RIIGI INFOSÜSTEEMI AMET

Tõnu Grünberg
Justiits- ja Digiministeerium
info@justdigi.ee

Teie 06.03.2026 nr 7-1/1078

Meie 06.04.2026 nr 1.1-20/26281

Tagasiside EL küberturvalisuse määrusele

Austatud Tõnu Grünberg

Küberturvalisuse määruse muudatused

ENISA konverentsil väljendasid rakendajad üle Euroopa ootust töörahule, võimalusega enne järgmisi muudatusi mõistliku perioodi jooksul kehtestatud reegleid rakendada. Nõustume selle seisukohaga. Praegused muudatused seoses nt NIS2-ga ei adresseeri tõenäoliselt väga suurt osa praktikas ilmnenud või veel ilmnevaid probleeme, eriti arvestades, et paljude riikide poolt direktiivi ülevõtmine viibis, sh Eestil. Uued muudatused tähendaksid niigi põhjalikult muudetus küberturvalisuse raamistiku uuesti muutmist sisulistes aspektides.

Muudatused, mis on planeeritud, näitavad selget ambitsiooni suurendada tsentraliseeritust ning vähenda liikmesriikide otsustuspädevust. Kuigi ühisturu mõistes on see ambitsioon arusaadav, ei ole see liikmesriikide ja nende erinevuste vaatest põhjendatud. Eestil on ühelt poolt väga arenenud digiriik ja teiselt poolt ka selge, meie vajadustele vastav, eripärasid, sh väiksust ja turuosalisi arvestav küberturvalisuse tagamise süsteem. Kesksete meetmete ülimuslikkus liikmesriigi kehtestatud nõuete ees võib mõjutada negatiivselt saavutatud tasakaalu.

Järgnevalt toome välja erinevad murekohad ja tähelepanekud seoses Küberturvalisuse määruse ja NIS2 direktiivi kavandatavate muudatustega.

ENISA rolli suurenemine

1. Nii CSA2 kui NIS2.2 ettepanekute oluline osa on ENISA rolli suurendamine. Selle juures on mitmed küsitavused ja murekohad. Eesmärk on suurem tsentraliseeritus, kuid pole selge selle tegelik kasutegur, samas tähendab see selgelt suuremaid kulusid.
2. Euroopa Komisjon on öelnud, et nende eesmärk ei ole teha ENISA-st CSIRTi, mis reageerib intsidentidele. On arusaadav, et ENISA roll CSIRT võrgustikus (edaspidi: CNW) on suurem kui ainult sekretariaadi oma. Sestap soovitame sõnastada ettepanekus ENISA rolli CNW-s palju täpsemalt ning ühes ääremärkusega, mis kirjeldab, mida tähendab, et

ENISA on CNW liige ja milles seisnevad selle liikmelisusega kaasnevad õigused ja ülesanded. Tähelepanu tasub pöörata ka asjaolule, rahvusvahelised partnerid ei pruugi üheselt mõista, mida tähendab, et ENISA on CNW liige - võib jääda väärarusaam, et ENISA on üks Euroopa Liidu CSIRTidest, isegi kui CSA2 järgi ta seda ei ole.

3. ENISA suurem roll tähendab ka suuremat ja intensiivsemat koostööd liikmesriikidega. CSA2 näeb ette NLO ja SNE-d, kuid tuleb arvestada, et spetsialistid CSIRT-is, järelevalves ja riskianalüütikud on erinevad inimesed - ei saa vaid ühe-kahe inimese peale üles ehitada kogu sisulist koostööd. Koostöö tugineb inimestel ja see tähendab lisaks kirjalikule suhtlusele ka reisikulusid - kuidas neid kaetakse. Tagajärjeks võib olla väiksemate riikide kõrvale jäämine ja marginaliseerumine.
4. CSA2 ütleb, et ENISA hakkab komisjoni nõustama ja abistama ELi küberpoliitika ja väljatöötamisel (artikkel 4). Varem oli kirjas ainult "policies", nüüd ka "legislation". Ehk siis ENISA-l oleks suurem roll küberõiguse väljatöötamisel, samas artikkel 1 rõhutab jätkuvalt sõltumatust. Tekib küsimus, mida “assist” hõlmab ja kui suures mahus ning intensiivsusega hakkab ENISA õigusloomesse panustama. Selline mandaat muudab hägusaks piiri rakendusasutuse ja seadusandliku võimu vahel, andes kvaasi-seadusandlikud õigused. Samas ei ole ENISA-l samaväärset vastutust kui on seda Komisjonil. Samal ajal luuakse artikliga 10 senisest suurem operatiivse koostöö mandaat: koostöö toetamise asemel hakkab ENISA rohkem ise ka ülevaadetesse ja olukorra teadlikkuse panustama.
5. Artikkel 11(1)(g) sätestab, et ENISA analüüsib ka lunavara meetodite, nõuete ja mõju trende. Mõistetav on vajadus piiriülese informatsiooni ja tervikvaate järgi, mis võimaldaks teha põhjendatud ning otstarbekaid poliitikaotsuseid. Teisalt juhime tähelepanu, et ENISA analüüsid on kõrge abstraktsustasandiga, ei sisalda tundlikku, kuid tihti olulist teavet ning valmivad pika ajaperioodi peale olles seega valmimise ajaks tihti teatud määral aegunud. Seega tasub sellise ülesande ettenägemisel arvestada eeltoodud piirangutega ning arvestada, et selline analüütika saab ennekõike informeerida kõrgema tasanadi poliitikaotsuseid, kuid pole ilmselt suure kasuteguriga operatiivsele tasandile.
6. Mitmes sättes on sisse toodud ja rõhutatud Europoli ja ENISA koostöö. Koostöö eeldab usaldust ja head infovahetust. Tuleb arvestada, et Europol ja CSIRT-id tegutsevad erineva loogika alusel. CSIRT-ide toimise eeldus on kiirus, konfidentsiaalsus ja neutraalsus, samas kui Europol lähtub uurimis- ja tõendamisraamistikest. Praktikas on näiteks CSIRT-võrgustikus üleval probleem õiguspärase ligipääsu küsimusega, mille puhul pole Europol suutnud liikmesriikidele tõestada, kuidas nad saavutavad ligipääsu andmetele ilma küberturvalisuse põhimõtteid rikkumata. Seega on koostöö eelduseks selged piirid ja tagatised, mida praegune ettepanek ei adresseeri. See omakorda tähendab, et koostöö võib jääda vaid formaalseks.
7. Artikkel 12 näeb ette varase hoiatuse (*early alerts*) süsteemi. Küsimus on, kas süsteem teatud määral ei dubleeri juba olevasolevaid teavitusskeeme (CNW-s, CERT-EU). Teiseks, arvestades, et ENISA tugineb kaudsele infole, on küsimus, kuidas tagatakse, et teavitused on piisavalt operatiivsed ja informatiivsed. Lisaks on osa teavitussüsteemist ka soovituste tegemine. Näeme siin teatavat ohukohta kui ENISA, kes ei seira EE küberruumi, teeb soovitusi meie ettevõtetele teadmata kõiki olulisi asjaolusid ja nimetatud soovitused ei ole kohandatud vastavatele oludele. Lisaks võib siin tekkida olukord, kus riiklik CSIRT jääb välja oluliselt infovahetusest ja kontaktist üksusega.

8. Lisaks on neil ettepaneku kohaselt konkreetne roll (*shall assist*) ka lunavararünnetele vastamise osas (artikkel 13(3). Kuigi on toodud, et see toimub koostöös CSIRT-idega, jätab see ebamääraseks koostöö vahekorra ja jätab õhku küsimuse, kas ENISA hakkab nende eest või nendega paralleelset lunavara intsidentidele reageerima. See on laiem küsimus sellest, kas ENISA-l on liikmesriike toetav roll või hakkab ENISA-st saama/kujunema CSIRT. Kuigi Komisjon on seda eitanud, näitavad kõnealused mandaadilaiendused teistpidist suundumust. Konkreetsemalt näeme siin ohtu tungida CSIRTi ja riigi pädevuses. Säte viitab küll koostööle CSIRT-idega, kuid ei sisalda selget nõuet liikmesriigi nõusolekule, mida on kasutatud muudes sätetes.
9. Artikkel 13(3) sätestab ka, et "*For that purpose, ENISA shall establish a helpdesk and in particular make use of the enhanced shared situational awareness of the cyber threat and incident landscape pursuant to Article 11(1), first subparagraph, points (a) and (g) of this Regulation*." Sellest võib järeldada, et ENISA hakkab pakuma osaliselt SOC teenust. Sellega seoses tekib taas küsimus riikliku CSIRTi ja ENISA tegevuse kattuvusest või põrkumisest. Tekstist ei selgu, kuidas toimub koordinatsioon operatiivse toe pakkumisel ning kuidas toimub infovahetus. Tekib oht, et oluline informatsioon ei jõua seetõttu CSIRT-ini või, et üksus saab riiklikult ja ENISA tasandilt erinevaid suuniseid. Samuti on küsitav, millise kvaliteediga tuge saab ENISA tasandilt pakkuda, arvestades, et spetsiifiline teadmus oludest on siiski riiklikul tasandil.

Euroopa küberturvalisuse sertifitseerimisraamistiku lihtsustamine

10. Sertifitseerimisraamistik näeb ette liikmesriikidele kohustuse aktsepteerida sertifikaate ilma õiguseta täiendavalt auditeerida.
11. Tuleb arvestada, et keskselt väljatöötatud sertifitseerimisskeem ei pruugi piisaval määral ajaga kaasas käia ning esitatavad nõuded on kompromiss erinevate lävendite vahel. Arvestades liikmesriikide siiski erinevat küberturvalisuse taset ei ole vastuvõetav ega mõistlik panna kohustust tingimusteta sellist sertifikaati aktsepteerida ning säilima peaks võimalus vajadusel täiendavalt auditeerida nõuetele vastavust.
12. Lisaks tuleb silmas pidada vastavushindamisasutuste (conformity assessment bodies, CAB) võimalikku erinevat praktikat, mis võib kaasa tuua kohtalluvuse valimist (f*orum shopping*) lähtuvalt soodsamaist praktikast. Kuigi on ettenähtud mehhanism CAB-i tegevuse nõuetele vastamiseks (artikkel 94), on see selgelt ajakulukas protsess mis ei võimalda tagasi pöörata juba tehtud otsuseid. Ehk ettenähtud usaldus sertifikaatide vastu on suur, kui kontrollimehhanismid on kaudsed ja nõrgad.
13. Fundamentaalsemal tasemel võib sertifikaadi tingimusteta ja täiendava kontrollita aktsepteerimise kohustus olla vastuolus liikmesriikide pädevusega julgeoleku küsimustes. Küberturvalisusel on oluline koht riigi julgeolekus. Pandud kohustus välistab aga riigi võimaluse välistada mingeid tehnoloogiaid või teostada efektiivset kontrolli. **Seega tõstatub küsimus, kas ettenähtud raamistik on kooskõlas Euroopa Liidu toimimise artikliga 4(2), eeskätt selle viimase lausega.**

IKT tarneahela turvalisuse raamistik

14. Laias laastus IKT tarneahela turvalisuse raamistik (98-105) tegeleb mitte-tehniliste riskide maandamisega kõrge kriitilisusega sektorite tarneahelates ja meetmed kehtiksid NIS2 I ja

II lisa üksustele. Artikkel 100 kohaselt saab määratleda kolmandaid riike küberturvalisuse vaatest riskiriigiks (designation of third countries posing cybersecurity concerns). Oluline on ka see, et sinna alla ei lähe ainult kolmandate riikide firmad, vaid ka firmad mis on kolmanda riigi kontrolli all või nt mille omanik on kolmanda riigi kodanik.

15. Üldiselt toetame riskiriikide määramise mehhanismi, sest see annab võimaluse vähendada kriitilises infrastruktuuris sõltuvust kõrge riskiga riikide tootjate toodeid. RIA vaatest pigem positiivne, et aktsepteeritakse, et tarneahela riskid on laiemad, kui kitsas mõistes tehnoloogilised.
16. Ettepanek annab otsustuspädevuse kolmandate riikide määramiseks küberturvalisusele ohtu kujutavateks riikide hulka Komisjonile. Liikmesriigid küll panustavad läbi ohuhinnangu ja konsultatsioonide, kuid nende roll jääb selgelt nõuandvaks. Seejuures ei näe raamistik ette võimalusi ei leevendusteks ega ka liikmesriigi poolseks karmimaks lähenemiseks (kuigi art 98(3) näeb ette justkui vastava õiguse, on see allutatud ühisturu nõuetele). Juhime tähelepanu, et kuna otsustel on suure tõenäosusega lisaks mõjule julgeolekule ka oluline majanduslik mõju, on ka arvestatav risk protsessi politisserumisele, mis omakorda võib õõnestada selle usaldusväärsust.
17. Artikkel 103 näeb ette, et komisjon võib rakendusaktiga ette näha seadmed ja komponendid, mille kasutamine on NIS2-s ettenähtud sektorites tegutsevatele ettevõtetele keelatud, ning anda neile üleminekuks tähtaja. Kui peab hakkama vahetama välja tooteid, siis millised on eeldatavalt need tähtajad ja kas sellele tuleb ka mingi täiendav EL-i tugi?
18. 99(1) kohaselt võib Komisjon või 3 liikmesriiki algadata, et NIS CG viiks läbi rkiskianalüüsi. Sätte alusel on silmas peetud süvitsi, põhjalikku riskihindamist, kuid samas on ajaraam vaid kuus kuud. RIA vaatest tekitab küsimusi NIS CG raames võimekus sellist hindamist läbi viia. Täna ei ole RIA panus NIS CG-sse FTE-de mõttes sellises mahus, et sisukalt sellisesse riskihindamisse panustada; küsitav on, kas teistegi riikide panus seda võimaldab. Seega eeldab selline raamistik riigide, sh Eesti suuremat panust NIS CG-sse.
19. Segaseks jääb protsessi n-ö omanik – kuigi NIS CG justkui viib seda läbi, on Komisjonil arvestatavad hoovad selle üle. Lisaks, riskihindamisel on oluline kaal kuna sellest sõltub hilisem kõrge-riskiga tootjate määratlemine, seega on liikmesriikide panusel väga oluline kaal, kuid kontroll protsessi üle on minimaalne (läbi NIS CG).

NIS2 direktiivi ettepanekud

1. On tervitatav, et teatud üksuste kategooriaid täpsustatakse. Samas oleks hädavajalik, et täpsustataks mõisteid laiemalt. Näiteks järelevalve mõisted (ad hoc audit, targeted audit, and regulaar audit)**.** Mõisted peaks olema kooskõlas ka standardiseeritud terminoloogiaga. Praegu kasutatav terminoloogia, mis pole ühegi turbevaldkonna termonoloogiaga süstemaatiliselt kooskõlas. Sellegi korrastamine on täiesti välja jäänud teema ja probleemid aina progresseeruvad.
2. Keskmise suurusega ettevõtte kategooria asendamine *Small mid-cap* kategooriaga
    a. Ettepanek ei võta laias laastus arvesse väiksemate riikide turuolukorda. Eestis kukuvad enamus ettevõtteid alla selle piiri. See omakorda tähendab, et enamus direktiivi lisas I toodud valdkondades tegutsevad ettevõtted jäävad üliolulise üksuse regulatsiooni alt välja ja seega ei ole kohustatud võtma ka vastavaid

turvameetmeid ning nende üle järelevalve on võimalik teostada vaid *ex post* ehk kui midagi on juba juhtunud.

   b. Ettevõtete suuruste määratluse muutmine selleks, et skoopi vähendada, jätab tähelepanu alt aga välja ettevõtete mõju proportsionaaluse ja sõltuvuse digitaalsest elemendist, võrgu- ja infosüsteemidest. See jookseb ka peamise kriitikana NIS2 kohta läbi teaduskirjandusest.

3. Artikliga 5 nähakse ette, et kui Komisjon on andnud rakendusmääruse art 21(5) alusel, kuulub kohaldamisele viimati nimetatu ning liikmesriigid ei või kehtestada täiendavaid nõudeid. Sellisele regulatsioonile oleme kindlasti vastu. Liikmesriikidel peab jääma võimalus kehtestada täiendavaid nõudeid, pidades silmas riigi eripära. Praegusel juhul oleks välistatud näiteks Eesti-spetsiifilised turvanõuded valdkonna üksustele, kellele on kehtestatud ka rakendusmäärus. Samuti kaasneb selle ettepanekuga kinni kirjutamise oht – olukorras, kus rakendusmäärus ei ole enam ajakohane, ei ole sellise regulatsiooni korral võimalik riigil kehtestada selle kategooria üksustele aja- ja asjakohasemaid nõudeid. Küsitav on aga komisjoni võime asjakohaseid tehnilisi, metodoloogilisi sektoripõhiseid nõudeid kehtestada piisava agiilsusega, et need oleksid ja jääksid asjakohaseks. Praegu on ühe rakendusakti sektorina välja toodud ka pilvandmetöötlusteenuse osutajad ja andmekeskusteenuse osutajad – RIA hinnangul ei ole rakendusmäärus piisav, pidades silmas ka Eesti digiriigi eripärasid ja täiendavaid, riigispetsiifili nõudeid. Samas marginaliseerub E-ITS ja seeläbi ka muud kohalikud ettevõtluse algatused (Cybsis, Kordon, PlanPRO jne). Siin võiks jääda valdkondlike soovituslike standardite tasemele ja mitte üle reguleerida.
4. Küberturvalisuse seisundi (*cyber posture*) sertifikaadi osas vt kommentaare ülalt seoses sertifitseerimisraamistikuga.
5. Praegu ettenähtud ülevõtmisaeg 12 kuud on ilmselt liiga lühike periood, arvestades, et üleminek ja kohanemine seniste muutustega kestab veel pikalt.

Lugupidamisega

(allkirjastatud digitaalselt)

Joonas Heiter
peadirektor

Liina Lumiste
Liina.Lumiste@ria.ee