Eesti Perearstide Seltsi tagasiside Vabariigi Valitsuse 9. detsembri 2022. a määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ muutmise eelnõule

08.08.2025

Soovime avaldada tunnustust ministeeriumi suunale kujundada küberturvalisuse regulatsioon viisil, mis toetab proportsionaalsemate ja jõukohasemate nõuete kehtestamist teenuseosutajatele. Usume, et regulatsiooni subjektide jaoks arusaadavamad, lihtsamad ja jõukohasemad meetmed aitavad kaasa infoturbe taseme tõstmisele ning regulatsiooni sisulisele rakendamisele eri väiksemates ettevõtetes.

Samas peame vajalikuks juhtida tähelepanu mõnele aspektile, mille täpsustamine aitaks kaasa määruse rakendamisele ning vähendaks tõlgendamisriske. Teeme alljärgnevalt ettepanekud määruse sõnastuse, seletuskirja ning määruse lisas toodud meetmete täpsustamiseks.

Ettepanekud määruse sõnastuse kohta

1) **Teeme ettepaneku § 5^1 lõige 1 sõnastuses jätta välja sõna „üksikasjalikud“.** Terminite „esmased meetmed“ ja „üksikasjalikud meetmed“ paralleelne kasutus võib tekitada regulatsiooni rakendamisel ebaselgust. Kuna määruse lisa täpsustab rakendatavad meetmed, ei ole lõikes 1 vaja eraldi rõhutada nende üksikasjalikkust.
2) Teeme ettepaneku lisada § 5^1 lõike 2 lõppu või lõikena 3 järgmine sõnastus: „**Teenuse osutaja võib lõikes 2 sätestatud konkreetse meetme jätta rakendamata juhul, kui see ei ole asjakohane või riskianalüüsi alusel, rakendades vajadusel kompenseerivaid meetmeid**“. Sõnastuse lisamise eesmärk on suurendada määruse paindlikkust ja rakendatavust, võimaldades teenuse osutajal jätta esmaste turvameetmete loetelus nimetatud konkreetse meetme rakendamata juhul, kui see ei ole tema tegevuse kontekstis asjakohane või kui riskianalüüs näitab, et selle rakendamine ei ole vajalik (nt juhul, kui risk on muude meetmete abil piisavalt maandatud). Võimalus rakendada alternatiivseid (nn kompenseerivaid) meetmeid tagaks, et turvameetmete üldine eesmärk – võrgu- ja infosüsteemide kaitse – jääb täidetuks, vältides seejuures olukorda, kus teenuse osutaja peab rakendama meetmeid, mis ei ole tema tegevuse seisukohalt põhjendatud ega proportsionaalsed. Näiteks ei tundu proportsionaalne, et väikeettevõte peaks elektroonikakaupluse tasuta kogu tarneahela ulatuses tundma (meetmete p 4.1) või kasutama ekraanilukku või pääsukoodi töötajate ühiskasutuses olevas „nuputelefonis“, mida kasutata ainult helistamiseks (meetmete p 7.9).
3) Teeme ettepaneku, et §-is 5^1 sätestatud esmaste turvameetmete rakendamise kohustus võiks kohalduda üksnes nende ettevõtjate suhtes, kellele ei kohaldu § 3 lõike 1 alusel antud määrusega sätestatud kohustused. Kahe nõuetekomplekti täitmise kohustus suurendab põhjendamatult halduskoormust ning nõuete vahel võib tekkida vastuolusid. E-ITS rakendamisel ei pruugi olla esmased meetmed alati täpselt määruses sõnastatud kujul olla täidetud, kuivõrd nõuete sõnastused ei ole kattuvad ning e-ITS võimaldab ka teatavat paidlikkust.

Ettepanekud seletuskirja kohta

1) Kuna tõdesime, et määruse ja seletuskirja lugejad said regulatsioonist erinevalt aru, palume seletuskirja mõnes aspektis täiendada, et määrus oleks seda rakendama kohustatud isikute jaoks üheselt arusaadav. Teeme ettepaneku tuua seletuskirjas selgemalt välja:

- kas „mõlemad tingimused peavad olema täidetud“ selleks, et tekiks e-ITS rakendamis kohustus või vastupidi selleks, et § 5^1 sätestatud nõuete järgimine oleks piisav. Näiteks, kas 60 töötaja ja 6 miljoni euro suuruse aastakäibega ettevõtja suhtes kohalduvad e-ITS/ISO27001 rakendamise kohustus ning täitma auditikohustus või mitte;
- kas väikese suurusega ettevõtjaks kvalifitseeruv elutähtsa teenuse osutaja peab rakendama eITS/ISO27001 ning täitma auditikohustust või piisab §-is 5^1 sätestatud meetmetest. Meie hinnangul on mõistlik ja proportsionaalne, kui väikese suurusega ettevõtjaks kvalifitseeruva elutähtsa teenuse osutaja puhul piisab §-is 5^1 sätestatud meetmetest, kuivõrd väikeses

organisatsioonis annab lihtsamate ja konkreetsemate nõuete rakendamine meie hinnangul parema lõpptulemuse ning toob kaasa proportsionaalsema ressursikulu ja halduskoormuse.

2) Palume seletuskirjas korrigeerida üldiste turvameetmete hindamise ajakulu hinnangut (p 6.2, järeldus mõju olulisuse kohta). Nõustume, et muudatus vähendab oluliselt väikeettevõtjate halduskoormust, kuid seletuskirjas praegu välja toodud „1-2 tundi ühe hindamiskorra kohta" ei ole kaugeltki realistlik – juba näiteks ainuüksi infotehnoloogia varade arvestuse kontrollimine ja uuendamine võtab rohkem aega – ja see on üks kohustus paljudest. Lisaks näib, et arvestatud ei ole regulaarselt nõutavate tegevustega (nt personalikoolitused, personali juhendamine jms).

Ettepanekud esmaste turvameetmete kohta (määruse lisa)

Teeme ettepaneku sõnastada punktid järgmisel (lisatud tekstiosad on märgistatud allajoonimise ning eemaldatud tekstiosad läbirkiipsutamisega):

- **1.5. määrama igale infotehnoloogiaseadmele vastutava kasutaja, kui seade on antud ainult või valdavalt ühe isiku kasutusse**. - *Põhjendus: ühiskasutuses olevate seadmete puhul on mitu võrdväärset kasutajat, kellel pole administraator õigusi, ning seadme haldaja (väikeettevõtetes on selleks sageli IT-teenuse pakkuja). Vastutava kasutaja määramine ei oleks kunstlik ja ei kajastaks tegelikkust. Teenuse osutaja vastutab nii ehk nii oma seadmete eest ning punkti 1.4 kohaselt on tal kohustus pidada kõigi seadmete üle arvestust.*
- **2.3. kasutama võrgu- ja infosüsteemides personaalseid pääsuõigusi, välja arvatud juhul, kui süsteem seda mõistlikult ei võimalda**. - *Põhjendus: nt ühiskasutuses olevale EKG-aparaadile vm spetsiifilistele seadmetele ei ole alati võimalik luua erinevaid kasutajakontosid.*
- **3.4. olulise teabe kinnitamiseks eelistama digitaalset allkirjastamist suulisele või kirjalikku taasesitamist võimaldavale vormile**; - *Põhjendus: mitmeti mõistetavuse vältimiseks tuleks täpsustada, millega võrreldes tuleks digitaalset allkirjastamist eelistada. Määrus ei tohiks kohustada eelistama digitaalset allkirjastamist omakäelisele allkirjastamisele, need on TsÜS § 80 kohaselt võrdsustatud.*
- **3.6. varundama regulaarselt tööks vajalikke andmeid, hoidma olulisi varundatud andmeid töösüsteemist eraldi ja testima varundatu põhjal oluliste andmete taastamist**; - *Põhjendus: eraldi asukohta varundamist ja taastamise testimist on proportsionaalne nõuda oluliste andmete puhul. Osade andmekategooriate puhul võiks nt SharePointi / OneDrive versioonihaldus olla piisav.*
- **4.1. tundma oma olulisi tarnijaid ja väliste teenuste osutajaid ning nende tausta, kriitiliste tarnijate puhul kogu tarneahela ulatuses, ning rakendama meetmeid lähtudes riigi koostatud avalikest ohuhinnangutest ja riskianalüüsidest tarnijate kohta**; - *Põhjendus ja küsimused: kas mõistame õigesti, et tarnijaks loetakse ka näiteks elektroonikakauplust, kust väikeettevõtja arvuteid või printereid ostab? Kui nii, siis ei tundu kaugeltki proportsionaalne kõigi tarnijate suhtes kogu tarneahela ulatuses taustauuringuid teha. Kui nt elektroonikakauplust ei ole mõeldud tarnija all, siis paluksime näiteks määruse seletuskirjas vm juhendmaterjalis anda tarnija piiritlemise kohta juhiseid. Samuti paluksime võimalusel täpsustada, kas eeldame õigesti, et silmas on peetud konkreetselt võrgu- ja infosüsteemidega seotud tarnijaid ja väliste teenuste osutajaid (mitte nt prügiveo teenuse pakkujaid, vee-ettevõtteid jne). Lisaks loodame, et terviseandmete infosüsteemide tarnijad muutuvad iseseisvateks infoturbenõuete ning järelevalve subjektideks. Väikeettevõtjatest perearstikeskustel puudub kompetents ning võimekus nende üle sisulise järelevalve teostamiseks.*
- **4.2. kokku leppima oluliste tarnijate ja väliste teenuste osutajatega kirjalikult taasesitatavas vormis konfidentsiaalsete andmete vahetamiseks vajalikud turvanõuded ning kasutatava teenuse tingimused**. – *Põhjendus: nõue on vajalik ja proportsionaalne juhul, kui tegemist on olulise tarnija/teenusega või vahetatakse konfidentsiaalseid andmeid.*
- **5.1. koolitama personali, kuidas ära tunda intsidente, ~~kuidas tuvastada nende mõju ja ulatust ning~~ kuidas neid vältida ja kuidas intsidentide puhul toimida**; - *Põhjendus:*

väikeettevõttes ei peaks olema intsidentide mõju ja ulatuse tuvastamine nö tavapersonali ülesanne. Personali tuleks koolitada intsidentide vältimise ja äratundmise osas ning juhendada neid intsidendi korral IT-partnerit/IT-spetsialisti ja infoturbe eest vastutavat isikut teavitama.

- **7.3. pidama arvestust kasutatava tarkvara, ~~tarkvara nõrkuste~~ ja litsentside üle ning uuendama litsentse õigel ajal**; - *Põhjendus: tarkvara nõrkuste üle arvestuse pidamine ei ole realistlik ega otstarbekas ülesanne. Cert.ee uudiskirjades on iga päev teated uutest nõrkustest. Pigem on oluline teadaolevatele olulistele nõrkustele vajadusel reageerida (kaetud punktiga 7.4).*
- **7.4. kasutama turvalist, usaldusväärset ja kehtiva toega tarkvara, sealhulgas eemaldama infotehnoloogiaseadmetest ja telefonidest tarkvara, mis on aegunud või mida ei kasutata. Põhjendatud erandid tuleb dokumenteerida ning vajadusel rakendada lisaturvameetmeid.** – *Põhjendus: vahel puuduvad alternatiivid, süsteeme saab vajadusel ülejäänud võrgust eraldada. Ka VEITS juhendab kahtluse korral kaaluma tarkvara väljavahetamist (p 7.4), mitte ei kohusta selleks kõigil juhtudel.*
- **7.6. ~~tagama võrgu- ja infosüsteemide ning rakenduste turvasündmuste logimise ja logide kättesaadavuse~~; sõnastus asendada järgmiselt: Süsteemide seadistamisel eelistama võimalusel valikuid, mis võimaldavad võrgu- ja infosüsteemide ning rakenduste turvasündmuste logimist ning logide säilitamist vähemalt 90 päeva**. – *Põhjendus: kättesaadavust ei ole võimalik tagada määratlemata ajaks. Väikeettevõtjalt on proportsionaalne nõuda olemasolevate logimisvõimaluste võimalikult head kasutust, mitte aga logihalduse süsteemide kasutuselevõttu. Terviseinfo süsteemidel on eraldiseisvad logimisnõuded (tervishoiuteenuse osutamise dokumenteerimise tingimused ja kord § 3[1] lg 2). Kaaluda võib ka lahendust, et teenuse osutaja enda süsteemides tuleb logisid säilitada fikseeritud aeg ning sisseostetavates süsteemides kasutada ära süsteemi olemasolevad logimisvõimalused.*
- **7.9. kasutama tööks vajalikes seadmetes, sealhulgas mobiilseadmes, mis sisaldavad olulisi või konfidentsiaalseid andmeid, pääsukoodi või ekraanilukku**; - *Põhjendus: nt ühiskasutuses olevale nuputelefonide puhul, mida kasutatakse ainult helistamiseks, ei ole nõue asjakohane.*
- **7.13. rakendama automaatika- või muu andmesideühendusega seadme kasutamise korral lisaturvameetmeid või keelama seadmes andmeside kasutamise, sealhulgas kaughalduse, välja arvatud madala riskiga seadmed**; - *Põhjendus: näiteks juhtmevabad kõrvaklapid, hiir, klaviatuur jms ei töötle tundlikku teavet ega võimalda kaugjuhtimist, mistõttu ei ole nende puhul andmeside keelamine otstarbekas ega tehniliselt mõistlik.*
- **9.1 ja 9.2 „tagamise" asemel peaks olema kohustus „rakendada meetmeid"** (sarnaselt punktile 9.5). Sel moel oleks kohustuste keelekasutus ühtlasem ning kohustused realistlikumad, keskendudes meetmete rakendamisele, mitte absoluutse tulemuse „tagamisele", mida ei pruugi olla võimalik igas olukorras garanteerida.
- **9.3. vältima tööruumides kõrvaliste isikute liikumist saatjata, eelkõige ruumides, kus hoitakse seadmeid või töödeldakse andmeid**; - *Põhjendus: nõue ei tohiks kohalduda näiteks ootealade, koridoride, tualettruumi jms suhtes.*

Lugupidamisega

Eesti Perearstide Selts