EESTI
INFOTEHNOLOOGIA JA
TELEKOMMUNIKATSIOONI
LIIT

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

Teie 06.03.2026 e-kirjaga

Meie 31.03.2026 nr 6.1-2/58

Arvamus küberturvalisuse paketi ettepanekute kohta

Eesti Infotehnoloogia ja Telekommunikatsiooni Liit (ITL) esitab käesolevaga sisendi Eesti seisukohtadesse Euroopa Komisjoni 20.01.2026 avaldatud küberpaketi kohta, mis sisaldab küberturvalisuse 2. määruse vastuvõtmise ettepanekut (Cybersecurity Act 2, edaspidi CSA2) ja küberturvalisuse 2. direktiivi (edaspidi NIS2) muutmise ettepanekuid.

ITL-i üldised seisukohad

1) **Küberturvalisus on väga oluline valdkond ja selle regulatsioon on tervikuna selgelt vajalik**. Kuna küberturvalisuse määrusega ei ole saavutatud soovitud eesmärke, siis toetame selle ülevaatamist ja muutmist.

2) **Teeme ettepaneku võtta Euroopa Liidu (EL) küberturvalisuse paketi suuremaks eesmärgiks regulatsioonide päriselt lihtsustamine,** sealhulgas kattumiste ja dubleerimiste vähendamine NIS2, finantssektori digitaalse tegevuskerksuse määruse (DORA), küberkerksuse määruse (CRA) ja muude asjakohaste raamistike vahel. See võimaldaks ettevõtetel ja asutustel suunata ressursid vastavuse tagamise ja tõendamise asemel meetmete rakendamisele, mis praktikas aitavad luua suuremat turvalisust. Kehtivad küberturvalisust ja digiteemasid reguleerivad õigusaktid on keerulised ja mahukad ning seepärast on neid rakendavatel organisatsioonidel raske mõista, millised on kõige olulisemad meetmed, mis tagaksid nende turvalisuse. Kuna regulatsioonid on mahukad, siis ruumi lihtsustamiseks ja ühtlustamiseks neis jagub.

3) **Uute täiendavate riskihaldusemeetmete kaalumisel ja kehtestamisel tuleb lähtuda sellest, et kõik kohuslased erinevates riikides oleks võimelised neid täitma**. Nende regulatsioonide eesmärgiks tagada EL-i kõigis liikmesriikides turvalisuse ühtlaselt (harmoneeritult) kõrge tase. Kui ettevõtted tegutsevad mitmes riigis, siis tuleb praegu

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

praktikas tegelda tegeliku turvalisuse tagamise asemel erinevate riikide regulatsioonide erisuste tuvastamise ning nendega kohandumisega. Seega tuleb regulatsioonide läbivaatamisel ja uuendamisel lähtuda minimaalsuse printsiibist ning sellest, et need ei tekitaks rakendamisel ülemäärast ressursikulu ega tekitaks ainult läbi erinevate nõuete täitmise kinnitamise eksitavat tunnet tegelikust turvalisusest.

4) **Küberturvalisuse regulatsioone kehtestades ja muutes on oluline arvestada suuremat eesmärki milleks on õiguskindluse- ja selguse tagamine ning osapooltele aja andmine regulatsioonide sisuliseks rakendamiseks**. Hetkel oleme olukorras, kus viimastel aastatel on vastu võetud mitmeid mahukad regulatsioone, mida juba on asutud muutma. Leiame, et oluline on lasta juba kehtestatud regulatsioonidel piisava ajaperioodi jooksul toimida. Seejärel teha nende mõjude ja tulemuste kohta analüüs mille järelduste põhjal saab otsustada muutmise vajalikkuse üle. Heitlik õigusruum kus toimuvad pidevad muudatused ja uute kohustuste kehtestamine nõuab nii era kui avalikult sektorilt ebavajalikke investeeringuid ja protseduuride muutmist. Tuleb jätta rohkem ruumi riskipõhiseks tegutsemiseks kuna see loob pidevalt muutuvas olukorras võimaluse paindlikult riske hallata mitte käituda nõuete, mis tegelikult põhinevad mineviku intsidentidel, järgi.

ITL-i seisukohad CSA2 ettepaneku kohta:

1. **ENISA mandaadi uuendamine, uute ülesannete ja pädevuste lisamine**

ITL-ina tegime CSA ülevaatamise käigus ettepaneku, et ENISA-le ei määrataks uusi täiendavaid rolle, mis ei ole kooskõlas tema seniste võimekustega. Uute ülesannete lisamise asemel soovitasime ENISA-l keskenduda oma põhiülesannetele ja vältida liigset laienemist kõrvalteemadele, mis võivad takistada tõhusat tegutsemist põhivaldkondades ja nende arendamist. Konkreetsemalt leidsime, et ENISA peaks keskenduma EL-i küberturvalisuse valdkonna õigusaktide, nagu küberturvalisuse 2. direktiiv (NIS2), finantssektori digitaalse tegevuskerksuse määruse (DORA) ja küberkerksuse määruse (CRA) rakendamist abistavate tehniliste spetsifikatsioonide ning juhiste väljatöötamisele.

CSA2 ettepanekuga ENISA rolli ei kitsendata, vaid reformitakse ja antakse uusi tegevusvaldkondi, näiteks seoses tarneahela turvalisuse ja oskustega. Seega on oht ENISA tegevuse fookuste veel suuremale hajumisele.

ENISA kui üks teavituspunkt

Kordame Euroopa Komisjoni avaldatud digivaldkonna lihtsustamispaketile ehk digiomnibussile ITL-i poolt 19.12.2025 esitatud tagasisides sisaldunud seisukohta mille kohaselt toetame erinevate intsidentide raporteerimiseks ühise keskkonna loomist. Novembris 2025 avaldatud nn digiomnibussi ettepanekus pakkus Euroopa Komisjon välja ühise teavitamiskanali loomise, et sama intsidendi puhul ei tuleks mitmes kohas ning mitu korda teavitada.

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

Selline üks teavitamiskanal on kindlasti tervitatav, eriti piiriüleselt tegutsevate ettevõtete jaoks ning me toetame seda.

Hetkel peab mitmes Euroopa Liidu riigis tegutsev küberturvalisuse erinevate regulatsioonide alla langev ettevõte tegema teavitust kohalikele CERT-idele eraldi ja erinevatel dokumendi vormidel.

Sealjuures tekib täiendav oluline ressursikulu ettevõttele iga riigi CERT-iga eraldi suhtlemisel, kui teavituse kohta tuleb lisaküsimusi. Ettevõtte jaoks läheb seega kaotsi intsidendi lahendamiseks vajalik aeg ning muud ressursid, kuna tuleb suhelda mitme asutusega teavituse teemal. Seetõttu toetame ülesandeid, mis ENISA-le antakse CSA2 ettepaneku artikliga 15.

Seoses ühtse teavituskanaliga lisame, et lihtsustamise eesmärki silmas pidades tuleb olla ambitsioonikam ning ühtlustada ka teavitamise aegasid, vorme jm EL-i küberturvalisuse õigusaktides, kuna see hoiab kokku mitmes riigis tegutsevate ettevõtete ressursse.

2. Sertifitseerimisskeeme puudutava regulatsiooni laiendamine

ITL on järjepidevalt toetanud vabatahtlikke standardeid ja sertifitseerimist. CSA2 ettepanek võimaldab kehtestada kohustuslikke standardeid (art 71 lg 3).

CSA2 ettepaneku kohaselt saaks tulevikus sertifitseerimisskeeme kasutada ettevõtte tegevuse nõuetele vastavuse tõendamiseks ja vastavuseelduse saamiseks asjakohastele ELi õigusaktidele.

Kuivõrd see ei ole kohustus, siis leiame, et kohustusliku sertifitseerimise sätestamine ei ole vajalik. Iga õigusakti kohuslane saab tellida endale välise sõltumatu hinnangu, millega tõendatakse vastavust õigusaktidele. Täiendava sertifikaadi andmine ei tõsta vastavust tõendanud ettevõtte tegevuse kvaliteeti, küll aga suurendab bürokraatiat ja võib tõsta turule sisenemise barjääre.

Lisaks võiks uus skeem hakata mõjutama ISO 27001, E-ITS või muude juba kehtivate ja tunnustatud sertifitseerimise skeeme. Seega pole mõistetav, et kui tekib uus sertifitseerimisskeem, mis on erinev vastavuse tõendamisest juba kehtivatele standarditele, siis milliste kriteeriumite põhjal peaks ettevõte otsustama, millise skeemi alusel sertifitseerimist teha.

Samas küberkerksuse õigusakti (CRA) vaates on vaja selgust ja kaetust sertifitseerimisskeemidega, mis on täna veel puudu. Omaette küsimus on see kuidas tagatakse sertifitseerimisskeemide kirjeldused ja koolitused sertifitseerimisprotsessi läbiviijatele nii, et liikmesriigid oleksid CRA rakendamisega ajagraafikus.

Kokkuvõtteks jääb meile arusaamatuks, miks soovitakse lisada CSA2 nõue uue sertifikaadi järele.

3. Üldine raamistik turvalise IKT tarneahela jaoks

CSA2 artiklitega 98 jj antakse Euroopa Komisjonile õigus kehtestada meetmeid, et tagada info-ja kommunikatsioonitehnoloogia (IKT) tarneahela turvalisus.

Meile jääb väljapakutava regulatsiooni eesmärk arusaamatuks, kuna olemasolevad EL-i küberturvalisuse õigusaktid juba tagavad piisava juhendmaterjali ja tehniliste standardite

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

olemasolu. Näiteks peavad ettevõtted ja asutused NIS2 täitmiseks viima läbi riskide hindamise ning sealhulgas tuleb hinnata ka tarneahela riske. Lähtudes hinnangu tulemustest tuleb rakendada vastavaid meetmeid.

Tarneahela riskide hindamise üksikasjalikul reguleerimisel võib juhtuda, et see kaotab kiiresti oma ajakohasuse. Nimelt koostatakse regulatsioon olemasolevate tarneahelate näidete põhjal. Samas on iga uus tarneahel uut tüüpi juhtum ja seda ei ole võimalik ette kirjeldada. Kui organisatsioon(id) rakendavad riskipõhisuse põhimõtteid sisuliselt, mitte formaalselt olemasolevate regulatsioonide alusel, ei ole vajadust täiendava regulatsiooni järele.

Täiendavast regulatsioonist palju olulisem on tagada juba kehtivate regulatsioonide rakendamist abistava materjali ajakohasus ja praktiline tugi kohustatud subjektidele.

4. Tarneahela turvalisuse erinormid elektroonilise side sektorile

CSA2 ettepaneku artiklitega 110 ja 111 kehtestatakse elektroonilise side võrkude osas keeld kasutada suure riskiga tarnijaid ning see jõustuks hiljemalt 36 kuu pärast suure riskiga tarnijate nimekirja avaldamist. Põhimõttelisel tasandil on mõistetav keeld riikliku julgeoleku kaalutlustel kasutada kõrge riskiga tarnijaid elektroonilise side võrkude tuumiksüsteemides.

Siiski on oluline arvestada, et tarneahela turvalisuse (kõrge riski määratlemine) EL-i tasandile tõstmine ning ettepanekus välja pakutud lühikesed üleminekutähtajad (36 kuud) tekitavad Euroopa ettevõtetele kindlasti olulisi riske. Näiteks seoses tarneahelate erinevate ülesehitustega, teostatavuse ja investeeringute mõistlikkusega.

Samuti eeldab kõrge riskiga riikide nimekirjade kujundamine EL-i tasandil poliitilist konsensust, mis võib olla erinevate liikmesriikide vahel raskesti saavutatav.

ITL-i ettepanekud ja küsimused artiklite 110 ja 11 osas on järgmised:

1) Teeme ettepaneku antud sätete rakendumise üleminekuaega pikendada ja siduda üleminekuaeg olemasolevate seadmete elueaga. Märgime, et CSA2 ettepanekus sisalduv väga lühike tähtaeg võib kaasa tuua tarneraskused ja tellimuste koondumise vähestele tarnijatele. Samuti suurendab see ettevõtete kulusid hüppeliselt (sh uued hanked, integratsioon, teenuse katkestustega seotud tegevused seadmete ümbervahetamisel jms).

2) Kuivõrd sideettevõtjad on hankinud seadmed ajal, mil nende kasutus oli lubatud ja on neid kasutanud õiguspäraselt, tekib küsimus ka enne nende tegeliku eluea lõppu väljavahetamisega seotud kulude hüvitamisest. Seda teemat ei ole CSA2 ettepanekus üldse käsitletud.

3) Lisaks tekitab küsimusi kõrge riskiga tarnija määramine. Kuivõrd selle nimekirja koostab CSA2 ettepaneku kohaselt Euroopa Komisjon koos liikmesriikidega lähtudes julgeolekukaalutlustest, ei hakka selle otsuse tagamaad olema läbipaistvad ettevõtjatele. Seetõttu jääb ettevõtjatele seadmeid hankides ebakindlus, millistele kriteeriumitele vastavalt täpselt võidakse Euroopa Komisjoni poolt mõni tarnija tulevikus lubamatuks või

kõrgema riskiga tarnijaks lugeda. Seetõttu on ka eriti oluline, et üleminekuperiood oleks piisavalt pikk või alternatiivselt oleks sätestatud kompensatsioonimehhanism ja ettevõtjad saaksid teabe tarnija staatuse muutumisest võimalikult varakult.

4) Kahjuks on jätkuvalt ka väga palju lahtisi küsimusi, sest ei ole teada, mida täpselt hõlmavad komisjoni rakendusaktid. Lisaks on artikli 110 lõigete 4 ja 5 sõnastuse kohaselt Euroopa Komisjonil õigus, mitte kohustus vastu võtta rakendusakte, mis tekitab väga ebakindla olukorra. Samuti tekib küsimus, mis saab Euroopa Liidu 5G küberturvalisuse tööriistakastist (Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures), mis võeti vastu 2020. aastal liikmesriikide küberturvalisuse asutuste koostöö raames ning mille aluseks on Euroopa Komisjoni soovitus (EL) 2019/534 5G-võrkude küberturvalisuse kohta.

5) Lisaks tekkis praktilisi küsimusi. Kui keeld kohaldub komponentidele, siis kas hooldus ja tugiteenused on sama tootja poolt siiski lubatud? Või kui tehakse tarkvarauuendusi nt juba kõrge riskiga tootja kasutuses olevale tarkvaral, kas see oleks lubatud?

ITL-i seisukohad NIS2 muutmise ettepaneku kohta:

1. **Subjektide nimekirja täpsustamine ja täiendamine**

ITL toetab, et täpsustakse NIS2 subjektide nimekirja. Mitmed subjektide kategooriad on kehtivas NIS2-s sõnastatud segaselt ja direktiivi ülevõtmisel on osutunud üheks raskemaks küsimuseks mõista, kes on NIS2 kohuslased. Kahjuks näeb NIS2 muutmise ettepaneku artikkel 1 punkt 1 ette vaid uute subjektide lisamise NIS2 artiklisse 2.

Teeme ettepaneku, et artikkel 2 vaadatakse tervikuna üle ja täpsustatakse sisuliselt vastavalt liikmesriikide poolt esitatud küsimustele.

Teeme ettepaneku viia NIS2 sisse muudatus, mis kohustab pädevat asutust teavitama ise kohuslasi, et nad on NIS2 kohuslased või pädeva asutuse poolt tehtud eelhinnangu kohaselt nad võivad osutuda NIS 2 kohuslasteks. Hetkel on selle osas liikmesriikides suur segadus ja erinev praktika, kuna paljud NIS2 kohuslased ei oska ennast määratleda subjektina ja seega ei rakenda ka vajalikke riskihalduse meetmeid. Leiame, et EL-is peaks subjektide määramine olema ühetaoline ning ettevõtted ja asutused ei peaks ise end subjektina üles andma.

2. **Üksuste subjektsuse lävendi tõstmine**

NIS2 muutmise ettepanekuga tõstetakse üliloluliste üksuste subjektsuse lävend keskmise suurusega ettevõtetelt (kuni 250 töötajat ja aastakäive kuni 50 miljonit eurot või bilansimaht kuni 43 miljonit eurot vastavalt Euroopa Komisjoni soovitusele (2003/361/EÜ) väikese keskmise turukapitalisatsiooniga ettevõteteni (kuni 750 töötajat ja aastakäive kuni 150 miljonit eurot või bilansimaht kuni 129 miljonit eurot vastavalt Euroopa Komisjoni soovitusele (EL) 2025/1099). See tähendaks praktikas NIS2 mõttes üliloluliste üksuste arvu vähenemist.

ITL-ina toetame seda muudatust.

3. Täiendavate siseriiklike küberturvalisuse riskihalduse meetmete kehtestamise keeld

Toetame NIS2 muutmise ettepaneku artikkel 1 punktiga 7 tehtavat muudatust (NIS2 art 21 lg 5 muutmine), mille kohaselt ei või liikmesriigid kehtestada täiendavaid nõudeid, kui Euroopa Komisjon on kehtestanud küberturvalisuse riskijuhtimismeetmed NIS2 art 21 lg 5 alusel. Hetkel kehtib Eestis kõigile küberturvalisuse seaduse subjektidele kohustus rakendada sõltuvalt suurusest kas esmaseid turvanõudeid või kohalikku E-ITS standardit, millega loetakse võrdsustatuks ka ISO 27001 sertifikaat. See tähendab, et NIS2 art 21 lg 5 alusel kehtestatud rakendusmääruse (EL) 2024/2690 subjektiks olevad digiteenuse osutajad peavad Eestis täitma lisaks kohalikke riskihalduse meetmeid (KüTS-i alusel kehtestatud turvameetmed). See tähendab topeltkoormust, erisuste otsimist ja nõuete võrdlemist. See omakorda viib suurema halduskoormuseni ja võimalik, et ka paralleelsete nõuete rakendamiseni. Piiriüleselt tegutsevate digiteenuste osutajate jaoks tähendab see riigikohaseid erisusi.

Juhime tähelepanu, et osa rakendusakte on veel välja andmata, mistõttu ei ole selge, kas nendes sisalduvad nõuded oleksid leebemad või rangemad nendest, mida Eesti hetkel või tulevikus plaanib rakendada. Lisaks ei ole ka Komisjonile sätestatud tähtaega, millal vastavad rakendusaktid peaksid jõustuma. Teeme ettepaneku sätestada NIS2-s ka rakendusaktide vastuvõtmise tähtajad, et tagada õigusselgus.

4. Lunavara rünnakute andmete kogumine

Hetkel kehtib NIS2 üle võtnud küberturvalisuse seaduse alusel kohustus teavitada küberintsidentidest. Leiame, et kehtivas regulatsioonis sisalduv kohustus katab ära ka lunavara rünnakud. NIS2 muutmise ettepanekus sisalduva eraldi lunavara rünnakuid (kui ainult ühte rünnaku viisi paljudest) puudutava regulatsiooni (NIS2 ettepaneku art 1 punkt 8) lisamine eraldiseisvalt ei muudaks olukorda. Seega tekkis küsimus, miks soovitakse lunavaraga seotud rünnakute eraldi regulatsiooni lisada. Kas hetkel kehtiv regulatsioon ei kata ära seda küberintsidendi osa?

Samuti jääb ebaselgeks, millal (*upon request*) ja millises mahus andmeid täpselt soovitakse. Kui eraldi lunavara rünnakuid käsitlev regulatsioon jääb alles, siis teeme ettepaneku see põhjalikumalt lahti kirjutada. Näiteks võib makseandmete avaldaminekaasa tuua ettevõtjatele sanktsioonidega seotud riske, kui olid sunnitud siiski mingis olukorras lunaraha maksma isikutele, kes on seotud sanktsioneeritud jurisdiktsiooniga. Seetõttu oleks vajalik selge *safe harbour* klausel ettevõtjatele vastavate teavituste tegemisel.

NIS2 muutmise ettepaneku kohta toome täiendava olulise teemana välja DORA rakendamise IKT teenuse osutajatele.

Täname Justiits- ja Digiministeeriumit, et arvestasite Euroopa Komisjoni digiomnibussi määruse ettepanekule Eesti seisukohti koostades ITL-i ettepanekut lahendada küsimus NIS2 ja DORA paralleelsetest kohustustest IKT teenuse osutajatele. Teeme ettepaneku korrata seda seisukohta ka küberpaketile Eesti poolt tagasisidet andes. See teema on vaja lahendada, et vähendada ettevõtete halduskoormust ja lihtsustada regulatsioone.

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

Kehtivate õigusaktide kohaselt on DORA subjektid vabastatud NIS2 täitmisest, kuid NIS2 subjektid, kes osutavad teenuseid DORA subjektidele, peavad DORA subjektide nõudel vastama ka DORA-le. See tekitab NIS2 subjektidest IKT teenuse osutajatele, kes soovivad oma teenuseid osutada ka finantssektori asutustele, väga suurt halduskoormust. Seetõttu on ITL-i ettepanek muuta nii NIS2-te kui ka DORA-t selliselt, et NIS2 direktiivi kohuslased, kes osutavad finantssektori asututele IKT teenuseid, ei pea tõendama eraldi DORA-le vastavust, vaid need turvanõuded tunnistatakse samaväärseteks, kui nad vastavad NIS2 alusel kehtestatud nõuetele.

Lõpetuseks avaldame lootust, et leiate võimaluse küberpaketis sisalduvate ettepanekute kohta Eesti seisukohti koostades ITL-i arvamust arvestada. Palume võimalusel jagada meiega ka Eesti seisukohtade kavandit.

Lugupidamisega

/allkirjastatud digitaalselt/

Doris Põld
Tegevjuht

Keilin Tammepärg, keilin.tammeparg@itl.ee