EESTI
INFOTEHNOLOOGIA JA
TELEKOMMUNIKATSIOONI
LIIT

Pr Liisa-Ly Pakosta
Justiits- ja digiminister
Justiits- ja Digiministeerium
Suur-Ameerika 1
10122 TALLINN

Teie 27.06.2025 nr 8-1/5574-1

Meie 8.08.2025 nr 6.1-2/96-1

Arvamus määruse „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ muutmise eelnõu kohta

Täname Eesti Infotehnoloogia ja Telekommunikatsiooni Liidu (ITL) kaasamise eest määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ muutmise eelnõu (edaspidi: eelnõu) menetlusse. Oleme eelnõud analüüsinud ja esitame selle kohta järgmised seisukohad ning ettepanekud.

1. **Esmaste turvameetmete kohaldamise ulatus**

ITL toetab eelnõu eesmärki lihtsustada mikro- ja väikeettevõtjate ning kohaliku omavalitsuse hallatavate asutuste küberturvalisuse tagamise nõudeid ja eelnõuga kavandatavat muudatust, mille kohaselt peavad nimetatud isikud hakkama E-ITS või ISO/IEC 27001 standardi asemel järgima esmaseid turvameetmeid.

Samas jääb meile arusaamatuks, miks muudetakse eelnõuga esmased turvameetmed kohustuslikuks kõigile küberturvalisuse seaduse subjektidele ehk ka neile, kellel on kohustus järgida nimetatud standardeid. Eelnõuga väiksemate ettevõtete ja asutuste halduskoormust vähendades suurendatakse seda suuremate jaoks. Standardi rakendamisel peavad küberturvalisuse subjektid üle käima kõik meetmed ning põhjendama, kui nad teatud meedet ei rakenda. Eelnõu jõustumine tooks kaasa selle, et kui ettevõte on otsustanud, et mõni standardi meede ei ole nende jaoks mõistlik, siis tuleb seda meedet (kui see kattub eelnõu lisas toodud esmase turvameetmega) siiski kohaldada ja seda mitte riskihaldusest tulenevalt, vaid sellepärast, et õigusakt sätestab sellise kohustuse.

ESTONIAN ASSOCIATION OF INFORMATION
TECHNOLOGY AND TELECOMMUNICATIONS
Lõõtsa 2b, 11415 Tallinn, Estonia
+372 617 7145
info@itl.ee / www.itl.ee

Teeme ettepaneku kehtestada eelnõuga esmased turvameetmed kohustuslikuna ainult eelnõu § 1 punktis 4 toodud isikutele.

2. Eelnõu jõustumine

Eelnõu jõustumine on planeeritud juba 1. septembriks käesoleval aastal, mis jätab subjektidele väga vähe aega määruse täitmiseks. Kuna nõuete täitmine on tagatud küberturvalisuse seadusest tuleneva järelevalve ja karistustega, siis **teeme ettepaneku kehtestada pikem jõustumise aeg.** Pikem jõustumisaeg on vajalik kindlasti juhul, kui ITL-i ettepanekut käesoleva kirja punktis 1 ei aktsepteerita ehk määruses toodud meetmeid peavad hakkama täitma kõik küberturvalisuse seaduse subjektid, kuna ka standardite järgijad peavad sel juhul hakkama oma vastavust eelnõus toodud meetmetele üle kontrollima.

3. Ettepanekud eelnõu seletuskirja kohta

Esiteks teeme ettepaneku lisada eelnõu seletuskirja mõjude peatükki mõju küberturvalisuse teenuse osutajatele. Hetkel käsitletakse seal ainult mõju eelnõu subjektidele ning põgusalt ka küberkeskkonnale. Samas on oluline välja tuua, et küberturvalisuse teenuseid pakkuvate ettevõtete poolt vaadates väheneb nende hulk, kellele standardile vastavuse alast nõustamist pakkuda.

Teiseks teeme ettepaneku parandada eelnõu seletuskirja peatüki „Eelnõu vastavus Euroopa Liidu õigusele“ sõnastust. Hetkel on seal kirjas, et eelnõu ei ole seotud Euroopa Liidu õiguse ülevõtmisega. Tegelikkuses on eelnõu väga tugevalt seotud NIS2 direktiivi skoobi defineerimisega – kes on küberturvalisuse seaduse subjektid ja millised kohustused neile rakenduvad.

4. Tagasiside eelnõu lisale „Esmased turvameetmed“

Mitmed eelnõu lisas toodud turvameetmed tekitavad küsimusi ning tunduvad ebamõistlikud. Kui nõuda kõigilt küberturvalisuse subjektidelt selles lisas toodud kõigi nõuete järgimist, siis hakatakse tegelema vastavuse riskidega, mitte tegelike infoturbe riskidega.

ITL-i konkreetsemad kommentaarid, küsimused ja ettepanekud eelnõu lisa kohta on toodud käesoleva kirja lisas.

ESTONIAN ASSOCIATION OF INFORMATION
TECHNOLOGY AND TELECOMMUNICATIONS
Lõõtsa 2b, 11415 Tallinn, Estonia
+372 617 7145
info@itl.ee / www.itl.ee

5. Muud tähelepanekud eelnõu kohta

Eelnõu § 1 punktiga 2 lisatav pilvteenuse mõiste tekitab küsimuse, miks on vaja see täies ulatuses eraldi defineerida. Mõiste on olemas küberturvalisuse seaduses ja seda muudetakse NIS2 direktiivi üle võtva küberturvalisuse seaduse muutmise eelnõuga. Kui eelnõuga muudetavas määruses on oluline rõhutada, et määruse kontekstis on pilvteenus ainult avaliku sektori poolt pakutav teenus, siis ei peaks seda tegema uue definitsiooniga.

Lugupidamisega

/allkirjastatud digitaalselt/

Doris Põld
Tegevjuht

Lisa: Tagasiside eelnõu lisale „Esmased turvameetmed“ 3 lehel

Keilin Tammepärg, keilin.tammeparg@itl.ee

Lisa: Tagasiside eelnõu lisale „Esmased turvameetmed“

- Lisa punkt 1.1. *„määrama infoturbe eest vastutava isiku*;" – selline üldine kohustus vajab läbi mõtlemist. Tekib küsimus, kui vastutavaks isikuks määratakse infoturbejuht, kes paikneb organisatsioonis kuskil mitmeid kihte otsustamistasandist kaugemal ning tal ei ole ka ressursse eraldatud siis, kes ikkagi vastutab.
- Lisa punkt 1.2. *„välja töötama võrgu- ja infosüsteemide turvareeglid*..." Kus on defineeritud, mis on "turvareeglid"? Kellele need kehtestatakse?
- Lisa punkt 1.5. *„määrama igale infotehnoloogiaseadmele vastutava kasutaja*“. Kas kasutaja peaks määrama pigem igale süsteemile?
- Lisa punkti 2 pealkiri ning alampunktide sisu ei lähe kokku. Teeme ettepaneku kas laiendada pealkirja näiteks lisades „ning kasutajaõiguste valdkonnas“ või liigutada kasutajaõiguste/halduse teemad asjakohasesse punkti.
- Lisa punkt 2.1.“ *tutvustama personalile küberhügieeni- ja infoturbereegleid ning tagama neile vastava koolituse vähemalt ühel korral aastas*". Mõiste "küberhügieen" on väga vaieldav, sest (ametlik) definitsioon puudub. Kohustuse sisu peab aga olema nii subjektide kui ka järelvalvaja jaoks üheselt selge. Teiseks on kohustus teha koolitust vähemalt ühel korral aastas nõue, mille peab tehtuks märkima ja mille mõju riskikäitumisele võib olla negatiivne – triviaalseid infoturbe koolitusi võidakse hakata pidama tüütuks kohustuseks, mis kujundab negatiivse hinnangu infoturbe suhtes. Võimalusi tagada/kontrollida töötajate infoturbe teadlikkust on rohkem, kui kord aastas toimuv koolitus. Näiteks võib läbi viia testi ja kui töötaja vastab kõigele õigesti, siis koolitust ta enam läbima ei pea.
- Lisa punkt 2.7. *„kasutama võrgu- ja infosüsteemis vaid kontrollitud ning arvele võetud andmekandjaid ning keelama kontrollimata või tundmatute infotehnoloogiavahendite kasutamise*." Meede ei pruugi olla kõikidel juhtudel ja 100% rakendatav. Näiteks avalik-õiguslik organisatsioon peab teatud ulatuses võimaldama juurdepääse organisatsiooni hallatavale võrgule ja/või süsteemidele ka kasutajatele nende oma seadmetega ja teinekord ka andmekandjatega. Määruse meetme detailsus peab olema sellisel tasemel, et kõik, kes on kohustatud meedet järgima, saavad seda praktikas ka teostada.
- Teeme ettepaneku lisada punkti 2 lõppu uus punkt (2.9) järgmises sõnastuses: „kasutama ainult selleks mõeldud ning heaks kiidetud vahendeid, teenuseid ja süsteeme.“
- Lisa punkt 3.1. *„hindama, millised andmed ning võrgu- ja infosüsteemid on vajalikud igapäevaseks kasutamiseks…*“. Igapäevane kasutus ei ole hea määratlus. Teeme

ESTONIAN ASSOCIATION OF INFORMATION
TECHNOLOGY AND TELECOMMUNICATIONS
Lõõtsa 2b, 11415 Tallinn, Estonia
+372 617 7145
info@itl.ee / www.itl.ee

ettepaneku kasutada selle asemel sõnastust: „on vajalikud igapäevaste ülesannete ja eesmärkide täitmiseks.“

- Lisa punkt 4.1. „*tundma oma tarnijaid ja väliste teenuste osutajaid ning nende tausta kogu tarneahela ulatuses ning rakendama meetmeid lähtudes riigi koostatud avalikest ohuhinnangutest ja riskianalüüsidest tarnijate kohta*;" Seda võib püüda teha ja saab teha teatud piirini, aga seda saab teha maksimum 2-3 tarneahela lüli osas. Kui ahel on pikem, siis see ei ole praktikas teostatav. Suured teenusepakkujad (välismaised korporatsioonid) ei pruugi üldse oma tarneahela kohta infot jagada. Sellest sõnastusest võib muuhulgas välja lugeda, et riik teeb riskianalüüse tarnijate kohta. Kas on läbi mõeldud see nõue ka riigihangete kontekstis ja tulemas juhised, kuidas hindamist hankeprotsessis teostada?
- Lisa punkt 4.2. „*kokku leppima tarnijatega ja väliste teenuste osutajatega kirjalikult taasesitatavas vormis andmete vahetamiseks vajalikud turvanõuded ning kasutatava teenuse tingimused.*" Teeme ettepaneku asendada „andmete vahetamiseks vajalikud turvanõuded“ sõnastusega "andmete töötlemise nõuded".
- Lisa punkt 5.1. „*koolitama personali, kuidas ära tunda intsidente, kuidas tuvastada nende mõju ja ulatust ning kuidas neid vältida ja kuidas intsidentide puhul toimida*;" Sättes on mitmed asjad kokku pandud, mis võiksid olla eraldi käsitletud. . Esiteks, “personal” viitab üldiselt kõikidele organisatsiooni töötajatele. Kõik töötajad peaksid teadma, mida teha, kui nende arvates toimub midagi kahtlast - keda informeerida, kuidas informeerida. Sarnaselt nagu "kui märkad midagi kahtlast, helista 112, räägi, mis juhtus“. Need inimesed ei pea suutma tuvastada intsidendi mõju või ulatust, vaid peavad teadma, millised on võimalikud küberintsidendid ning kuidas intsidendikahtlustest teavitada. Teine sihtrühm on intsidendi edasise käsitlemisega seotud töötajaid (võib olla ka sisse ostetud teenus), kelle hulgas peab olema inimesi, kes oskavad tuvastada intsidendi ulatust ja hinnata mõju. Teiseks: intsidentide vältimine on ennetav tegevus ja seda katab lisa punkt 2.1.
- Lisa punkt 5.2. „*määrama isiku, kes koordineerib intsidentide lahendamist, asjaomaste asutuste ja koostööpartnerite teavitamist ning on nende kontaktisik*“. Teeme ettepaneku lisada siia nimekirja intsidentide registreerimise.
- Lisa punkt 6.3. „*järgima turvalise e-kirjavahetuse põhimõtteid ja vältima tundmatute manuste või hüperlinkide avamist*". See on sisuline punkt, mida katavad lisa punktid 1.2 ja 2.1. Kas määruses toodud kohustuslikud meetmed peaksid olema sellises detailsuses, defineerides sisuliselt organisatsiooni turbereegleid? Kui on tegemist väikese organisatsiooniga, kus riskide hindamist ei tehta ning rakendatud turve järgib ette antud nõuete nimekirja, siis on see variant. Suuremas organisatsioonis, kus rakendatakse E-ITSi või ISO27001 standardit, ilmselt mitte.
- Lisa punkt 6.4. „*tutvustama personalile telefoni- ja videokõnede tegemise turbe põhimõtteid*". Sama kommentaar, mis punktile 6.3

ESTONIAN ASSOCIATION OF INFORMATION
TECHNOLOGY AND TELECOMMUNICATIONS
Lõõtsa 2b, 11415 Tallinn, Estonia
+372 617 7145
info@itl.ee / www.itl.ee

- Lisa punkt 6.6. „*pidama kasutuses olevate pilvteenuste ja nendega seotud riskide arvestust*." Kui nõude sihtrühmaks on väiksed organisatsioonid, siis oleks hea kaaluda selle punkti sõnastust, et mida soovitakse saavutada. Riskide arvestuse pidamine ei peaks olema eesmärgiks omaette.
- Lisa punkt 7 tervikuna - kas määruse loojad oskavad hinnata, milliseid ressursse (raha ja teadmised, sh rakendused ja personal, kes oskab neid asju teostada) läheb nende tegevuste tegemiseks vaja? Võtame näiteks punkti 7.6, kas määrusandjal on teada, mida maksab turvalogide kogumise ülesehitamine ja käigushoidmine? Kas on mõeldud, mis peaks olema selle mõte, kui logisid tegelikult ei monitoorita?
- Lisa punkt 7.10. „*kavandama meetmed juhuks, kui seade läheb kaotsi, varastatakse või läheb katki*". Kuna defineerimata on, mis on infotehnoloogiaseade, siis kas ikka tõesti on vaja kõikide seadmete jaoks hakata meetmeid välja töötama? Kui organisatsioon teeb riskide hindamist, siis ta rakendab meetmeid vastavalt oma riskihalduse plaanile.
- Lisa punkt 9.3. „*vältima ruumides kõrvaliste isikute liikumist saatjata, eelkõige ruumides, kus hoitakse seadmeid või töödeldakse andmeid*;" Avalikke teenuseid pakkuvates organisatsioonides võib sellises sõnastuses meede olla mitte teostatav.

ESTONIAN ASSOCIATION OF INFORMATION
TECHNOLOGY AND TELECOMMUNICATIONS
Lõõtsa 2b, 11415 Tallinn, Estonia
+372 617 7145
info@itl.ee / www.itl.ee