib konkreetsel juhul seisneda nii riski aktsepteerimises, vähendamises, ülekandmises kui ka vältimises, kuid peab olema asjakohane, võttes arvesse riskide realiseerumise võimalikku mõju nii infosüsteemi omanikule endale kui ka teiste isikute õigustatud huvidele.[19] Meetme valik peab tegevuse laadi ja ulatust arvesse võttes olema vajalik, kohane ja piisav ohu ennetamiseks, väljaselgitamiseks ja küberintsidendi aset leidmise korral selle lahendamiseks ning süsteemi taastevõimekuse tagamiseks.

Punktis 3 sätestatud kahjuliku mõju vähendamise põhimõte näeb ette, et küberintsidendi korral tuleb kasutusele võtta abinõud, piiramaks intsidendi negatiivset mõju nii teistele süsteemidele kui ka teiste isikute õigushüvedele ning tähendab, et see peab andma ühiskonnas ka soovitud tagajärje - ohu ennetamise ning selle kiire tõrjumise. Küberintsidendi mõju minimeerimise vahendiks on nii vajalikud tehnoloogilised ja korralduslikud abinõud kui ka küberintsidendist teavitamine.

Vastavad kohustused sätestab eelnõu 2. peatükk.

Punkt 4 näeb ette koostööpõhimõtte riigi ja teenuseosutajate vahel, mis arvestaks ka teenuste omavahelist sõltuvust.[20] Eesti küberturvalisuse korraldus on olnud selle tekkimisest saati fundamentaalselt koostöine ja ka pärast seaduse jõustumist on oluline koostöökultuuri

[17] https://www.valitsus.ee/sites/default/files/content-editors/arengukavad/kuberjulgeoleku_strateegia_2008-2013.pdf; https://www.valitsus.ee/sites/default/files/content-editors/arengukavad/kuberjulgeoleku_strateegia_2014-2017.pdf

[18] „Küberjulgeoleku strateegia 2008–2013“, lk 8; sama ka „Küberjulgeoleku strateegia 2014–2017“ lk 7.

[19] OECD, 1. jagu, punktid 2, 5–6, 8.

[20] Sama aluspõhimõtte määratleb ka OECD soovitus „Digital Security Risk Management for Economic and Social Prosperity“ (2015), punkt 4.

säilitamine riigi ja erasektori, sh Riigi Infosüsteemi Ameti kui pädeva asutuse ja seaduse subjektidest teenuseosutajate vahel.

Koostöö riigi ja erasektori vahel on ka kehtiva küberjulgeoleku strateegia üks aluspõhimõtetest. 2011. aastal moodustati riigi- ja erasektori koostöö arendamiseks kriitilise informatsiooni infrastruktuuri kaitse komisjon (KIIK komisjon)[21]. Riigi Infosüsteemi Amet on viinud elutähtsate teenuste osutajate töötajatele läbi küberturbekoolitusi, korraldanud infosüsteemide turvatestimisi ning konsulteerinud intsidentide ilmnemisel ja neile reageerimisel. Elutähtsate teenuste osutajaid kaasatakse riigisisestele ja rahvusvahelistele küberõppustele. Koostöös ettevõtjatega töötab Riigi Infosüsteemi Amet välja turvaseire-süsteemi, et parandada teenuseosutajate võimekust küberrünnete ja pahavara avastamiseks nende arvutivõrkudes ning võimaldada ohuteadete edastamist, vähendades seeläbi rünnetest tulenevaid kahjusid ning maandades teenuste toimepidevusele avalduda võivaid riske.

On oluline, et seaduse jõustumisega ei muutuks Eesti senine küberturvalisuse korraldus reageerivamaks ega orienteeruks ümber järelevalvele ja haldussunnile, vaid vastavate mehhanismide sätestamine seaduses tagab üksnes täiendava aluse ühiskonna ja majanduse toimimist ohustavate küberintsidentide ennetamiseks, väljaselgitamiseks ja neile reageerimiseks. Koostööpõhimõtte seaduses sätestamisel on seetõttu niihästi käitumist suunav kui ka kommunikatiivne ülesanne.

Punkt 5 sätestab põhiõiguste kaitse põhimõtte, mida toetavad nii NIS direktiiv kui ka OECD eelviidatud soovitus.[22] Säte on suuniseks riikliku järelevalve teostamisel igal üksikjuhul, tagamaks, et meetmete kohaldamisel tagataks põhiõiguste ja põhivabaduste kaitse, sh väljendusvabaduse, informatsioonivabaduse ning isikuandmete kaitse. Küberturvalisuse riskide haldamisel peavad nii teenuseosutaja kui ka riik austama teiste isikute seaduslikke õigusi ja huve ja ühiskonna huve laiemalt. Eelnõus sätestatud põhiõiguste kaitse põhimõte hõlmab ka isiku identiteedi, sh digitaalse identiteedi kaitset.

Eelnõu §-d 7–8 sätestavad kohustused küberturvalisuse tagamisel.

Eelnõu § 7 sätestab teenuse osutaja süsteemi turvanõuded.

Lõige 1 sätestab üldeesmärgid, millele teenuse osutaja poolt vastavalt tema tegevuspõhisele riskihindamisele valitud turvameetmed peavad suunatud olema. Turvameetmeid on vaja rakendada selleks, et küberintsidente ennetada, küberintsidente lahendada, ja ka selleks, et küberintsidendi aset leidmise korral oleks selle mõju teenuse toimepidevusele minimaalne. Küberintsidendi ennetamine kätkeb endas riskide hindamist ja vastavate meetmete rakendamist minimeerimaks küberintsidentide tekkimise võimalust. Küberintsidentide lahendamine algab küberintsidendi tuvastamisega, jätkub vastavate meetmete kasutusele võtmisega eesmärgiga leida lahendus ning päädib süsteemi tavapärase töörežiimi taastamisega. Küberintsidendi mõju minimeerimise eesmärgiks on tagada teenuse võimalikult suur toimepidevus olukorras, kus küberintsident on toimunud. Sellest tulenevalt on oluline teenuse osutajal rakendada organisatsioonilisi, füüsilisi ja infotehnilisi turvameetmeid. Kehtestatud meetmed peavad vastama olulise teenuse osutaja tegevusala vajadustele. Organisatsioonilised meetmed peavad tagama info kättesaadavuse põhjendatud juhul vastava

[21] Küberjulgeoleku strateegia defineerib KIIK komisjoni ülesande järgmiselt: „Elutähtsat teenust osutavate asutuste küberturbe- ja IT-juhte koondava komisjoni tegevuse eesmärk on vahetada operatiivselt teavet, tuvastada probleeme ning teha ettepanekuid riigi elutähtsa infrastruktuuri küberjulgeoleku parandamiseks."
[22] NIS direktiivi preambuli punkt 75, OECD soovituse punkt 3.

juurdepääsuloa saanud isikutele. Teenuse osutaja peab määrama need isikud, kes vastutavad turvameetmete rakendamise ning küberintsidentide lahendamise eest. Nimetatud isikutel peab olema tagatud juurdepääs kogu vajaminevale infole. Füüsilised meetmed näevad ette näiteks teenuse osutaja ruumidesse ligipääsu piiramise, nõuded erinevatele häiresüsteemidele ning stabiilse elektrivarustuse tagamise. Näiteks võib olla vajadus oluliste teenuste osutajatel süsteemi töö katkemise vältimiseks dubleerida andmehoidlaid või hoida servereid füüsiliselt eraldatud kohtades. Infotehnilised meetmed kätkevad endas näiteks süsteemidesse ligipääsu piiramist paroolidega ning süsteemide kaitsmist tulemüüriga. Pidev tarkvara uuendamine ning pahavara tõrjuvate programmide kasutamine peab olema olulise teenuse osutajale kohustus.

Süstemaatiline lähenemine küberturvalisust mõjutavate riskide tuvastamiseks, hindamiseks ja analüüsimiseks hõlmab ka organisatsioonis kehtestatud poliitikate, protseduuride ja tegevuste pidevat seiret, mis aitab organisatsioonil vältida potentsiaalseid kahjujuhtumeid ja vähendada nende tagajärjel tekkida võivaid otseseid ja kaudseid kulutusi. IT-riskide järjepidev ja korrapärane hindamine aitab parendada organisatsiooni juhtimisprotsesse, suurendada tegevuste ja kulutuste läbipaistvust ning selgitada investeeringute majanduslikku põhjendatust.

Lõige 2 kohustab teenuse osutajaid lõikes 1 sätestatud eesmärke täitma ning sõnastab teenuse osutaja kohustused küberturvalisuse tagamise korraldamisel. Punktis 1 sätestatud süsteemi ja sellega seotud infovarade riskide hindamise nõue kätkeb teenuse osutaja kohustust määrata kindlaks süsteemide ja nendega seotud infovarade töökindlust ohustavad potentsiaalsed sündmused või asjaolud, mis võivad põhjustada katkestusi süsteemide töös või kahjustada infovara. Riskide hindamise käigus tuleb välja selgitada süsteeme ja nende infovara mõjutavad võimalikud ohud ja nõrkused (füüsilised kahjustused, loodussündmused, tehnilised tõrked, kuid ka erinevad seadmete manipuleerimise võimalused), hinnata ohtude realiseerumise tõenäosust ja nendega kaasnevaid kahjusid ning valida ohtude realiseerumise vältimiseks sobivad turvameetmed.

Punktis 2 sätestatud dokumenteerimisnõuded võivad erinevates infoturbe standardites varieeruda. Tehnilise dokumentatsiooni üks peaeesmärk on toetada infosüsteemide töö taastamist mõistliku aja jooksul. Teiseks eesmärgiks on anda asutuse või ettevõtte juhtkonnale teavet, mis võimaldab võtta soovitaval tasemel vastu infoturbe tagamiseks vajalikke otsuseid. Täpsemad nõuded IT-riskide analüüsimise dokumenteerimiseks kehtestatakse eelnõu jõustumisel Vabariigi Valituse määrusega, mis võrreldes eelnõu väljatöötamise ajal HOS-i § 41 lõike 3 alusel Vabariigi Valitsuse poolt 03.08.2017 vastu võetud määruses nr 133 „Elutähtsa teenuse infosüsteemide ning nendega seotud infovarade turvameetmed“ (RT I, 09.08.2017, 3) sätestatust ei erine ja seega enamikule eelnõu kohaldamisalasse jäävatele teenuse osutajatele uusi kohustusi kaasa ei too. Riskianalüüsi koostamiseks eelnõu üksikasjalikke vormistamise nõudeid ette ei näe – näiteks elutähtsate teenuste osutajate puhul võib riskianalüüs olla nii HOS-i § 38 lõikes 3 punktis 1 sätestatud toimepidevuse riskianalüüsi osa kui ka eraldiseisev dokument. Seega eelnõus sätestatud kohustus ei konkureeri HOS-is elutähtsa teenuse osutaja toimepidevuse riskianalüüsile kehtestatud nõuetega.

Punkti 3 kohaselt peavad teenuse osutajad tagama küberintsidentide tuvastamiseks vajaliku süsteemi seire. Aktiivsete võrgukomponentide nõuetekohase töö ja kõikide konfiguratsiooniparameetrite õigsuse tagamiseks tuleb sisse seada regulaarne, võimalikult automaatne kontrolliprotsess. Selle juurde kuuluvad näiteks regulaarsed funktsioonikontrollid, muudatuste kehtestamine ja nende rakendamise kontrollimine, samuti logifailide ja teadete seire, et varakult tuvastada süsteemi tavapärast toimimist ohustavaid turvanõrkusi,

manipuleerimiskatseid ja ebakorrapärasusi (nt võrgukasutus kasvas hüppeliselt, veebiserveril skaneeritakse teenuseporte, kommutaatoril lülitus port välja, kasutaja lukustas valesti parooli sisestades konto, printer lõpetas jooksvate tööde printimise). Seireinfo kogumine võib toimuda näiteks protsesside, tarkvara või tehnilise seireseadme paigaldamise teel, et tuvastada süsteemi ohustav tegevus või pahavara. Seireseadme eesmärk on tuvastada kõrvalekaldeid tavapärasest tegevusest võrgus, mis kujutavad süsteemi turvalisusele ohtu – näiteks sisemine oht (ühendatakse või eemaldatakse võrku seade või irdmeediakandja, mis ei tohiks võrgus olla, tööarvutisse paigaldatakse tööga mitteseotud tarkvara), kuid ka võrgu konfiguratsioonide muutused, kahjurvara jne. Teenuse osutaja võrguühendusele paigaldatud seireseade monitoorib süsteemis toimuvat liiklust, talletades vastavad ründe tunnused lokaalselt. Seade võimaldab konfigureeritud parameetrite alusel ründe tuvastamist nii teenuse kui ka ründevektori põhiselt ning vajadusel ka sissetuleva liikluse blokeerimist. Seireseade on vajalik analüüsi tööriist tuvastamaks toimunud küberintsidendi tekkepõhjuseid, et neid olulistes süsteemides aegsasti tuvastada. Seirelahenduse kasutamise põhjendatud vajaduse kohta saab näitena tuua Viru Keemia Grupi (VKG) juhtumi, mida Riigi Infosüsteemi Ameti küberturvalisuse teenistuse 2016. aasta kokkuvõte[23] kajastab.

Riigi Infosüsteemi Ametil on kohustus analüüsida küberintsidentide tekkepõhjuseid üldiselt ja tõsta teenuse osutajate ning riigi ohuteadlikkust info jagamisega. Kuivõrd süsteeme ohustav pahavara areneb kiiresti ja oht piirdub harva vaid ühe teenuseosutaja süsteemidega, võimaldab kursis olek uute ründevektoritega küberintsidentide ohtu ja mõju laienemist vähendada. Seetõttu nähakse teenuse osutajale ette kohustus edastada Riigi Infosüsteemi Ametile teenuseosutaja poolt tuvastatud pahavara tunnused ning anonümiseeritud koondteabest lähtub Riigi Infosüsteemi Amet avalikkusele ja teenuseosutajatele ohuteadete edastamisel.[24] Teavet võib Riigi Infosüsteemi Ametile edastada automaatselt või kasutades Riigi Infosüsteemi Ameti loodud vastava teabe edastamise kanaleid. Metoodika ja teabe edastamise lahendus (teabe koosseis, edastamise sagedus ja viis) lepitakse kokku teenuse osutajatega koostöölepingus. Võimaliku seiresüsteemi soetusmaksumus jääb vahemikku 5000–100 000 eurot, mis sõltub mh ka andmemahtude suurustest. Riigi Infosüsteemi Amet saab teenuse osutaja kasutusse anda tasuta tarkvara.

Punktis 4 sätestatud kohustus piirata süsteemi juurdepääsu või kasutamist on vajalik ja põhjendatud, kui esineb objektiivsetele asjaoludele tuginev kahtlus, et süsteemi tabanud küberintsident võib mõjutada teise süsteemi tööd ning vajalik on küberintsidendi levikut tõkestada või süsteemi turvalisus taastada[25]. Süsteemile või selle osale (veebilehele, infosüsteemile) ligipääsu blokeerimise või infosüsteemist algatatavate sessioonide piiramise vajadus võib tõusetuda, et tõkestada võrgu kaudu teistesse süsteemidesse kahjurvara jagamist. Samuti võib see vajalik olla juhul, kui nakatunud seade on väljastpoolt kontrollitud robotvõrgu (*botnet*) liige, mis ohustab suuremat ringi kasutajaid või elutähtsa teenuse osutamiseks kasutatavaid süsteeme näiteks teenustõkestusrünnete (*Denial of Services* ehk DoS) või *Distributed Denial of Service* ehk DDoS) läbiviimise või andmevarguse kaudu. Süsteemi kasutamise piiramise kohustus puudutab võrku ühendatud seadet, mis võib olla autonoomne või toetada teenuste toimimist (nt automaat- ja kaugjuhtimisega seadmed,

[23] Riigi Infosüsteemi Ameti küberturvalisuse teenistuse 2016. a kokkuvõte. https://www.ria.ee/public/Kuberturvalisus/RIA-kuberturbe-aastaraport-2016.pdf

[24] Nt Riigi Infosüsteemi Ameti kodulehe ja sotsiaalmeedia (https://www.ria.ee/ee/kuberturvalisuse-uudised.html ja https://twitter.com/cert_ee) kaudu edastatavad avalikud ohuteated.

[25] Ühe näitena tuua 27.06.2017 hommikul maailma tabanud uut lunavaralainet, mille käigus levis pahavara seda tabanud ettevõtte süsteemides ülikiiresti. Esimesed nakatumised toimusid Ukrainas, kus teadaolevalt nakatus pahavaraga üle 12 500 tööjaama. Ööpäeva jooksul tuli teateid nakatumistest kokku 64 riigis, sealhulgas Eestis. Vt nt Riigi Infosüsteemi Ameti blogis avaldatud artiklit: https://blog.ria.ee/petya-voi-notpetya/

juhtseadmed ehk kontrollerid) või muid seadmeid, mis on võrku ühendatud. Juurdepääsu piiramine või ajutine blokeerimine võib olla vajalik näiteks ka juhul, kui süsteemi osa (nt veebileht) lekitab süsteemis hoitavat konfidentsiaalset teavet või isikuandmeid.

Juurdepääsu piiramise kohustus võib olla nii välja- (teise süsteemi haldajale) kui sissepoole (teistele ettevõttesisestele süsteemidele) suunatud. Näiteks võib tõusetuda vajadus eemaldada teatud seadmed võrgust, et vältida pahavara levikut kontorivõrgust tootmisvõrku ja seeläbi vältida olulise teenuse toimepidevust mõjutavat intsidenti. Eluliseks näiteks Eesti praktikast on 2016. a aset leidnud lunavaraintsidendid meditsiini- ja transpordisektorist, kus lunavara levis kasutaja tööjaama kaudu terve asutuse infosüsteemi.[26] Konkreetsetel juhtudel kujutas kasutajatele põhjendamatult ulatuslike juurdepääsuõiguste andmine juba iseenesest halba administreerimispraktikat, mis võimendas intsidenti organisatsiooni tasemel. Sarnane olukord võib aga tekkida ka juhul, kui süsteemide seotus on funktsionaalselt põhjendatud – näiteks 2017. a juunis levis NotPetya arvutiviirus peamiselt kontsernisiseseid infosüsteeme pidi (Eesti ainsad konkreetse lunavarakampaania ohvrid nakatusid välisriigi emaettevõtte kaudu). Sellisel juhul on intsidendi leviku tõkestamiseks ja selle mõju vähendamiseks sobiv ja põhjendatud süsteemile juurdepääsu piiramine.

Punkt 5 kohustab teenuse osutajat kontrollima turvameetmete rakendamise piisavust ja vastavust. Nõuetele vastavuse kontrollimise üks meetod on auditi läbiviimine. Auditeerijaks võib olla pädev sõltumatu isik, kelleks võib olla vastavat kvalifikatsiooni omav audiitor või pädev riigiasutus, kelle ülesannete hulka vastav tegevus kuulub. Auditi toiminguid, mille tulemus annab sõltumatu hinnagu, võib asendada ka nn enesehindamisega. enesehindamine peab hõlmama süsteemi korrashoiu ja töökindluse tagamise kontrollimiseks vajalikke toiminguid. Teenuse osutajal on kohustus turvameetmete rakendamise kontrolli tulemused dokumenteerida. Turvameetmete rakendamise kontrolli tulemused peavad olema ajakohased kogu võrgu- ja infosüsteemi elutsükli vältel. Ajakohasus tähendab, et elutsükli vältel süsteemis läbiviidud muudatuste korral või uute turvaohtude ilmnemisel tuleb asjakohaseid süsteemi turvemeetmeid kontrollida vahetult peale muudatuse rakendamist.
Auditi tulemused tuleb Riigi Infosüsteemi Ametile esitada nõudmisel ning regulaarset dokumentide esitamise kohustust eelnõuga ette ei nähta[27].
Lõige 3 sätestab teenuse osutajale kohustuse tagada süsteemi turvanõuete täitmine juhul, kui süsteemi kasutamine volitatakse edasi teisele isikule. Sätte eesmärk on tagada, et kõik missioonikriitiliste süsteemide kasutamisega seotud osapooled hoolitseksid süsteemi turvalisuse tagamise eest vajalikul, ettenähtud tasemel.

Punkt 6 kohustab säilitama dokumentatsiooni vähemalt kolm aastat alates dokumendi loomisest. Tegemist on menetlusliku tähtajaga.

Lõikes 4 antakse volitusnorm Vabariigi Valitsusele täpsustamaks määrusega teenuse osutamiseks vajalikke turvanõudeid, millega täpsustatakse nõudeid riskide analüüsimiseks, turvameetmete rakendamiseks ning küberintsidentidest teavitamise aluseid. Olemuslikult on tegemist HOS-i § 41 lõike 3 alusel Vabariigi Valitsuse poolt 03.08.2017 vastu võetud määruses nr 133 „Elutähtsa teenuse infosüsteemide ning nendega seotud infovarade

[26] Riigi Infosüsteemi Ameti küberturvalisuse teenistuse 2016. a kokkuvõte, lk 9.
[27] NIS direktiivi artikli 15 punktis 2 sätestatu kohaselt tuleb järelevalvet teostavale asutusele esitada tõendid turvapõhimõtete tõhusa rakendamise kohta, näiteks pädeva asutuse või tunnustatud audiitori poolt läbi viidud turvaauditi tulemused, ning viimasel juhul teeksid need tulemused ja nende aluseks olevad tõendid kättesaadavaks pädevale asutusele. Teabe või tõendite esitamist taotledes esitavad pädevad asutused taotluse eesmärgi ja täpsustavad, millist teavet nõutakse.

turvameetmed“ (RT I, 09.08.2017, 3) kehtestatud nõuetega, millele lisaks määratakse kindlaks küberintsidendi olulisuse kriteeriumid küberintsidendist teavitamise kohustuse rakendumise korral. Määruse andmise volitusnorm tuuakse HOS-ist käesolevasse eelnõusse.

Eelnõu § 8 sätestab teenuse osutaja olulise mõjuga küberintsidendist teavitamise kohustuse. Lõige 1 kohustab teenuse osutajat Riigi Infosüsteemi Ametit küberintsidendist teavitama. Küberintsidendist teavitamisel on oluline kiirus, mille pärast on sätestatud, et teavitada tuleb viivitamatult, kuid on antud ka maksimaalne ajaline tähtaeg, milleks on 24 tundi küberintsidendist teada saamisest.

Lõige 2 sätestab teenuse osutajale teavitamiskohustuse. Nähakse ette, et teenuse osutaja peab olulisest küberintsidendist teavitama isikut, keda küberintsident võib mõjutada. Juhul, kui teenuse osutaja mõistliku aja jooksul teavituskohustust ei täida, siis lõikes 3 on antud Riigi Infosüsteemi Ametile volitus teavitada küberintsidendist mõjutatud isikut, mis ühtib korrakaitse seaduse §-s 26 sätestatuga. Kõigi teavitamistoimingute tegemisel, mis sisaldavad isikute õiguste kahjustamise võimalust, peab Riigi Infosüsteemi Amet kaaluma selle meetme proportsionaalsust ja teenuse osutaja võimalikku ärihuvide kahjustamist. Seepärast nähakse ette, et Riigi Infosüsteemi Amet peab enne teavitamist ja teabe avalikustamist puudutatud isikut sellest informeerima ja anda talle võimaluse vastuväidete esitamiseks.

Lisaks küberintsidendi toimumise faktile on oluline kindlaks teha ka küberintsidendi tekkepõhjused, lahendamiseks kulunud aeg, rakendatud abinõud ja küberintsidendi mõju. Kuna intsidendi puhul on esmajärjekorras oluline tegeleda selle lahendamisega, siis eelnimetatud teavet sisaldav raport tuleb lõike 4 kohaselt esitada Riigi Infosüsteemi Ametile pärast küberintsidendi lahendamist.

Lõige 5 sätestab, et kui küberintsident põhjustab isikuandmetega seotud rikkumise, teavitab Riigi Infosüsteemi Amet küberintsidendist Andmekaitse Inspektsiooni. Arvestades, et erinevad süsteemid sisaldavad vähemal või rohkemal määral isikuandmeid, võib küberintsidendi tagajärjeks olla isikuandmete töötlemise nõuete rikkumine. Seetõttu peavad Riigi Infosüsteemi Amet ja Andmekaitse Inspektsioon omavahel koostööd tegema ja asjakohast teavet vahetama.

Lõige 6 sätestab, et küberintsidentidest teavitamise ja raporti esitamise korra ja olulise mõjuga küberintsidendi kriteeriumid sätestab Vabariigi Valitsus määrusega. Kriteeriumitena tuuakse määruses välja näiteks teenuse katkestusest hõlmatud inimeste arv ja katkestuse kestus, küberintsidendi mõju sisuline ulatus, küberintsidendi mõju geograafiline ulatus ja küberintsidendi mõju teistele teenustele.

Lõige 7 sätestab, et teenuse osutaja on kohustatud teavitama Riigi Infosüsteemi Ametit digitaalse teenuse osutajat puudutavast intsidendist, kui tema teenus sõltub käesoleva seaduse §-s 4 määratletud digitaalse teenuse osutaja teenusest ning intsident mõjutab teenuse toimepidevust. Tegemist on direktiivi artikli 16 lõikest 5 tuleneva kohustusega.

Eelnõu § 9 sätestab süsteemi turvanõuded riigi ja kohaliku omavalitsuse üksuse süsteemi pidamisele.

Lõikes 1 sätestatakse, et riigi- ja kohaliku omavalitsuse asutuse süsteemi pidamisele laienevad käesoleva seaduse § 7 lõigetes 1, 2 ja 3 sätestatud kohustused ning §-s 8 sätestatud

küberintsidendist teavitamise nõuded. Olemuslikult pole viidatud eelnõu sätetes kehtestatud nõuded avaliku sektori asutustele uued, kuivõrd need sisalduvad avaliku sektori asutustele kohalduva infosüsteemide kolmeastmelise etalonturbe süsteemi (edaspidi *ISKE*) meetmetes, mille järgimise nõue on kehtestatud AvTS-i § 43^9 lõike 1 punkti 4 alusel Vabariigi Valitsuse poolt välja antud määruses „Infosüsteemide turvameetmete süsteem“ (edaspidi *ISKE määrus*).[28]

Samas tuleb AvTS-i kohaselt avaliku sektori asutustel rakendada turvameetmeid üksnes seesugustele infosüsteemidele, mis on AvTS-i tähenduses andmekogud.[29] Infosüsteemideks, mida ei saa mahutada andmekogu mõiste alla ning mis ISKE määruse mõttes pole kõik käsitletavad andmekoguga seotud infovarana, on näiteks nimeserverid, ajaserverid, meiliserverid, virtualiseerimisplatvormid, kataloogiteenus, failiserverid, testserverid, testkeskkonnad, pääsusüsteemid, monitooringu süsteemid, kettamassiivid, ruuterid, erinevad võrgu infrastruktuuri arenduskeskkonnad ja asutuse arvutivõrku ühendatud tööjaamad. Praktikas on olnud üsna sagedad olukorrad, kus asutused infosüsteemide turvalisuse tagamise kohustuse vältimiseks infosüsteeme andmekogudena ei käsitle ning neid riigi infosüsteemi haldussüsteemis (edaspidi *RIHA*) ei registreeri.

Puudulik infoturve soosib mistahes ohtude realiseerumist. Üheks suurimaks ohuks on erinevad sihitud ründed, millest võib näidetena tuua teenustõkestusründed, mille puhul koormatakse sihitud server suure hulga päringutega üle ning teenus muutub kasutajatele kättesaamatuks, või siis ründed, millega tuvastatakse erinevate teenuste olemasolu (ingl *port scan*) neile kuuluvatel IP-aadresside vahemikel. Uuendamata veebihaldustarkvara võimaldab veebilehele üles seada õngitsuslehe, paigaldada sellele ebasobivat sisu või veebilehte näotustada. Samuti on ohu allikaks uuendamata tööjaamad ja muud arvutivõrku ühendatud seadmed. Kuna kõik võrgus olevad seadmed on omavahel ühendatud, võimaldavad haavatavustega seadmed lihtsustada rünnete läbiviimist ja seada ohtu lisaks konkreetse haavatavusega seadmele ka arvutivõrgus asuvad andmekogud.

Küberintsidentide aset leidmine ei sõltu sellest, kas tegemist on infosüsteemi või andmekoguga. Näiteks võib pahavaraga nakatuda nii andmekogu käitav andmebaas kui ka tavaline faili- või meiliserver, mis ei pruugi olla seotud andmekogudega AvTS-i mõistes. Samuti võib siinkohal näiteks tuua tööjaamad ja serverid, millele ei ole paigaldatud turvapaiku ehk teisisõnu esinevad neis paikamata haavatavused, mille ärakasutamine on üheks sagedasemaks pahavara leviku viisiks. Riigi Infosüsteemi Ametile laekunud intsidentide teavituste seast leiab hulgaliselt näiteid intsidentide kohta, mis on juhtunud infosüsteemidega: veebilehtede näotustamine, turvavead veebilehtedel, pahavara jagavad serverid, krüptoviirustega nakatumine, aga ka kontode kaaperdamine, andmete lekkimine, konfiguratsioonivead, riistvara rikked, ühenduste katkemine jne. Paljude puhul neist võib tegemist olla kohatiste põhjus-tagajärg seostega (näiteks kui veebilehe näotustamine on põhjustatud turvaveast veebilehel, st risk on realiseerunud ja haavatavust on ära kasutatud). Avaliku sektori asutused pole puutumata jäänud ka lunavara juhtumitest. CERT-EE poolt on registreeritud juhtumeid, kus asutuse võrgukataloog nakatus lunavaraga või e-posti filtrist

[28] https://iske.ria.ee/8_03/

[29] Täiendavalt andmekogudele on osade avaliku sektori asutuste infosüsteemidele turvameetmete rakendamise kohustus sätestatud HOS-is, mille § 41 lõike 4 alusel välja antud Vabariigi Valituse määrus „Riigi osutatavad teenused ja avaliku võimu ülesanded, millele laienevad elektroonilise turvalisuse tagamise nõuded“ (RT I, 09.08.2017, 4) loetleb üles riigi teenused, mille osutamiseks kasutavad infosüsteemid ei pruugi kõik ilmtingimata olla andmekogud AvTS-i mõttes.

pääses läbi e-kiri selle manuses olnud lunavaraga. Samuti on esinenud juhtumeid, kus administraatori kontoga on arvutisse paigaldatud klahvinuhk[30].

Regulatsioon peab infosüsteemidest järjest kasvava sõltuvusega riigi turvalist toimimist toetama, olles selge ning vältima mitmetitõlgendamist[31]. Tänu tänapäevaste IT-lahenduste integreeritusele on infosüsteemide käsitlemine üksikute andmekogudena juba aegunud. Riigiasutuste ja kohaliku omavalitsuse (edaspidi *KOV*) üksuste infosüsteemide ebapiisav turvalisuse tase ei ole mitte üksnes oht andmete lekkele, vaid infosüsteemide töökindluse ja usaldusväärsuse tagamine on kogu riigi toimimise vaatest hädavajalik. Ka Riigikontroll on oma tähelepanekutes haldusreformi läbiviimise riskide kohta märkinud, et kui andmekogu pidamise elementaarseid turvalisusnõudeid ei järgita, on risk, et omavalitsuse kogutud tundlikud andmed satuvad ühinemise käigus või järel valedesse kätesse.[32] Riigi tervikliku küberturvalisuse tagamise vaatest ei ole otstarbekas riigi- ja KOV-i üksuse puhul kaitsmist vajavaid infosüsteeme eristada ka avalike teenuste osutamise kaudu, kuivõrd terviklikku ja süsteemset kaitset vajavad eranditult kõik avalike ülesannete täitmiseks kasutatavad infosüsteemid ja nende alamsüsteemid sõltumata infosüsteemi funktsioonist või sellest, kas infosüsteemi kasutuselevõtmine tuleb reguleerida selle põhimäärusega või infosüsteemi kaudu osutatakse avalikku teenust. Seetõttu eelnõu jõustumisel riigi osutavate teenuste loetelu, millele laienevad elektroonilise turvalisuse tagamise nõuded, seaduse rakendusaktiga ei kehtestata ning Vabariigi Valituse 03.08.2017 määrus nr 134 „Riigi osutatavad teenused ja avaliku võimu ülesanded, millele laienevad elektroonilise turvalisuse tagamise nõuded“ (RT I, 09.08.2017, 4) tunnistatakse kehtetuks. Laialdane virtualiseerimise kasutamine võimaldab ka infoturbelahendusi efektiivsemalt kasutusele võtta ning vaadelda organisatsiooni infosüsteemi ühtse tervikuna.

Kuivõrd andmekogude pidamiseks kasutatavad infosüsteemid on üks infosüsteemide alaliike, ei ole eelnõuga sätestatud kohustust rakendada nende kaitseks turvameetmeid olemuslikult uus ning selle täitmine ei nõua asutustelt lisaressurssi tingimusel, et andmekogude pidamisel AvTS-i alusel kehtestud nõudeid järgitakse[33]. Riigi- ja KOV-i asutustel ei ole eelnõuga sätestatud kohustuse jõustumisel täiendavat turvastandardit tarvis kasutusele võtta. AvTS-i alusel jäävad avaliku teabe töötlemiseks peetava ja AvTS-i tähenduses andmekogu pidamise nõuded kehtima ja eelnõuga sätestatud kohustusi täpsustab AvTS § 43^{9} lõike 1 punkti 4 alusel Vabariigi Valitsuse poolt välja antud ISKE määrus, mille ajakohastamine viiakse vajalikus osas läbi eelnõu kooskõlastamise ajal. Selle raames on plaanis kaasata muu hulgas ka kohalike omavalitsuste liitude esindajad, et riigieelarve läbirääkimistel oleks võimalik välja tuua tegelikud vajadused ning puudujäägid KOV-ide vaatest.

Eelnõu §-d 10–12 sätestavad nõuded digitaalse teenuse osutajatele.

---

[30] Ingl *keylogger*. Kurjategijad kasutavad klahvinuhki salajase info – paroolid, krediitkaardinumbrid jms – teadasaamiseks.

[31] Andmekogu mõiste ühetaoline sisustamine on asutuste poolt praktikas lubamatut mitmetitõlgendavust põhjustanud (riigi infosüsteemi kuuluv andmekogu, andmekogu, mis on asutatud seaduse või selle alusel antud õigusaktiga, riigi andmekogu, asutusesiseseks töökorralduseks kasutatav andmekogu – näiteks dokumendiregister).

[32] Riigikontrolli tähelepanekud haldusreformi läbiviimise riskide kohta, lk 2. http://www.riigikontroll.ee/tabid/206/Audit/2438/language/et-EE/Default.aspx

[33] Riigi Infosüsteemi Amet viis eelnõu väljatöötamise ajal mõningate asutuste seas läbi küsitluse, milles pea kõik osalenud kinnitasid, et suuremate asutuste jaoks oluliselt midagi väga ei muutu, sest ministeeriumite allasutused juba rakendavad infoturvet nii andmekogudele kui ka infosüsteemidele. Üksnes Eesti suurim KOV vastas, et lihtsam on turvet rakendada andmekogude kaupa, kuna nende asutuse andmekogud on enamik suhteliselt madala turbeastmega.

Eelnõu § 10 sätestab turvanõuded digitaalse teenuse osutaja süsteemile. Digitaalse teenuse osutaja on kohustatud tegema kindlaks riskid, mis ohustavad süsteemi turvalisust ning rakendama riskide juhtimiseks asja- ja ajakohaseid korralduslikke ja tehnilisi meetmeid. Selleks, et selgitada välja riskid ning neid riske juhtida, on lõikes 2 sätestatud aspektid, mida digitaalse teenuse osutaja peaks süsteemi turvalisuse tagamisel meetmete valikul arvesse võtma. Hinnata tuleks taristu turvalisust, küberintsidentide ennetamist, tuvastamist ja lahendamist, toimepidevuse haldamist, seiret, auditeerimist ja testimist ning vastavust rahvusvahelistele standarditele. Vastavalt direktiivi artiklile 16 (8) on Euroopa Komisjonil õigus võtta vastu otsekohalduvaid rakendusakte, et täpsustada süsteemi turvalisuse tagamisel arvesse võetavaid elemente ja intsidendi mõju olulisuse hindamise parameetreid. Seetõttu on lõikes 3 sätestatud nõue, et digitaalse teenuse osutaja peab juhinduma Euroopa Komisjoni rakendusmäärusest. Rakendusmäärust ei ole veel 2017. a septembrikuu seisuga avaldatud. Juhul, kui küberintsident on toimunud, siis lõikes 4 on sätestatud digitaalse teenuse osutaja kohustus selliseks olukorraks valmistuda ning rakendada asjakohaseid meetmeid, et minimeerida küberintsidendi mõju osutatava teenuse toimepidevusele.

Eelnõu § 11 seab digitaalse teenuse osutajale küberintsidendist teavitamise kohustuse. Digitaalse teenuse osutaja teavitab pädevat asutust või CSIRT-i küberintsidendist, millel on oluline mõju teenusele, viivitamata pärast küberintsidendist teada saamist. Eestis on pädevaks asutuseks ja ühtlasi ka CSIRT-iks Riigi Infosüsteemi Amet. See ei pruugi nii olla teistes liikmesriikides. Teavitama peab liikmesriiki, kus digitaalse teenuse osutaja on asutatud võikus asub kontserni emaettevõte. Kolmanda riigi puhul võib teate esitamine toimuda sinna, kus on kolmandast riigist pärit ettevõtja määranud esindaja. Seetõttu on antud võimalus teavitada vastava liikmesriigi pädevat asutust või CSIRT-i. Digitaalse teenuse osutaja edastab teavituse viisil, mis on temale kõige sobilikum. Teavituse edastamisel on eelkõige oluline teavitamise kiirus, mitte niivõrd viis, kuidas teave edastatakse. Teade peab sisaldama teavet, mis võimaldab pädeval asutusel või CSIRT-il kindlaks teha küberintsidendi piiriülene mõju. Sellegipoolest on Eestis Riigi Infosüsteemi Ametil võimalus digitaalse teenuse osutajatele anda ka juhiseid ja soovitusi, mis aitavad teavitust tulemuslikult edastada ning lihtsustavad teabe edastamist. Vastavad juhendid avaldatakse Riigi Infosüsteemi Ameti veebilehel (www.ria.ee). Sarnaselt § 10 lõikes 3 esitatud viitele Euroopa Komisjoni rakendusmäärusele, on direktiivi artiklis 16 (8) esitatud viide rakendusmääruse kehtestamiseks. Rakendusmäärus aitab digitaalse teenuse osutajal hinnata küberintsidendi mõju olulisust, et tuvastada teatamisvajadus. Direktiivi eesmärk digitaalse teenuse osutajate nõuete kehtestamise osas on eelkõige seotud liikmesriikidevahelise piiriülese koostöö tugevdamisega ning turvalisema küberkeskkonna loomisega. Seetõttu on lõikes 5 sätestatud, et digitaalse teenuse osutaja esitatud teabe põhjal teavitab Riigi Infosüsteemi Amet teisi mõjutatud liikmesriike, juhul kui küberintsidendil on oluline mõju digitaalse teenuse toimepidevusele. Kuna direktiivi eesmärk on ka laiemas plaanis kodaniku kaitsmine küberohtude eest, on olukordi, kus avalikkuse teavitamine hoiab ära suurema kahju või suurendab isikute teadlikkust. Seetõttu on lõikes 6 antud Riigi Infosüsteemi Ametile õigus teavitada avalikkust. Seda võib teha juhul, kui avalikkuse teavitamine on vajalik küberintsidendi ärahoidmiseks ja käimasoleva küberintsidendi lahendamiseks. Teavitamisel on oluline teha koostööd ka digitaalse teenuse osutajaga ning seetõttu on nähtud ette kohustus enne teavitamist temaga konsulteerida. Riigi Infosüsteemi Amet võib pärast digitaalse teenuse osutajaga konsulteerimist teavitada küberintsidendist avalikkust või kohustada digitaalse teenuse osutajat ise avalikkust teavitama. Lõikes 7 on esitatud välistus, mis kohaldub juhul, kui digitaalse teenuse osutajal puudub teave küberintsidendi olulisuse kindlaksmääramise kohta.

Eelnõu § 12 sätestab Eestis tegutsevale, kuid kolmandas riigis asutatud digitaalse teenuse osutajale kohustuse määrata esindaja. Vastav kohustus on ette nähtud direktiivi artiklis 18 lõikes 2, kusjuures on märgitud, et esindaja võib määrata sinna liikmesriiki, kus ka tegelikult teenust osutatakse. Määratud esindaja kontaktandmed tuleb teha vahetult ja püsivalt kättesaadavaks. Üheks selliseks võimaluseks on avaldamine digitaalse teenuse osutaja veebilehel. Esindaja määramine on vajalik selleks, et teenuse kasutajal, kolmandal osapoolel, mõjutatud osapoolel ja järelevalveasutustel oleks teada, kes esindab digitaalse teenuse osutajat käesoleva seaduse ulatuses olevates küsimustes. Ühtlasi sõltub esindaja määramisest ka järelevalve jurisdiktsioon. Kolmandast riigist pärit digitaalse teenuse osutaja üle toestab järelevalvet selle riigi pädev asutus, kuhu ta on määranud endale esindaja.

Eelnõu § 13 sätestab Riigi Infosüsteemi Ameti pädevuse ning ülesanded küberintsidentide ennetamisel ja lahendamisel.

NIS direktiivi kohaselt täidab CSIRT mitmeid ülesandeid, näiteks: intsidentide seire riigis, riskide ja intsidentide kohta varajaste hoiatuste esitamine ning teabe levitamine asjakohastele sidusrühmadele, intsidentidele reageerimine ja pidev riskide ja intsidentide analüüsimine. Eestis on Riigi Infosüsteemi Amet peamine küberintsidentidega tegelev ametiasutus[34]. Kuigi Riigi Infosüsteemi Ameti roll järelevalveasutusena tuleneb erinevatest seadustest, siis küberturvalisuse ennetus- ja planeerimisalased ülesanded, sh küberintsidentide käsitlemine, küberturbe seire teostamine ja ohuteadete edastamine, tulenevad majandus- ja kommunikatsiooniministri 25.04.2011 määrusest nr 28 „Riigi Infosüsteemi Ameti põhimäärus“ (edaspidi *Riigi Infosüsteemi Ameti põhimäärus*) (RT I, 29.12.2016, 14). Muu hulgas on Riigi Infosüsteemi Ameti põhimääruse § 9 kohaselt Riigi Infosüsteemi Ameti ülesanneteks käsitleda Eesti arvutivõrkudes toimuvaid ja ametile raporteerituid turvaintsidente, annab hoiatusi turvaintsidentide ennetamiseks ning tegeleda kasutajate turvateadlikkuse tõstmisega ja koostada raporteid Eesti arvutivõrkudes toimunud intsidentidest ja pahavara levikust. Lisaks sellele on Riigi Infosüsteemi Ameti ülesanne teostada küberturbe seiret, hinnates perioodiliselt küberkeskkonna turvalisust ja sellega seotud riske ning nende mõju Eesti riigile ja elutähtsatele teenustele, sealhulgas teostada riigiasutuste vahelise andmeside turvaseiret ning koordineerida riigi infosüsteemi teiste komponentide turvaseire teostamist.

Seaduse tasemel on RIA ülesannetest reguleeritud järelevalvepädevus teatud valdkondade võrgu- ja infosüsteemide turvalisuse üle, mis seisneb kontrollimisfunktsiooni täitmises selle üle, kas ettevõtjad ja asutused järgivad nendes valdkondades sätestatud turvameetmeid. Samal ajal on jäetud seaduse tasandil reguleerimata ohtu ennetavad ja tõrjuvad tegevused, nagu küberintsidentide (sh ka küberrünnakute poolt põhjustatud intsidentide) käsitlemine, hoiatuste ehk ohuteadete andmine küberintsidentide ennetamiseks (näiteks levivate lunavara kampaaniate korral) ning küberturbe seire teostamine.

HOS § 2 lõige 3 sätestab kriisireguleerimise termini, mis on meetmete süsteem, mis hõlmab hädaolukorra ennetamist, hädaolukorraks valmistumist ja hädaolukorra lahendamist. HOS-i seletuskirjas täpsustatakse, et ennetamine hõlmab tegevusi, mis võivad olla mh õiguslikud (näiteks tuletegemise keeld metsas või jäälemineku piiramine) kui ka teadlikkust tõstvad (teavitamine, koolitamine). Kriisireguleerimise põhimõtete järgi (HOS-i § 3) vastutab iga asutus oma valdkonna kriisireguleerimisülesannete täitmise eest ning täidab põhitegevusega

[34] 2016. a. advokaadibüroo LEXTAL teostatud „Kübervaldkonna õigusanalüüs“ raames läbi viidud intervjuudest selgus, et kokkuleppeliselt peetakse Riigi Infosüsteemi Ametit kübervaldkonna eest vastutavaks asutuseks. https://www.ria.ee/public/Kuberturvalisus/Kubervaldkonna-oigusanaluus-Lextal-2016.pdf

seotud ülesandeid ka hädaolukorra ja eriolukorra ajal, kui HOS-is või teistes õigusaktides ei ole sätestatud teisiti.

Riigi Infosüsteemi Ameti tegevus küberintsidentide ennetamisel ja nende lahendamisel ühtib küll HOS-i §-s 3 sätestatud kriisireguleerimise ühe põhimõttega, mille kohaselt teevad asutused ja isikud hädaolukordade ennetamisel, nendeks valmistumisel koostööd ning pakuvad üksteisele abi, kuid nagu eelnevalt märgitud, täidab Riigi Infosüsteemi Amet käesoleval ajal oma ülesandeid üksnes asutuse põhimääruse alusel, mis on seega ka HOS-is sätestatud ennetustegevuse läbiviimisel, hädaolukorras ohu tõrjumisel ja hädaolukorra lahendamisel ebapiisav. Lisaks sellele on HOS hädaolukorda reguleeriv seadus, kuid küberintsident või selle oht ei pruugi kaasa tuua hädaolukorda. Puudujäägile Riigi Infosüsteemi Ameti tegevust puudutavas regulatsioonis ning vajadusele sätestada Riigi Infosüsteemi Ameti ülesanded seaduse tasemel on viidatud ka varasemates õigusanalüüsides.[35]

Kuivõrd avalik võim on õigustatud tegutsema üksnes siis, kui seadus annab selleks volituse, tuleb eelnimetatud ülesannete täitmiseks Riigi Infosüsteemi Ameti ülesanded ja volitused seaduse tasemel sätestada. Eesti Vabariigi põhiseaduse (RT I, 15.05.2015, 2) (edaspidi *PS*) § 3 lõike 1 esimese lause kohaselt teostatakse riigivõimu üksnes põhiseaduse ja sellega kooskõlas olevate seaduste alusel. Sellest tuleneb täitevvõimu põhiseaduslik seotus seaduse ja õigusega, mis on üks vabadusliku õigusriigi möödapääsmatutest tingimustest. Riigikohus on oma otsuses[36] selgitanud, et seaduslikkuse kui (rahvusvahelise) õiguse üldtunnustatud põhimõtte ning PS-i §-s 3 sätestatud printsiibi kohaselt võib põhiõigusi ja vabadusi piirata üksnes seaduse alusel. Seadusega kindlaksmääratud ja avalikustatud õiguste ja vabaduste piiramise kord ning avalikkus võimaldab valikuvabaduse ning tagab võimaluse vältida võimu kuritarvitust. Põhjaliku seadusandliku regulatsiooni puudumine ja varjatus jätab aga isiku ilma õigusest informatsioonilisele enesemääratlusele, valida käitumisjoont ja end kaitsta. Sealjuures peab sellised küsimused, millega piiratakse isikute põhiõigusi, otsustama seadusandja ning seadusandja ei saa seda edasi delegeerida täitevvõimule[37]. PS-i § 3 lõike 1 esimene lause sisaldab seega olulisuse põhimõtet ja seadusliku aluse nõuet. See tähendab, et igal põhiõiguse riivel peab olema seaduslik alus ning seadusandja ei saa aluse kehtestamist delegeerida täitevvõimule. Riigikohus on oma praktikas leidnud, et avalik võim on õigustatud tegutsema üksnes siis, kui seadus annab selleks volituse[38], mistõttu eeldab põhiõiguste piiramine seadusandjast alamalseisva organi poolt seadusandja volitust. Sellest tulenevalt sätestatakse eelnõus Riigi Infosüsteemi Ameti volitused küberintsidentide käsitlemiseks, ohuteadete edastamiseks ning küberturbe seire teostamiseks, mis puudutavad ka teisi isikuid (eraõiguslikke isikuid, avalik-õiguslikke isikuid ja teisi riigiasutusi).

Lõikes 1 sätestatakse Riigi Infosüsteemi Ameti pädevus küberturvalisuse tagamisel – koordineerida küberintsidendi lahendamist, kui see on põhjustanud ka näiteks hädaolukorra ohu või hädaolukorra HOS-i tähenduses. Selline vajadus võib tekkida, kui küberintsidendist puudutatud ettevõttel või asutusel puudub piisav ressurss või kompetents või küberintsidendi lahendamiseks on vajalik koordineerida mitmete asutuste vahelist koostööd.

---

[35] *Ibid*. Lisaks: 2013. a advokaadibüroo SORAINEN AS teostatud „Kriisireguleerimise valdkonna juriidiline analüüs“ https://www.siseministeerium.ee/sites/default/files/dokumendid/kriisireguleerimise_valdkonna_juriidiline_analuus.pdf . 04.09.2017.
[36] RKPJKo III-4/A-1/94.
[37] *Ibid*.
[38] 3-3-1-41-00.

Lõikes 2 sätestatakse, et Riigi Infosüsteemi Amet teostab küberintsidentide ennetamiseks üldist seiret, analüüsib süsteemide turvalisust ohustavaid riske ning nende mõju Eesti riigile ja teenuste toimepidevusele. Seire eesmärgiks on järgmiste küberintsidentide ärahoidmine, kuid ka küberintsidentide lahendamise võimekuse suurendamine. Üldist seiret, mida teostab CERT-EE, saab liigitada peamiselt kolmeks:
1. riigiasutuste infosüsteemide seire
2. riigiasutuste andmeside (ASO) võrguliikluse seire
3. .ee avatud võrkude seire

Eesti võrgu seire teel otsitakse haavatavaid seadmeid ja programme. Võrkude seiret on võimalik teha avalikult kasutatava tarkvaraga ning see on kättesaadav igaühele, mitte üksnes riigiasutustele. Kuigi sellise tegevusega ei kaasne isikuandmete ega privaatsuse riivet, peab seesuguseks tegevuseks vastav volitusnorm olema siiski sätestatud seaduse tasemel, kuivõrd seaduslikkuse põhimõttest peab riigiasutuse tegevusel olema seaduslik alus.

Lõikes 3 sätestatakse Riigi Infosüsteemi Ametile volitus edastada isikutele küberintsidentide ennetamiseks ja lahendamiseks ohuteateid, mis võimaldavad rakendada küberintsidendi mõju vältivaid või vähendavaid abinõusid. Nimetatud teated edastatakse asjakohasel viisil, mis tagab tõhusalt teadete kättesaamise potentsiaalselt mõjutatud isikutele.

Teavitamine puudutab mitte üksnes teenuste osutajaid, vaid ka teisi kasutajaid, keda tuleb ohtu kujutavast küberintsidendist teavitada. Teavitamise all peetakse silmas konkreetsest ohust teavitamist (küberintsidendi korral) kui ka kaudsest ohust teavitamist (näiteks uutest ründevektoritest teavitamine või tarkvara uuendamise soovitused). Teavitamise viis sõltub olenevalt olukorrast ja teavitatavate isikute ringist – näiteks võib Riigi Infosüsteemi Amet avalikkusele ohuteateid edastada ringhäälingu, ajakirjanduse või interneti vahendusel, üksikkasutajat aga sideettevõtja kaasabil. Teavitamine kujutab endast nn pehmet meedet, mis kellegi õigusi ei riiva ka juhul, kui Riigi Infosüsteemi Amet avalikustab avaliku korra kaitsmise huvides andmeid mõne konkreetse küberintsidendi kohta, kuivõrd üldsusele avalikustatav teave on üldistatud kujul, milles ei tooda välja isikute eraelu ja perekonnaelu või ettevõtete ettevõtlusvabadust ja ärihuvide riivavaid asjaolusid.

Lõikes 4 sätestatakse, et Riigi Infosüsteemi Ametil on õigus välisriigile, Euroopa Võrgu- ja Infoturbe Agentuurile või muule organisatsioonile edastada küberintsidentide ennetamise ja lahendamisega seotud teavet käesolevas seaduses sätestatud ülesannete või Euroopa Liidu õigusest tuleneva kohustuse täitmiseks või välislepinguga ettenähtud juhtudel ja korras. Kuivõrd pole välistatud, et küberintsidentide kohta käiv teave (selle tekkepõhjused, mõjutatud isikud jmt) võib omada puutumust isikuandmete töötlemise rikkumisega, riigi julgeoleku tagamisega, kuriteoga, kuid ka riigisaladuse või salastatud välisteabega, edastatakse teave iga kord ka vastavale pädevale asutusele (Andmekaitse Inspektsioonile, Kaitsepolitseiametile, Politsei- ja Piirivalveametile, Välisluureametile). Koostöörühmas ja CSIRT-ide võrgustikus küberintsidentide kohta teabe jagamine võib kaasa tuua isikuandmete töötlemise vajaduse, kuid igal üksikjuhtumil tuleb hinnata, kas isikuandmete edastamine osana küberintsidenti puudutavast teabest on ilmtingimata vajalik küberintsidendi lahendamiseks või selle edasise leviku piiramiseks.

Lõikes 5 sätestatakse, et kuna küberintsident ja sellekohane teave võib olla tundlik, on oluline, et Riigi Infosüsteemi Amet kaitseks teabe edastamisel kooskõlas kehtiva õigusraamistikuga teabe konfidentsiaalsust ning arvestaks teenuse osutaja või digitaalse teenuse osutaja

turvalisuse ja ärihuvidega. Andmete edastamisel ja muul viisil töötlemisel tuleb järgida isikute õigust eraelu puutumatusele, ettevõtlusvabadusele ja omandile.

Eelnõu § 14 sätestab küberintsidentide registri asutamise ja pidamise õigusliku aluse ja registri pidamise eesmärgi. Kuivõrd tegemist on andmekoguga, peab register olema asutatud seaduse alusel. Registri põhimääruse kavand saadetakse kooskõlastusele koos eelnõuga.

Eelnõu § 15 sätestab riikliku ja haldusjärelevalve teostamise. Eelnõus ja selle alusel kehtestatud õigusaktides sätestatud nõuete täitmise üle teostab riiklikku ja haldusjärelevalvet Riigi Infosüsteemi Amet.

Lõige 2 sätestab järelevalve erisuse digitaalse teenuse osutajate suhtes. Vastavalt NIS direktiivile on digitaalse teenuse osutajate järelevalve *ex post*, mistõttu on vaja sätestada erisus. Riiklikku järelevalvet digitaalse teenuse osutajate nõuete täitmise üle teostatakse üksnes juhul, kui järelevalveasutust teavitatakse, et digitaalse teenuse osutaja ei täida §-des 10 ja 11 kehtestatud nõudeid. Lisaks sellele on oluline ka jurisdiktsiooni küsimus nende teenuse osutajate suhtes, kes on asutatud Eestis või kelle emaettevõte on asutatud Eestis, või kolmanda riigi digitaalse teenuse osutaja suhtes, kellel on Eestis esindaja. Järelevalvepädevus laieneb just sellistele digitaalse teenuse osutajatele.

Eelnõu § 16 sätestab riikliku järelevalve erimeetmed.

Riigi Infosüsteemi Amet täidab KorS-st tulenevalt korrakaitseorgani ülesannet ning talle laienevad korrakaitseorgani volitused vastavalt eriseadustega kehtestatud piirangutele. Vastavalt KorS-i §-le 133[1] võib korrakaitseorgan KorS-is sätestatud riikliku järelevalve teostamiseks kohaldada korrakaitseseaduse §-des 30, 31, 32, 49, 50, 51, 52 sätestatud riikliku järelevalve erimeetmeid KorS-is sätestatud alusel ja korras. Riikliku järelevalve menetluse eesmärgiks on ohu avalikule korrale tõrjumine: preventiivne eesmärk, sh süüteoennetus ning veel lõpetamata süüteo tõkestamine. Lõikes 1 on loetletud korrakaitse erimeetmed, mis kohaldavad kõikide seaduse reguleerimisalas olevate teenuse osutajate suhtes. Lõikes 2 on esitatud täiendav meede, mida kohaldatakse teenuse osutajate suhtes, kes peab täitma eelnõu § 7 ja 8 nõudeid. Lõike 2 erimeedet ei kohaldata digitaalse teenuse osutaja suhtes, kuna tegemist oleks ebaproportsionaalse meetmega. Nimelt on NIS direktiivi digitaalse teenuse osutajate regulatsioon maksimumharmoniseerimine ning turu reguleerimine direktiivist rangemate nõuetega ei ole võimalik.

Eelnõu § 17 sätestab Riigi Infosüsteemi Ametile küberintsidendi tõkestamise õiguse andmise.

PS-i §-st 13 tulenevalt on igaühel õigus riigi ja seaduse kaitsele. PS-i § 14 järgi on riigil kohustus luua põhiõiguste kaitseks kohased menetlused[39], mis teisisõnu tähendab, et isikul on kaitseõigusest tulenevalt õigus nõuda riigi aktiivset sekkumist ja riigil on kohustus võtta tarvitusele vastavad abinõud kolmanda isiku suhtes. Riigi poolt ohu mittetõrjumine võib ühiskonnas tekitada ebakindlust ja usaldamatust riigi vastu[40]. Sealjuures on isikul õigus nõuda riigilt seda, et riik looks vastavad asutused ning annaks neile asutustele piisavad volitused, et nendel asutustel oleks võimalik faktiliselt isiku põhiõiguseid kaitsta[41].

[39] RKPJKo 3-4-1-4-03, punkt 16.
[40] Korrakaitse seaduse eelnõu 424 SE II seletuskiri lk 2.
[41] HOS-i § 12 lõike 1 alusel saab Riigi Infosüsteemi Amet, juhul kui küberintsidendi mõõtmed eskaleeruvad hädaolukorraks, asuda viidatud sätte alusel hädaolukorra lahendamist juhtima. HOS-i seletuskirjas täpsustatakse, et viidatud normis räägitakse hädaolukorra lahendamisest, mitte aga hädaolukorra ohu tõrjumisest. See, milliseid

Sekkumismeetme sätestamist toetab ka rahvusvahelise õiguse hoolsuskohustuse (*due diligence*) põhimõte, mille kohaselt on riigil kohustus tagada, et tema territooriumil asuvat taristut ei kasutataks teisi riike kahjustavaks tegevuseks. Põhimõte sisaldab nii riigi kohustust teiste riikide ees kui ka nõudeõigust nende suhtes: ühelgi riigil ei ole õigust teadlikult lubada oma territooriumi kasutada teise riigi territooriumi või seal asuvaid isikuid või vara kahjustavaks tegevuseks, kui sellisel tegevusel on tõsine tagajärg ja kahju tekkimine on selgelt ja veenvalt tõendatud.[42] Vastava kohustuse rikkumine annab kannatanud riigile õiguse kasutada vastumeetmeid kohustust rikkunud riigi suhtes, mh toimida viisil, mis muul juhul kujutaks endast rahvusvahelise õiguse (nt suveräänsus- ja mittesekkumispõhimõtte) rikkumist.[43]

Samasugust hoolsuskohustuse nõuet toetab ÜRO küberturvalisuse valitsusekspertide grupi (UN Group of Government Experts) 2015. aasta konsensusraport, mis sedastab, et riigid ei tohiks teadlikult lubada oma territooriumil kübervahendite abil teiste riikide õiguste rikkumist ega elutähtsa teenuse osutamiseks kasutatava taristu kahjustamist ning peaksid kohaste meetmetega tagama elutähtsate teenuste kaitse küberohtude eest.[44] Konsensuslikult pidasid hoolsuspõhimõtet siduvaks ka Tallinna Käsiraamatu koostanud õiguseksperdid.[45]

Lõikes 1 sätestatakse meetme kohaldamise üldalus ning eesmärk. Tegu on *ultima ratio* abinõuga, kui küberintsident ohustab inimeste elu või tervist, suure väärtusega varalist hüve (sh paljude teiste elutähtsate või ühiskondlikult oluliste süsteemide või avalikku korda[46]. Meetme kohaldamisele peab eelnema kaalumine selle kohaldamise adressaadiks oleva isiku ja teiste, olukorrast mõjutatud isikute põhiõiguste vahel, mis avaldub selles, et Riigi Infosüsteemi Amet peab tagama küberintsidendi õiguspärase ja otstarbeka lahendamise. Kaalutlusõigus avaldub selles, et haldusorgan saab valida avaliku võimu ülesande või avaliku võimu ülesande teostamist toetava ülesande kindla, õiguspärase ja otstarbeka täitmise tagamise meetmete vahel.

HOS-i sätteid hädaolukorra ohu korral kohaldatakse, on sätestatud HOS-i §-s 17, mille kohaselt juhib hädaolukorda juhtiv asutus hädaolukorra lahendamist mh õigusaktides ning hädaolukorra lahendamise plaanis sätestatu kohaselt (HOS § 14 lõige 4) ja lähtudes Vabariigi Valitsuse 22.06.2017 määrusest nr 112 „Hädaolukorra lahendamise juhtimise, lahendamisel osalevate asutuste ja isikute koostöö, avalikkuse teavitamise ja asutustevahelise teabevahetuse ning ulatusliku evakuatsiooni läbiviimise nõuded ja kord“ (RT I, 28.06.2017, 39). Samas HOS ega selle alusel antud määrused ei sätesta Riigi Infosüsteemi Ametile konkreetseid meetmeid küberintsidendist tingitud hädaolukorra ohu tõrjumiseks ega hädaolukorras, ammugi nn tavaolukorras, mis ei ole veel HOS-is sätestatud kriisiolukorra mõõtmeid võtnud. Ometi võivad küberruumis toimuvad intsidendid kiiresti kriisiks eskaleeruda ja nende tagajärjel tekkivad mõjud otsest varalist, keskkonna- või tervisekahju põhjustada.

[42] Põhimõte pärineb Rahvusvahelise Kohtu otsustest Trail Smelter Arbitration (U.S. *vs.* Can.), 3 R.I.A.A. 1911, 1963 (Arb. Trib. 1941) ja Corfu Channel (UK *vs.* Alb.), Judgment, 1949 I.C.J. 4, 22 (April 9).

[43] Draft articles on Responsibility of States for Internationally Wrongful Acts (2001). http://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf. Artiklid 22, 49–54.

[44] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. (2015) A/70/174 , III osa, punktid c, f ja g.

[45] Tallinn Manual on the International Law of Cyber Warfare (2013), Rule 5.

[46] Enamasti mõistetakse avaliku korrana mis tahes seaduslikkust, põhiseadusliku korra mõiste hõlmab riigi institutsioonide (riigivõimu) toimimist, olulisemate põhiõiguste tunnustamist ja inimväärikuse tunnustamist. Põhiseaduslik kord moodustab avaliku korra tuuma. Põhiseadusliku korra hulka kuuluvad need avalikku korda tagavad normid, mis loovad riigi võimaluse eksisteerida ja ühiskonnasuhteid reguleerida. KorS § 4 lg 1 sätestab avaliku korra kui ühiskonna seisundi, milles on tagatud õigusnormide järgimine ning õigushüvede ja isikute subjektiivsete õiguste kaitstus.

Lõikes 1 kirjeldatud toimingud süsteemi kasutamist või juurdepääsu süsteemile piirata on varieeruvad (nt süsteemi või selle komponentide sulgemine või välja lülitamine, samuti süsteemi või selle komponentide ligipääsude piiramine, erinevate funktsioonide sulgemine või peatamine, infosüsteemi nn süstitud (*injected*) pahatahtlike komponentide välja lülitamine, kustutamine või sulgemine). Meetme rakendamisel tuleb järgida isikute õigust eraelu puutumatusele ja isikuandmete kaitsele, samuti sõnumisaladusele, ettevõtlusvabadusele ning õigust omandile. Et järelevalvemeetme rakendamine kujutab endast avaliku ülesande täitmist, on taolisel eesmärgil isikuandmete töötlemine lubatud. Meede on eesmärgi saavutamiseks sobiv, sest riigi kaitsekohustusest tulenevalt peab ulatuslikuma ning kiiresti leviva küberintsidendi korral olema seaduses sätestatud õigus isikute subjektiivsete hüvede kaitseks ohu tõrjumiseks sekkuda ka avaliku võimu asutuse enda poolt juhul, kui muud meetmed on küberintsidendi leviku tõkestamiseks ammendunud, mis tähendab, et kohustust ei ole võimalik sundtäita asendustäitmise või sunniraha rakendamisega või need sunnivahendid ei ole piisavalt efektiivsed. Meede on vajalik, sest KorS-is sätestatud meetmed ei ole küberintsidendist tingitud kõrgendatud ohu väljaselgitamiseks või selle tõrjumiseks piisavad.

Eelnõus ette nähtud sekkumisõiguse sätestamine on küberruumis avalikku korda ähvardava kõrgendatud ohu korral on antud meetmega on vajalik, et tagada ohule operatiivne reageerimine. Sellise küberintsidendi võib olla põhjustanud näiteks küberrünnak[47]. Samas on küberintsidendi ilmsikstulekul selle tekkepõhjuseid (näiteks administreerimisviga või tahtlik ja suunatud tegevusest põhjustatud intsident) kindaks määrata sageli võimatu ning need selginevad küberintsidendi lahendamise ajal või isegi pärast seda. Küberintsidendi kui ühe avaliku korra rikkumise väljendusvormi kiire tõrjumise vajaduse aspektist ei oma tähtsust selle toimepanija isiku tuvastamine ega toimepanemise asjaolud.

Meede on ka mõõdukas, sest kõrgendatud ohu väljaselgitamise või selle tõrjumise vajadus Riigi Infosüsteemi Ameti poolt saab tulla kohaldamisele üksnes siis, kui küberintsidenti pole õnnestunud lahendada tavapäraste meetmetega ning küberintsidendi kiire levik ohustab selle neutraliseerimata jätmise korral väga paljude inimeste elu või tervist või võib põhjustada teiste infosüsteemide kasutajatele suurt majanduslikku kahju.

KorS § 29 sätestab üldnormi, mille kohaselt võib pädev korrakaitseorgan ise kohaldada meetmeid ohu tõrjumiseks või korrarikkumise kõrvaldamiseks, kui avaliku korra eest vastutavat isikut ei ole või kui isik ei saa või ei saa õigel ajal ohtu tõrjuda või korrarikkumist kõrvaldada. Seda üldnormi täpsustavad KorS- § 49 (vallasasja läbivaatus) ning KorS-i § 50 (valdusesse sisenemine). KorS-i seletuskirjas selgitatakse, et asja ja omandi mõistete määratlemisel võib lähtuda neile tsiviilõiguses, tsiviilseadustiku üldosa seaduses (RT I, 12.03.2015, 106, edaspidi *TsÜS*) ja asjaõigusseaduses (RT I, 12.03.2015, 106, edaspidi *AÕS*),

[47] Küberrünnakuna, mis on küberturvalisuse peamine ohuallikas, mõistetakse igasugust tegevust, mis on suunatud arvutivõrgu funktsioonide kahjustamisele poliitilistel või rahvusliku (riigi) turvalisuse kaalutlustel (O.A. Hathaway, R. Crootof, P. Levitz, H. Nix, A. Nowlan, W. Perdue, J. Spiegel. The law of cyber attack. – California Law Review 2012/100 (4), lk 826). Definitsiooni autorid selgitavad, et tegemist on aktiivse teoga, mis avaldub kas süüteona või selle vastase kaitsetegevusena. Nimetatud aktiivne tegevus võib ilmneda erinevatel viisidel: tungitakse vastase arvutisüsteemi või rünnatakse seda, pannakse arvutisüsteem käituma valdaja tahte vastaselt või kahjustatakse muul viisil selle toimimist. Rünnaku objekt peab olema konkreetne arvutisüsteem, millele on võimalik kommunikatsioonikanaleid kasutades ligi pääseda – tavapäraselt interneti kaudu. Viimane definitsiooni osa – poliitiline või rahvuslik (riiklik) kaalutlus – on element, mis eristab küberrünnakut küberkuriteost. Riikliku toimija poolt algatatud agressiivne kübertegevus on oht teise riigi julgeolekule ning seetõttu käsitletakse seda küberrünnakuna. Olenevalt ulatusest võib see võtta ka kübersõja mõõtmed. Riigisektori välise toimija poolt toimepandud tegu saab küberrünnakuna käsitleda juhul, kui see on seotud poliitilise või rahvusliku (riikliku) turvalisuse kaalutlusega. Vastasel juhul on tegemist küberkuriteoga (interneti teel toime pandud vargused, piraatlus ja intellektuaalomandi vargus jm).

antud sisust (TsÜS § 49, AÕS § 68 lõige 1). Võrgu ja infosüsteemi puhul pole tegemist vallasasjaga TsÜS-i § 50 lõike 2 ja § 49 lõike 1 alusel. TsÜS-i kommentaaride kohaselt ei ole arvutiprogrammid asjad, vaid mõttetegevuse tagajärjel tekkinud immateriaalne hüve[48]. Kuigi konkreetse seadme (nt arvuti) puhul võib olla tegemist vallasasjaga, ei saa selles sisalduvad programmid ja info olla vallasasjad, mistõttu ei ole võimalik nende läbivaatust KorS-i § 49 alusel läbi viia. Samal põhjusel ei ole võimalik infosüsteemi sisenemist käsitleda valdusesse sisenemisena. AÕS-i § 32 sisustab valdust tegeliku võimuna asja üle. Samuti viidatakse KorS-i § 50 lõikes 1 sisenemisele piiratud või tähistatud kinnisasjale, ehitisse, eluruumi või ruumi, sealhulgas avada uksi, väravaid ja kõrvaldada muid takistusi. Kuigi infosüsteemis on võimalik samuti „uksi avada“, viidatakse §-s 50 selgelt kinnisasjale sisenemisele, mida infosüsteemid (sh ka mis tahes võrku ühendatud seadmed) aga selgelt pole.

Lõige 2 loetleb need juhud, millal on põhjendatud süsteemi kasutamise või juurdepääsu süsteemile piiramine. Selleks et põhiõiguste riive oleks piisavalt selge ja ettenähtav, on meetme kohaldamist piiritletud lõike 2 punktides 1–4 esitatud kumulatiivsete eeltingimustega.

Lõikes 3 nähakse ette kohustus esimesel võimalusel süsteemi haldajat meetme kohaldamisest teavitada. Teavitamise eesmärk on tagada süsteemi haldajale võimalus nõuda meetme rakendamise tulemusel talle tekitatud kahju hüvitamist ja teiseks tagada süsteemi haldajale õigus saada teavet kooskõlas hea halduse põhimõttega teda puudutava menetluse ja menetlustoimingute läbiviimise kohta.

Lõige 4 sätestab, et meetme kohaldamise protokollimine on kohustuslik. See kohustus tagab nõuetekohase dokumentatsiooni olemasolu.

Lõike 5 alusel saab meedet kohaldada üksnes Riigi Infosüsteemi Ameti peadirektori vastava korralduse alusel, millega tagatakse meetme kohaldamise üle otsustamine vajalikult kõrgel tasandil, et vältida avaliku võimu omavoli rakendamist.

Eelnõu § 18 sätestab haldusjärelevalve teostamise.

Lõikega 1 antakse Riigi Infosüsteemi Ametile õigus saada juurdepääs süsteemidele, sh kasutatavale tarkvarale, ning haldusjärelevalve käigus kontrollida infovara kasutamist.

Lõige 2 sätestab tingimused, millal võib Riigi Infosüsteemi Amet siseneda asutuse infosüsteemi haldaja või muu õigustatud isiku loata.

Lõige 3 loetleb juhud, millal on põhjendatud süsteemi kasutamise või juurdepääsu süsteemile piiramine.

Lõikes 4 nähakse ette kohustus esimesel võimalusel süsteemi haldajat meetme kohaldamisest teavitada.
Lõige 5 sätestab, et meetme kohaldamise protokollimine on kohustuslik. See kohustus tagab nõuetekohase dokumentatsiooni olemasolu.

Lõike 6 alusel saab meedet kohaldada üksnes Riigi Infosüsteemi Ameti peadirektori vastava korralduse alusel, millega tagatakse meetme kohaldamise üle otsustamine vajalikult kõrgel tasandil,

[48] § 49, p.3.1.3.

Eelnõu § 19 piiritleb vastutuse nõuete rikkumise eest. Füüsilist isikut karistatakse käesolevas seaduses ja selle alusel sätestatud õigusaktides sätestatud turvanõuete rikkumise eest rahatrahviga kuni 200 trahviühikut. Juriidilise isiku puhul on rahatrahvi suuruseks 20 000 eurot. Kuna eelnõu reguleerib Eesti küberturvalisuse tagamist ning kohustused ja nõuded on sätestatud piiritletud ringile ning olulistele ja suurematele teenuse osutajatele, siis on vajalik piisavalt kõrgete trahvimäärade määramine, et tagada meetme soovitud mõju.

Eelnõu § 20 sätestab väärteo menetleja, kelleks on Riigi Infosüsteemi Amet.

Eelnõu §-d 21–26 on rakendussätted**.**

Rakendussätetega muudetakse seadusi, kus turvanõuete rakendamise kohustuses viidati HOS-ile. Käesolevas eelnõus on vastavad nõuded esitatud §-des 7 ja 8 ning eriseaduste muutmine on tingitud vastava viite korrektseks muutmisest.

Ainsaks sisuliseks uueks sätteks on § 22 lõige 5, mis sätestab Riigi Infosüsteemi Ametile teabe andmise kohustuse.

Elektroonilise side seaduse (edaspidi *ESS*) kehtiva redaktsiooni § 102 lõike 2 kohaselt võib andmeid sideteenuse kasutamise üksikasjade kohta, sidevõrgu kaudu edastatava sõnumi sisu ja vormi kohta ning andmeid sõnumi edastamise aja ja viisi kohta avaldada üksnes kliendile ja kliendi nõusolekul ka kolmandatele isikutele. Ilma kliendi nõusolekuta võib sideettevõtja eelnimetatud andmeid või nende osasid edastada järgmistele asutustele:
1) kriminaalmenetluse seadustiku kohaselt uurimisasutusele, jälitusasutusele, prokuratuurile ja kohtule;
2) julgeolekuasutusele;
3) väärteomenetluse seadustiku kohaselt Andmekaitse Inspektsioonile, Finantsinspektsioonile, Keskkonnainspektsioonile, Politsei- ja Piirivalveametile, Kaitsepolitseiametile ning Maksu- ja Tolliametile;
4) väärtpaberituru seaduse kohaselt Finantsinspektsioonile;
5) tsiviilkohtumenetluse seadustiku kohaselt kohtule;
6) jälitusasutusele kaitseväe korralduse seaduses, maksukorralduse seaduses, politsei ja piirivalve seaduses, relvaseaduses, strateegilise kauba seaduses, tolliseaduses, tunnistajakaitse seaduses, turvaseaduses, vangistusseaduses ja välismaalaste seaduses sätestatud juhtudel;
7) Tehnilise Järelevalve Ametile.

Kuivõrd Riigi Infosüsteemi Ametit nimetatud loetelus ei ole, siis sideettevõtjatel Riigi Infosüsteemi Ametile andmete edastamise kohustus puudub. Teabe saamise õigus on seotud eelnõu §-s 12 sätestatud Riigi Infosüsteemi Ameti ülesande täitmiseks (Riigi Infosüsteemi Amet teostab süsteemide kaitse tagamiseks ja küberintsidentide ennetamiseks üldist seiret ja edastab ohuteateid) ja vajalik näiteks olukorras, kus Riigi Infosüsteemi Amet CERT saab teiste riikide väliskolleegidelt informatsiooni, et Eesti arvutivõrgus asuv seade on nakatunud ohtliku pahavaraga, mis võib ohustada Eestis asuvaid elutähtsa teenuse osutajaid. Ohu kõrvaldamiseks peab Riigi Infosüsteemi Ameti CERT tuvastama pahavara jagava seadme ja tegema kindlaks ka ründeobjektid (sh nakatunud seadmed). Sealjuures on Riigi Infosüsteemi Ameti CERT-il vaja välja saata ohuteateid sideettevõtjale, et nende võrgus on teatud IP-aadresside puhul tuvastatud pahavara.

Ohu tõrjumiseks eelnevalt kirjeldatud viisil on Riigi Infosüsteemi Ameti CERT-il vaja tuvastada, millise IP-aadressiga seade ohtu põhjustab või millise IP-aadressiga seadet

ohustatakse. IP-aadressi tuvastamise järel on vaja analüüsida ka interneti kasutamise ajalugu, et tuvastada probleemi allikas – kuidas sattus seadmesse või programmi kahjurvara. Ohtu põhjustava või ohustatud allika tuvastamine saab toimuda üksnes võrguvoo info alusel, mis peab kätkema interneti seansi algust, lõppu, seadme IP-aadressi, protokolli ja pordi numbrit (serveripoolne pordinumber ehk kliendilt serverisse liikuvate pakettide sihtport ja vastuspakettide lähteport).

Eelkirjeldatud võrguvoo info puhul on ESS-i § 111[1] kontekstis osaliselt tegemist lõike 3 punktis 6 kirjeldatud andmetega, milleks on viidatud sätte kohaselt internetiseansi alguse ja lõpu kuupäev ning kellaaeg konkreetse ajavööndi järgi koos internetiprotokolli aadressiga, mille on kasutajale eraldanud internetiteenuse osutaja, ja kasutajatunnusega. Sideandmete küsimise korral saab Riigi Infosüsteemi Ameti järelepärimise sisu olla seotud ainult säilitatavate andmetega. Vastavalt ESS-i § 111[1] lõikele 4 säilitatakse sideandmeid üks aasta side toimumise ajast alates, kui need sideteenuse osutamise käigus on loodud või neid on töödeldud. Eeltoodust nähtub, et tegemist ei ole täiesti uut liiki teabe andmise kohustusega ning põhjendamatu oleks kahtlus, et sideettevõtjate poolt Riigi Infosüsteemi Ameti CERT-ile edastatav teave ei ole kaitstud kolmandate asjassepuutumatute isikute eest.

Tuleb rõhutada, et IP-aadresside puhul ei seostata neid kasutajaga, vaid seadmetele omistatud IP-aadressidega, mistõttu isikuandmete töötlemist ei toimu. Seetõttu nähakse eelnõus ESS-i täiendavas sättes ette ka selge välistus kasutajatega seotud andmete väljaandmiseks sideettevõtjate poolt. Eelnõu jõustumisel on Riigi Infosüsteemi Ameti CERT-ile sideettevõtjate poolt edastatav teave sedavõrd tehnilist laadi, et selle töötlemine CERT-i poolt PS-i §-s 26 kaitsealasse jäävat perekonna- ja eraelu puutumatust ei riiva.

Juhul, kui küberintsidendist põhjustatud ohu tõrjumiseks on vajalik kasutaja teavitamine, siis eelkirjeldatud info alusel saab Riigi Infosüsteemi Amet vajadusel välja saata ohuteateid sideettevõtjatele, et nende võrgus on teatud IP-aadresside puhul tuvastatud pahavara, ning paluda neil IP-aadressi kasutajat teavitada, mis on kooskõlas ESS-i § 101 lõikes 2 sideettevõtjale sätestatud kohustusega, mille kohaselt peab sideettevõtja konkreetse ohu korral sideteenusele või sidevõrgu turvalisusele viivitamata teavitama klienti sellisest ohust mõistlikul viisil, ning kui oht pole sideettevõtja poolsete meetmetega kõrvaldatav, siis ka võimalikest abivahenditest ja nendega kaasnevatest kuludest.

Tehniline võimekus andmete säilitamiseks on sideettevõtjatel juba olemas ning seega küberintsidentide efektiivseks lahendamiseks vajaminevate andmete väljaküsimiseks nende säilitamise ega väljaandmise korraldamine märkimisväärseid lisaressursse ei nõua. CERT-i teabepäringute arv võib aastas olla hinnanguliselt 200, millest igale vastamiseks (sh teabe süntees olenevalt selle päringu sisust) kuluks hinnanguliselt 15 minutit.

Eelnõu § 27 sätestab seaduse jõustumise kuupäeva, milleks on 10. mai 2018. a. Erandina jõustub seaduse § 9 2020. a 1. jaanuaril.

4. Eelnõu terminoloogia

Küberturvalisuse seaduse eelnõuga võetakse kasutusele uued terminid:

– **võrgu- ja infosüsteem** (edaspidi *süsteem*) on elektroonilise side võrk ESS-i § 2 punkti 8 tähenduses, seade või omavahel ühendatud või seotud seadmete rühm, millest vähemalt ühes toimub mõne programmi kohaselt digitaalsete andmete automaatne töötlemine, või digitaalsed

andmed, mida salvestatakse, töödeldakse, saadakse päringutega või edastatakse eelnimetatud komponentide poolt nende töö, kasutamise, kaitsmise või hooldamise jaoks.

– **süsteemi turvalisus** on süsteemi võime panna teatava kindlusega vastu mis tahes tegevusele, mis seab ohtu töödeldavate andmete või nendega seotud, süsteemi kaudu pakutavate või juurdepääsetavate teenuste kättesaadavuse, autentsuse, tervikluse ja konfidentsiaalsuse.

– **infovara** on informatsioon, andmed ja nende töötlemiseks vajalik tarkvara, vajalikud tehnilised rakendused ning muud vahendid. Definitsioon pärineb infoturbe juhtimise süsteemi määrusest, mis kehtestati Vabariigi Valitsuse seaduse § 27 lõike 3 alusel. Määrus kehtestab valitsusasutuse infoturbe juhtimise süsteemi ning ministeeriumi kantsleri ja asutuse juhi ja infoturbejuhi ülesanded. HOS-i § 41 lõige 1 sätestab, et elutähtsa teenuse osutaja on kohustatud tagama elutähtsa teenuse osutamiseks kasutatavate infosüsteemide ja nendega seotud infovara turvameetmete alalise rakendamise.

– **küberintsident** on sündmus, mis kahjustab süsteemi turvalisust.

– **digitaalse teenuse osutaja esindaja** on Euroopa Liidus asuv füüsiline või juriidiline isik, kes on määratud tegutsema väljaspool liitu asuva digitaalse teenuse osutaja nimel ja kelle poole võib liikmesriigi pädev asutus või CSIRT pöörduda digitaalse teenuse osutaja asemel seoses digitaalse teenuse osutaja käesolevast seadusest tulenevate kohustustega. Kui digitaalse teenuse osutaja, kelle asukoht ei ole liidus, osutab teenuseid liidu piires, peaks ta nimetama oma esindaja. Selgitamaks välja, kas digitaalse teenuse osutaja pakub teenuseid liidu piires, tuleks kindlaks teha, kas on ilmne, et digitaalse teenuse osutaja kavatseb osutada teenuseid ühes või mitmes liikmesriigis asuvatele isikutele. Kavatsuse kindlakstegemiseks ei piisa vaid sellest, et liidus on juurdepääs digitaalse teenuse osutaja või vahendaja veebisaidile, e-posti aadressile või muudele kontaktandmetele, samuti ei piisa digitaalse teenuse osutaja asukohariigiks oleva kolmanda riigi üldkasutatava keele kasutamisest. Digitaalse teenuse osutaja kavatsus pakkuda teenuseid liidu piires võib ilmneda sellistest asjaoludest, nagu ühes või mitmes liikmesriigis üldiselt kasutatava keele või vääringu kasutamine koos võimalusega tellida teenuseid selles teises keeles või liidus paiknevate klientide või kasutajate nimetamine. Esindaja peaks tegutsema digitaalse teenuse osutaja nimel ning pädevatel asutustel või CSIRT-il peaks olema võimalik esindajaga ühendust võtta. Digitaalse teenuse osutaja peaks kirjaliku volitusega sõnaselgelt määrama esindaja tema nimel tegutsema seoses käesoleva direktiivi kohaste kohustustega, sealhulgas intsidentidest teatamise kohustusega.

– **internetipõhine kauplemiskoht** on infoühiskonna teenus, mis võimaldab tarbijakaitseseaduse tähenduses tarbijatel ja kauplejatel sõlmida kauplejatega internetipõhiseid müügi- või teenuse osutamise lepinguid kas internetipõhise kauplemiskoha veebisaidil või kaupleja veebisaidil, mis kasutab internetipõhise kauplemiskoha pakutavaid andmetöötlusteenuseid. NIS direktiivi kohaselt võimaldab internetipõhine kauplemiskoht tarbijatel ja kauplejatel sõlmida kauplejatega internetipõhiseid müügi- või teenuse osutamise lepinguid ning see on selliste lepingute sõlmimise lõplik sihtkoht. See ei peaks hõlmama internetipõhiseid teenuseid, mille abil üksnes vahendatakse kolmandate isikute teenuseid ja mille abil saab lõpuks lepingu sõlmida. Seetõttu ei peaks see hõlmama internetipõhiseid teenuseid, mis võrdlevad erinevate kauplejate konkreetsete toodete või teenuste hinda ning suunavad kasutaja seejärel eelistatud kaupleja juurde toodet ostma. Internetipõhise kauplemiskoha pakutavad andmetöötlusteenused võivad hõlmata tehingute töötlemist, andmete koondamist või kasutajate profiilianalüüsi. Tarkvarapoode, mis tegutsevad

kolmandate isikute loodud rakenduste või tarkvaraprogrammide digitaalset levitamist võimaldavate veebipoodidena, tuleks käsitada internetipõhise kauplemiskoha ühe liigina.

– **internetipõhine otsingumootor** on infoühiskonna teenus, mis võimaldab kasutajatel teha otsinguid üldjuhul kõikidel veebisaitidel või konkreetses keeles veebisaitidel mis tahes teemal võtmesõna, fraasi või muu sisendi vormis päringu alusel ning saadab vastuseks lingid, kust võib leida teavet taotletud sisu kohta. NIS direktiivi kohaselt võimaldab internetipõhine otsingumootor kasutajal teha mis tahes teemal esitatud päringu alusel otsinguid üldiselt kõikidel veebisaitidel. Teise võimalusena võib otsingumootor keskenduda mõnes kindlas keeles veebisaitidele. NIS direktiivis esitatud internetipõhise otsingumootori määratlus ei peaks hõlmama teatavaid otsingufunktsioone, mis piirduvad konkreetse veebisaidi sisuga, olenemata sellest, kas väline otsingumootor võimaldab otsingufunktsiooni. Samuti ei peaks see hõlmama internetipõhiseid teenuseid, mis võrdlevad erinevate kauplejate konkreetsete toodete või teenuste hinda ning suunavad kasutaja seejärel eelistatud kaupleja juurde toodet ostma.

– **pilvandmetöötlusteenus** on infoühiskonna teenus, mis võimaldab juurdepääsu skaleeritavale ja paindlikule jagatavale andmetöötlusressursside kogumile. NIS direktiivi kohaselt tähendab mõiste „pilvandmetöötlusteenus“ teenust, mis võimaldab juurdepääsu jagatavate andmetöötlusressursside skaleeritavale ja paindlikule kogumile. Andmetöötlusressursid hõlmavad selliseid ressursse nagu võrgud, serverid või muu taristu, hoidlad, rakendused ja teenused. Mõiste „skaleeritav“ osutab andmetöötlusressurssidele, mis on nõudluse kõikumisega toimetulekuks pilveteenuse osutaja poolt paindlikult jaotatud, olenemata ressursside geograafilisest asukohast. Mõistet „paindlik kogum“ kasutatakse selliste andmetöötlusressursside kirjeldamiseks, mida pakutakse ja mis tehakse kättesaadavaks vastavalt nõudlusele, et kiiresti suurendada või vähendada kättesaadavaid ressursse vastavalt töökoormusele. Mõistet „jagatav“ kasutatakse selliste andmetöötlusressursside kirjeldamiseks, mida pakutakse paljudele kasutajatele, kellel on ühine juurdepääs teenusele, kuid andmete töötlemine toimub eraldi iga kasutaja jaoks, kuigi teenust osutatakse samade elektrooniliste seadmete abil.

– **CSIRT (*Computer security incident response team*)** on ekspertide grupp, mille ülesandeks on küberintsidendi tuvastamist, analüüsimist ja ohjeldamist ning küberintsidendile reageerimist toetavad toimingud. Eestis täidab riikliku CSIRT-i ülesandeid pädev asutus. CSIRT-i grupid koosnevad küberturbe spetsialistidest, kelle peamine tegevusvaldkond on küberintsidentidega seotud juhtumitele reageerimine. Grupid osutavad teenuseid, mis on vajalikud nii nende juhtumite lahendamiseks kui ka klientide toetamiseks küberintsidentidest taastumisel. Riskide leevendamiseks ja nõutavate vastuste arvu vähendamiseks osutab enamik CSIRT-e klientidele ka ennetus- ja koolitusteenuseid. Lisaks annavad grupid nõu kasutusel oleva tarkvara ja riistvara haavatavuse kohta ning teavitavad kasutajaid nõrkadele kohtadele suunatud rünnakuvõimalustest ja viirustest.

5. Eelnõu vastavus Euroopa Liidu õigusele

Eelnõul on otsene puutumus Euroopa Parlamendi ja nõukogu direktiiviga 2016/1148/EL. Euroopa Liidu õigusele vastavust on analüüsitud konkreetsete sätete juures eraldi. Eelnõu vastab Euroopa Liidu õigusele. Vastavustabel esitatud seaduse lisas 1.

6. Seaduse mõjud

Sihtgrupp

Euroopa Liidu liikmesriigid on NIS direktiivi raames kohustatud võtma vastu riikliku võrgu- ja infosüsteemide turvalisuse strateegia ning määrama riiklikult pädeva asutuse, ühtse kontaktpunkti ja CSIRT-i, mille ülesanne on seotud võrgu- ja infosüsteemide turvalisusega. Direktiivi abil luuakse koostöörühm, mille eesmärk on toetada ja hõlbustada strateegilist koostööd ja teabevahetust ning luua liikmesriikide vahel usaldust ja kindlustunnet. Täiendavalt luuakse küberturbe intsidentide lahendamiste üksuste võrgustik (CSIRT-ide võrgustik), et aidata luua liikmesriikide vahel usaldust ja kindlustunnet ning edendada kiiret ja tõhusat operatiivkoostööd. Samuti luuakse turva- ja teatamisnõuded oluliste teenuste operaatoritele ja digitaalse teenuse osutajatele.

Eelnõu väljatöötamises osalesid avaliku ja erasektori esindajad. Käesolev seadus reguleerib ka järelevalvemeetmete korraldust. Järelevalve on rakendamise seaduses korraldatud selliselt, et oleks arvestatud olemasolevaid ressursse ja pädevusi.

6.1 Sotsiaalne, sealhulgas demograafiline mõju

Seadusega ei kaasne otseseid demograafilisi mõjusid. Seadus omab teatud sotsiaalset mõju. Süsteemide turvalisuse tagamiseks rakendatavad meetmed tervishoiusfääris aitavad kindlustada katkematu vältimatu abi ja statsionaarse eriarstiabi osutamise haiglavõrgu piirkondliku haigla ja keskhaigla pidaja poolt. Samuti on mõjutatud üldarstiabi osutavad perearstid, kes peavad moderniseerima oma infosüsteeme ning võtma kasutusele vastavad meetmed turvanõuete täitmiseks. Sellega kaasneb mõningane vajadus tervishoiuasutustel ja perearstidel investeerida infotehnoloogilistesse oskustesse ja kasutatavate süsteemide turvalisuse tõstmisesse. Käesoleva eelnõu mõju on väike, kuna üldjoontes olid võrreldavad kohustused juba sätestatud HOS-iga.

Kaudne mõju võib olla tööturule, kus võib suureneda vajadus sobiva kvalifikatsiooniga ekspertide järele. Küberturvalisuse tagamiseks on laiemalt terves Eestis vaja kvalifitseeritud tööjõudu, kes suudab tagada häid, töötavaid ja uudseid küberturbelahendusi erinevates majandusharudes. Eesti ühiskonnas on aina levinumad infotehnoloogilised meetodid inimeste osalemiseks ühiskondlike protsesside mõjutamisel. IKT areng toob kaasa teenuste parema kättesaadavuse ja kasutusmugavuse, parandab riigi toimimise läbipaistvust ja kodanike osalemisvõimalust ning kärbib nii avaliku kui ka erasektori kulusid. Samas kaasneb tehnoloogia suureneva osatähtsusega ühiskonna, majanduse ja riigi sõltuvus juba harjumispärastest e-lahendustest ning kinnistub ootus tehnoloogia tõrgeteta toimimisele. Selle tõttu on ka väga oluline, et IKT-lahenduste kasutamine oleks turvaline. Käesolevas seaduses ettenähtud meetmetel on kindlasti positiivne mõju tagamaks osalustehnoloogiate jätkusuutlikku toimumist.

6.2 Mõju riigi julgeolekule ja välissuhetele

Kuna regulatsiooni eesmärk on aidata kaasa infosüsteemide turvalisuse tagamisele, mõjutab see otseselt ühiskonna turvalisust ja omab seeläbi positiivset mõju ka riigi julgeolekule.

Regulatsiooni tulemusena süsteemide turvalisuse tase tõuseb ning luuakse parem intsidentide lahendamise korraldus, mis aitab omakorda efektiivsemalt võidelda kuritegevuse vastu. Näiteks kui kurjategijal on soov nakatada süsteeme pahavaraga, siis suurema turvalisuse taseme puhul muutub see tunduvalt keerulisemaks. Kuna küberkuritegevuse puhul on

tegemist asümmeetrilise ohuga, kus väga väikeste vahenditega on võimalik tekitada suurt kahju, vähendatakse seega potentsiaalsete ohtude võimalust. Seadus mõjutab erinevaid infosüsteeme ja e-lahendusi, tõstes nende turvalisust ja vähendades nende haavatavust, mis omakorda muudab ka kurjategijate elu keerulisemaks. Samuti mõjub süsteemide turvalisuse taseme tõus ka heidutusega potentsiaalsete rünnakute vastu. Need süsteemid, mida on keerulisem rünnata (näiteks aukude otsimine tagaukses, näotustamine või infopäringud), sunnivad ründajaid valima uusi sihtmärke või hoopiski loobuma oma plaanidest.

Küberturvalisuse seadus mõjutab tugevalt küberturvalisust ning IT-süsteemidega seotud hädaolukordadeks valmistumist ja tagajärgedega tegelemist. Seadus võimaldab tugevdada ühiskonna jaoks määrava tähtsusega teenuste toimimiseks kasutatavate võrgu- ja infosüsteemide kaitset, ennetades võrgu- ja infosüsteeme ohustavaid küberintsidente ning hoides ära või vähendades küberintsidentidest põhjustatud kahjulikke tagajärgi.

Reguleerimise vajaduse tingib Eesti riigi ja ühiskonna sõltuvus e-lahenduste toimimisest, rahva usaldusest e-teenuste vastu ning vajadusest tagada teenuste küberturvalisuse tase ka tulevikus, kuivõrd tehnoloogia areng on väga kiire ja tekitab seetõttu juurde ka uusi riske. Eelnõu mõjutab ka korrakaitseorganite tööd, nimelt sätestatakse Riigi Infosüsteemi Ameti kui erikorrakaitseasutuse õigused küberintsidente ennetada, tuvastada ja lahendada. Eelnõu sätestab Riigi Infosüsteemi Ameti ülesannete raames küberintsidentide (sh ka küberrünnakute poolt põhjustatud intsidentide) käsitlemise, hoiatuste ehk ohuteadete andmise küberintsidentide ennetamiseks ning küberturbe seire teostamise õigused.

Küberintsidentide ennetamiseks, tõrjumiseks ja lahendamiseks valmisolek on seotud ka riigikaitse ja julgeolekuga. Eesti julgeolekupoliitika alustes on kirjas: „Eesti küberruum on kaitstav, kui riik ja ühiskond tervikuna selle kaitsmises osalevad, kui selleks on ette valmistatud vastavad spetsialistid ning ühiskond teab virtuaalmaailma ohtusid ja oskab neid parimal viisil vältida ning probleemide korral reageerida. /…/ Küberjulgeolek algab iga üksiku asutuse küberturvalisusest. /…/ Küberruumi kaitset arendab riik pidevalt. Eesti jälgib oma küberruumi ning kontrollib infoturbenõuete rakendamist riigi ja oluliste teenuste osutajate infosüsteemides. Sellega kindlustab riik, et olukord küberruumis vastab kehtivatele standarditele ja ohupildile ning ühtlasi koolitab ja nõustab teenuse osutajaid. Eesti peab valmistuma olukorraks, kus informatsiooni tervikluses on põhjust kahelda, ja olema valmis toime tulema mõjudega, mis sellel on digitaalsete teenuste toimimisele ja kasutajate usaldusele nende teenuste vastu.“[49] Eelnõu mõjutab riigi julgeolekut küberturvalisuse taseme tõusu kaudu, läbi mille tagatakse süsteemide järjepidev võimalikult tõrgeteta toimimine.

Regulatsioon mõjutab ka välissuhteid ja erinevate asutuste võimekust (näiteks Riigi Infosüsteemi Amet ja Politsei- ja Piirivalveamet), eelkõige kuna tegemist on regulatsiooniga, mis on EL-i liikmesriikidele kohustuslik ning selle tõttu avarduvad ka riikide koostöömehhanismid küberintsidentide lahendamise võimekuse tõstmisel, intsidentide alase informatsiooni ning parimate praktikate jagamisel. Riigi Infosüsteemi Ametil tekib õigus välisriigile, Euroopa Võrgu- ja Infoturbe Agentuurile või muule organisatsioonile edastada küberintsidentide ennetamise ja lahendamisega seotud teavet.

6.3 Majanduslik mõju

[49] https://riigikantselei.ee/sites/default/files/content-editors/Failid/2017.05.31_jpa_riigikogu.pdf

Võrgu- ja infosüsteemide turvalisusel on vahetu mõju ka majanduskeskkonna toimimisele. Vastus Eesti majanduse väljakutseks peetud suutlikkusele pakkuda kõrgema lisandväärtusega tooteid ja teenuseid seisneb suuresti digilahenduste kasutuselevõtus või uute digitaalsete toodete pakkumises. Oodatav konkurentsieelis realiseerub vaid juhul, kui digitaalsete lahenduste toimepidevus, terviklus ja konfidentsiaalsus on tagatud, sest need määravad otseselt toote või teenuse usaldusväärsuse. Samamoodi on e-riigi ja riigi pakutavate e-teenuste toimimine lineaarselt sõltuv nende turvakindlusest (nii tegelikust kui tajutavast), mis vahetult mõjutab inimeste usaldust e-riigi vastu.

Isikutel, kes hakkavad kuuluma olulise teenuse osutajate hulka, tekib direktiivi ülevõtmisel turvameetmete rakendamise kohustus ning teavitamiskohustus. Seega tekib isikutel, kes ei ole eelnevalt turvameetmete rakendamiseks kulutusi teinud, ilmselt lisaressursi vajadus (näiteks personalikulu, IT-süsteemide arendamise kulu, riskianalüüsi koostamise kulu). Samas on paljud ettevõtjad, kelle teenuste toimimine oluliselt sõltub IT-st (nt elutähtsate teenuste osutajad HOS-i mõttes), ka praegusel ajal kohustatud turvameetmeid rakendama ning selleks vastavad vahendid planeerinud. Risk, et ettevõtjad ei soovi uute regulatsioonide tingimustes Eestis tegutseda, on väike, sest direktiivi vastuvõtmise korral on kõikidel EL-i liikmesriikidel kohustus uus regulatsioon jõustada. Küll aga tuleb leida koostöös ettevõtetega võimalikud parimad lahendused, mis lihtsustaks nendepoolsete kohustuste täitmist võimalikult optimaalsel moel.

NIS direktiivi rakendamisest tulenevad muudatused panevad täiendavaid kohustusi teenuse osutajatele ja digitaalsete teenuste osutajatele elektroonilise turvalisuse tagamisel. Muudatused puudutavad suhteliselt kitsast ringi ettevõtjaid, millest valdavale osale analoogsed nõuded laienevad juba praegu kehtiva HOS-i põhjal (olulise teenuse osutajad), millest lähtuvad infoturbe tagamise nõuded ja intsidentidest teavitamise kohustus. Potentsiaalselt lisanduvad veel digitaalsete teenuste osutajad. Kodanike halduskoormust regulatsiooni uuendused ei mõjuta.

Muudatused puudutavad kitsast ringi ettevõtjaid. Mõnevõrra suureneb halduskoormus pädeva asutuse ja ettevõtja vahelises suhtluses, seda eelkõige intsidentidest raporteerimise ning päringutele vastamise kohustuse võrra nende osas, kes pole varem sellist kohustust pidanud täitma (EIS, ERR, perearstid). Eelnõu mõjutab infoühiskonna arengut, kuna eelnõust tulenevate kohustuste tagamisel on vajalik piisavate IT-alaste (täpsemalt küberturbe) oskuste olemasolu, et tagada süsteemide turvalisus. Muudatused tagavad infoühiskonna teenuste parema kättesaadavuse täiendavate turvameetmete olemasolu kaudu. Muutes infosüsteeme turvalisemaks ning pahavarale raskesti kättesaadavamaks, tagab see ka Eesti ühiskonna e-teenuste jätkupidevuse ning funktsioneerimise. Paralleelset mõjutab turvalisus ka Eesti kui e-ühiskonna positiivset kuvandit ning suurendab meie koostööd nii riigi tasandil riigi ja ettevõtete vahel kui ka rahvusvahelisel areenil.

6.4 Mõju loodus- ja elukeskkonnale

Regulatsioon aitab valmistuda ette ning ennetada keskkonnaalaseid õnnetusi, mis võivad kaasneda näiteks energeetikasektoris tegutsevate ettevõtete IT-süsteemidesse ebaseadusliku sisenemisega. Selle tulemusena võidakse rivist välja lüüa olulised süsteemid, mis omakorda toovad kaasa energiatootmise vähenemise või täieliku peatumise. Sama kehtib ka joogivee varustamisega seotud ettevõtete osas. Täiendavad turvanõuded, mis tulenevad käesolevast eelnõust, aitavad kaasa IT-süsteemide turvalisuse tagamisele ning samuti aitavad vähendada selliste stsenaariumite teket, mis võivad ühiskonna igapäevaelu pärssida. Selliste sündmuste

tekkimise võimalus on küll väga väike ning otsene mõju loodus- ja elukeskkonnale puudub, kuid siiski peab riskide hindamisel sellega arvestama.

6.5 Mõju regionaalarengule

Muudatuste mõju regionaalarengule on väike ja pigem kaudne. Avalike põhiteenuste kättesaadavus, mis tagatakse täiendavate turvameetmete kaudu, aitab kaasa ühiskonna toimimisele igas Eesti piirkonnas. Piirkondlik koostöö IT-turvalisust tagavate ettevõtetega võib suureneda, samuti võivad mõned töökohad juurde tekkida nii suurlinnadesse kui ka väiksematesse piirkondadesse.

6.6 Mõju riigiasutuste ja kohaliku omavalitsuse korraldusele

Direktiivist tulenevate täiendavate kohustuste täitmisega (nagu näiteks järelevalve teostamine turvameetmete rakendamise üle olulise teenuse osutajate ning digitaalsete teenuste pakkujate poolt, intsidenditeabe menetlemine, rahvusvaheliste koostööülesannete täitmine) kaasneb Riigi Infosüsteemi Ametile vajadus täiendava personaliressursi järele, millega omakorda kaasnevad täiendavad kulud. Riigiasutustel tekib kohustus küberintsidentide tekkes Riigi Infosüsteemi Ametiga vajaduspõhiselt koostööd teha. Avalike teenuste kvaliteet võib tõusta e-teenuste süsteemide parema vastupanuvõime tõttu. Asutuste sees võib olla vajadus täiendavate kvalifikatsiooninõuete järele küberintsidentide ennetamiseks ja lahendamiseks, mistõttu võidakse kas tööle võtta uusi isikuid või koolitada juba olemasolevaid IT-eksperte.

Mõjutatud sihtrühm
RIA järelevalveosakonnal on eelnõu jõustumisel vaja lisaks vähemalt ühte järelevalve eksperti. Ulatuse suurenemine ja järelevalvatavate hajutatus üle riigi nõuab täiendavat ressurssi kontrollitoimingute läbiviimisel. Hetkel on kontrollitoimingute läbiviimine piiratud, kuna enamus järelevalvetoiminguid viiakse läbi vähemalt kahe ametniku poolt. Kontrollitoimingute paralleelne teostamine tänaste ressursside juures ei ole võimalik. Senine järelevalvepraktika on näidanud, et üksnes kirjaliku menetluse käigus kogutud teave osutub puudulikuks. Kohapealse kontrolli käigus on võimalik asjaolusid välja selgitada järelevalvatavale vähem koormaval viisil ja seetõttu muuta toiminguid oluliselt efektiivsemaks. Samuti suureneb tehnilise kompetentsi vajadus, mida menetlustoimingute läbiviimisel teenusena sisse osta ei ole võimalik. Ühe järelevalveametniku koormamine erinevate kompetentsidega ei võimalda probleemidega süvitsi tegeleda ja nende algpõhjuseid välja selgitada. Kompetentside diferentseerimine erinevate ametnike vahel võimaldab probleeme efektiivsemalt välja selgitada ja seeläbi tõhustada menetluste läbiviimist. Töömaht on Riigi Infosüsteemi Ametil järelevalveosakonnal hinnanguliselt samaväärse mahuga kui näiteks Andmekaitse Inspektsioonil, kus võrdlusena on ametis 8 inspektorit ja 2 eksperti. Tehnilise Järelevalve Ameti analoogses struktuuriüksuses on 9 töötajat (side- ja meediateenuste osakond) ja Finantsinspektsioonis 15 (finantsteenuste järelevalve divisjon). Kaasnev palgakulu Riigi Infosüsteemi Ametile ühe lisanduva eksperdi korral on 36 000 eurot aastas.

NIS direktiivi ülevõtmine üleeuroopaliselt suurendab Riigi Infosüsteemi Ameti küberturvalisuse teenistuse jaoks oluliselt töömahtu seoses rahvusvaheliste töörühmade ja tegevustega ning sidepidamisfunktsiooni täitmisel ühtse kontaktpunkti rollis. Kohustused tekivad seoses sisulistest ja formaalsetest koostööformaatidest NIS koostöörühmas ning CSIRT-i võrgustikus, kus on vaja täita nii tehnilisi, operatsioonilisi kui ka strateegilisi ülesandeid. Mõlemas koostöövõrgustikus viiakse koostööd ellu mitmetes alatöörühmades, kus

töötatakse välja platvorme, keskkondi, tööriistu küberintsidentide lahendamise toetamiseks kui ka kujundatakse operatsioonilist koostöömudelit, hädaolukordadeks valmisoleku ja õppuste poliitikat EL-i liikmeriikide küberturvalisuse üksuste vahel ning üleselt. Riigi Infosüsteemi Ametis on seni rahvusvaheliste teemadega tegelemiseks eraldatud ressurssi vaid ühe ametikoha jagu, seejuures vastava ametikoha ülesanneteks on nii e-riigi kui ka küberturvalisuse valdkonna teemade koordineerimine. Samuti suurendab töökoormust Riigi Infosüsteemi Ameti roll ühtse kontaktpunktina seoses intensiivsema rahvusvahelise koostööga. Üleeuroopalisel tasandil on vajalik määrata rahvusvahelise koostöö sisustamiseks ja ülesannete täitmiseks Eesti poolt Riigi Infosüsteemi Ameti küberturvalisuse teenistusele vähemalt kaks ametikohta, mida täitvate isikute ülesandeks on osaleda töörühmade töös ning vahendada Eesti sisendeid. Samuti saab nende ametikohtade täitmisel katta hetkel puuduoleva küberturvalisuse alase koordinatsiooni töötasandil teiste EL-i liikmesriikidega. Arvestuslikku kulu aastas tuleks kahe ametikoha tarbeks planeerida *ca* 93 000 eurot personalifondiks ja töökohakuludeks.

Seoses NIS direktiiviga suurenevale subjektide ringile, eelkirjeldatud intensiivistuvale rahvusvahelisele koostööle ja rahvusvahelisi mõõtmeid omandanud ulatuslikele küberintsidentidele (nt 2017 Wannacry ja Petya) on samuti tarvis rohkem tähelepanu pöörata kriisideks valmisolekule nii sisemiselt kui ka rahvusvahelises plaanis. Hetkel katab küberturvalisuse teenistuses kogu riigisisest hädaolukorraks valmisoleku planeerimist ja elluviimist, sisemist väljaõpet meeskondadele ning rahvusvahelist kriisialast koostööd (nt rahvusvaheliste õppuste kontekstis) üks Riigi Infosüsteemi Ameti ametikoht. Seoses NIS direktiivist tuleneva rahvusvahelise koostöö intensiivistumisega on vaja hakata oluliselt rohkem panustama EL-i tasandi koosvõime tekitamisele piiriüleste kriisidega hakkamasaamiseks. Samuti on vaja hakata korraldama rohkem väljaõpet suuremale arvule subjektidele, et tagada nende riigisisestest kui ka rahvusvahelistest kriisialastest vajadustest teadlikkus ja kerksus küberkriisidega hakkamasaamiseks. Selle tarbeks oleks vaja eraldada Riigi Infosüsteemi Ameti küberturvalisuse teenistusele täiendav ametikoht, mis tegeleks hädaolukorraks valmisoleku, õppuste ja koolituste korraldamisega. Arvestuslikku kulu aastas tuleks selle tarbeks planeerida *ca* 45 000 eurot personalifondiks ja töökohakuludeks.

CERT-il on juba käesoleval ajal suurenenud töömaht üldiste intsidentide ja rünnete arvu kasvust tingitult, millest tulenevalt on vajadus täiendava tehnilise analüütiku ametikoha loomise ja täitmise järele. Nimetatud ametikoha ülesanded hõlmavad logide, intsidentide ning pahavara analüüsimist, tulemuste koostamist ning jagamist nii rahvusvaheliste organisatsioonidega kui ka riigi pädevate ametiasutustega (liikmesriikide CERT-id, Eesti julgeolekuasutused). Arvestuslikku kulu aastas tuleks antud ametikoha tarbeks planeerida *ca* 45 000 eurot.

6.7 Muud otsesed või kaudsed mõjud

Seadusega ei kaasne muid otseseid või kaudseid mõjusid.

7. Seaduse rakendamisega seotud riigi ja kohaliku omavalitsuse tegevused, eeldatavad kulud ja tulud

Võrreldes kehtiva õigusega lisanduvad teenuste osutajatele ja digitaalse teenuse osutajatele täiendavad kohustused, millega (sõltuvalt asutuse praegusest praktikast võrgu- ja infosüsteemide kaitsel) võivad suureneda asutuste töökoormus ning kaasneda ka täiendavad personalialased ja IT-taristu uuendamise või loomisega seotud kulud.

Seoses KOV-ide erineva ISKE rakendamise tasemega ning arvestades käimasolevat haldusreformi antakse KOV-idele üleminekuperioodiks neli aastat. Nelja aasta all peetakse silmas nelja planeeritud riigieelarve aastat, mille raames on KOV-idel võimalus esitada rahastustaotlusi infoturbe taseme tõstmiseks vajalike eelarveliste vahendite saamiseks, esitades selleks eelarvetaotlused. KOV-idel on võimalus esitada järgmiseks riigieelarvetaotluste lisavooruks eelarve lisataotlusi, mille tähtaeg on märtsis 2018. a.

Ühe võimalusena nähakse eelnõu väljatöötamise ajal võimaliku rahastamise võimalusena järgmist riigieelarve läbirääkimiste vooru, millega KOV-id saavad läbi eelarvetaotluste esitamise sisustades vajaduse, millega saaksid paremini rakendada ISKE-t. KOV-ides, rakendatakse ISKE-t peamiselt L- ja M- klassi turvaklassidele, aga kuna järjepidev kontroll puudub, siis rakendamine on ebaühtlane. Riigi infosüsteemid on omavaheliselt seotud läbi ristsõltuvuste, mistõttu on KOV-id oluline tagada riigi infosüsteemi toimimine erinevate infosüsteemide vahel. Teise rahastusettepanekuna nähakse veel struktuuritoetuste seaduse alusel määrus perioodi 2014-2020, siiski rahastusvõimalused sõltuvad KOV-ide IT-strateegiast. KOV-idele on hetkel välja töötatud minimaalsed IKT minimaalsed nõuded, mis aitab kaasa parema infoturbetaseme tõstmisele.

8. Rakendusaktid

Eelnõuga kaasneb kaheksa seaduse muutmise vajadus. Koos seaduse jõustumisega peab jõustuma küberintsidentide registri põhimäärus ja teenuse osutamiseks kasutatavate süsteemide ja nendega seotud infovarade turvanõuded ning küberintsidendist teavitamise kord. Määruste kavandid on seletuskirja lisas.

Võrgu- ja infosüsteemide turvalisuse loomise tagajärjel muutmist vajavad seadused on järgmised:

1. elektroonilise side seadus (https://www.riigiteataja.ee/akt/123032017006?leiaKehtiv)
2. hädaolukorra seadus (https://www.riigiteataja.ee/akt/103032017001)
3. lennundusseadus (https://www.riigiteataja.ee/akt/103032017016)
4. raudteeseadus (https://www.riigiteataja.ee/akt/116052017003)
5. sadamaseadus (https://www.riigiteataja.ee/akt/103032017024)
6. tervishoiuteenuste korraldamise seadus (https://www.riigiteataja.ee/akt/103032017025)
7. Eesti Rahvusringhäälingu seadus (https://www.riigiteataja.ee/akt/113032014020?leiaKehtiv)
8. krediidiasutuste seadus (https://www.riigiteataja.ee/akt/102112011008)

9. Seaduse jõustumine

Seadus jõustub 10. mail 2018. a.

Seaduse jõustumisaeg on seotud 6. juuli 2016. a direktiivi (EL) nr 2016/1148 meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidu nõudega, et kõik liikmesriigid on kohustatud üle võtma direktiivi hiljemalt 9. maiks 2018. a. Seega on käesoleva seaduse jõustumine vajalik, et 6. juulil 2016. a rakendatud direktiiv oleks terviklikult kohaldatav.

10. Eelnõu kooskõlastamine, huvirühmade kaasamine ja avalik konsultatsioon

Eelnõu väljatöötamisele eelnes VTK, mis saadeti ametlikult kooskõlastusringile 17.03.2017. Sellele eelnes huvirühmade kaasamine töörühma loomise kaudu. 2016. a novembris kaasati huvirühmade esindajad ning Majandus- ja Kommunikatsiooniministeeriumi eestvedamisel alustas kooskäimist NIS direktiivi ülevõtmise töörühm. Lisaks sellele arutati töörühmas ka seaduse rakendamisega seonduvaid tegevusi. Töörühma koosseisu kuulusid riiklike asutuste esindajatest Laura Kask (Majandus- ja Kommunikatsiooniministeerium), Madis Raaper (Majandus- ja Kommunikatsiooniministeerium), Mait Heidelberg (Majandus- ja Kommunikatsiooniministeerium), Liis Rebane (Majandus- ja Kommunikatsiooniministeerium), Toomas Vaks (Riigi Infosüsteemi Amet), Lauri Luht (Riigi Infosüsteemi Amet), Kristiina Laanest (Riigi Infosüsteemi Amet), Elsa Neeme (Riigi Infosüsteemi Amet), Kadri Kaska (Riigi Infosüsteemi Amet), Galina Danilišina (Siseministeerium), Ursula Kimmel (Siseministeerium), Sten Tikerpe (Siseministeerium), Malle Piirsoo (Kaitseministeerium), Peeter Papstel (Kaitseministeerium), Margit Gross (Justiitsministeerium), Kaitsepolitseiameti esindajad, Andres Klemm (Rahandusministeeriumi Infotehnoloogiakeskus), Urmo Parm (Andmekaitse Inspektsioon), Ivar Treimann (Politsei- ja Piirivalveamet), Priit Kleemann (Politsei- ja Piirivalveamet), Oskar Gross (Politsei- ja Piirivalveamet) ning Tiit Hallas (Siseministeeriumi infotehnoloogia- ja arenduskeskus). Eesti Infotehnoloogia ja Telekommunikatsiooni Liit (ITL) esindas info- ja telekommunikatsiooniga tegelevaid ettevõtteid ja organisatsioone, kelle poolt kuulusid töörühma koosseisu Jüri Jõema (ITL), Kaido Raiend (AS SEB Pank), Eva Jakunin (Telia Eesti AS), Sulev Sulsenberg (Telia Eesti AS), Kaspar Kaalep (Elektrilevi OÜ), Maksim Gluhhovtsenko (Elektrilevi OÜ) ning Tõnis Tajur (Elektrilevi OÜ). Samuti oli kaasatud ka Eesti Panga esindaja Margus Kukkur.

Eelnõu esitatakse EISi kaudu ministeeriumitele kooskõlastamiseks ning arvamuse avaldamiseks Eesti Linnade Liidule, Eesti Maaomavalitsuste Liidule, Eesti Infotehnoloogia ja Telekommunikatsiooni Liidule ja Eesti Pangaliidule, Eesti Interneti Sihtasutusele, Riigi Infokommunikatsiooni Sihtasutusele, Eesti Rahvusringhäälingule, MTÜ Eesti Perearstide Seltsile.

Algatab Vabariigi Valitsus

Euroopa Liidu direktiivi 2016/1148/EL ja Eesti õigusaktide vastavustabel

EL-i õigusakti norm	**EL-i õigusakti normi ülevõtmise kohustus Jah / Ei / Valikuline**	**EL-i õigusakti normi sisuliseks rakendamiseks kehtestatavad riigisisesed õigusaktid**	**Kommentaarid**
Artikkel 1 **Reguleerimisese ja kohaldamisala** 1. Käesolevas direktiivis sätestatakse meetmed võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge taseme saavutamiseks liidus, parandades seeläbi siseturu toimimist. 2. Selle eesmärgi saavutamiseks tehakse käesoleva direktiiviga järgmist: a) sätestatakse kõigile liikmesriikidele kohustus võtta vastu riiklik võrgu- ja infosüsteemide turvalisuse strateegia; b) luuakse koostöörühm, mille eesmärk on toetada ja hõlbustada strateegilist koostööd ja teabevahetust ning luua usaldust ja kindlustunnet liikmesriikide vahel; c) luuakse küberturbe intsidentide lahendamise üksuste võrgustik („CSIRTide võrgustik“), et aidata luua liikmesriikide vahel usaldust ja kindlustunnet ning edendada kiiret ja tõhusat operatiivkoostööd; d) luuakse turva- ja teatamisnõuded oluliste teenuste operaatoritele ja digitaalse teenuse osutajatele; e) sätestatakse liikmesriikidele kohustused määrata riiklikud	Art 1 lg 1 Ei Art 1 lg 2 punkt a Jah Art 1 lg 2 punkt b, c Ei Art 1 lg 2 punkt d Jah Art 1 lg 2 punkt e Jah Art 1 lg 3 Ei Art 1 lg 4 Ei Art 1 lg 5 Jah Art 1 lg 6 Ei Art 1 lg 7 Ei	Art 1 lg 2a - MKM põhimäärus § 20 lg 1 Art 1 lg 2d – KüTS § 7–8, 10–11 Art 1 lg 2e – KüTS § § 3 p 9 ja § 5 Art 1 lg 5 – KüTS § 13 lg 5	

pädevad asutused, ühtsed kontaktpunktid ja CSIRTid, mille ülesanded on seotud võrgu- ja infosüsteemide turvalisusega. 3. Käesoleva direktiiviga ette nähtud turva- ja teatamisnõudeid ei kohaldata ettevõtjatele, kelle suhtes kohaldatakse direktiivi 2002/21/EÜ artiklite 13a ja 13b nõudeid, ega usaldusteenuse osutajatele, kelle suhtes kohaldatakse määruse (EL) nr 910/2014 artikli 19 nõudeid. 4. Käesolev direktiiv ei piira nõukogu direktiivi 2008/114/EÜ (1) ega Euroopa Parlamendi ja nõukogu direktiivide 2011/93/EL (2) ja 2013/40/EL (3) kohaldamist. 5. Ilma et see piiraks ELi toimimise lepingu artikli 346 kohaldamist, tuleks teavet, mis on liidu ja siseriiklike õigusnormide, näiteks ärisaladust käsitlevate õigusnormide kohaselt konfidentsiaalne, vahetada komisjoni ja teiste asjakohaste asutustega ainult siis, kui selline teabevahetus on vajalik käesoleva direktiivi kohaldamiseks. Vahetada võib ainult teavet, mis on teabevahetuse eesmärgi seisukohast oluline ja proportsionaalne. Teabevahetus peab tagama asjaomase teabe konfidentsiaalsuse ning oluliste teenuste operaatorite ja digitaalse teenuse osutajate turvalisuse ja ärihuvide kaitse. 6. Käesolev direktiiv ei piira liikmesriikide võetavaid meetmeid, mille eesmärk on tagada riigi põhifunktsioonid ja eelkõige riigi julgeolek, sealhulgas sellise teabe kaitsmise meetmed, mille avalikustamist ta			

peab oma oluliste julgeolekuhuvide vastaseks, ning säilitada avalik kord, eelkõige selleks, et võimaldada kuritegude uurimist, avastamist ja nende eest vastutusele võtmist. 7. Kui sektoripõhine liidu õigusakt nõuab oluliste teenuste operaatoritelt või digitaalse teenuse osutajatelt nende võrgu- ja infosüsteemide turvalisuse tagamist või intsidentidest teatamist, tingimusel et sellised nõuded on toimelt vähemalt samaväärsed käesolevas direktiivis sätestatud kohustustega, kohaldatakse kõnealuse sektoripõhise liidu õigusakti sätteid.			
Artikkel 2 **Isikuandmete töötlemine** 1. Isikuandmete töötlemine käesoleva direktiivi alusel toimub kooskõlas direktiiviga 95/46/EÜ. 2. Käesoleva direktiivi kohane isikuandmete töötlemine liidu institutsioonide ja asutuste poolt toimub kooskõlas määrusega (EÜ) nr 45/2001.	Art 2 Ei		
Artikkel 3 **Minimaalne ühtlustamine** Ilma et see piiraks artikli 16 lõike 10 kohaldamist ja liidu õigusest tulenevaid liikmesriikide kohustusi, võivad liikmesriigid võtta vastu või säilitada sätteid eesmärgiga saavutada võrgu- ja infosüsteemide turvalisuse kõrgem tase.	Art 3 Ei		
Artikkel 4 **Mõisted** Käesolevas direktiivis kasutatakse	Art 4 lg 1, 2 Jah Art 4 lg 3 Jah	Art 4 lg 1 – KüTS § 3 p 1	Art 4 lg 5, 8, 9, 11–12, 13–16 ei tule siia

järgmisi mõisteid: 1) „võrgu- ja infosüsteem“– a) elektrooniline sidevõrk direktiivi 2002/21/EÜ artikli 2 punktis a sätestatud tähenduses; b) seade või omavahel ühendatud või seotud seadmete rühm, millest vähemalt ühes toimub mõne programmi kohaselt digitaalsete andmete automaatne töötlemine, või c) digitaalsed andmed, mida salvestatakse, töödeldakse, saadakse päringutega või edastatakse punktidega a ja b hõlmatud komponentide poolt nende töö, kasutamise, kaitsmise või hooldamise jaoks; 2) „võrgu- ja infosüsteemide turvalisus“ – võrgu- ja infosüsteemi võime panna teatava kindlusega vastu mis tahes tegevusele, mis seab ohtu salvestatud, edastatud või töödeldud andmete või nendega seotud, võrgu- ja infosüsteemi kaudu pakutavate või juurdepääsetavate teenuste kättesaadavuse, autentsuse, tervikluse ja konfidentsiaalsuse; 3) „riiklik võrgu- ja infosüsteemide turvalisuse strateegia“ – raamistik, mis näeb ette võrgu- ja infosüsteemide turvalisuse liikmesriigi tasandi strateegilised eesmärgid ja prioriteedid; 4) „oluliste teenuste operaator“ – II lisas osutatud liiki avaliku või erasektori üksus, mis vastab artikli 5 lõikes 2 sätestatud kriteeriumidele; 5) „digitaalne teenus“ – Euroopa Parlamendi ja nõukogu direktiivi (EL) 2015/1535 (1) artikli 1 lõike 1 punktis b määratletud teenus,	Art 4 lg 4 Jah Art 4 lg 5 Valikuline Art 4 lg 6 Jah Art 4 lg 7–12 Valikuline Art 13–16 Valikuline Art 4 lg 10 Jah Art 4 lg 17–19 Jah	Art 4 lg 2 – KüTS § 3 p 2 Art 4 lg 3 MKM põhimäärus § 20 lg 1 Art 4 lg 4 – KüTS § 2 lg 1 Art 4 lg 6 – KüTS § 3 lg 1 Art 4 lg 7 – KüTS § 3 p 4 Art 4 lg 10 – VITS § 3 p 5 Art 4 lg 17 – VITS § 3 p 6 Art 4 lg 18 – VITS § 3 p 7 Art 4 lg 19 – VITS § 3 p 8	seadusesse.

mis kuulub ühte III lisas loetletud liiki; 6) „digitaalse teenuse osutaja“– juriidiline isik, kes pakub digitaalset teenust; 7) „intsident“ – sündmus, mis tegelikult kahjustab võrgu- ja infosüsteemide turvalisust; 8) „intsidendi käsitlemine“– intsidendi tuvastamist, analüüsimist ja ohjeldamist ning intsidendile reageerimist toetavad protseduurid; 9) „risk“– mõistlikult tuvastatav asjaolu või sündmus, mis võib kahjustada võrgu- ja infosüsteemide turvalisust; 10) „esindaja“ – liidus asuv füüsiline või juriidiline isik, kes on sõnaselgelt määratud tegutsema väljaspool liitu asuva digitaalse teenuse osutaja nimel ja kelle poole võib liikmesriigi pädev asutus või CSIRT pöörduda digitaalse teenuse osutaja asemel seoses digitaalse teenuse osutaja käesolevast direktiivist tulenevate kohustustega; 11) „standard“ – määruse (EL) nr 1025/2012 artikli 2 punktis 1 määratletud standard; 12) „spetsifikatsioon“–määruse (EL) nr 1025/2012 artikli 2 punktis 4 määratletud tehniline spetsifikatsioon; 13) „interneti vahetuspunkt (IXP, *Internet Exchange Point*)“– võrgustik, mis võimaldab rohkem kui kahe sõltumatu autonoomse süsteemi omavahelist ühendamist, eelkõige selleks, et hõlbustada internetiliikluse vahetamist;, IXP			

võimaldab üksnes autonoomsete süsteemide omavahelist ühendamist; IXP ei nõua ühegi kahe osaleva autonoomse süsteemi vahel kulgeva internetiliikluse kulgemist mõne kolmanda autonoomse süsteemi kaudu, ei muuda sellist liiklust ega sekku sellesse mingil muul viisil; 14) „domeeninimede süsteem“– hierarhilise jaotamise põhimõttel toimuv nimede andmise süsteem võrgus, mis edastab domeeninimede päringuid; 15) „domeeninimede süsteemi teenuse osutaja“ – üksus, mis osutab internetis domeeninimede süsteemi teenuseid; 16) „tippdomeeninimede register“ – üksus, mis haldab ja teostab interneti domeeninimede registreerimist konkreetse tippdomeeni all; 17) „internetipõhine kauplemiskoht“ – digitaalne teenus, mis võimaldab Euroopa Parlamendi ja nõukogu direktiivi 2013/11/EL (1) artikli 4 lõike 1 punktis a määratletud tarbijatel ja punktis b määratletud kauplejatel sõlmida kauplejatega internetipõhiseid müügi- või teenuse osutamise lepinguid kas internetipõhise kauplemiskoha veebisaidil või kaupleja veebisaidil, mis kasutab internetipõhise kauplemiskoha pakutavaid andmetöötlusteenuseid; 18) „internetipõhine otsingumootor“ – digitaalne teenus, mis võimaldab kasutajatel teha otsinguid üldjuhul kõikidel veebisaitidel või konkreetses			

keeles veebisaitidel mis tahes teemal võtmesõna, fraasi või muu sisendi vormis päringu alusel ning saadab vastuseks lingid, kust võib leida teavet taotletud sisu kohta; 19) „pilvandmetöötlusteenus“– digitaalne teenus, mis võimaldab juurdepääsu skaleeritavale ja paindlikule jagatavate andmetöötlusressursside kogumile.			
Artikkel 5 **Oluliste teenuste operaatorite identifitseerimine** 1. 9. novembriks 2018 identifitseerivad liikmesriigid iga II lisas osutatud sektori ja allsektori puhul need oluliste teenuste operaatorid, kelle tegevuskoht on nende territooriumil. 2. Artikli 4 punktis 4 osutatud oluliste teenuste operaatori identifitseerimise kriteeriumid on järgmised: a) üksus osutab teenust, mis on oluline elutähtsa ühiskondliku ja/või majandustegevuse säilitamise seisukohast; b) kõnealuse teenuse osutamine sõltub võrgu- ja infosüsteemidest ning c) intsidendil oleks oluliselt häiriv mõju nimetatud teenuse osutamisele. 3. Lõike 1 kohaldamiseks koostab iga liikmesriik lõike 2 punktis a osutatud teenuste loetelu. 4. Lõike 1 kohaldamiseks, juhul kui üksus osutab lõike 2 punktis a osutatud teenust kahes või enamas liikmesriigis, konsulteerivad kõnealused liikmesriigid üksteisega. Konsulteerimine	Art 5 lg 1 Jah Art 5 lg 2 Ei Art 5 lg 3 Ei Art 5 lg 4 Ei Art 5 lg 5 Ei Art 5 lg 6 Ei Art 5 lg 7 Ei	Art 5 lg 1 – KüTS § 27	

toimub enne identifitseerimist käsitleva otsuse tegemist. 5. Liikmesriigid vaatavad korrapäraselt ja vähemalt iga kahe aasta tagant pärast 9. maid 2018 läbi identifitseeritud oluliste teenuste operaatorite nimekirja ja vajaduse korral ajakohastavad seda. 6. Koostöörühma roll on kooskõlas artiklis 11 osutatud ülesannetega toetada liikmesriike järjepideva lähenemisviisi võtmisel oluliste teenuste operaatorite identifitseerimise protsessis. 7. Artiklis 23 osutatud läbivaatamise eesmärgil ja 9. novembriks 2018 ning pärast seda iga kahe aasta tagant esitavad liikmesriigid komisjonile vajaliku teabe, et komisjon saaks hinnata käesoleva direktiivi rakendamist, eelkõige liikmesriikide lähenemisviiside järjepidevust seoses oluliste teenuste operaatorite identifitseerimisega. Kõnealune teave hõlmab vähemalt järgmist: a) riiklikud meetmed, mis võimaldavad oluliste teenuste operaatorite identifitseerimist; b) lõikes 3 osutatud teenuste loetelu; c) iga II lisas osutatud sektori puhul identifitseeritud oluliste teenuste operaatorite arv ning operaatori tähtsus asjaomases sektoris; d) piirmäärad (kui need on olemas), mille abil määrata kindlaks asjakohane teenuse osutamise tase viitega artikli 6 lõike 1 punktis a osutatud teenusest sõltuvate kasutajate arvule või asjaomase oluliste teenuste operaatori tähtsusele,			

millele on osutatud artikli 6 lõike 1 punktis f. Komisjon võib selleks, et aidata kaasa võrreldava teabe esitamisele, võtta vastu asjakohased tehnilised suunised käesolevas lõikes osutatud teabe parameetrite kohta, võttes seejuures võimalikult suurel määral arvesse ENISA arvamust.			
Artikkel 6 **Oluline häiriv mõju** 1. Artikli 5 lõike 2 punktis c osutatud häiriva mõju olulisuse kindlakstegemisel võtavad liikmesriigid arvesse vähemalt järgmisi sektoritevahelisi tegureid: a) asjaomase üksuse poolt osutatavatest teenustest sõltuvate kasutajate arv; b) muude II lisas osutatud sektorite sõltumine üksuse poolt pakutavast teenusest; c) intsidentide võimalik mõju (raskusaste ja kestus) majandus- ja ühiskondlikule tegevusele või avalikule julgeolekule; d) üksuse turuosa; e) intsidendist mõjutatud geograafilise ala võimalik ulatus; f) üksuse tähtsus teenuse piisava kvaliteedi säilitamisel, võttes arvesse alternatiivide olemasolu kõnealuse teenuse osutamiseks. 2. Selleks et teha kindlaks, kas intsidendil oleks oluline häiriv mõju, võtavad liikmesriigid asjakohasel juhul arvesse ka sektoripõhiseid tegureid.	Art 6 lg 1 Jah Art 6 lg 2 Ei	Art 6 lg 1 – KüTS § 8 lg 5 sätestatud VV määrus „Teenuse osutamiseks kasutatavate süsteemide ja nendega seotud infovarade turvanõuded ning küberintsidendist teavitamise kord“	
Artikkel 7 **Riiklik võrgu- ja infosüsteemide turvalisuse strateegia** 1. Iga liikmesriik võtab vastu	Art 7 lg 1 Jah Art 7 lg 2 Ei	Art 7 lg 1 – MKM põhimäärus § 20 lg 1 ja	Art 7 lg 3 pole vaja seaduse tasandil sätestada

riikliku võrgu- ja infosüsteemide turvalisuse strateegia, milles määratletakse strateegilised eesmärgid ning asjakohased poliitilised ja regulatiivsed meetmed, mille abil saavutada võrgu- ja infosüsteemide turvalisuse kõrge tase ja seda säilitada, ning mis hõlmab vähemalt II lisas osutatud sektoreid ja III lisas osutatud teenuseid. Eelkõige käsitletakse riiklikus võrgu- ja infosüsteemide turvalisuse strateegias järgmisi küsimusi: a) riikliku võrgu- ja infosüsteemide turvalisuse strateegia eesmärgid ja prioriteedid; 19.7.2016 L 194/15 Euroopa Liidu Teataja ET b) juhtimisraamistik, mille toel riikliku võrgu- ja infosüsteemide turvalisuse strateegia eesmärgid ja prioriteedid ellu viia; see hõlmab valitsusasutuste ning muude asjaomaste osalejate ülesandeid ja vastutust; c) valmisoleku-, reageerimis- ja taastemeetmete, sh avaliku ja erasektori koostöö kindlaksmääramine; d) riikliku võrgu- ja infosüsteemide turvalisuse strateegiaga seotud haridus-, teadlikkuse suurendamise ja koolitusprogrammide kirjeldus; e) riikliku võrgu- ja infosüsteemide turvalisuse strateegiaga seotud teadus- ja arendustegevuse kavade kirjeldus; f) riski hindamise kava riskide kindlakstegemiseks; g) riikliku võrgu- ja infosüsteemide turvalisuse strateegia rakendamises osalevate erinevate osalejate loetelu. 2. Liikmesriigid võivad paluda	Art 7 lg 3 Valikuline	„Küberjulgeoleku strateegia 2014–2017“[50]	

[50] https://www.valitsus.ee/sites/default/files/content-editors/arengukavad/kuberjulgeoleku_strateegia_2014-2017.pdf

ENISA abi riiklike võrgu- ja infosüsteemide turvalisuse strateegiate väljatöötamisel. 3. Liikmesriigid edastavad oma riikliku võrgu- ja infosüsteemide turvalisuse strateegia komisjonile kolme kuu jooksul pärast selle vastuvõtmist. Seda tehes võivad liikmesriigid jätta välja strateegia elemendid, mis on seotud riikliku julgeolekuga.			
Artikkel 8 **Riiklikud pädevad asutused ja ühtne kontaktpunkt** 1. Iga liikmesriik määrab võrgu- ja infosüsteemide turbe vallas ühe või mitu riiklikku pädevat asutust („pädev asutus“), kes hõlmavad vähemalt II lisas osutatud sektoreid ja III lisas osutatud teenuseid. Liikmesriigid võivad määrata selle ülesande olemasolevale asutusele või olemasolevatele asutustele. 2. Pädevad asutused jälgivad käesoleva direktiivi kohaldamist riigi tasandil. 3. Iga liikmesriik määrab võrgu- ja infosüsteemide turbe vallas riikliku ühtse kontaktpunkti („ühtne kontaktpunkt“). Liikmesriigid võivad määrata selle ülesande olemasolevale asutusele. Kui liikmesriik nimetab ainult ühe pädeva asutuse, siis on see pädev asutus ka ühtne kontaktpunkt. 4. Ühtne kontaktpunkt täidab sidepidamisfunktsiooni, et tagada liikmesriikide asutuste piiriülene koostöö teiste liikmesriikide asjaomaste asutuste, artiklis 11 osutatud koostöörühma ja artiklis 12 osutatud CSIRTide	Art 8 lg 1 Jah Art 8 lg 2 Jah Art 8 lg 3 Jah Art 8 lg 4 Ei Art 8 lg 5 Ei Art 8 lg 6 Ei Art 8 lg 7 Ei	Art 8 lg 1 – KüTS § 5 Art 8 lg 2 – KüTS § 13 Art 8 lg 3 – KüTS § 5	Art 8 lg 7 MKM / EL esindus ülesanne

võrgustikuga. 5. Liikmesriigid tagavad, et pädevatel asutustel ja ühtsetel kontaktpunktidel on piisavad ressursid, et oma ülesandeid tulemuslikult ja tõhusalt täita ning seeläbi saavutada käesoleva direktiivi eesmärgid. Liikmesriigid tagavad määratud esindajate tõhusa, tulemusliku ja turvalise koostöö koostöörühmas. 6. Pädevad asutused ja ühtne kontaktpunkt peavad vajaduse korral ja kooskõlas siseriikliku õigusega konsulteerima ja tegema koostööd asjakohaste riiklike õiguskaitse- ja andmekaitseasutustega. 7. Iga liikmesriik teatab komisjonile viivitamata pädeva asutuse ja ühtse kontaktpunkti määramisest, nende ülesannetest ja nende hilisemast muutmisest. Iga liikmesriik avalikustab määratud pädeva asutuse ja ühtse kontaktpunkti. Komisjon avaldab määratud ühtsete kontaktpunktide loetelu.			
Artikkel 9 **Küberturbe intsidentide lahendamise üksused (CSIRTid)** 1. Iga liikmesriik määrab ühe või mitu I lisa punktis 1 sätestatud nõuetele vastava CSIRTi, kes hõlmavad vähemalt II lisas osutatud sektoreid ja III lisas osutatud teenuseid ning kes vastutavad riskide ja intsidentide käsitlemise eest põhjalikult määratletud protseduuri kohaselt. CSIRTi võib luua pädeva asutuse osana. 2. Liikmesriigid tagavad, et CSIRTidel on I lisa punktis 2 osutatud ülesannete tulemuslikuks	Art 9 lg 1 Jah Art 9 lg 2 Ei Art 9 lg 3 Ei Art 9 lg 4 Ei Art 9 lg 5 Ei	Art 9 lg 1 KüTS § 3 p 9	Art 9 lg 4 RIA tööülesanne

täitmiseks piisavad ressursid. Liikmesriigid tagavad oma CSIRTide tõhusa, tulemusliku ja turvalise koostöö artiklis 12 osutatud CSIRTide võrgustikus. 3. Liikmesriigid tagavad, et CSIRTidel on riigi tasandil juurdepääs asjakohasele, turvalisele ja töökindlale side- ja infotaristule. 4. Liikmesriigid teatavad komisjonile, millised on CSIRTide volitused ja intsidentide käsitlemise protseduuri peamised elemendid. 5. Liikmesriigid võivad paluda ENISA abi riiklike CSIRTide väljatöötamisel.			
Artikkel 10 **Koostöö liikmesriigi tasandil** 1. Kui sama liikmesriigi pädev asutus, ühtne kontaktpunkt ja CSIRT on üksteisest eraldiseisvad, teevad nad käesolevas direktiivis sätestatud kohustuste täitmiseks koostööd. 2. Liikmesriigid tagavad, et pädevad asutused või CSIRTid saavad käesoleva direktiivi kohaselt esitatud teated intsidentide kohta. Kui liikmesriik otsustab, et CSIRTid ei saa teateid, tuleb CSIRTidele anda nende ülesannete täitmiseks vajalikus ulatuses juurdepääs andmetele intsidentide kohta, millest on teatanud oluliste teenuste operaatorid artikli 14 lõigete 3 ja 5 kohaselt või digitaalse teenuse osutajad artikli 16 lõigete 3 ja 6 kohaselt. 3. Liikmesriigid tagavad, et pädevad asutused või CSIRTid teavitavad ühtseid kontaktpunkte	Art 10 lg 1 Ei Art 10 lg 2 Jah Art 10 lg 3 Ei	Art 10 lg 2 – KüTS §-d 8 ja 11	Art 10 lg 3 RIA tööülesanne

käesoleva direktiivi kohaselt esitatud intsidente käsitlevatest teadetest. Ühtne kontaktpunkt esitab 9. augustiks 2018 ning pärast seda üks kord aastas koostöörühmale saadud teadete kohta koondaruande, mis sisaldab teadete arvu ja teatatud intsidentide laadi ning vastavalt artikli 14 lõigetele 3 ja 5 ning artikli 16 lõigetele 3 ja 6 võetud meetmeid.			
Artikkel 11 **Koostöörühm** 1. Käesolevaga luuakse koostöörühm, et toetada ja hõlbustada liikmesriikidevahelist strateegilist koostööd ja infovahetust, luua usaldust ja kindlustunnet ning saavutada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase liidus. Koostöörühm täidab oma ülesandeid kaheaastaste tööprogrammide alusel, nagu on osutatud lõike 3 teises lõigus. 2. Koostöörühm koosneb liikmesriikide, komisjoni ja ENISA esindajatest. Kui see on asjakohane, võib koostöörühm kutsuda oma töös osalema asjakohaste sidusrühmade esindajaid. Komisjon tagab sekretariaadi teenused. 3. Koostöörühmal on järgmised ülesanded: a) anda strateegilisi suuniseid artikli 12 kohaselt loodud CSIRTide võrgustiku tegevuse kohta; b) vahetada parimaid tavasid artikli 14 lõigetes 3 ja 5 ja artikli 16 lõigetes 3 ja 6 osutatud intsidentidest teatamisega seotud teabevahetuse kohta; c) vahetada parimaid tavasid liikmesriikide vahel ning aidata	Art 11 Ei		

koostöös ENISAga liikmesriike võrgu- ja infosüsteemide turvalisuse alase suutlikkuse suurendamise alal; d) arutada liikmesriikide suutlikkust ja valmisolekut ning hinnata vabatahtlikkuse alusel riiklikke võrgu- ja infosüsteemide turvalisuse strateegiaid ja CSIRTide tõhusust ning teha kindlaks parimad tavad; e) vahetada teavet ja parimaid tavasid teadlikkuse suurendamise ja koolituse kohta; f) vahetada teavet ja parimaid tavasid võrgu- ja infosüsteemide turvalisusega seotud teadus- ja arendustegevuse kohta; g) kui see on asjakohane, siis vahetada kogemusi võrgu- ja infosüsteemide turvalisuse küsimustes liidu asjakohaste institutsioonide, organite ja asutustega; h) arutada asjakohaste Euroopa standardiorganisatsioonide esindajatega artiklis 19 osutatud standardeid ja spetsifikatsioone; i) koguda parimaid tavasid riskide ja intsidentide kohta; j) analüüsida igal aastal artikli 10 lõike 3 teises lõigus osutatud koondaruandeid; k) arutada võrgu- ja infosüsteemide turvalisusega seotud õppuste, haridusprogrammide ja koolituse osas tehtud tööd, sealhulgas ENISA tööd; l) vahetada ENISA abiga parimaid tavasid seoses oluliste teenuste operaatorite identifitseerimisega liikmesriikide poolt, sealhulgas mis puudutab riskide ja intsidentidega seotud piiriüleseid sõltuvusseoseid; m) arutada artiklites 14 ja 16 osutatud intsidentidest teatamise korda. Koostöörühm koostab 9. veebruariks 2018 ja seejärel iga			

kahe aasta tagant tööprogrammi eesmärkide ja ülesannete täitmiseks võetavate meetmete kohta, mis peab olema kooskõlas käesoleva direktiivi eesmärkidega. 4. Koostöörühm esitab artiklis 23 osutatud ülevaate jaoks ja 9. augustiks 2018 ning pärast seda iga pooleteise aasta tagant aruande, milles hinnatakse käesoleva artikli kohaselt tehtud strateegilisest koostööst saadud kogemusi. 5. Komisjon võtab vastu rakendusaktid, millega kehtestatakse koostöörühma toimimiseks vajalik menetluskord. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 22 lõikes 2 osutatud kontrollimenetlusega. Esimese lõigu kohaldamise eesmärgil esitab komisjon esimese rakendusakti eelnõu artikli 22 lõikes 1 osutatud komiteele hiljemalt 9. veebruariks 2017.			
Artikkel 12 **CSIRTide võrgustik** 1. Käesolevaga luuakse riiklike CSIRTide võrgustik, et aidata luua liikmesriikide vahel usaldust ja kindlustunnet ning edendada kiiret ja tõhusat operatiivkoostööd. 2. CSIRTide võrgustik koosneb liikmesriikide CSIRTide ja CERT-EU esindajatest. Komisjon osaleb CSIRTide võrgustikus vaatlejana. ENISA tagab sekretariaadi töö ja toetab aktiivselt CSIRTide-vahelist koostööd.	Art 12 Ei		

3. CSIRTide võrgustikul on järgmised ülesanded: a) vahetada teavet CSIRTide teenuste, tegevuste ja koostöösuutlikkuse kohta; b) intsidendist potentsiaalselt mõjutatud liikmesriigi CSIRTi esindaja taotlusel vahetada ja arutada asjaomast intsidenti ja sellega seonduvaid riske käsitlevat mittetundlikku äriteavet, aga samas võib iga liikmesriigi CSIRT keelduda sellesse arutellu panustamast, kui on olemas oht, et see kahjustab intsidendi uurimist; c) vahetada ja teha vabatahtlikkuse alusel kättesaadavaks mittekonfidentsiaalset teavet üksikute intsidentide kohta; d) liikmesriigi CSIRT esindaja taotlusel arutada koordineeritud reageerimist sama liikmesriigi jurisdiktsioonis tuvastatud intsidendile ning võimaluse korral määratleda koordineeritud reageerimine; e) toetada liikmesriike piiriüleste intsidentide käsitlemisel nende vabatahtliku vastastikuse abistamise põhimõttel; f) arutada, uurida ja teha kindlaks täiendavaid operatiivkoostöö vorme, sealhulgas seoses järgmisega: i) riskide ja intsidentide kategooriad; ii) varajased hoiatused; iii) vastastikune abi; iv) koostöö põhimõtted ja kord juhtudeks, kui liikmesriigid reageerivad piirülestele riskidele ja intsidentidele; g) teavitada koostöörühma oma tegevusest ja punkti f kohaselt arutatud täiendavatest operatiivkoostöö vormidest ning taotleda sellega seonduvaid suuniseid;			

h) arutada võrgu- ja infosüsteemide turvalisusega seotud õppustelt, sealhulgas ENISA korraldatud õppustelt, saadud kogemusi; i) arutada üksiku CSIRT taotlusel kõnealuse CSIRT suutlikkust ja valmisolekut; j) anda suuniseid, et hõlbustada operatiivsete tavade lähendamist seoses käesoleva artikli operatiivkoostööd käsitlevate sätete kohaldamisega. 4. Artiklis 23 osutatud läbivaatamise eesmärgil ja 9. augustiks 2018 ning pärast seda iga pooleteise aasta tagant esitab CSIRTide võrgustik aruande, milles hinnatakse käesoleva artikli kohaselt tehtud operatiivkoostööst saadud kogemusi ning mis sisaldab järeldusi ja soovitusi. See aruanne esitatakse ka koostöörühmale. 5. CSIRTide võrgustik sätestab oma töökorra.			
Artikkel 13 **Rahvusvaheline koostöö** Liit võib kooskõlas ELi toimimise lepingu artikliga 218 sõlmida kolmandate riikide või rahvusvaheliste organisatsioonidega rahvusvahelisi lepinguid, mis võimaldavad neil osaleda ja korraldada nende osalust mõningates koostöörühma tegevustes. Sellistes lepingutes arvestatakse vajadusega tagada andmete piisav kaitse.	Art 13 Ei		
Artikkel 14 **Turvanõuded ja intsidentidest teatamine** 1. Liikmesriigid tagavad, et oluliste teenuste operaatorid võtavad asjakohased ja proportsionaalsed tehnilised ja korralduslikud meetmed, et	Art 14 lg 1, 2 Jah Art 14 lg 3 Jah Art 14 Lg 4 Jah	Art 14 lg 1 KüTS § 7 lg 1, 2 Art 14 lg 2 – KüTS § 7 lg 1, 2 Art 14 lg 3 –	

hallata riske, mis ohustavad nende töös kasutatavate võrgu- ja infosüsteemide turvalisust. Tehnika taset arvesse võttes tagatakse nende meetmetega olemasolevale ohule vastav võrgu- ja infosüsteemide turvalisuse tase. 2. Liikmesriigid tagavad, et oluliste teenuste operaatorid võtavad asjakohased meetmed, selleks et ennetada ja minimeerida oluliste teenuste osutamiseks kasutatavate võrgu- ja infosüsteemide turvalisust kahjustavate intsidentide mõju, eesmärgiga tagada kõnealuste teenuste järjepidevus. 3. Liikmesriigid tagavad, et oluliste teenuste operaatorid teatavad põhjendamatu viivituseta pädevale asutusele või CSIRTile intsidentidest, millel on oluline mõju nende pakutavate oluliste teenuste järjepidevusele. Teated peavad sisaldama teavet, mis võimaldab pädeval asutusel või CSIRTil teha kindlaks intsidendi igasugune piiriülene mõju. Teatamine ei suurenda teavitava osapoole vastutust. 4. Intsidendi mõju olulisuse kindlakstegemiseks võetakse arvesse eriti järgmisi parameetreid: a) olulise teenuse katkemisest mõjutatud kasutajate arv; b) intsidendi kestus; c) intsidendist mõjutatud geograafilise ala ulatus. 5. Oluliste teenuste operaatori teates esitatud teabe põhjal teavitab pädev asutus või CSIRT teisi mõjutatud liikmesriike, juhul kui intsidendil on oluline mõju oluliste teenuste järjepidevusele	Art 14 Lg 5 Jah Art 14 Lg 6 Jah Art 14 Lg 7 Ei	KüTS § 8 lg 1 Art 14 lg 4 – KüTS § 8 lg 5 viidatud VV määrus „Teenuse osutamiseks kasutatavate süsteemide ja nendega seotud infovarade turvanõuded ning küberintsidendist teavitamise kord“ Art 14 lg 5 – KüTS § 13 lg 5 Art 14 lg 6 – KüTS § 8 lg 3	

asjaomases liikmesriigis. Seda tehes kaitseb pädev asutus või CSIRT kooskõlas liidu õigusega või liidu õigusele vastavate siseriiklike õigusaktidega oluliste teenuste operaatori turvalisust ja ärihuve ning tema poolt teates esitatud teabe konfidentsiaalsust. Kui olukord seda võimaldab, esitab pädev asutus või CSIRT teate esitanud oluliste teenuste operaatorile asjakohase teabe intsidendist teatamise järelmeetmete kohta, näiteks teabe, mis võib aidata intsidenti tõhusalt käsitleda. Pädeva asutuse või CSIRT taotlusel edastab ühtne kontaktpunkt esimeses lõigus osutatud teated teiste puudutatud liikmesriikide ühtsetele kontaktpunktidele. 6. Pärast konsulteerimist teate esitanud oluliste teenuste operaatoriga võib teate saanud pädev asutus või CSIRT teavitada üldsust üksikutest intsidentidest, juhul kui üldsuse teadlikkus on vajalik intsidendi ärahoidmiseks või käimasoleva intsidendi lahendamiseks. 7. Koostöörühmas koos tegutsevad pädevad asutused võivad koostada ja võtta vastu suuniseid olukordade kohta, kus oluliste teenuste operaatoritelt nõutakse intsidentidest teatamist, sealhulgas parameetrite kohta, millega määratakse kindlaks intsidendi mõju olulisus, nagu on osutatud lõikes 4.			
Artikkel 15 **Rakendamine ja jõustamine** 1. Liikmesriigid tagavad, et pädevatel asutustel on vajalikud õigused ja vahendid, et hinnata seda, kas oluliste teenuste operaatorid täidavad artiklist 14	Art 15 lg 1, 2, 3 Jah Art 15 lg 4 Jah	Art 15 lg 1 – KüTS § 15 lg 1 ja 2; § 16 lg 1 ja lg 2 Art 15 lg 2 – KüTS § 15 lg 1 ja	

tulenevaid kohustusi, ning selle mõju võrgu- ja infosüsteemide turvalisusele. 2. Liikmesriigid tagavad, et pädeval asutusel on õigused ja vahendid nõudmaks, et oluliste teenuste operaatorid esitaksid a) oma võrgu- ja infosüsteemide turvalisuse hindamiseks vajaliku teabe, sealhulgas dokumenteeritud turvapõhimõtted; b) tõendid turvapõhimõtete tõhusa rakendamise kohta, näiteks pädeva asutuse või tunnustatud audiitori poolt läbi viidud turvaauditi tulemused, ning viimasel juhul teeksid need tulemused ja nende aluseks olevad tõendid kättesaadavaks pädevale asutusele. Teabe või tõendite esitamist taotledes esitavad pädevad asutused taotluse eesmärgi ja täpsustavad, millist teavet nõutakse. 3. Pärast lõikes 2 osutatud teabe või turvaauditite tulemuste hindamist võivad pädevad asutused anda oluliste teenuste operaatoritele siduvaid juhiseid nende töö parandamiseks. 4. Kui intsident põhjustab isikuandmetega seotud rikkumise, teeb pädev asutus selle lahendamisel tihedat koostööd andmekaitseasutustega.		2; § 16 lg 1 ja 2 Art 15 lg 3 – KüTS § 13 lg 3 Art 15 lg 4 – KüTS § 8 lg 6	
<u>Artikkel 16</u> **Turvanõuded ja intsidentidest teatamine** 1. Liikmesriigid tagavad, et digitaalse teenuse osutajad teevad kindlaks riskid, mis ohustavad nende võrgu- ja infosüsteemide turvalisust, mida nad kasutavad III lisas osutatud teenuste osutamisel liidus, ning võtavad asjakohased ja proportsionaalsed	Art 16 lg 1 Jah Art 16 lg 2 Jah Art 16 lg 3 Jah Art 16 lg 4 Jah Art 16 lg 5 Jah Art 16 lg 6 Jah Art 16 lg 7 Jah Art 16 lg 8 Ei Art 16 lg 9 Ei Art 16 lg 10 Jah	Art 16 lg 1 - KüTS § 10 lg 1 ja 2 Art 16 lg 2 – KüTS § 10 lg 4 Art 16 lg 3 – KüTS § 11 lg 1 Art 16 lg 4 –	

tehnilised ja korralduslikud meetmed, et neid riske juhtida. Tehnika taset arvesse võttes tagatakse nende meetmetega olemasolevale ohule vastav võrgu- ja infosüsteemide turvalisuse tase ning võetakse arvesse järgmisi elemente: a) süsteemide ja rajatiste turvalisus, b) intsidentide käsitlemine, c) talitluspidevuse haldamine, d) seire, auditeerimine ja testimine, e) vastavus rahvusvahelistele standarditele. 2. Liikmesriigid tagavad, et digitaalse teenuse osutajad võtavad meetmeid, et vältida ja minimeerida nende intsidentide mõju, mis kahjustavad nende poolt III lisas sätestatud teenuste liidus osutamiseks kasutatavate võrgu- ja infosüsteemide turvalisust, eesmärgiga tagada kõnealuste teenuste järjepidevus. 3. Liikmesriigid tagavad, et digitaalse teenuse osutajad teatavad pädevale asutusele või CSIRTile põhjendamatu viivituseta igast intsidendist, millel on oluline mõju nende poolt liidus osutatavale III lisas sätestatud teenusele. Teated peavad sisaldama teavet, mis võimaldab pädeval asutusel või CSIRTil teha kindlaks intsidendi piiriülese mõju olulisus. Teatamine ei suurenda teavitava osapoole vastutust. 4. Intsidendi mõju olulisuse hindamiseks võetakse arvesse eelkõige järgmisi parameetreid: a) intsidendist mõjutatud kasutajate ja eelkõige nende kasutajate arv, kes sõltuvad asjaomasest teenusest oma		KüTS § 11 lg 3 Art 16 lg 5 – KüTS § 8 lg 7 Art 16 lg 6 – KüTS § 11 lg 6 Art 16 lg 7 – KüTS § 11 lg 7 Art 16 lg 10 – KüTS § 3 lg 2	

teenuste osutamisel; b) intsidendi kestus; c) intsidendist mõjutatud geograafilise ala ulatus; d) teenuse toimimise katkemise ulatus; e) majandus- ja ühiskondlikule tegevusele avalduva mõju ulatus. Intsidendist teatamise kohustust kohaldatakse üksnes juhul, kui digitaalse teenuse osutajal on juurdepääs teabele, mis on vajalik esimeses lõigus osutatud kriteeriumide täitmise hindamiseks. 5. Kui oluliste teenuste operaator sõltub tähtsa ühiskondliku ja majandustegevuse säilitamiseks olulise teenuse osutamisel kolmandast isikust digitaalse teenuse osutajast, peab operaator teatama digitaalse teenuse osutajat kahjustava intsidendi mis tahes olulisest mõjust oluliste teenuste järjepidevusele. 6. Kui see on asjakohane ja eelkõige juhul, kui lõikes 3 osutatud intsident puudutab kahte või enamat liikmesriiki, peab pädev asutus või CSIRT teavitama teisi mõjutatud liikmesriike. Seda tehes kaitsevad pädevad asutused, CSIRTid ja ühtsed kontaktpunktid kooskõlas liidu õigusega või liidu õigusele vastavate siseriiklike õigusaktidega digitaalse teenuse osutaja turvalisust ja ärihuve ning esitatud teabe konfidentsiaalsust. 7. Pärast konsulteerimist asjaomase digitaalse teenuse osutajaga võivad pädev asutus või CSIRTid ja, kui see on asjakohane, teiste asjaomaste liikmesriikide asutused või CSIRTid teavitada üldsust üksikutest intsidentidest või			

nõuda, et digitaalse teenuse osutaja seda teeks, juhul kui üldsuse teadlikkus on vajalik intsidendi ärahoidmiseks või käimasoleva intsidendi lahendamiseks või kui intsidendi avalikustamine on muul moel üldsuse huvides. 8. Komisjonil on õigus võtta vastu rakendusakte, et täpsustada veelgi käesoleva artikli lõikes 1 osutatud elemente ja lõikes 4 loetletud parameetreid. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 22 lõikes 2 osutatud kontrollimenetlusega hiljemalt 9. augustiks 2017. 9. Komisjon võib võtta vastu rakendusakte, millega kehtestada teatamisnõuete suhtes kohaldatavad formaadid ja menetlused. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 22 lõikes 2 osutatud kontrollimenetlusega. 10. Liikmesriigid ei kehtesta digitaalse teenuse osutajate suhtes täiendavaid turva- või teatamisnõudeid, ilma et see piiraks artikli 1 lõike 6 kohaldamist. 11.V peatükki ei kohaldata komisjoni soovituses 2003/361/EÜ (1) määratletud mikro- ja väikeste ettevõtjate suhtes.			
Artikkel 17 **Rakendamine ja jõustamine** 1. Liikmesriigid tagavad, et pädevad asutused võtavad vajaduse korral meetmeid järgneva järelevalve käigus, kui neile esitatakse tõendid, et digitaalse teenuse osutaja ei täida artiklis 16 sätestatud nõudeid. Tõendid võib esitada teise liikmeriigi pädev asutus, kus	Art 17 lg 1 Jah Art 17 lg 2 Jah Art 17 lg 3 Ei	Art 17 lg 1 – KüTS § 15 lg 3 Art 17 lg 2 – KüTS § 15 lg 1	

teenust osutatakse. 2. Lõike 1 kohaldamisel on pädevatel asutustel vajalikud õigused ja vahendid, et nõuda digitaalse teenuse osutajatelt a) nende võrgu- ja infosüsteemide turvalisuse hindamiseks vajaliku teabe, sealhulgas dokumenteeritud turvapõhimõtete esitamist; b) artiklis 16 sätestatud nõuete täitmata jätmise heastamist. 3. Kui digitaalse teenuse osutaja peamine tegevuskoht või esindaja asuvad ühes liikmesriigis, kuid tema võrgu- ja infosüsteemid asuvad ühes või mitmes teises liikmesriigis, teevad peamise tegevuskoha või esindaja liikmesriigi pädev asutus ja kõnealuste teiste liikmesriikide pädevad asutused koostööd ja vajaduse korral abistavad üksteist. Abi ja koostöö võivad sisaldada asjaomaste pädevate asutuste vahelist teabevahetust ja taotlusi võtta lõikes 2 osutatud järelevalvemeetmed.			
Artikkel 18 **Jurisdiktsioon ja territoriaalsus** 1. Käesoleva direktiivi kohaldamise eesmärgil käsitatakse digitaalse teenuse osutajat selle liikmesriigi jurisdiktsiooni alla kuuluvana, kus on tema peamine tegevuskoht. Digitaalse teenuse osutaja peamiseks asukohaks loetakse liikmesriiki, kui tema peakorter asub kõnealuses liikmesriigis. 2. Digitaalse teenuse osutaja, kelle asukoht ei ole liidus, kuid kes osutab liidus III lisas osutatud teenuseid, peab määrama oma esindaja liidus. Esindaja asukohaks on üks nendest liikmesriikidest, kus teenuseid	Art 18 lg 1 Ei Art 18 lg 2 Jah Art 18 lg 3 Ei	Art lg 18 lg 2 – KüTS § 12	

osutatakse. Digitaalse teenuse osutajat käsitatakse selle liikmesriigi jurisdiktsiooni alla kuuluvana, kus on esindaja asukoht. 3. Esindaja määramine digitaalse teenuse osutaja poolt ei piira kohtumenetlusi, mida võiks algatada digitaalse teenuse osutaja enda vastu.			
Artikkel 19 **Standardimine** 1. Selleks et edendada artikli 14 lõigete 1 ja 2 ning artikli 16 lõigete 1 ja 2 ühtset rakendamist, innustavad liikmesriigid võrgu- ja infosüsteemide turvalisust käsitlevate Euroopa või rahvusvaheliselt heaks kiidetud standardite ja spetsifikatsioonide kasutamist, ilma et nad seejuures nõuaksid või soosiksid konkreetset tüüpi tehnoloogia kasutamist. 2. ENISA koostab koostöös liikmesriikidega nõuanded ja suunised seoses tehniliste valdkondadega, mida tuleks lõike 1 puhul arvesse võtta, ning seoses olemasolevate, sealhulgas liikmesriikide standarditega, mis võimaldaksid neid valdkondi hõlmata.	Art 19 lg 1, 2 Ei		
Artikkel 20 **Vabatahtlik teatamine** 1. Ilma et see piiraks artikli 3 kohaldamist, võivad üksused, mis ei ole määratletud kui oluliste teenuste operaatorid ega digitaalse teenuse osutajad, teatada vabatahtlikult intsidentidest, millel on oluline mõju nende osutatavate teenuste järjepidevusele. 2. Teadete läbivaatamisel järgivad	Art 20 Ei		

liikmesriigid artiklis 14 sätestatud menetlust. Liikmesriigid võivad vaadata kohustuslikud teated läbi enne vabatahtlikke teateid. Vabatahtlikud teated vaadatakse läbi üksnes juhul, kui selline läbivaatamine ei ole asjaomaste liikmesriikide jaoks ebaproportsionaalselt ega liigselt koormav. Vabatahtlik teade ei pane teate esitanud üksusele mingeid kohustusi, mida tal ei oleks tekkinud juhul, kui ta ei oleks kõnealust teadet esitanud.			
Artikkel 21 **Karistused** Liikmesriigid kehtestavad sätted karistuste kohta, mida rakendatakse käesoleva direktiivi kohaselt vastu võetud siseriiklike õigusnormide rikkumise korral, ning võtavad kõik vajalikud meetmed nende rakendamise tagamiseks. Kehtestatud karistused peavad olema tõhusad, proportsionaalsed ja hoiatavad. Liikmesriigid teatavad kõnealustest sätetest ja meetmetest komisjonile hiljemalt 9. maiks 2018, samuti teatavad nad viivitamata kõigist neid mõjutavatest hilisematest muudatustest.	Art 21 Jah	Art 21 KüTS § 19 lg 1, 2; § 20	
Artikkel 22 **Komiteemenetlus** 1. Komisjoni abistab võrgu- ja infoturbesüsteemide komitee. Nimetatud komitee on komitee määruse (EL) nr 182/2011 tähenduses. 2. Käesolevale lõikele viitamisel kohaldatakse määruse (EL) nr 182/2011 artiklit 5.	Art 22 Ei		
Artikkel 23 **Läbivaatamine** 1. Komisjon esitab 9. maiks 2019	Art 23 Ei		

Euroopa Parlamendile ja nõukogule aruande, milles antakse hinnang liikmesriikide lähenemisviiside järjepidevusele oluliste teenuste operaatorite identifitseerimisel. 2. Komisjon vaatab käesoleva direktiivi toimimise korrapäraselt läbi ning esitab aruande Euroopa Parlamendile ja nõukogule. Sel eesmärgil ning strateegilise ja operatiivkoostöö täiendavaks edendamiseks võtab komisjon arvesse koostöörühma ja CSIRTide võrgustiku aruandeid strateegilisel ja operatiivtasandil saadud kogemuste kohta. Komisjon hindab läbivaatamise käigus ka II ja III lisas esitatud loetelusid ning järjepidevust oluliste teenuste operaatorite ja teenuste identifitseerimisel II lisas osutatud sektorites. Esimene aruanne esitatakse 9. maiks 2021.			
Artikkel 24 **Üleminekumeetmed** 1. Ilma et see piiraks artikli 25 kohaldamist ja selleks, et anda liikmesriikidele lisavõimalusi teha ülevõtmisperioodil asjakohast koostööd, alustavad koostöörühm ja CSIRTide võrgustik oma vastavalt artikli 11 lõikes 3 ja artikli 12 lõikes 3 sätestatud ülesannete täitmist 9. veebruariks 2017. 2. Ajavahemikuks 9. veebruarist 2017 kuni 9. novembrini 2018 ning selleks, et toetada liikmesriikide järjepidevat lähenemisviisi oluliste teenuste operaatorite identifitseerimisel, arutab koostöörühm nende riiklike meetmete protsessi, sisu ja liiki, mis võimaldavad identifitseerida oluliste teenuste operaatorid	Art 24 Ei		

konkreetses sektoris vastavalt artiklites 5 ja 6 sätestatud kriteeriumidele. Koostöörühm arutab liikmesriigi taotlusel ka asjaomase liikmesriigi konkreetseid riiklike meetmete kavandeid, mis võimaldavad identifitseerida oluliste teenuste operaatorid konkreetses sektoris vastavalt artiklites 5 ja 6 sätestatud kriteeriumidele. 3. Liikmesriigid tagavad 9. veebruariks 2017 ja käesoleva artikli kohaldamisel asjakohase esindatuse koostöörühmas ja CSIRTide võrgustikus.			
Artikkel 25 **Ülevõtmine** 1. Liikmesriigid võtavad vastu ja avaldavad käesoleva direktiivi järgimiseks vajalikud õigus- ja haldusnormid 9. maiks 2018. Liikmesriigid teatavad nendest viivitamata komisjonile. Nad kohaldavad kõnealuseid meetmeid alates 10. maist 2018. Kui liikmesriigid need sätted vastu võtavad, lisavad nad nendesse või nende ametliku avaldamise korral nende juurde viite käesolevale direktiivile. Sellise viitamise viisi näevad ette liikmesriigid. 2. Liikmesriigid edastavad komisjonile käesoleva direktiiviga reguleeritavas valdkonnas nende poolt vastu võetud põhiliste siseriiklike õigusnormide teksti.	Art 25 lg 1 Jah Art 25 lg 2 Ei	Art 25 lg 1 KüTS § 28	Art 25 lg 2 MKM tööülesanne
Artikkel 26 **Jõustumine** Käesolev direktiiv jõustub kahekümnendal päeval pärast selle avaldamist *Euroopa Liidu Teatajas*.	Art 26 Ei		
Artikkel 27	Art 27 Ei		

Adressaadid Käesolev direktiiv on adresseeritud liikmesriikidele.			