EESTI INFOTEHNOLOOGIA JA TELEKOMMUNIKATSIOONI LIIT

Pr Urve Palo
Majandus- ja
Kommunikatsiooniministeerium
Suur-Ameerika 1
10122 TALLINN

Teie 03.10.2017 nr 2-2/17-0344/17-8149

Meie 24.10.2017 nr 6.1-1/31-2

Arvamus küberturvalisuse seaduse eelnõu kohta

Eesti Infotehnoloogia ja Telekommunikatsiooni Liit (ITL) analüüsis Teie poolt 03.10.2017. arvamuse avaldamiseks edastatud küberturvalisuse seaduse eelnõud (edaspidi: eelnõu). Oleme esitanud varasemalt arvamuse ka eelnõu väljatöötamiskavatsuse kohta (ITL-i arvamus 17.04.2017 nr 6.1-1/31-1) ning esitanud eelnõu menetluse käigus Majandus- ja Kommunikatsiooniministeeriumi ja Riigi Infosüsteemi Ameti ametnikele ettepanekuid nii kirjalikult kui ka kohtumiste käigus. Käesolevaga esitame eelnõu kohta oma põhiseisukohad ning detailsemad kommentaarid ja ettepanekud konkreetsete sätete lõikes.

1. Üldised seisukohad

1.1. Eelnõu regulatsiooni ulatus

1.1.1. Eelnõuga **reguleeritav valdkond ehk küberturvalisus on liiga lai.** Kuigi eelnõu eesmärk on lisaks Euroopa Liidu direktiivi nr 2016/1148 (6. juulist 2016, meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus, edaspidi: NIS direktiiv) ülevõtmisele Riigi Infosüsteemi Ameti (edaspidi: RIA) kui küberintsidentide ennetamise ja lahendamise eest vastutava asutuse pädevuse ning volituste reguleerimine, ei käsitle eelnõu vaatamata selle pealkirjale kõiki küberturvalisusega seotud teemasid, näiteks küberjulgeolekut. Oleme seisukohal, et kõiki küberturvalisusega seotud teemasid ei saa ega peagi selles eelnõus käsitlema.

Eelnõu seletuskirjas püütakse küll selgitada, miks käsitletakse „kübervaldkonda“. Ka need põhjendused (sh asjaolu, et nii on kirjas RIA põhimääruses) pigem toetavad arusaama, et nn kübervaldkond on oluliselt laiem kui antud seaduse regulatsiooniala. Seetõttu on ITL-i hinnangul eksitav nimetada see eelnõu küberturvalisuse seaduseks. Eelnõu reguleerimisala ja

muuhulgas pealkiri peaks olema sarnaselt NIS-direktiivis kasutatavatele terminitele võrgu- ja infosüsteemide turvalisuse seadus.
Ka tunnistatakse eelnõu seletuskirjas (lk 3), et NIS direktiivi ülevõtmise ajaraami arvestades ei ole eelnõuga võimalik kogu nn kübervaldkonna normide laiapõhjaline revisjon, mistõttu puudutab eelnõu eelkõige NIS direktiivi ülevõtmise ja järelevalvemeetmetega seonduvat. Seetõttu on eksitav nimetada seda küberturvalisuse seaduseks. Seaduse pealkiri peab kajastama seaduse sisu.

1.1.2. NIS direktiiv sätestab liikmesriigile kohustuse identifitseerida oluliste teenuste osutajad vastavalt direktiivi lisas II osutatud sektoritele ja allsektoritele. Eelnõus on otsustatud direktiivis sätestatud valdkondade kõrval nimetada olulise teenuse osutajateks ka kõik elutähtsa teenuse osutajad hädaolukorra seaduse (HOS) mõttes. See tähendab, et ühelt poolt laiendatakse direktiivi regulatsiooni ning teiselt poolt laiendatakse mõnes mõttes ka HOS-i regulatsiooni kehtestades kohustused ettevõtetele, kes uue (01.07.2017. jõustunud) HOS-i regulatsiooni alt välja jäeti. **ITL on seisukohal, et Eestis ei tuleks laiendada direktiivi regulatsiooni sellises mahus**. Vastamata on küsimus, miks laiendatakse Eestis NIS-direktiivi regulatsioon valdkondadesse, mida direktiiv reguleerimisalana ei kata. Näiteks elektroonilise side teenuse osutajad välistab direktiiv selgesõnaliselt, aga Eestis on nad elutähtsa teenuse osutajatena eelnõu kohaldamisalas.
Kuigi eelnõu § 3 lg 3 kohaselt identifitseerib RIA eelnõu kohaldamisalas olevad teenuse osutajad hiljemalt 09.11.2018, **palume tungivalt teha seda varem, et kõigil asjaosalistel oleks üheselt selge, kellele see regulatsioon laieneb.**

1.2. RIA õigused, volitused ja pädevused

1.2.1. **Eelnõus keskendutakse väga suures mahus RIA-le lisaõiguste andmisele lõpuni põhjendamata, milliste probleemide lahendamiseks neid õiguseid vaja** on ning milline on vastutus, kui neid õiguseid kasutatakse tasakaalustamatult või ebakompetentselt. Eelnõu kohaldub vaid teatud kindlatele ettevõtetele ehk elutähtsa teenuse osutajatele, kriitiliste infrastruktuuri haldajatele ning digitaalsete teenuste osujatajalele, aga samas antakse RIA-le nende üle järelevalve teostamiseks väga ulatuslikud õigused. Leiame, et tegu on ebaproportsionaalse sekkumisega ettevõtlusvabadusse. Kui reaalne praktika nõuaks tõepoolest selliseid meetmeid, peaks RIA-l olema õigus kohaldada neid kõikide ettevõtete suhtes.

1.2.2. **Eelnõu koostamisel on lähtutud eeldusest, et suured ja turvalisusse tegelikult investeerivad ettevõtted tähtsustavad ikkagi võrkude ja infosüsteemide turvalisust liiga vähe ja seepärast peab RIA olema nende süsteemide olukorraga reaalajas kursis,** samas kui eelnevalt on ettevõtted läbinud kõik ettenähtud analüüsid, auditid, jms. Samas jäävad eelnõu skoobist välja näiteks valdav enamik sideettevõtjaid. Täna tegutseb Eestis vastavalt Tehnilise Järelevalve Ameti aastaraamatule 2016216 sideettevõtet, kellest elutähtsat teenust või eelnõus nimetatud tingimustel kaabelleviteenust osutavad ITL-i hinnangul kuus ettevõtet.

1.2.3. **ITL-i liikmeskonda kuuluvate ettevõtete hinnangul toimuks eelnõu käesoleval kujul vastuvõtmise järgselt liiga ulatuslik sekkumine ettevõtlusvabadusse.** Näiteks on eelnõu loogika kohaselt iga intsidendi puhul tegu küberintsidendiga, kuni pole tõestatud vastupidist. See ei arvesta aga ettevõtete lepinguvabadust ehk õigust omavahel kokku leppida teenuse tasemetes (teenustaseme/SLA kokkulepped) ja lubatud katkestuste aegades.

1.2.4. Eelnõu annab RIA-le õiguse saada seireinfot teenuse osutajate süsteeme ohustava tegevuse või tarkvara kohta (§ 7 lg 2 p 3) ning samuti õiguse võtta süsteemide juhtimine üle (§ 17). Leiame, et eelnõu annab võimaluse nn tagauste loomiseks RIA-le ning meie hinnangul ei ole **selliste nn tagauste loomine tänases Eesti ühiskonnas aktsepteeritav**, mistõttu on ITL kindlalt selliste kohustuste kehtestamise vastu. Eesti soovib eelnõu seletuskirja kohaselt olla maailmas küberturvalisuse vallas juhtiv riik ning samast eeldusest on lähtutud ka eelnõu koostamisel. Leiame, et nn tagauste soodustamine ja julgustamine õigusaktiga on midagi, mida peaks häbenema, mitte eeskujuks seadma.

1.2.5. **Eelnõu eksib oluliselt rollide lahususe põhimõtte vastu lubades RIA-l anda ise endale volitusi teatud korrakaitseliste toimingute tegemiseks.** Oleme seisukohal, et ka küberturvalisuse alaste rikkumiste ja järelevalve korral tuleb lähtuda üldisest põhimõttest, mille kohaselt on korrakaitse teostamine Siseministeeriumi haldusalas ning lubasid erimeetmete rakendamiseks annavad prokuratuur ja kohtud. ITL ei näe põhjust, miks infotehnoloogia valdkonda teisiti käsitletakse ning kogu pädevus selles vallas RIA-le antakse. Lisaks on RIA ise avalikus sektoris üks olulisemaid teenuseosutajaid X-tee ning ASO võrguga, kellest sõltuvad teised teenused. Samas on RIA selle eelnõu kontekstis järelevalve teostaja. See on ka põhjuseks, miks peab olema korraldatud rollide lahusus.

1.2.6. Täna on RIA küberintsidentide ennetamisel ja lahendamisel ettevõtetele nõustavaks partneriks ning tegevusi tehakse kokkulepete alusel. ITL-ile teadaolevalt töötab see praktikas hästi, mistõttu leiame, et **koostöö võiks ka edaspidi olla küberturvalisuse tagamisel olulisel kohal**.

1.3. Eelnõu mõjud

1.3.1. **Eelnõu kasvatab oluliselt ettevõtete halduskoormust**, sest see mõjutab mitmeid erinevaid ettevõtteid ja riigiasutusi ning ettevõtetele kehtestatavate kohustustega sekkutakse oluliselt nende tegutsemisvabadusse. Samal ajal hinnatakse eelnõu seletuskirjas (p 6.3) ekslikult halduskoormuse kasvu ettevõtetele väikeseks. Eelnõu § 22 p 5 sätestatud uue päringu vastuse koostamiseks kuluvat aega hinnatakse eelnõu seletuskirjas 15 minutile, tegelikkuses on see pikem ning isegi kui see aeg oleks õige ja päringuid oleks maksimaalselt 200, siis teeb see 50 töötundi aastas.

1.3.1. Eelnõu koostamise käigus toimunud mitmete kohtumiste põhjal on ITL-il tekkinud arusaam, et **regulatsiooni kõiki aspekte selle tegelikuks rakendamiseks ja mõjusid ettevõtetele ei ole koostamise käigus läbi analüüsitud.**

2. **Ettepanekud eelnõu sätete kohta**

2.3. **Mõisted (eelnõu § 2)**

2.3.1. Eelnõu § 2 punktides 1 ja 4 on defineeritud **süsteemi** ja **küberintsidendi** mõisted üsna laialt. Kuna eelnõu § 8 lg 1 nõuab teavitamist ainult olulise mõjuga intsidendist, siis võib seda aktsepteerida. Samas peame vajalikuks, et eelnõu seletuskirjas tuuakse nende mõistete kohta reaalseid näited ehk avatakse mõisted üheselt mõistetavalt. Hetkel seda tehtud ei ole (seletuskirja osa 4, alates lk 28).

Rõhutame siinkohal üle, et ITL ei ole nõus lähenemisega, et iga intsident (s.h näiteks tugijaama kinnituspoldi allakukkumine mobiilimastist või maakaabli katki kaevamine nii, et tegelikult on olemas paralleelne toimiv sideühendus) on küberintsident, kuni pole tõendatud vastupidist. Leiame, et teenuse osutajaid tuleb selles küsimuses usaldada ning vastutus intsidendi määratlemise osas peaks lausuma neil.

Selleks, et regulatsioon oleks rakendatav, peavad olulised mõisted ja nendega seotud kohustused olema mõistetavad kõigile, sh ka näiteks võrguinseneridele. Uus seadus ei tohiks juba eos sisaldada ebaselgusi, mis jäävad juristidele praktikas vaidlemiseks.

2.3.2. Eelnõu § 2 punktis 6 defineeritud **internetipõhise kauplemiskoha** puhul jääb ebaselgeks, mida täpsemalt on mõeldud selle all, et tegu peab olema sellise kaupleja veebisaidiga, mis kasutab internetipõhise kauplemiskoha pakutavaid andmetöötlusteenuseid. Mis saab siis, kui kasutusel on hoopis kolmanda isiku poolt pakutavad andmetöötlusteenused? Seetõttu teeme ettepaneku selguse huvides kustutada definitsioonist viimane rida *(„…mis kasutab internetipõhise kauplemiskoha pakutavaid andmetöötlusteenuseid*“). Tegemist on ebavajaliku täpsustusega, mis selgitamise asemel teeb asja segasemaks.

2.3.3. Eelnõu § 2 punktis 7 on defineeritud **internetipõhine otsingumootoriteenus**. ITL-ile jääb arusaamatuks, miks on oluline siin välja tuua keelepõhine eristus. Siis võiks mõelda veel riigi vms eristust ja see nimekiri võib olla päris pikk. On ju olemas ka otsingumootoreid teatud süsteemide põhiselt, nt raamatukogude võrgustik. Seega ei ole selliste erisuste väljatoomine meie hinnangul põhjendatud ja seetõttu teeme ettepaneku sõnastada see definitsioon järgmiselt: „*internetipõhine otsingumootoriteenus – infoühiskonna teenus, mis võimaldab kasutajal teha otsingut üldjuhul kõikidel või ~~konkreetses keeles~~ piiratud hulgal veebisaitidel mis tahes teemal…*“.

2.4. **Digitaalse teenuse osutaja (eelnõu § 4)**

2.4.1. Juhime tähelepanu, et digitaalse teenuse osutaja piirmäärad (raamatupidamise seaduse § 3 punktid 14 ja 15) on rangemad, kui NIS-direktiivis. Viimane viitab selles küsimuses Komisjoni soovitusele 2003/361/EÜ. Küsimuses on selles, kas väikeettevõtja käibepiir on 10 või 8 miljonit eurot aastas. ITL on seisukohal, et Eesti ei peaks rakendama direktiivi rangemalt.

2.4.2. Peame äärmiselt vajalikuks, et riik tegeleks senisest aktiivsemalt eelnõust tulenevate kohustuste teavitamise ja selgitamisega digitaalsete teenuste osutajatele. Tegemist on teenuse osutajatega, kes seni on olnud võrdlemisi vähe reguleeritud ning nad peavad saama teadlikuks neile eelnõuga rakenduvatest olulistest kohustustest.

2.5. **Teenuse osutaja süsteemi turvameetmed (eelnõu § 7)**

2.5.1. ITL teeb ettepaneku kustutada § 7 lg 1 punktist 3 järgmine lauseosa „*või teise sõltuva teenuse toimepidavusele või süsteemile ja sellega seotud infovarale avalduva mõju ennetamiseks.“*

Juhtime tähelepanu, et teise sõltuva (antud kontekstis olulise) teenuse toimepidavusele või süsteemile avalduda võiva mõju ennetamine saab toimida vaid ühe süsteemi piires. Teenuse osutaja ei saa mitte kuidagi teise sõltuva teenuse toimepidavusele avalduda võivat mõju ennetada. Teenuse osutaja ei saa ise ammendavalt teada, kes tema teenusest sõltuvad. Teenuse osutajate asetamine sellisesse ahelasse ei ole loogiline. Kui selline olukord tekib, siis kehtivad eelnõu kohaselt teavitamise kohustused.

2.5.2. ITL teeb ettepaneku sõnastada eelnõu § 7 lg 2 punkt 3 järgmiselt:

„*tagama süsteemi turvalisust ohustava tegevuse või tarkvara tuvastamiseks süsteemi seire, mis võimaldab küberintsidendi ennetamist ja toimunud küberintsidendi tekkepõhjuste väljaselgitamist, ning edastama teabe süsteemi oluliselt ohustava tegevuse või tarkvara kohta Riigi Infosüsteemi Ametile*“;

Kuna vastavalt eelnõu §-le 8 tuleb RIA-t teavitada vaid olulise mõjuga intsidentidest, peaks ka süsteemi ohustavast tegevusest või tarkvarast teavitama siis, kui tegemist on olulise ohuga. Vastasel juhul on tegu väga suure halduskoormusega ettevõtetele ning meie hinnangul ka RIA ülekoormamisega tarbetu teabega. Kindlasti ei tohi vastava sätte alusel luua nn tagauksi teenuste osutajate süsteemidesse, millele viitab siinkohal eelnõu seletuskiri (lk 13-14).

2.5.3. ITL toetab eelnõu § 7 lõiget 3, sest see kehtestab väga olulise põhimõtte, mille kohaselt kui teenuse osutaja volitab süsteemi haldamise teisele isikule, siis vastutab teenuse osutaja ise selle eest, et see teine isik tagab süsteemi turvameetmete rakendamise. Samas leiame, et eelnõu seletuskirjas tuleks seda küsimust rohkem avada ning üle kontrollida, kas eelnõu tekst on ikka selles küsimuses üheselt mõistetav. Nimelt võib eelnõust välja lugeda IT-teenuse osutajate kohustuse justkui tagada teatud SLA-d, kuigi tegelikult peaks oluliste teenuste osutajad (kellel on töövahendiks infosüsteemid ja side) olema need, kellele eelnõu kohustused seab. Nemad peavad IT-, side-, elektri-, kütuse-, usaldusteenuse- ja teiste teenuste osutajatelt (kellest osa on eelnõu tähenduses teenuse osutajad) omakorda lepingutega vastavat teenust tellima. See ahel ei ole eelnõus hetkel piisavalt läbi mõeldud, sest teenuse osutajateks eelnõu mõttes on nii lennujaam, sideteenuse osutaja, elektriteenuse osutaja kui ka usaldusteenuse osutaja, kuid nt lennujaama süsteemide toimimise eest peab vastutama selgelt lennujaam.

Ehk siis kõik teenuse osutajad on eelnõu kohaselt pandud võrdselt vastutama ühe teenuse osutaja tegevuse eest.

2.6. **Teenuse osutaja küberintsidendist teavitamine (eelnõu § 8)**

2.6.1. Teeme ettepaneku sätestada üldised intsidendi olulisuse kriteeriumid eelnõu tekstis. Nõustume, et neid ei saa detailselt eelnõusse kirjutada, kuna need on valdkonnapõhised, aga üldpõhimõtted peaksid ITL-i hinnangul sisalduma seaduses, et hiljem ei laiendataks eelnõu § 8 lõikes 6 sisalduva volitusnormi alusel antavas määruses teenuse olulisuse kohaldamisala oluliselt. Aluseks tuleb võtta kriteeriumid, mis on sätestatud NIS direktiivi artiklis 14 (4).

2.6.2. Teeme ettepaneku täpsustada eelnõu § 8 lõiget 2 järgmiselt: „*Teenuse osutaja on kohustatud teavitama isikut, keda küberintsident võib otseselt ja oluliselt mõjutada.*“ Meie hinnangul selle sätte eesmärk ei ole teavitada kõiki Eesti elanikke igast intsidendist, mis potentsiaalselt võib neid mõjutada. Leiame, et teavitus peaks olema rohkem suunatud, et sellest ka reaalselt kasu oleks.

2.6.3. Eelnõu § 8 lõikega 5 seoses sooviksime selgust, kas need, kes teavitavad RIA-t küberintsidendist, mis põhjustab isikuandmete töötlemise rikkumise, ei pea eraldi Andmekaitse Inspektsiooni (edaspidi AKI) teavitama ehk kas RIA võtab üle selle kohustuse õigeaegselt AKI-t teavitada?

2.6.4. Eelnõu § 8 lg 6 sisalduva volitusnormi juures peab olema kirjas, et olulisuse kriteeriumid kehtestatakse (küll ühes määruses) valdkonnapõhiselt, kuna küberintsidendid on erinevates valdkondades väga erinevad ning see, mis omab olulist mõju ühe eelnõu kohaldamisalas oleva teenuse osutaja puhul, ei pruugi seda omada teise puhul. Juhul, kui seda eelnõusse ei lisata, palume lisada vastav põhimõte eelnõu seletuskirja.

2.6.5. Eelnõusse on lisandunud § 8 lg 7, mis sätestab teenuse osutaja kohustuse teavitada digitaalse teenuse osutaja küberintsidendist, kui sellest sõltub teenuse osutaja enda teenus. ITL-ile jääb arusaamatuks, miks see säte on lisatud. Millist lisaväärtust see annab võrreldes § 8 lõikega 1, mille kohaselt teenuse osutaja peab teavitama küberintsidendist? Kui teenuse osutaja teenus on mõjutatud, siis kohaldubki juba § 8 lg 1. Lisaks soovime selgitust, keda selles sättes viidatud digitaalsete teenuste osutajate all sisuliselt mõeldakse? Ühtlasi juhime tähelepanu, et selle normi aluseks olev NIS direktiivi art 16 (5) sätestab, et teavitama peab „mis tahes olulisest mõjust oluliste teenuste järjepidevusele“.

2.7. **Riikliku järelevalve erimeetmed (eelnõu § 16)**

2.7.1. ITL-ile jääb arusaamatuks, miks on õigustatuks isikuks antud paragrahvi tähenduses korrakaitseorgan. Samal ajal sätestab eelnõu § 15, et riiklikku ja haldusjärelevalvet teostab RIA. Õigusselguse huvides oleks korrektne ka antud sättes selgelt sätestada, kes on see korrakaitseorgan, kellel on õigus neid erimeetmeid kasutada.

2.7.2. Teiseks tekkis meil küsimus, miks RIA ei tee nende õiguste kasutamiseks politseiga koostööd. ITL-ile jääb mõistetamatuks, miks RIA-le neid eriõigusi vaja on.

2.8. **Küberintsidendi tõkestamine (eelnõu § 17)**

2.8.1. ITL teeb ettepaneku võtta eelnõust välja § 17, kuna ITL-i hinnangul ei ole õigustatud anda RIA-le õigus siseneda teenuse osutaja süsteemi valdaja või muu isiku loata ning selle süsteemi juhtimine üle võtta. Tegu on ebaproportsionaalse sekkumisega teenuse osutajate äritegevusse. Antud juhul tuginetakse vaid RIA hinnangutele, mitte reaalsetele juba tekkinud olukordadele. Lisaks on olemas muud vahendid, millega on võimalik saavutada sama tulemus. Ühtlasi oleme seisukohal, et RIA-l puudub teadmine ja kogemus niivõrd erinevate valdkondade infosüsteemide kohta, sh riigile kuuluvate infosüsteemide kohta (vt analoogne õigus §-is 18). Näiteks on eelnõu mõttes süsteem, mille juhtimist võib üle võtta sideettevõtte elektroonilise side võrk või elektrijaama juhtimissüsteem, mille kummagi tegelikuks juhtimiseks RIA spetsialistidel pädevus puudub. Seepärast võib RIA poolt süsteemi juhtimise ülevõtmine tuua kaasa isegi suurema ohu teenuste toimepidavusele kui algne küberintsident.

2.8.2. Juhul, kui § 17 jääb eelnõusse alles, peame äärmiselt vajalikuks, et sätet kirjutatakse oluliselt täpsemaks. Selline küberintsidendi tõkestamine RIA poolt tohib toimuda vaid juhul, kui seda tehakse juba teadaoleva ohu kõrvaldamiseks (mitte ohu väljaselgitamiseks) konkreetses süsteemi osas, teenuse osutajaga on eelnevalt konsulteeritud ning luba selleks on saadud võimude lahususe põhimõtet silmas pidades. Samuti peab regulatsioon kirjeldama sekkumismeedet mitte maksimaalsena (süsteemi sisenemine ja juhtimise ülevõtmine kui lai üldvolitus), vaid eristades erinevaid sekkumist vajavaid olukordi ja andes selgeid volitusi erinevate olukordade jaoks.
Eeltoodust tulenevalt teeme ettepaneku muuta eelnõu § 17 järgmiselt:

2.8.2.1. Eelnõu § 17 lg 1 sõnastatakse järgmiselt: „*Riikliku järelevalve teostamisel võib Riigi Infosüsteemi Amet ohtliku süsteemi komponendi juhtimise vahetult või kaughalduse teel üle võtta ning küberintsidendist põhjustatud kõrgendatud ohuallika väljaselgitamiseks või tõrjumiseks süsteemi komponendi kasutamist või süsteemi komponendile juurdepääsu piirata.“*
Selgitus: esiteks ei ole mitte kuidagi õigustatud see, et RIA tungib süsteemi sisse selleks, et vaadata, kas seal on üldse oht. Ohu olemasolu peab olema enne kindlaks tehtud ning süsteemi tullakse selleks, et ohuallikas välja selgitada või seda tõrjuda. Teiseks ei saa see õigus kehtida kogu teenuse osutaja süsteemi osas, vaid ainult selle süsteemi komponendi osas, kust oht lähtub.

2.8.2.2. Eelnõu § 17 lg 2 p 2 sõnastatakse järgmiselt: „*süsteemi haldaja ei nõustu ise küberintsidenti lahendama või ei saa sellega õigeaegselt hakkama*“.
Selgitus: Käesoleva meetme kohaldamisest tuleb süsteemi haldajat teavitada enne meetme rakendamist. See tähendab, et meetme rakendamiseks peab olema üheselt selge, et teenuse osutaja ei lahenda seda intsidenti ise. Teenuse osutaja peab ise ütlema välja, et ta ei tegele intsidendiga, sest ta ei saa, ei oska või ei taha seda teha. . Õigusnormist peab nähtuma üheselt, et enne meetme rakendamist on teenuse osutaja käest küsitud.

Kui teenuse osutajat enne ei teavitata, võib tekkida olukord, kus teenuse osutajal on hiljem võimatu või äärmisel juhul väga keerukas tuvastada, kust nö algavad küberintsidendist põhjustatud probleemid ja teenuse/süsteemi mittetoimimine ning kust omakorda RIA sekkumisest tingitud probleemid. Eelnev teavitamine on oluline ka seetõttu, et teenuse osutaja teaks, et süsteemis toimetab RIA, mitte ei arvaks, et tegu on süsteemi tunginud küberkurjategijaga.

2.8.2.3. Eeltoodust tulenevalt palume ka § 17 lg 3 ümber sõnastada selliselt, et süsteemi haldajat teavitatakse enne meetme kohaldamist.
Selgitus: eelnõu sõnastusest ei ole võimalik välja lugeda, et eelnevalt on süsteemi omanikuga püütud ühendust saada, et ta ise intsidenti lahendama hakkaks.

2.8.2.4. Võimude lahususe põhimõttest tulenevalt teeme ettepaneku nimetada meetme kohaldamiseks õigustatud isikuks § 17 lõikes 5 prokuratuur. Vastasel juhul võimaldab eelnõu RIA-l võtta ise endale volitusi.

2.8.3. Lisaks rõhutame, et selle ja teiste erimeetmete rakendamisel tuleb järgida korrakaitse seaduses sätestatud põhimõtteid. Näiteks tuleb selle kohaselt lisaks protokollimisele koguda ja lisada protokollile vajalikud tõendid, mis näitavad, et situatsioon vastas tingimustele ning mida kaughalduse või ülevõtmise käigus tegelikult tehti. Kui need kohustused sisalduvad muus õigusaktis, teeme ettepaneku neile sõnaselgelt viidata (isegi kui õigusaktide koostamise nõuded seda ette ei näe), kuna antud eelnõu puhul tegemist on õigusaktiga, mille rakendamine peab olema selle täitjatele väga selge ja üheselt mõistetav.

2.9. **Sideettevõtjate poolt RIA-le teabe andmise kohustus (eelnõu § 22 lg 5 ehk** elektroonilise side seaduse täiendamine paragrahviga 114[3])

2.9.1. ITL on seisukohal, et see säte tuleb eelnõust välja jätta ning teema tuleb käsitleda koos elektroonilise side seaduse § 111[1] ülevaatamisega, mis on hetkel Justiitsministeeriumil käsil. Kindlasti tuleb vältida olukorda, kus Eesti õiguskorda lisandub uus paragrahv, mis on juba selle vastuvõtmise hetkel vastuolus Euroopa Kohtu lahendiga.

2.9.2. Juhime tähelepanu, et üldjuhul võimaldab seadme info tuvastada ka kasutaja andmeid ja siin on oht kasutajate privaatsussesse põhjendamatuks sekkumiseks ning seda samuti hinnangulise tunnetuse alusel („ohustatud“). Nimelt soovib RIA saada infot IP-aadressi kohta. See aga kuulub isikuandmete hulka (sellele seisukohale asus Andmekaitse Inspektsioon oma juhises „IP-aadress ja privaatsus“[1], lisaks kohaldatakse Eestis alates 25. maist 2018 Euroopa Liidu andmekaitse üldmäärust, mis nimetab isikuandmetena võrguidentifikaatori).

2.9.3. Lisaks tuleb arvestada, et seadmed kuuluvad tavaliselt klientidele, mistõttu ei pruugi praktikas andmete väljastamine ilma kasutaja tuvastamist võimaldavate andmeteta olla võimalik, mis tähendab, et ka sel põhjusel ei

[1] http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/ip_ja_privaatsus.pdf

ole võimalik logi väljastada. Või ei oma logi enam tõendusväärtust. Seega tuleks seda infot küsida otse klientide käest.

2.9.4. Rõhutame, et sellise kohustuse kehtestamine elektroonilise side teenuse osutajatele toob kaasa oluliselt suureneva halduskoormuse, kuna sättes nõutud andmete esitamiseks tuleb luua uus andmeprofiil ehk teha päringu profileerimist.

3. **Lõpetuseks**

ITL-i liikmed soovivad, et koostatav küberturvalisuse eelnõu saaks olema praktikas rakendatav. See tähendab, et seadusesse ei tohi kirjutada õigusnorme, millest juba nende koostajad erinevalt aru saavad. Arvestama peab ka sellega, et seadust peavad üheselt mõistma nii tehnilised töötajad, turbejuhid, riskijuhid kui ka teised, kes ei ole seaduste tõlgendamisega kokku puutunud.

Seaduse koostamisel ei tohi jääda lootma seda rakendavate isikute tervele mõistusele ning normaalselt toimivale suhtlusele eri osapoolte vahel. Õigusnormid peavad olema üheselt mõistetavad ning kõik õiguste ja vabaduste piirangud peavad olema proportsionaalsed oma eesmärgiga.

ITL tänab võimaluse eest osaleda eelnõu menetluses ning loodab, et MKM leiab võimaluse arvestada ITL-i ülaltoodud ettepanekuid. Vajadusel oleme valmis Teiega kohtuma selleks, et esitatud seisukohti ja ettepanekuid täiendavalt selgitada.

Lugupidamisega

/allkirjastatud digitaalselt/

Jüri Jõema
Tegevjuht

Keilin Tammepärg, keilin.tammeparg@itl.ee, 6177 145