EUROOPA KOMISJONI VASTUSED

EUROOPA KONTROLLIKOJA ERIARUANDELE

ELi institutsioonide, organite ja asutuste küberturvalisus: valmisoleku üldine tase ei vasta ohtudele

Sisukord

Käesolevas dokumendis on esitatud Euroopa Komisjoni vastused Euroopa Kontrollikoja eriaruandes sisalduvatele tähelepanekutele kooskõlas finantsmääruse artikliga 259. Vastused avaldatakse koos eriaruandega.

I. KOMISJONI VASTUSTE LÜHIKOKKUVÕTE

a) Sissejuhatus

Küberturvalisusest on saanud Euroopa Komisjoni üks peamisi poliitilisi ja tegevusprioriteete. Koroonaviiruse kriis on suurendanud meie sõltuvust digiteenustest (pilvandmetöötlus, mobiilseadmed ja tehisintellekt). Viimasel kahel aastal on hakatud palju rohkem kodust töötama. Seetõttu on küberkuritegevus ja küberspionaaž – kaks peamist ohtu, millega ELi institutsioonid, organid ja asutused kokku puutuvad – internetis samuti hoogu kogunud. Komisjon on sellest suundumusest teadlik. Ta on võtnud küberturvalisuse valdkonnas järjepidevalt ja otsustavalt juhtrolli. 2019. aastal jõustus küberturvalisuse määrus, mis laiendas muu hulgas Euroopa Liidu Küberturvalisuse Ameti (ENISA) volitusi ja muutis need alaliseks. Määrusega käivitati ka ENISA ja CERT-EU (kõiki ELi institutsioone, organeid ja asutusi toetav infoturbeintsidentidega tegelev rühm) ametlik koostöö. 2020. aastal tegi komisjon ettepaneku tugevdada küberturvalisuse direktiivi. Seadusandjad on muudatustes peaaegu kokkuleppele jõudnud.

2020. aasta küberjulgeoleku strateegia sisaldas ka kolme meedet, mis mõjutavad ELi institutsioonide, organite ja asutuste küberturvalisust. Komisjon teatas määrusest infoturbe kohta ELi institutsioonides ja asutustes, määrusest ELi institutsioonide, organite ja asutuste ühiste küberturvalisuse eeskirjade kohta ning oma kavatsusest anda CERT-EU-le uus õiguslik alus, et suurendada selle volitusi ja rahastamist ning tagada piisavad vahendid suurenevate ohtude ja riskide ning sagedasemate intsidentide kontekstis.

Nende ettepanekute ettevalmistustööd edenevad. Kolleegium ei ole neid veel vastu võtnud, kuid eeldatavasti võetakse need vastu 2022. aasta esimeses kvartalis. Institutsioonide vahel selles ettevalmistusetapis arutatud olulised küsimused on seotud ettepaneku õigusliku alusega ning kõigi ELi institutsioonide, organite ja asutuste fiskaalvõimekusega nii oma küberturvalisuse vajaduste rahastamise kui ka CERT-EU, eelarve ja eelkõige ametikohtade toetamiseks vajalike vahendite leidmise osas.

ELi institutsioonide, organite ja asutuste küberturvalisuse alase valmisoleku tase on erinev. Mitmel neist on kübervalmiduse valdkonnas head tulemused ning nad peaksid juhtrollis jätkama, stimuleerides ja innustades edasist arengut kogu küberturvalisuse maastikul. Mõõdetavate edusammude saavutamiseks tuleb tunnistada, et ELi institutsioonide, organite ja asutuste valmisolek on erinev, ja seada prioriteedid, suunates parandusmeetmed esmajoones sinna, kus tuvastatud puudused põhjustavad suurimat riski.

b) Komisjoni seisukoht kontrollikoja peamiste tähelepanekute ja soovituste kohta

Komisjon väljendab heameelt kontrollikoja aruande üle ELi institutsioonide, organite ja asutuste küberturvalisuse kohta. Ta võtab teadmiseks, et aruandes rõhutatakse kõigi ELi institutsioonide, organite ja asutuste infoturbe ja küberturvalisuse alaste ühiste õigusraamistike tähtsust küberturvalisuse üldise taseme tõstmisel. Komisjon märgib, et kontrollikoja peamised tähelepanekud ja soovitused ei ole seotud komisjoni enda tegevuse küberturvalisuse kui sellisega, vaid komisjoni poliitilise rolliga õigusaktide ettepanekute esitamisel ELi institutsioonide, organite ja asutuste kübervalmiduse parandamiseks.

Tulevaste määrustega, mis käsitlevad ELi institutsioonide organite ja asutuste infoturvet ning ELi institutsioonide, organite ja asutuste ühiseid küberturvalisuse eeskirju, kehtestatakse ühised eeskirjad kõrgetasemelise infoturbe ja küberturvalisuse saavutamiseks, kuid nende rakendamine iga ELi institutsiooni, organi ja asutuse organisatsioonilises ja tegevuslikus kontekstis (eelkõige nende ohu- ja riskiprofiilid) jääb nende autonoomsesse vastutusalasse. Kavandatav küberturvalisust käsitlev määrus sisaldab vastavusmehhanisme, mis on asjakohased ja proportsionaalsed uute eeskirjade eesmärgi ja kohaldamisalaga, ilma et see piiraks institutsioonide, organite ja asutuste autonoomiat.

Komisjon juhib praegu digipöörde institutsioonidevahelise komitee küberturvalisuse allrühma. Allrühma juht vahetub rotatsiooni korras vähemalt korra kahe aasta jooksul. Tuleb märkida, et allrühma tööks ei ole eraldatud sihtotstarbelisi vahendeid: kõik meetmed põhinevad osalejate vabatahtlikel jõupingutustel.

Komisjon nõustub CERT-EU vahendite ja volituste suurendamise ideega.

Seega toetab komisjon aruande peamisi tähelepanekuid ja soovitusi. Meie üksikasjalikku seisukohta on selgitatud III jaos esitatud lisamärkustes. Komisjon nõustub ka soovitustega 1a, 1b, 1c, 1d, 1e, 1f ja 1g ning 2a, 2b ja 2c.

c) Viimased sündmused ja järgmised sammud

ELi institutsioonide, organite ja asutuste peadirektorite tasandil on lõpule viidud ametlik konsultatsioon kahe määruse (infoturve ja küberturvalisus) konsolideeritud eelnõude üle. Enne paketi valmimist ja selle vastuvõtmist kolleegiumis 2022. aasta esimeses kvartalis hinnatakse saadud tagasisidet.

II. KOMISJONI VASTUSED KONTROLLIKOJA PEAMISTELE TÄHELEPANEKUTELE

1. ELi institutsioonide, organite ja asutuste küberturvalisuse küpsusaste

Komisjon nõustub, et ELi institutsioonide, organite ja asutuste poolt küberturvalisusele tehtavate kulutuste taseme jälgimisel on oluline võtta arvesse ohte ja riske.

Ka inimressursside puhul mõjutavad ELi institutsioonide, organite ja asutuste personali stabiilsust mitmed tegurid. Spetsialiseerunud küberturvalisuseksperte on üha keerulisem värvata. Paljudel juhtudel ei ole personalieeskirjad eriprofiilidele kohandatud (värbamine, karjääriareng, koolitamine). Peale selle tähendab eelarvepädevate institutsioonide üldine surve ELi institutsioonide, organite ja asutuste töötajate arvule seda, et uutes prioriteetsetes valdkondades, nagu küberturvalisus, on endiselt täitmata ametikohti, eelkõige sisemistes operatiivteenistustes.

Juhtimise ja riskijuhtimise valdkonnas tehtud edusammudele viitamisel tuleks arvesse võtta asjaolu, et nõuetele vastavuse järelevalve liigub nüüd katseprojekti etapist lõpliku kasutuselevõtu etappi. Seega on katvus ootuspäraselt seni üsna väike. Nõuetele vastavuse projekt on järgmine etapp pikaajalises kübervalmiduse suurendamise protsessis, mis algas ühise riskimetoodika

määratlemisega, ühiste vahendite väljatöötamisega, nõrkusehalduse käivitamise ning varade inventari seire, testimise ja valideerimisega. Sel pikal teel on tehtud edusamme, kuigi komisjoni varabaas on keerukas, sest enam kui 50 peadirektoraati ja rakendusametit haldavad enam kui 1000 infosüsteemi.

2. ELi institutsioonide, organite ja asutuste koostöömehhanismid

CERT-EU on fenomenaalne edulugu koostöö edendamisel mitte ainult ELi institutsioonide, organite ja asutuste vahel, vaid ka Euroopa tasandil, kuna ta on osalenud küberturvalisuse direktiivi alusel loodud küberturbe intsidentide lahendamise üksuste (CSIRT) võrgustikus täisliikmena. Nii on CERT-EU hea näide koostöö ja küberturvalisuse teenuste tõhustamise kohta. Kontrollikoja tähelepanekud CERT-EU kohta näitavad väga selgelt, et CERT-EU teeb silmapaistvat tööd üha vaenulikuma küberohtude maastiku ja pideva ressursside nappuse tingimustes.

Praeguse institutsioonidevahelise kokkuleppe kohaselt esindab ELi detsentraliseeritud asutusi ja ühisettevõtteid CERT-EU juhtnõukogus ametlikult ENISA. Peale selle väljendab nende seisukohti juhtnõukogu koosolekutel IKT nõuandekomitee (ICTAC) esindaja, kellel on lubatud koosolekutel osaleda, et aidata ENISAt asutuste esindamisel, kuid kes ei ole ametlikult juhtnõukogu liige ega osale hääletustel. Kavandatavas määruses käsitletakse asutuste piisavat esindatust CERT-EU juhtnõukogus, täiendades juhtnõukogu koosseisu kuni kolme esindajaga, kelle nimetab liidu asutuste võrgustik (EUAN) IKT nõuandekomitee ettepanekul.

Digipöörde institutsioonidevahelise komitee küberturvalisuse allrühmas osalemine toimub parimal võimalikul viisil ja iga ELi institutsiooni, organi või asutuse kindlaksmääratud tasemel. Uue küberturvalisuse raamlepingu koostamisel käsitletakse hanketeabe paremat jagamist. See on oluline teema küberturvalisuse allrühma 2. töörühma raames.

Mis puudutab ühiseid vahendeid selliste teenuste jaoks nagu e-post ja videokonverentsid, siis on juba olemas võimalus kasutada SECEM-2 süsteemi, mille komisjon on rakendanud kõigi ELi institutsioonide, organite ja asutuste jaoks krüpteeritud e-posti saatmiseks. See sõltub krüpteerimisvõtmete ja sertifikaatide tõhusast haldamisest. Lisaks on väljatöötamisel vahend SECABC, mis võimaldab institutsioonide vahel liikuva e-posti krüpteerimist. Kavas on teha see kõigile huvitatud ELi institutsioonidele, organitele ja asutustele kättesaadavaks 2022. aastast. Salastamata tundliku teabe jaoks on olemas turvalised videokonverentsid ja neid saab ajutiselt laiendada ka teistele ELi institutsioonidele, organitele ja asutustele, hallates koosolekul osalejate identiteeti. Tundliku teabe jagamist käsitletakse ka kavandatavas infoturbe määruses (ühise märgistamise abil).

3. Teabe jagamine oluliste intsidentide või nõrkuste kohta

Asjaolu, et kõik ELi institutsioonid, organid ja asutused ei teavita CERT-EUd olulistest intsidentidest ja nõrkustest, käsitletakse küberturvalisuse määruse eelnõus kooskõlas komisjoni ettepanekuga küberturvalisuse 2. direktiivis[1]. Rakendamise tase sõltub lisaressurssidest, mida autonoomsed ELi

[1] Ettepanek võtta vastu Euroopa Parlamendi ja nõukogu direktiiv, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega tunnistatakse kehtetuks direktiiv (EL) 2016/1148, COM(2020) 823 final.

institutsioonid, organid ja asutused sellele eraldavad. Sellise teavitamise jõustamise ulatus on endiselt piiratud, sealhulgas kavandatavas määruses selle praegusel kujul, kuna ELi institutsioonid, organid ja asutused on institutsionaalselt sõltumatud. Kavandatav küberturvalisust käsitlev määrus sisaldab vastavusmehhanisme, mis on asjakohased ja proportsionaalsed uute eeskirjade eesmärgi ja kohaldamisalaga, ilma et see piiraks institutsioonide, organite ja asutuste autonoomiat.

III. KOMISJONI VASTUSED KONTROLLIKOJA JÄRELDUSTELE JA SOOVITUSTELE

1. soovitus. Parandada kõigi ELi institutsioonide, organite ja asutuste küberturvalisuse alast valmisolekut ühiste siduvate eeskirjade ja CERT-EU jaoks suuremate vahendite eraldamise abil.

Esildatud määruse tekst sisaldab konkreetseid meetmeid, mille eesmärk on veelgi tõsta küberturvalisuse ühtset taset. Nimetatud meetmed võetakse üle küberturvalisuse kavadesse, mis koostatakse ja rakendatakse ELi institutsioonide, organite ja asutuste tasandil nende enda küberturvalisuse juhtimise raamistiku alusel.

Komisjon nõustub selle soovitusega. Seoses konkreetsete alasoovitustega märgib komisjon järgmist:

a) Komisjon nõustub soovitusega 1a. Määruse eelnõu sisaldab sätteid juhtimis- ja kontrolliraamistike kohta, mis kehtestatakse iga ELi institutsiooni, organi ja asutuse kõrgeima juhtkonna tasandil, et tagada kõigi küberriskide tõhus ja usaldusväärne juhtimine.
b) Komisjon nõustub soovitusega 1b. Määruse eelnõus rõhutatakse küberturvalisuse haldamise riskipõhist lähenemisviisi, tehes selgeks, et hindamisele peaksid järgnema meetmed, IT-turvalisuse kavad ja oluliste kontrollide tegelik rakendamine.
c) Komisjon nõustub soovitusega 1c. Küberturvalisuse haridus-, teadlikkuse suurendamise ja koolitusprogramme nimetatakse määruse eelnõus küberturvalisuse lähtestsenaariumi osana.
d) Komisjon nõustub soovitusega 1d. Meie kogemused näitavad, et kuigi korrapärased auditid ja testid on hädavajalikud, ei ole need edasimineku tagamiseks piisavad. Seepärast on punktis a nimetatud küberturvalisuse juhtimise raamistiku osana vaja korrapärast aruandlust ja läbipaistvust.
e) Komisjon nõustub soovitusega 1e. Määruse eelnõu sisaldab sätteid selle kohta, et ELi institutsioonid, organid ja asutused teavitavad CERT-EU-d olulistest küberohtudest, nõrkustest ja intsidentidest.
f) Komisjon nõustub soovitusega 1f. Komisjon toetab vajadust suurendada CERT-EU vahendeid. Määruse eelnõu teksti lisatakse sätted, mis käsitlevad personali ning ELi institutsioonide, organite ja asutuste rahalist toetust.

g) Komisjon nõustub soovitusega 1g. Kavandataval määrusel on täitmismehhanismid, mis on proportsionaalsed sätete eesmärgi ja kohaldamisalaga, pidades silmas ELi institutsioonide, organite ja asutuste institutsionaalset autonoomiat. Tulevase määruse sisu sõltub seadusandliku menetluse tulemusest ja tuleneb ELi seadusandja otsusest komisjoni ettepaneku kohta.

2. soovitus. Toetada ELi institutsioonide, organite ja asutuste vahel täiendavat sünergiat valitud valdkondades.

Komisjon, kes juhib praegu digipöörde institutsioonidevahelise komitee (ICDT) küberturvalisuse allrühma, nõustub soovitustega edendada lahendusi tundliku teabe järjepidevaks ja turvaliseks jagamiseks, küberturvalisuse projekte käsitleva teabe süsteemseks jagamiseks ning küberturvalisuse teenuste ühisteks hankeraamistikeks ja lepinguteks.

Komisjon nõustub selle soovitusega. Seoses konkreetsete alasoovitustega märgib komisjon järgmist:

a) Komisjon nõustub soovitusega 2a. Komisjon toob tehnilised algatused ja teenused ICDT küberturvalisuse allrühma, et edendada ja toetada ühiseid vahendeid tundliku teabe jagamiseks, kasutades selliseid teenuseid nagu e-post ja videokonverents. Samuti märgime, et kavandatavas infoturbe määruses käsitletakse salastamata tundliku teabe ühist märgistamist ja ühiseid käitlemiseeskirju.
b) Komisjon nõustub soovitusega 2b. Selle küsimusega tegelevad ICDT küberturvalisuse allrühma kuuluvad olemasolevad töörühmad. Uue küberturvalisuse raamlepingu ettevalmistamisel tegeletakse hanketeabe jagamise parandamisega.
c) Komisjon nõustub soovitusega 2c. ELi institutsioonidel, organitel ja asutustel on juba juurdepääs komisjoni hallatavatele IKT valdkonna institutsioonidevahelistele raamlepingutele. Uue küberturvalisuse raamlepingu koostamine kooskõlastatakse ICDT küberturvalisuse allrühmaga.

3. soovitus. Suurendada CERT-EU ja ENISA keskendumist kübervaldkonnas vähem küpsetele ELi institutsioonidele, organitele ja asutustele.

See soovitus on adresseeritud CERT-EU-le ja ENISA-le.