Euroopa Liidu
Nõukogu

Brüssel, 22. märts 2022
(OR. en)

7474/22

Institutsioonidevaheline dokument: 2022/0085(COD)

CYBER 93
TELECOM 116
JAI 383
INST 89
INF 32
CSC 119
CSCI 39
DATAPROTECT 81
FIN 353
BUDGET 2
CODEC 349
IA 30

ETTEPANEK

Saatja:	Euroopa Komisjoni peasekretär, allkirjastanud Martine DEPREZ, direktor
Kättesaamise kuupäev:	22. märts 2022
Saaja:	Jeppe TRANHOLM-MIKKELSEN, Euroopa Liidu Nõukogu peasekretär
Komisjoni dok nr:	COM(2022) 122 final
Teema:	Ettepanek: EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS, millega nähakse ette meetmed küberturvalisuse ühtlaselt kõrge taseme tagamiseks liidu institutsioonides, organites ja asutustes

Käesolevaga edastatakse delegatsioonidele dokument COM(2022) 122 final.

Lisatud: COM(2022) 122 final

EUROOPA
KOMISJON

Brüssel, 22.3.2022
COM(2022) 122 final

2022/0085 (COD)

Ettepanek:

EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS,

millega nähakse ette meetmed küberturvalisuse ühtlaselt kõrge taseme tagamiseks liidu institutsioonides, organites ja asutustes

{SWD(2022) 67 final} - {SWD(2022) 68 final}

SELETUSKIRI

1. ETTEPANEKU TAUST

• Ettepaneku põhjused ja eesmärgid

Käesoleva ettepanekuga luuakse raamistik ühiste küberturvalisuse normide ja meetmete tagamiseks liidu institutsioonides, organites ja asutustes. Ettepanekuga tahetakse veelgi parandada kõigi üksuste vastupidavusvõimet ja intsidentidele reageerimise suutlikkust. Ettepanek on kooskõlas komisjoni prioriteetidega muuta Euroopa digiajastule vastavaks ja luua tulevikuks valmis majandus, millest töötab inimeste heaks. Pealegi on turvalise ja vastupidava avaliku halduse tagamine ühiskonna kui terviku digipöörde alustala.

Käesolev ettepanek tugineb ELi julgeolekuliidu strateegiale (COM(2020) 605 final) ja ELi küberturvalisuse strateegiale digikümnendi jaoks (JOIN(2020) 18 final).

Käesoleva ettepanekuga ajakohastatakse CERT-EU kehtivat õigusraamistikku ning võetakse arvesse institutsioonide, organite ja asutuste digitaliseerimine viimaste aastate muutusi ja kasvu, aga ka küberohtude üldist arengut. COVID-19 kriisi puhkemine hoogustas mõlemat nimetatud tendentsi, samas kasvab intsidentide arv jätkuvalt ning mitmesugustest allikatest saavad alguse üha keerukamad ründed.

Kooskõlas sellega, kuidas liikmesriikides ja maailmas on paljud CERTid („infoturbeintsidentidega tegelevad rühmad“) nimetatud ümber küberturvalisuse keskusteks, muudetakse käesolevas ettepanekus ära CERT-EU nimi: ELi institutsioonide ja ametite „infoturbeintsidentidega tegelev rühm“ asendatakse liidu institutsioonide, organite ja asutuste „küberturvalisuse keskusega“, kuid alles jääb selle nime tuntuks saanud lühivorm „CERT-EU“.

• Kooskõla poliitikavaldkonnas praegu kehtivate õigusnormidega

Käesoleva ettepaneku eesmärk on suurendada liidu institutsioonide, organite ja asutuste küberturvalisuse alast vastupidavusvõimet küberohtudele kooskõlas kehtivate õigusaktidega.

- Direktiiv (EL) 2016/1148 meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus. Samuti on see kooskõlas ettepanekuga võtta vastu direktiiv (EL) XXXX/XXXX, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega tunnistatakse kehtetuks direktiiv 2016/1148 [küberturvalisuse 2. direktiivi ettepanek].
- Määrus (EL) 2019/881, mis käsitleb ENISAt (Euroopa Liidu Küberturvalisuse Amet) ning info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist (küberturvalisuse määrus).
- Ettepanek võtta vastu määrus (EL) XXXX/XXXX infoturbe kohta liidu institutsioonides, organites ja asutustes.
- Komisjoni 23. juuni 2021. aasta soovitus ühise küberüksuse loomise kohta.
- Komisjoni 13. septembri 2017. aasta soovitus (EL) 2017/1584 koordineeritud reageerimise kohta ulatuslike küberturvalisuse intsidentide ja kriiside korral.

Komisjoni 13. septembri 2017. aasta soovituse (EL) 2017/1584 (koordineeritud reageerimise kohta ulatuslike küberturvalisuse intsidentide ja kriiside korral) lisas on esitatud tegevuskava koordineeritud reageerimiseks ulatuslike piiriüleste küberturvalisuse intsidentide ja kriiside korral.

Euroopa Liidu Nõukogu rõhutas 9. märtsi 2021. aasta resolutsioonis, et küberturvalisus on hädavajalik nii riikide ja ELi tasandi avaliku halduse toimimiseks kui ka ühiskonna ja majanduse jaoks tervikuna, ning toonitas, kui tähtis on tugev ja järjepidev turvalisuse raamistik selleks, et kaitsta küberohtude eest kõiki ELi töötajaid, andmeid, sidevõrke, infosüsteeme ja otsustusprotsesse. Selle saavutamiseks tuleb eeskätt tõhustada liidu institutsioonide, organite ja asutuste vastupidavusvõimet ja parandada nende turvalisuskultuuri. Kättesaadavaks tuleb teha piisavad vahendid ja võimekus, muu hulgas CERT-EU volituste tugevdamise kontekstis.

2. ÕIGUSLIK ALUS, SUBSIDIAARSUS JA PROPORTSIONAALSUS

• Õiguslik alus

Käesoleva määruse õiguslik alus on Euroopa Liidu toimimise lepingu („ELi toimimise leping“) artikkel 298, milles on sätestatud, et liidu institutsioone, organeid ja asutusi abistab nende ülesannete täitmisel avatud, tõhus ja sõltumatu Euroopa halduskorraldus. Kooskõlas artikli 336 alusel vastu võetud personalieeskirjade ning teenistustingimustega kehtestavad Euroopa Parlament ja nõukogu seadusandliku tavamenetluse kohaselt määruste abil sel eesmärgil asjaomased sätted.

Infotehnoloogia on andnud liidu institutsioonidele, organitele ja asutustele uusi võimalusi kodanikega suhtlemiseks ja üldise tegevuse parandamiseks. Tehnoloogia areneb pidevalt ning koos sellega arenevad ka küberohud. Liidu institutsioonidest, organitest ja asutustest on saanud keeruliste küberrünnete jaoks väga atraktiivne sihtmärk. Tundub, et süsteemide ja nõuete kehtestamine küberturvalisuse tagamiseks aitab kaasa Euroopa halduskorralduse tõhususele ja sõltumatusele, nii et liidu institutsioonid, organid ja asutused saavad digitaalses maailmas oma ülesandeid täites tõhusamalt tegutseda.

Allpool 3. jaotises selgitatud praegused erinevused liidu institutsioonide, organite ja asutuste küberturvalisuse alastes hoiakutes ja lähenemisviisis küberturvalisuse valdkonnale on avatud, tõhusa ja sõltumatu Euroopa halduskorralduse jaoks täiendavad takistused. Ilma ühise lähenemisviisita areneksid liidu institutsioonide, organite ja asutuste küberturvalisuse alased hoiakud edasi eri suundades. Seega on nimetatud õiguslik alus asjakohane, arvestades et määrusega tahetakse luua liidu institutsioonide, organite ja asutuste küberturvalisuse ühine õigusraamistik.

• Subsidiaarsus

Määrus, millega nähakse ette meetmed küberturvalisuse ühtlaselt kõrge taseme tagamiseks liidu institutsioonides, organites ja asutustes, kuulub liidu ainupädevusse.

• Proportsionaalsus

Käesolevas määruses kavandatud õigusnormid ei lähe kaugemale, kui konkreetsete eesmärkide rahuldavaks täitmiseks vajalik. Kavandatud meetmed aitavad saavutada küberturvalisuse ühtlaselt kõrge taseme, minemata siiski kaugemale sellest, mis vajalik, et saavutada see eesmärk üha kasvavate riskide tingimustes.

• Vahendi valik

Määrus on vahetult kohaldatav ja seega sobiv õiguslik vahend, millega määrata kindlaks liidu institutsioonidele, organitele ja asutustele kehtestatavad kohustused ja neid kohustusi optimeerida. Määrus on sobivaim õiguslik vahend, et teha sihipäraseid parandusi.

3. EELHINDAMISE, SIDUSRÜHMADEGA KONSULTEERIMISE JA MÕJU HINDAMISE TULEMUSED

- **Eelhindamine**

CERT-EU hindas peamisi küberohte, millega liidu institutsioonid, organid ja asutused praegu kokku puutuvad või võivad lähitulevikus tõenäoliselt kokku puutuda.

Analüüsis jaotati tähelepanekud kolme kategooriasse:

- katsed tungida sisse liidu institutsioonide, organite ja asutuste IT-taristusse (kui selline katse on edukas, käsitletakse seda kui intsidenti, muul juhul registreeritakse see ikkagi kui tuvastatud katse);
- ohud, mis on tuvastatud liidu institutsioonide, organite ja asutuste läheduses (nt nendega seotud sektorites, sidusrühmade kogukondades või Euroopas);
- maailmas täheldatavad peamised ohusuundumused.

Lisaks võeti analüüsis arvesse oluliste suundumuste mõju sellele, kuidas liidu institutsioonid haldavad ja kasutavad oma IT-taristut ja -teenuseid. Sellised suundumused on näiteks:

- kaugtöö lisandumine,
- süsteemide viimine pilve,
- IT-teenusete üha sagedasem sisseostmine hanke korras.

Aastatel 2019–2021 on hüppeliselt kasvanud liidu institutsioone, organeid ja asutusi mõjutavate oluliste intsidentide[1] arv, mille taga on kõrgtehnoloogilise kinnisründeohu (*Advanced Persistent Threat* ehk APT) allikad. 2021. aasta esimesel poolel leidis aset sama palju olulisi intsidente kui kogu 2020. aastal. Seda näitab ka CERT-EUs 2020. aastal analüüsitud ekspertiistõmmiste, st mõjutatud süsteemide või seadmete sisust tehtud hetkvõtete arv, mis kolmekordistus võrreldes 2019. aastaga; oluliste intsidentide arv oli üle kümne korra suurem kui 2018. aastal.

2020. aastal püstitas CERT-EU juhtnõukogu uue strateegilise eesmärgi, et CERT-EU kindlustaks kõigi institutsioonide, organite ja asutuste kõikehõlmava küberkaitse, mis oleks piisavalt ulatuslik ja põhjalik ning kohaneks pidevalt olemasolevate või tulevaste ohtudega, nagu ründed mobiilsete seadmete, pilvekeskkondade ja esemevõrgu seadmete vastu.

Lisaks CERT-EU ohuanalüüsile on komisjon hinnanud küberturbe toimimist 20 liidu institutsioonis, organis ja asutuses. See hinnang annab ülevaate väljakujunenud küberturvalisuse tavadest ja küberturvalisuse haldamise võimekusest koos mõningate tehniliste turvameetmete väliste võrdlusalustega.

Hindamine tugines küsimustikele, millele need institutsioonid, organid ja asutused vastasid, avalikult kättesaadavatel andmetel ning teabele, mille liidu institutsioonid, organid ja asutused ise otse esitasid. Sealne teave on piisav, et teha praeguses olukorras järgmine järeldus:

- küberturvalisuse küpsuse tase, IT-taristu suurus ja võimekuse tase varieeruvad hinnatud liidu institutsioonides, organites ja asutustes väga suures ulatuses.

[1] „Oluline intsident“ – mis tahes intsident, v.a intsidendid, mille mõju on piiratud ja mille metoodika või tehnoloogia on tõenäoliselt juba hästi teada.

- Üldiselt on mitme liidu institutsiooni, organi ja asutuse tuvastus- ja reageerimisvõimekus küll küpsel tasemel, kuid nende küberturvalisuse haldamise suutlikkuse integreeritud riskijuhtimise tasemed on erinevad.
- Kuigi hinnatud liidu institutsioonide, organite ja asutuste küberturvalisuse raamistikud (strateegia, poliitika ja alusnormid) on määruse I lisas loetletud peamistes küberturvalisuse valdkondades üldiselt hästi paigas, ei ole mõnes liidu institutsioonis, organis ja asutuses küpsel tasemel toimepidevuse haldamist, vastavust, auditit ja pidevat täiustamist.
- Tõdeti, et hinnatud liidu institutsioonid, organid ja asutused rakendavad heaks tavaks peetavaid tehnilisi meetmeid ebaühtlaselt.

Kokkuvõttes näitab 20 liidu institutsiooni, organi ja asutuse analüüsimine, et nende haldustavad, küberhügieen, üldine võimekus ja küpsus on äärmiselt erinevad. Seepärast on väga oluline nõuda, et kõik liidu institutsioonid, organid ja asutused rakendaksid küberturvalisuse baastaset, et seeläbi vähendada küpsusetaseme erinevusi ja viia küberturvalisus kõigis liidu institutsioonides, organites ja asutustes ühtlaselt kõrgele tasemele.

Seni ei ole üheski liidu õigusaktis keskendutud liidu institutsioonide, organite ja asutuste küberturvalisusele ega võetud põhjalikult ette küberturvalisuse ohtude maastiku ja digitaliseerimise tõttu tekkivaid IT-riske.

- **Konsulteerimine sidusrühmadega**

Komisjon on konsulteerinud sidusrühmadega liidu institutsioonides, organites ja asutustes, aga ka liikmesriikide esindajatega nõukogus ja sidusrühmadega Euroopa Parlamendis. 25. juunil 2021 osalesid liikmesriikide ning liidu institutsioonide, organite ja asutuste asjaomaste sidusrühmade esindajad komisjoni korraldatud seminaril, et arutada tulevase määruse ettepaneku sisu.

- **Mõjuhinnang**

Käesolev ettepanek mõjutab liidu institutsioone, organeid ja asutusi. See tähendab, et eraldi mõjuhinnangut ei ole vaja, sest seda ei kohaldata liikmesriikide suhtes.

- **Põhiõigused**

Euroopa Liit tegutseb kindlalt selle nimel, et tagada põhiõiguste kaitse kõrge tase. Igasugune teabe jagamine käesoleva määruse põhjal toimub usaldusväärses keskkonnas ja austades täielikult õigust isikuandmete kaitsele, nagu on sätestatud Euroopa Liidu põhiõiguste harta artiklis 8 ja asjaomastes andmekaitsealastes õigusaktides, eelkõige Euroopa Parlamendi ja nõukogu määruses (EL) 2018/1725.

4. MÕJU EELARVELE

Turupõhised võrdlusalused ja uuringud[2] näitavad, et otsesed kulutused küberturvalisusele on kõikunud vahemikus 4–7 % organisatsiooni summaarsetest IT-kuludest. Samas näitab ohuanalüüs, mille CERT-EU tegi käesoleva seadusandliku ettepaneku toetuseks, et rahvusvahelisi organisatsioone ja poliitilisi organisatsioone ähvardavad ohud on kasvanud

[2] Allikas: Gartner, „Identifying the Real Information Security Budget“ (2016). See lisandub IT-turvalisuse kaudsetele kuludele seoses näiteks võrguturbe, tulemüüride ja viirusetõrjega ning süsteemi omaniku kohustustega, nagu riskihindamine ja turvameetmete rakendamine 2020. aasta dokumendi kohaselt moodustavad küberturvalisuse kulutused finantsasutustes 10–11 % IT-kuludest; allikas: DI_2020-FS-ISAC-Cybersecurity.pdf (deloitte.com).

ning seepärast oleks otstarbekam eraldada küberturvalisusele ligikaudu 10 % IT eelarvest. Sellise tegevuse täpset maksumust ei ole võimalik kindlaks määrata, sest ei ole üksikasjalikku teavet liidu institutsioonide, asutuste ja organite IT-kulutuste kohta ega selle kohta, kui suur osa kulutustest tehakse küberturvalisusele.

Seega on küll tõenäoline, et mitu liidu institutsiooni, organit ja asutust kulutavad küberturvalisusele vähem kui nad peaksid, kuid käesolev määrus ei too iseenesest kaasa praeguste kulude kasvu. Iga üksus peaks ka ilma käesoleva määruseta tagama küberturvalisuse piisava taseme. Määrus jätkab CERT-EU juhtnõukogu varasemat koostööd ja annab ametliku vormi osaliselt juba praegu toimuva teabevahetuse ühele kihile. Nagu on täpsustatud finantsselgituses, vajab CERT-EU oma laiendatud ülesannete täitmiseks täiendavaid ressursse ning need ressursid tuleks ümber jaotada CERT-EU teenuseid kasutavatelt liidu institutsioonidelt, organitelt ja asutustelt.

5. MUU TEAVE

- **Rakendamine ning järelevalve, hindamise ja aruandluse kord**

Institutsioonidevaheline küberturvalisuse nõukoda (IICB) peaks vaatama CERT-EU abiga läbi käesoleva määruse toimimise, korraldama hindamised ja esitama aruande oma järeldustega komisjonile. Komisjon peaks tagama korrapärase aruannete esitamise Euroopa Parlamendile, nõukogule, Euroopa majandus- ja sotsiaalkomiteele ning regioonide komiteele.

CERT-EU võib koostada ettepaneku juhenddokumendi või soovituse kohta, mille IICB võib otsustada vastu võtta. Juhenddokument on nõuandev dokument, mis on suunatud kõigile või mõnedele liidu institutsioonidele, organitele ja asutustele, soovitus aga on suunatud konkreetsele liidu institutsioonile, organile või asutusele. Üleskutse on CERT-EU nõuandev dokument, milles kirjeldatakse kiireloomulisi turbemeetmeid, mida liidu institutsioonid, organid ja asutused peaksid võtma kindlaksmääratud aja jooksul.

- **Ettepaneku sätete üksikasjalik selgitus**

Üldsätted

Määrusega nähakse ette meetmed, millega tagada küberturvalisuse ühtlaselt kõrge tase, ning seda kohaldatakse liidu institutsioonide, organite ja asutuste suhtes, et need saaksid täita oma ülesandeid avatult, tõhusalt ja sõltumatult. (Artiklid 1–3, 23–25)

Meetmed küberturvalisuse ühtlaselt kõrge taseme tagamiseks

Liidu institutsioonid, organid ja asutused on kohustatud kehtestama sisemise küberturvalisuse alaste riskide juhtimise, haldamise ja kontrollimise raamistiku, mis tagab kõigi küberturvalisuse riskide tulemusliku ja aruka juhtimise. Lisaks peavad institutsioonid, organid ja asutused võtma vastu küberturvalisuse baastaseme, et vähendada raamistiku kohaselt kindlaks tehtud riske, hinnata regulaarselt küberturvalisuse küpsuse taset ja võtta vastu küberturvalisuse kava. (Artiklid 4–8)

Institutsioonidevaheline küberturvalisuse nõukoda

Luuakse institutsioonidevaheline küberturvalisuse nõukoda, mis hakkab vastutama ühest küljest nii liidu institutsioonides, organites ja asutustes käesoleva määruse rakendamise järelevalve eest kui ka juhendama üldiste prioriteetide ja eesmärkide rakendamist CERT-EUs ja pakkuma CERT-EU-le strateegilist juhtimist. (Artiklid 9–11)

CERT-EU

CERT-EU aitab kaasa kõigi liidu institutsioonide, organite ja asutuste IT-keskkonna turvalisusele, andes neile nõu, aidates neil intsidente ära hoida, tuvastada ja leevendada ja intsidentidele reageerida ning tegutsedes nende küberturvalisuse alase teabevahetuse ja intsidentidele reageerimise koordineerimise keskusena. (Artiklid 12–17)

Koostöö- ja aruandekohustused

Määrusega tagatakse koostöö ja teabevahetus CERT-EU ning liidu institutsioonide, organite ja asutuste vahel, et suurendada usaldust ja kindlustunnet. Selle eesmärgi saavutamiseks võib CERT-EU paluda liidu institutsioonidel, organitel ja asutustel esitada asjakohast teavet ning CERT-EU võib vahetada liidu institutsioonide, organite ja asutustega teavet konkreetse intsidendi kohta, et hõlbustada samalaadsete küberohtude või intsidentide tuvastamist, ilma mõjutatud asjaosalise nõusolekuta. Sellist teavet, millest ilmneb küberturvalisuse intsidendi sihtmärgi identiteet, võib CERT-EU intsidendi kohta vahetada üksnes mõjutatud asjaosalise nõusolekul.

Eeskätt teatavad kõik liidu institutsioonid, organid ja asutused CERT-EU-le olulistest küberohtudest, olulistest nõrkustest ja olulistest intsidentidest ilma põhjendamatult viivitamata ja igal juhul hiljemalt 24 tunni jooksul pärast seda, kui on neist teada saanud. (Artiklid 18–22)

2022/0085 (COD)

Ettepanek:

EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS,

millega nähakse ette meetmed küberturvalisuse ühtlaselt kõrge taseme tagamiseks liidu institutsioonides, organites ja asutustes

EUROOPA PARLAMENT JA EUROOPA LIIDU NÕUKOGU,

võttes arvesse Euroopa Liidu toimimise lepingut, eriti selle artiklit 298,

võttes arvesse Euroopa Aatomienergiaühenduse asutamislepingut, eriti selle artiklit 106a,

võttes arvesse Euroopa Komisjoni ettepanekut,

olles edastanud seadusandliku akti eelnõu liikmesriikide parlamentidele,

toimides seadusandliku tavamenetluse kohaselt

ning arvestades järgmist:

(1) Digiajastul on info- ja kommunikatsioonitehnoloogia avatud, tõhusa ja sõltumatu liidu halduskorralduse alustala. Tehnoloogia areng ning digisüsteemide kasvav keerukus ja omavaheline seotus võimendavad küberturvalisuse riske ja suurendavad liidu halduskorralduse vastuvõtlikkust küberohtudele ja -intsidentidele, mis omakorda seab ohtu haldusasutuste toimepidevuse ja võime tagada oma andmete turvalisus. Tänapäeval on pilveteenuste kasutamise kasv, IT kasutamine kõikjal, intensiivne digitaliseeritus, kaugtöö ning tehnoloogia ja ühenduvuse areng liidu haldusüksuste kõigi tegevuste põhielemendid, kuid digivastupidavusvõime ei ole sellesse veel piisavalt sisse ehitatud.

(2) Liidu institutsioone, organeid ja asutusi ümbritsevad küberohud arenevad pidevalt. Ohusubjektide taktika, metoodika ja töövõtted arenevad pidevalt, kuid selliste rünnete peamised ajendid muutuvad vähe: alates väärtusliku avalikustamata teabe varastamisest, kuni raha teenimise, avaliku arvamusega manipuleerimiseni või digitaristu kahjustamiseni. Küberründe ir korraldatakse aina sagedamini ning ründed ise muutuvad keerukamaks ja automatiseeritumaks; sihikule võetakse ohtudele avatud ja üha suurenevad ründepinnad ning nõrkusi kasutatakse kiiresti ära.

(3) Liidu institutsioonide, organite ja asutuste IT-keskkonnad on omavahel seotud, andmevood on integreeritud ja nende kasutajad teevad tihedat koostööd. See omavaheline seotus tähendab, et isegi kui mõni katkestus piirdub esialgu ühe liidu institutsiooni, organi või asutusega, võib see kaasa tuua laiema ahelreaktsiooni, millel võib olla kaugeleulatuv ja pikaajaline negatiivne mõju ka teistele. Lisaks sellele on teatavate institutsioonide, organite ja asutuste IT-keskkonnad seotud liikmesriikide IT-keskkondadega ning see tähendab, et intsident ühes liidu üksuses võib seada ohtu liikmesriikide IT-keskkonna turvalisuse ja vastupidi.

(4) Liidu institutsioonid, organid ja asutused on atraktiivsed sihtmärgid, keda ähvardavad heade erialaste oskuste ja korralike ressurssidega ohusubjektid, aga ka muud ohud. Samas on kübervastupidavuse tase ning pahatahtliku kübertegevuse avastamise ja sellele reageerimise võime nendes üksustes väga erinev. Seepärast on Euroopa

halduskorralduse toimimiseks vaja, et liidu institutsioonid, organid ja asutused saavutaksid küberturvalisuse ühtlaselt kõrge taseme küberturvalisuse baastasemega (ehk küberturvalisuse baaseeskirjadega, mida võrgu- ja infosüsteemid ning nende operaatorid ja kasutajad peaksid küberturvalisuse riskide minimeerimiseks järgima), ning teabevahetuse ja koostööga.

(5) Direktiiviga [küberturvalisuse 2. direktiivi ettepanek], mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, tahetakse veelgi parandada avaliku ja erasektori üksuste, riikide pädevate asutuste ja organite ning tervikuna kogu liidu küberturvalisuse alast vastupidavusvõimet ja intsidentidele reageerimise suutlikkust. Seepärast on vaja, et liidu institutsioonid, organid ja asutused järgiksid seda eeskuju ja tagaksid normid, mis on direktiiviga [küberturvalisuse 2. direktiivi ettepanek] kooskõlas ja mille eesmärgid on sama ambitsioonikad.

(6) Küberturvalisuse ühtlaselt kõrge taseme saavutamiseks on vaja, et iga liidu institutsioon, organ ja asutus kehtestaks sisemise küberturvalisuse alaste riskide juhtimise, haldamise ja kontrollimise raamistiku, mis tagab kõigi küberturvalisuse riskide tulemusliku ja aruka juhtimise ning võtab arvesse toimepidevust ja kriisijuhtimist.

(7) Erinevused liidu institutsioonide, organite ja asutuste vahel eeldavad paindlikku rakendamist, sest üks ja sama lahendus ei sobi kõigile. Küberturvalisuse ühtlaselt kõrge taseme tagamise meetmed ei tohiks sisaldada kohustusi, mis sekkuvad otseselt liidu institutsioonide, organite ja asutuste ülesannete täitmisse või piiravad nende institutsioonilist sõltumatust. Seega peaksid need institutsioonid, organid ja asutused kehtestama oma küberturvalisuse raamistikud küberturvalisuse alaste riskide juhtimise, haldamise ja kontrollimise jaoks ning võtma vastu oma baastaseme ja küberturvalisuse kavad.

(8) Vältimaks ebaproportsionaalse finants- ja halduskoormuse kehtestamist liidu institutsioonidele, organitele ja asutustele, peaksid küberturvalisuse riskide juhtimise nõuded olema proportsionaalsed asjaomase võrgu- ja infosüsteemi puhul esineva riskiga, võttes seejuures arvesse selliste meetmete kõrget tehnilist taset. Iga liidu institutsioon, organ ja asutus peaks püüdma eraldada oma IT-eelarvest piisava osa oma küberturvalisuse taseme tõstmiseks; pikemas perspektiivis tuleks eesmärgiks seada ligikaudu 10 %.

(9) Küberturvalisuse ühtlaselt kõrge taseme saavutamiseks peab küberturvalisus kuuluma iga liidu institutsiooni, organi ja asutuse kõrgeima juhtimistasandi järelevalve alla, kes peaks kiitma heaks küberturvalisuse baastaseme, mis peaks maandama iga institutsiooni, organi ja asutuse kehtestatava raamistiku kohaselt kindlaks tehtud riske. Tegelemine küberturvalisuse kultuuriga, st igapäevase küberturvalisusega, on kõigis liidu institutsioonides, organites ja asutustes küberturvalisuse baastaseme lahutamatu osa.

(10) Liidu institutsioonid, organid ja asutused peaksid hindama riske, mis tulenevad suhetest tarnijate ja teenuseosutajatega, sh andmetalletuse ja andmetöötlusteenuste pakkujate või hallatavate turbeteenuste pakkujatega, ning võtma asjakohaseid meetmeid nende riskide vähendamiseks. Need meetmed peaksid olema küberturvalisuse baastaseme osa ning neid tuleks CERT-EU välja antavates juhenddokumentides ja soovitustes täpsemalt kirjeldada. Meetmete ja suuniste kindlaksmääramisel tuleks nõuetekohaselt arvesse võtta asjakohaseid ELi õigusakte ja põhimõtteid, sh võrgu- ja infoturbe koostöörühma tehtud riskihindamisi ja soovitusi, näiteks ELi kooskõlastatud riskihindamine ja ELi meetmepakett 5G-võrkude

turvalisuse tagamiseks. Lisaks võiks nõuda asjaomaste IKT toodete, teenuste ja protsesside sertifitseerimist vastavalt konkreetsetele ELi küberturvalisuse sertifitseerimise kavadele, mis on võetud vastu määruse (EL) 2019/881 artikli 49 kohaselt.

(11) Liidu institutsioonide ja organite peasekretärid otsustasid mais 2011 luua liidu institutsioonide, organite ja asutuste infoturbeintsidentidega tegeleva rühma (CERT-EU) eelrühma, kelle tegevuse üle teostaks järelevalvet institutsioonidevaheline juhtnõukogu. Juulis 2012 kinnitasid peasekretärid praktilise korra ja leppisid kokku CERT-EU kui alalise üksuse toetamises, et aidata institutsioonidevahelise küberturvalisuse alase koostöö ühe selge näitena jätkuvalt parandada liidu institutsioonide, organite ja asutuste infotehnoloogia turvalisuse üldist taset. Septembris 2012 loodi Euroopa Komisjoni rakkerühmana institutsioonidevaheliste volitustega CERT-EU. Detsembris 2017 sõlmisid liidu institutsioonid, organid ja asutused institutsioonidevahelise kokkuleppe CERT-EU ülesehituse ja töökorralduse kohta[3]. Seda korda tuleks edasi arendada, et toetada määruse rakendamist.

(12) Kooskõlas sellega, kuidas liikmesriikides ja maailmas on paljud CERTid nimetatud ümber küberturvalisuse keskusteks, tuleks ära muuta CERT-EU nimi: ELi institutsioonide ja ametite „infoturbeintsidentidega tegelev rühm“ tuleks asendada „küberturvalisuse keskusega“, kuid alles peaks jääma selle nime tuntuks saanud lühivorm „CERT-EU“.

(13) Paljud küberründed on osa laiematest rünnakutest, mis on suunatud liidu institutsioonide, organite ja asutuste rühmade vastu või huviringkondade vastu, kuhu kuuluvad ka liidu institutsioonid, organid ja asutused. Ettevaatava tuvastamise, intsidentidele reageerimise ja leevendusmeetmete võimaldamiseks peaksid liidu institutsioonid, organid ja asutused teatama CERT-EU-le olulistest küberohtudest, olulistest nõrkustest ja olulistest intsidentidest ning jagama asjakohaseid tehnilisi üksikasju, et teistes liidu institutsioonides, organites ja asutustes oleks võimalik samalaadseid küberohte, nõrkusi ja intsidente tuvastada või leevendada ja neile reageerida. Järgides samasugust lähenemisviisi, nagu on visandatud direktiivis [küberturvalisuse 2. direktiivi ettepanek], peaks üksustel olema kohustus esitada CERT-EU-le esialgne teade 24 tunni jooksul pärast seda, kui nad saavad teada olulisest intsidendist. Selline teabevahetus peaks andma CERT-EU-le võimaluse levitada teavet teistele liidu institutsioonidele, organitele ja asutustele ning asjaomastele partneritele, et aidata kaitsta liidu IT-keskkondi ja liidu partnerite IT-keskkondi samalaadsete intsidentide, ohtude ja nõrkuste eest.

(14) Lisaks sellele, et CERT-EU-le antakse rohkem ülesandeid ja laiem tegevusulatus, tuleks luua institutsioonidevaheline küberturvalisuse nõukoda (IICB), mis peaks soodustama küberturvalisuse ühtlaselt kõrget taset liidu institutsioonides, organites ja asutustes sellega, et teeb seiret selle üle, kuidas liidu institutsioonid, organid ja asutused käesolevat määrust rakendavad, ja järelevalvet CERT-EU üldiste prioriteetide ja eesmärkide rakendamise üle ning tagab CERT-EU strateegilise juhtimise. IICB peaks tagama institutsioonide esindatuse ning kaasama organite ja asutuste esindajad läbi liidu asutuste võrgustiku.

(15) CERT-EU peaks toetama küberturvalisuse ühtlaselt kõrge taseme tagamise meetmete rakendamist IICB-le tehtavate ettepanekutega juhenddokumentide või soovituste kohta või üleskutsetega esitamisega. IICB peaks sellised juhenddokumendid ja soovitused

[3] ELT C 12, 13.1.2018, lk 1–11.

heaks kiitma. Vajaduse korral peaks CERT-EU esitama üleskutseid, milles kirjeldatakse kiireloomulisi turbemeetmeid, mida liidu institutsioonid, organid ja asutused peaksid võtma kindlaksmääratud aja jooksul.

(16) IICB peaks seirama nii käesoleva määruse järgimist kui ka juhenddokumentide ja soovituste ning CERT-EU esitatud üleskutsete järelmeetmeid. Tehnilistes küsimustes peaks IICB-d toetama tehnilised nõuanderühmad, mille koosseis vastab IICB äranägemisele ja mis peaksid tegema tihedat koostööd CERT-EU, liidu institutsioonide, organite ja asutuste ja muude sidusrühmadega, nagu parasjagu vajalik. Vajaduse korral peaks IICB avaldama mittesiduvaid hoiatusi ja soovitama auditeid.

(17) CERT-EU ülesanne peaks olema aidata kaasa kõigi liidu institutsioonide, organite ja asutuste IT-keskkonna turvalisusele. CERT-EU peaks tegutsema samaväärsena koordineerijaga, kes on liidu institutsioonidele, organitele ja asutustele määratud Euroopa nõrkuste registrile nõrkuste koordineeritud avalikustamise jaoks, nagu on osutatud direktiivi [küberturvalisuse 2. direktiivi ettepanek] artiklis 6.

(18) 2020. aastal püstitas CERT-EU juhtnõukogu uue strateegilise eesmärgi, et CERT-EU kindlustaks kõigi liidu institutsioonide, organite ja asutuste kõikehõlmava küberkaitse, mis oleks piisavalt ulatuslik ja põhjalik ning kohaneks pidevalt olemasolevate või tulevaste ohtudega, nagu ründed mobiilsete seadmete, pilvekeskkondade ja esemevõrgu seadmete vastu. Strateegiline eesmärk hõlmab ka laia tegevusulatusega turbekeskusi, mis tegelevad võrkude seirega ja tõsiste ohtude pideva seirega. CERT-EU peaks toetama suuremate liidu institutsioonide, organite ja asutuste IT-turbe meeskondi, sh esmatasandi pideva seirega. Väiksematele ja mõnedele keskmise suurusega liidu institutsioonidele, organitele ja asutustele peaks CERT-EU pakkuma kõiki teenuseid.

(19) Samuti peaks CERT-EU täitma rolli, mis on talle direktiiviga [küberturvalisuse 2. direktiivi ettepanek] ette nähtud küberturbe intsidentide lahendamise üksuste (CSIRTide) võrgustikuga tehtavas koostöös ja teabevahetuses. Ühtlasi peaks CERT-EU kooskõlas komisjoni soovitusega (EL) 2017/1584[4] tegema koostööd ja koordineerima reageerimist asjaomaste sidusrühmadega. Küberturvalisuse kõrge taseme saavutamiseks kogu liidus peaks CERT-EU jagama intsidentide kohta käivat teavet riiklike partneritega. Samuti peaks CERT-EU tegema koostööd muude avaliku ja erasektori partneritega, sh NATOs, kui IICB on selle eelnevalt heaks kiitnud.

(20) Operatiivse küberturvalisuse toetamisel peaks CERT-EU kasutama Euroopa Liidu Küberturvalisuse Ameti (ENISA) olemasolevaid oskusteadmisi struktureeritud koostöö kaudu, nagu on sätestatud Euroopa Parlamendi ja nõukogu määruses (EL) 2019/881[5]. Asjakohasel juhul tuleks kahe üksuse vahel kehtestada erikord, et määrata kindlaks sellise koostöö praktiline kulg ja vältida tegevuse dubleerimist. CERT-EU peaks tegema Euroopa Liidu Küberturvalisuse Ametiga ohuanalüüsi alast koostööd ning jagama ametiga regulaarselt oma ohtude kaardistamise aruannet.

---

4 Komisjoni 13. septembri 2017. aasta soovitus (EL) 2017/1584 koordineeritud reageerimise kohta ulatuslike küberturvalisuse intsidentide ja kriiside korral (ELT L 239, 19.9.2017, lk 36).

5 Euroopa Parlamendi ja nõukogu 17. aprilli 2019. aasta määrus (EL) 2019/881, mis käsitleb ENISAt (Euroopa Liidu Küberturvalisuse Amet) ning info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist ja millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 (küberturvalisuse määrus) (ELT L 151, 7.6.2019, lk 15).

(21) Toetamaks komisjoni 23. juuni 2021. aasta soovituse[6] kohaselt loodud ühist küberüksust, peaks CERT-EU tegema koostööd ja vahetama teavet sidusrühmadega, et edendada operatiivkoostööd ja võimaldada olemasolevatel võrgustikel realiseerida liidu kaitsmisel kogu oma potentsiaali.

(22) Käesoleva määruse alusel töödeldavaid isikuandmeid tuleks töödelda kooskõlas andmekaitsealaste õigusaktidega, kaasa arvatud Euroopa Parlamendi ja nõukogu määrusega (EL) 2018/1725[7].

(23) CERT-EU ning liidu institutsioonid, organid ja asutused peaksid teavet käitlema kooskõlas õigusnormidega, mis on sätestatud määruses [kavandatud infoturbemäärus]. Et tagada turvalisusküsimuste koordineerimine, tuleks komisjoni julgeolekudirektoraadile ja IICB juhatajale ilma põhjendamatu viivituseta teatada kõigist juhtudest, kui riikide julgeoleku- ja luureteenistused algatavad või taotlevad kontaktivõttu CERT-EUga.

(24) CERT-EU teenused ja ülesanded on kõigi liidu institutsioonide, organite ja asutuste huvides ning seega peaks iga IT-eelarvega liidu institutsioon, organ ja asutus andma nende teenuste ja ülesannete jaoks oma õiglase panuse. Selline panus ei piira liidu institutsioonide, organite ja asutuste eelarveautonoomiat.

(25) IICB peaks CERT-EU abiga läbi vaatama ja hindama käesoleva määruse rakendamist ja teatama oma järeldustest komisjonile. Sellele sisendile toetudes peaks komisjon esitama aruande Euroopa Parlamendile, nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ning Regioonide Komiteele,

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

I peatükk
ÜLDSÄTTED

Artikkel 1
Reguleerimisese

Käesolevas määruses sätestatakse:

(a) liidu institutsioonide, organite ja asutuste kohustused kehtestada sisemise küberturvalisuse alaste riskide juhtimise, haldamise ja kontrollimise raamistik,

(b) liidu institutsioonide, organite ja asutuste kohustused seoses küberturvalisuse riskide juhtimise ja neist teatamisega,

(c) liidu institutsioonide, organite ja asutuste küberturvalisuse keskuse (CERT-EU) töökorralduse ja toimimise ning institutsioonidevahelise küberturvalisuse nõukoja töökorralduse ja toimimise eeskirjad.

---

6 Komisjoni 23. juuni 2021. aasta soovitus C(2021) 4520 ühise küberüksuse loomise kohta.

7 Euroopa Parlamendi ja nõukogu 23. oktoobri 2018. aasta määrus (EL) 2018/1725, mis käsitleb füüsiliste isikute kaitset isikuandmete töötlemisel liidu institutsioonides, organites ja asutustes ning isikuandmete vaba liikumist, ning millega tunnistatakse kehtetuks määrus (EÜ) nr 45/2001 ja otsus nr 1247/2002/EÜ (ELT L 295, 21.11.2018, lk 39).

Artikkel 2

Kohaldamisala

Käesolevat määrust kohaldatakse kõigi liidu institutsioonide, organite ja asutuste küberturvalisuse riskide juhtimise, haldamise ja kontrollimise ning CERT-EU ja institutsioonidevahelise küberturvalisuse nõukoja töökorralduse ja toimimise suhtes.

Artikkel 3

Mõisted

Käesolevas määruses kasutatakse järgmisi mõisteid:

(1) „liidu institutsioonid, organid ja asutused“ – liidu institutsioonid, organid ja asutused, mis on loodud Euroopa Liidu lepingu, Euroopa Liidu toimimise lepingu või Euroopa Aatomienergiaühenduse asutamislepinguga või nende lepingute alusel;

(2) „võrgu- ja infosüsteem“ – võrgu- ja infosüsteem direktiivi [küberturvalisuse 2. direktiivi ettepanek] artikli 4 punkti 1 tähenduses;

(3) „võrgu- ja infosüsteemide turvalisus“ – võrgu- ja infosüsteemide turvalisus direktiivi [küberturvalisuse 2. direktiivi ettepanek] artikli 4 punkti 2 tähenduses;

(4) „küberturvalisus“ – küberturvalisus direktiivi [küberturvalisuse 2. direktiivi ettepanek] artikli 4 punkti 3 tähenduses;

(5) „kõrgeim juhtimistasand“ – halduslikult kõige kõrgema tasandi juht, juhtkond või koordineerimise ja järelevalvega tegelev organ, võttes arvesse iga liidu institutsiooni, organi või asutuse kõrgema taseme juhtimise korda;

(6) „intsident“ – intsident direktiivi [küberturvalisuse 2. direktiivi ettepanek] artikli 4 punkti 5 tähenduses;

(7) „oluline intsident“ – mis tahes intsident, v.a intsidendid, mille mõju on piiratud ja mille metoodika või tehnoloogia on tõenäoliselt juba hästi teada;

(8) „suur rünne“ – intsident, millega toimetulekuks on vaja rohkem ressursse, kui mõjutatud liidu institutsioonis, organis või asutused ja CERT-EUs kasutada on;

(9) „intsidendi käsitlemine“ – intsidendi käsitlemine direktiivi [küberturvalisuse 2. direktiivi ettepanek] artikli 4 punkti 6 tähenduses;

(10) „küberoht“ – küberoht määruse (EL) 2019/881 artikli 2 punkti 8 tähenduses;

(11) „oluline küberoht“ – küberoht, millel eesmärk on põhjustada oluline intsident või millel on võimalus ja suutlikkus põhjustada oluline intsident;

(12) „nõrkus“ – nõrkus direktiivi [küberturvalisuse 2. direktiivi ettepanek] artikli 4 punkti 8 tähenduses;

(13) „oluline nõrkus“ – nõrkus, mille ärakasutamine põhjustab tõenäoliselt olulise intsidendi;

(14) „küberturvalisuse risk“ – mõistlikult tuvastatav asjaolu või sündmus, mis võib kahjustada võrgu- ja infosüsteemide turvalisust;

(15) „ühine küberüksus“ – liidu erinevate küberturvalisuse kogukondade jaoks tegutsev virtuaalne ja füüsiline koostööplatvorm, milles keskendutakse operatiivsele ja tehnilisele koordineerimisele, et tulla toime oluliste piiriüleste küberohtude ja intsidentidega komisjoni 23. juuni 2021. aasta soovituse tähenduses;

(16) „küberturvalisuse baastase“ – küberturvalisuse normide miinimumpakett, mida võrgu- ja infosüsteemid ning nende operaatorid ja kasutajad peavad järgima, et viia küberturvalisuse riskid miinimumi.

II peatükk
MEETMED KÜBERTURVALISUSE ÜHTLASELT KÕRGE TASEME TAGAMISEKS

Artikkel 4

Riskide juhtimine, haldamine ja kontrollimine

1. Iga liidu institutsioon, organ ja asutus kehtestab oma sisemise küberturvalisuse alaste riskide juhtimise, haldamise ja kontrollimise raamistiku (edaspidi „raamistik“), mis toetab üksuse missiooni ja selle institutsionaalset sõltumatust. Selle töö eest vastutab üksuse kõrgeim juhtimistasand, et tagada kõigi küberturvalisuse riskide tulemuslik ja usaldusväärne juhtimine. Raamistik tuleb kehtestada hiljemalt ... [15 kuud pärast käesoleva määruse jõustumist].

2. Raamistik peab hõlmama asjaomase institutsiooni, organi või asutuse kogu IT-keskkonda, sh ruumides kohapeal olev IT-keskkond, hanke korras sisse ostetavad varad ja teenused, mis asuvad pilvandmetöötluse keskkondades või mida majutavad kolmandad isikud, mobiilseadmed, ettevõttevõrgud, internetiga ühendamata koondisevõrgud ja mistahes seadmed, mis on ühendatud IT-keskkonnaga. Raamistik võtab arvesse toimepidevust ja kriisijuhtimist ning peab silmas tarneahela turvalisust ja selliste inimriskide juhtimist, mis võivad mõjutada mõjutatud liidu institutsioonide, organite ja asutuste küberturvalisust.

3. Iga liidu institutsiooni, organi ja asutuse kõrgeim juhtimistasand tegeleb järelevalvega selle üle, kuidas tema organisatsioon täidab küberturvalisuse riskide juhtimise, haldamise ja kontrollimisega seotud kohustusi, ilma et see piiraks muude juhtimistasandite ametlikke kohustusi nõuete täitmisel ja riskijuhtimisel oma vastutusalas.

4. Igas liidu institutsioonis, organis ja asutuses peavad olema toimivad mehhanismid, mis tagavad, et küberturvalisusele kulutatakse piisav osa IT-eelarvest.

5. Iga liidu institutsioon, organ ja asutus nimetab ametisse kohaliku küberturvalisuse ametniku või samaväärse ametikoha täitja, kes on kõigis küberturvalisuse aspektides ühtne kontaktpunkt.

Artikkel 5

Küberturvalisuse baastase

1. Iga liidu institutsiooni, organi ja asutuse kõrgeim juhtimistasand kiidab heaks üksuse enda küberturvalisuse baastaseme, et vähendada artikli 4 lõikes 1 osutatud raamistiku kohaselt kindlaks tehtud riske. Ta teeb seda oma missiooni toetamiseks ja institutsioonilise sõltumatuse teostamiseks. Küberturvalisuse baastase tuleb kehtestada hiljemalt ... [18 kuud pärast käesoleva määruse jõustumist] ning selles tuleb käsitleda I lisas loetletud valdkondi ja II lisas loetletud meetmeid.

2. Iga liidu institutsiooni, organi ja asutuse kõrgem juhtkond osaleb regulaarselt spetsiaalsetel koolitustel, et omandada piisavad teadmised ja oskused, et mõista ja hinnata küberturvalisuse riske ja riskide juhtimistavasid ning nende mõju organisatsiooni tegevusele.

Artikkel 6

Küpsustaseme hindamine

Iga liidu institutsioon, organ ja asutus hindab küberturvalisuse küpsuse taset vähemalt iga kolme aasta järel, kattes kõik IT-keskkonna elemendid, nagu on kirjeldatud artiklis 4, ja võttes arvesse asjaomaseid juhenddokumente ja soovitusi, mis on vastu võetud kooskõlas artikliga 13.

Artikkel 7

Küberturvalisuse kavad

1. Lähtudes küpsustaseme hindamise põhjal tehtud järeldustest ning võttes arvesse artikli 4 kohaselt kindlaks tehtud varasid ja riske, kiidab iga liidu institutsiooni, organi ja asutuse kõrgeim juhtimistasand pärast riskide juhtimise, haldamise ja kontrollimise raamistiku ja küberturvalisuse baastaseme kehtestamist ilma põhjendamatult viivitamata heaks küberturvalisuse kava. Kava eesmärk on suurendada asjaomase üksuse üldist küberturvalisust ja aidata seeläbi saavutada küberturvalisuse ühtlaselt kõrge tase liidu institutsioonides, organites ja asutustes või seda parandada. Selleks et toetada üksuse ülesannete täitmist institutsionaalse sõltumatuse alusel, sisaldab kava vähemalt I lisas loetletud valdkondi, II lisas loetletud meetmeid ning meetmeid, mis on seotud intsidentideks valmisoleku, intsidentidele reageerimise ja neist taastumisega, näiteks turvaseire ja logimine. Kava vaadatakse läbi vähemalt iga kolme aasta järel pärast artikli 6 kohaselt tehtud küpsustaseme hindamist.
2. Küberturvalisuse kavas kirjeldatakse, millised on töötajate ülesanded ja kohustused kava rakendamisel.
3. Küberturvalisuse kava arvestab muude kohaldatavate CERT-EU välja antud juhenddokumentide ja soovitustega.

Artikkel 8

Rakendamine

1. Kui küpsustaseme hindamine on lõpetatud, esitavad liidu institutsioonid, organid ja asutused nende tulemused institutsioonidevahelisele küberturvalisuse nõukojale. Kui turbekavad on valmis, teatavad liidu institutsioonid, organid ja asutused sellest institutsioonidevahelisele küberturvalisuse nõukojale. Nõukoja taotluse korral annavad nad aru käesoleva peatüki konkreetsete aspektide kohta.
2. Artikli 13 kohaselt välja antud juhenddokumendid ja soovitused toetavad käesoleva peatüki sätete rakendamist.

III PEATÜKK
INSTITUTSIOONIDEVAHELINE KÜBERTURVALISUSE NÕUKODA

Artikkel 9

Institutsioonidevaheline küberturvalisuse nõukoda

1. Luuakse institutsioonidevaheline küberturvalisuse nõukoda (IICB).
2. IICB ülesanded on järgmised:

(a) teha seiret selle üle, kuidas liidu institutsioonid, organid ja asutused käesolevat määrust rakendavad;

(b) teha järelevalvet CERT-EU üldiste prioriteetide ja eesmärkide rakendamise üle ning tagada CERT-EU strateegiline juhtimine.

3. IICBsse kuuluvad kolm esindajat, kelle nimetab liidu asutuste võrgustik (EUAN) oma IKT nõuandekomitee ettepanekul ja kes esindavad ise oma IT-keskkonda haldavate organite ja asutuste huve, ning üks esindaja, kes määratakse igast järgmisest organisatsioonist:

(a) Euroopa Parlament;

(b) Euroopa Liidu Nõukogu;

(c) Euroopa Komisjon;

(d) Euroopa Liidu Kohus;

(e) Euroopa Keskpank;

(f) Euroopa Kontrollikoda;

(g) Euroopa välisteenistus;

(h) Euroopa Majandus- ja Sotsiaalkomitee;

(i) Euroopa Regioonide Komitee;

(j) Euroopa Investeerimispank;

(k) Euroopa Liidu Küberturvalisuse Amet.

Liikmeid võivad abistada asendusliikmed. Juhataja võib IICB koosolekutele osalema kutsuda eespool loetletud organisatsioonide või muude liidu institutsioonide, organite ja asutuste muid esindajaid, kuid neil ei ole hääleõigust.

4. IICB võtab vastu kodukorra.

5. IICB määrab kooskõlas kodukorraga oma liikmete hulgast juhataja neljaks aastaks. Juhataja asendusliikmest saab samaks ajavahemikuks IICB täisliige.

6. IICB tuleb kokku juhataja algatusel, CERT-EU taotluse korral või mõne oma liikme taotluse korral.

7. Igal IICB liikmel on üks hääl. IICB otsused tehakse lihthäälteenamusega, kui käesolevas määruses ei ole sätestatud teisiti. Juhataja ei hääleta, välja arvatud häälte võrdse jagunemise korral, kui ta võib anda otsustava hääle.

8. IICB võib tegutseda lihtsustatud kirjaliku menetluse korras, mis algatatakse vastavalt IICB kodukorrale. Selle menetluse kohaselt loetakse asjaomane otsus juhataja määratud aja jooksul heakskiidetuks, kui mõni liige ei esita vastuväiteid.

9. CERT-EU juht või tema asendusliige osaleb IICB koosolekutel, kui IICB ei otsusta teisiti.

10. IICB sekretariaaditeenused tagab komisjon.

11. IKT nõuandekomitee ettepanekul liidu asutuste võrgustiku poolt nimetatud esindajad edastavad IICB otsused liidu asutustele ja ühisettevõtetele. Igal liidu organil ja asutusel on õigus esitada IICB esindajatele või juhatajale mistahes küsimus, mis tema arvates peaks pälvima IICB tähelepanu.

12. IICB võib tegutseda esimehe algatatud lihtsustatud kirjaliku menetluse korras, mille kohaselt loetakse asjaomane otsus juhataja määratud aja jooksul heakskiidetuks, kui mõni liige ei esita vastuväiteid.

13. IICB võib nimetada täitevkomitee, mis aitaks teda tema töös, ning delegeerida sellele osa oma ülesandeid ja volitusi. IICB kehtestab täitevkomitee kodukorra, kaasa arvatud selle ülesanded ja õigused, ning selle liikmete ametiaja pikkuse.

Artikkel 10
IICB ülesanded

Oma kohustusi täites teeb IICB eeskätt järgmist:

(a) vaatab läbi kõik CERT-EU-lt nõutud aruanded selle kohta, kuidas liidu institutsioonid, organid ja asutused käesolevat määrust on rakendanud;

(b) kiidab CERT-EU juhi ettepaneku põhjal heaks CERT-EU iga-aastase tööprogrammi ja jälgib selle rakendamist;

(c) kiidab CERT-EU juhi ettepaneku põhjal heaks CERT-EU teenuste kataloogi;

(d) kiidab CERT-EU juhi esitatud ettepaneku põhjal heaks CERT-EU tegevuse tulude ja kulude finantskalkulatsiooni, sh seoses personaliga;

(e) kiidab CERT-EU juhi ettepaneku põhjal heaks CERT-EU teenustaseme kokkulepete tingimused;

(f) vaatab läbi ja kiidab heaks CERT-EU juhi koostatud iga-aastase aruande, milles käsitletakse CERT-EU tegevust ja vahendite haldamist;

(g) kiidab heaks CERT-EU juhi ettepaneku põhjal kindlaks määratud CERT-EU põhilised tulemusnäitajad ja jälgib neid;

(h) kiidab heaks CERT-EU ja muude üksuste vahelised artikli 17 kohased koostöökokkulepped, teenustaseme kokkulepped või lepingud;

(i) loob nii palju tehnilisi nõuanderühmi kui vaja, et abistada IICB-d tema töös, kiidab heaks nende pädevuse ja määrab nende juhatajad.

Artikkel 11
Nõuete järgimine

IICB jälgib, kuidas liidu institutsioonid, organid ja asutused rakendavad käesolevat määrust ning vastuvõetud juhenddokumente, soovitusi ja üleskutseid. Kui IICB leiab, et liidu institutsioonid, organid või asutused ei ole käesolevat määrust või käesoleva määruse alusel välja antud juhenddokumente, soovitusi ja üleskutseid tulemuslikult rakendanud, võib ta teha järgmist, ilma et see piiraks asjaomase liidu institutsiooni, organi või asutuse sisemenetlusi:

(a) esitada hoiatuse; kui see on mõjuva küberturvalisuse riski tõttu vajalik, esitatakse hoiatus asjakohaselt piiratud sihtrühmale;

(b) soovitada auditi tegemiseks sobivat audiitorit.

IV peatükk
CERT-EU

Artikkel 12
CERT-EU missioon ja ülesanded

1. CERT-EU ehk kõigi liidu institutsioonide, organite ja asutuste sõltumatu institutsioonidevahelise küberturvalisuse keskuse ülesanne on aidata kaasa kõigi liidu institutsioonide, organite ja asutuste salastamata IT-keskkonna turvalisusele, andes neile küberturvalisuse alast nõu, aidates neil intsidente ära hoida, tuvastada ja leevendada ja intsidentidele reageerida ning tegutsedes nende küberturvalisuse alase teabevahetuse ja intsidentidele reageerimise koordineerimise keskusena.

2. CERT-EU täidab liidu institutsioonide, organite ja asutuste jaoks järgmisi ülesandeid:

   (a) toetab neid käesoleva määruse rakendamisel ja aitab käeoleva määruse kohaldamist koordineerida artikli 13 lõikes 1 loetletud meetmetega või IICB nõutud *ad hoc* aruannetega;

   (b) toetab neid teenustekataloogis kirjeldatud küberturvalisuse teenuste paketiga („baasteenused“);

   (c) hoiab alal samalaadsete organisatsioonide ja partnerite võrgustikku, et toetada teenuseid, nagu on kirjeldatud artiklites 16 ja 17;

   (d) juhib IICB tähelepanu teemadele, mis on seotud käesoleva määruse rakendamisega ning juhenddokumentide, soovituste ja üleskutsete rakendamisega;

   (e) annab aru liidu institutsioone, organeid ja asutusi ähvardavatest küberohtudest ning aitab kaasa ELi küberolukorrateadlikkusele.

3. CERT-EU toetab komisjoni 23. juuni 2021. aasta soovituse kohaselt loodud ühist küberüksust muuhulgas järgmistes valdkondades:

   (a) valmisolek, intsidentide koordineerimine, teabevahetus ja kriisidele reageerimine tehnilisel tasandil liidu institutsioonide, organite ja asutustega seotud juhtumite puhul;

   (b) operatiivkoostöö seoses küberturbe intsidentide lahendamise üksuste (CSIRTid) võrgustikuga (k.a vastastikuse abi valdkonnas) ja laiema küberturbekogukonnaga;

   (c) küberohuteadmus, sh olukorrateadlikkus;

   (d) kõik teemad, milleks on vaja CERT-EU tehnilist küberturvalisuse alast oskusteavet.

4. CERT-EU teeb Euroopa Liidu Küberturvalisuse Ametiga struktureeritud koostööd suutlikkuse suurendamise, operatiivkoostöö ja küberohtude pikaajalise strateegilise analüüsi vallas kooskõlas Euroopa Parlamendi ja nõukogu määrusega (EL) 2019/881.

5. CERT-EU võib pakkuda järgmisi teenuseid, mida ei ole kirjeldatud tema teenuste kataloogis („tasulised teenused“):

(a) teenused, mis toetavad liidu institutsioonide, organite ja asutuste IT-keskkonna küberturvalisust ja mida ei ole nimetatud lõikes 2, teenustaseme kokkulepete põhjal ja vastavalt kasutatavate ressursside olemasolule;

(b) teenused, mis toetavad liidu institutsioonide, organite ja asutuste küberturvalisuse toiminguid või projekte, välja arvatud nende IT-keskkonna kaitsmiseks mõeldud teenused, kirjaliku lepingu põhjal ja IICB eelneval heakskiidul;

(c) teenused, mis toetavad selliste organisatsioonide IT-keskkonna turvalisust, mis ei ole liidu institutsioonid, organid ja asutused, kuid teevad liidu institutsioonide, organite ja asutustega tihedat koostööd, näiteks kui neile on liidu õiguse alusel määratud ülesandeid või kohustusi, kirjaliku lepingu põhjal ja IICB eelneval heakskiidul.

6. CERT-EU võib korraldada küberturvalisuse õppusi või soovitada osaleda olemasolevatel õppustel tihedas koostöös Euroopa Liidu Küberturvalisuse Ametiga alati, kui see on asjakohane, et kontrollida liidu institutsioonide, organite ja asutuste küberturvalisuse taset.

7. CERT-EU võib pakkuda liidu institutsioonidele, organitele ja asutustele abi salastatud IT-keskkondade intsidentide puhul, kui asjaomane asjaosaline seda temalt selgelt taotleb.

Artikkel 13

Juhenddokumendid, soovitused ja üleskutsed

1. CERT-EU toetab käesoleva määruse rakendamist sellega, et annab välja järgmisi dokumente:

(a) üleskutsed, milles kirjeldatakse kiireloomulisi turbemeetmeid, mida liidu institutsioonid, organid ja asutused peaksid võtma kindlaksmääratud aja jooksul;

(b) ettepanekud IICB-le juhenddokumentide kohta, mis on adresseeritud kõigile liidu institutsioonidele, organitele ja asutustele või mõnedele nende hulgast;

(c) ettepanekud IICB-le soovituste kohta, mis on adresseeritud üksikutele liidu institutsioonidele, organitele või asutustele.

2. Juhenddokumendid ja soovitused võivad sisaldada:

(a) küberturvalisuse riskide juhtimise ja küberturvalisuse baastaseme üksikasjad või parendused;

(b) küpsustaseme hindamise ja küberturvalisuse kavade üksikasjad ning

(c) kui see on asjakohane, ühise tehnoloogia, arhitektuuri ja nendega seotud heade tavade kasutamine, et saavutada koostalitlusvõime ja ühised standardid direktiivi [küberturvalisuse 2. direktiivi ettepanek] artikli 4 lõike 10 tähenduses.

3. IICB võib CERT-EU ettepanekul võtta vastu juhenddokumente või soovitusi.

4. IICB võib anda CERT-EU-le korralduse esitada juhenddokumentide või soovituste ettepanekuid või üleskutseid või need tagasi võtta või neid muuta.

Artikkel 14

CERT-EU juht

CERT-EU juht esitab IICB-le ja IICB juhatajale korrapäraselt aruandeid CERT-EU tegevuse, finantsplaneerimise, tulude, eelarve rakendamise, teenustaseme kokkulepete ja sõlmitud kirjalike lepingute, vastaspoolte ja partneritega tehtava koostöö ning töötajate lähetuste kohta, sh artikli 10 lõikes 1 osutatud aruandeid.

Artikkel 15

Personali- ja finantsküsimused

1. Pärast IICB ühehäälse heakskiidu saamist nimetab komisjon ametisse CERT-EU juhi. Enne CERT-EU juhi ametisse nimetamist konsulteeritakse IICBga kõigis menetluse etappides, eeskätt töökuulutuste koostamise, avalduste läbivaatamise ja selle ametikohaga seotud valikukomisjonide ametisse nimetamise käigus.

2. Haldus- ja finantsmenetluste kohaldamisel tegutseb CERT-EU juht komisjoni alluvuses.

3. CERT-EU ülesandeid ja tegevusi, sh teenuseid, mida CERT-EU osutab artikli 12 lõigete 2, 3, 4 ja 6 ning artikli 13 lõike 1 alusel liidu institutsioonidele, organitele ja asutustele, mille tegevust rahastatakse mitmeaastase finantsraamistiku rubriigist „Euroopa avalik haldus“, rahastatakse komisjoni eelarve eraldi eelarverealt. CERT-EU-le ettenähtud ametikohti täpsustatakse komisjoni ametikohtade loetelu joonealuses märkuses.

4. Liidu institutsioonid, organid ja asutused, kellele ei ole lõikes 3 viidatud, teevad CERT-EU-le igal aastal rahalise eraldise teenuste eest, mida CERT-EU osutab vastavalt nimetatud lõikele 3. Vastavad eraldised põhinevad orientiiridel, mille on andnud IICB ja milles iga üksus ja CERT-EU on kokku leppinud teenustaseme kokkulepetes. Eraldised peavad moodustama õiglase ja proportsionaalse osa osutatud teenuste kogukuludest. Need kantakse lõikes 3 osutatud eraldi eelarvereale sihtotstarbelise tuluna vastavalt Euroopa Parlamendi ja nõukogu määruse (EL, Euratom) 2018/1046[8] artikli 21 lõike 3 punktile c.

5. Artikli 12 lõikes 5 määratletud ülesannetega seotud kulud katavad liidu institutsioonid, organid ja asutused, kes CERT-EU teenuseid tarbivad. Tulu kantakse eelarvereale, millelt kulusid kaetakse.

Artikkel 16

CERT-EU koostöö liikmesriikide samalaadsete asutustega

1. CERT-EU teeb liikmesriikide samalaadsete asutustega, sh CERTidega, riikide küberturvalisuse keskustega, CSIRTidega ja direktiivi [küberturvalisuse 2. direktiivi ettepanek] artiklis 8 osutatud ühtsete kontaktpunktidega koostööd ja vahetab teavet küsimustes, mis puudutavad küberohte, nõrkusi, intsidente ja võimalikke vastumeetmeid, ja kõiges, mis on asjakohane liidu institutsioonide, organite ja

[8] Euroopa Parlamendi ja nõukogu 18. juuli 2018. aasta määrus (EL, Euratom) 2018/1046, mis käsitleb liidu üldeelarve suhtes kohaldatavaid finantsreegleid ja millega muudetakse määrusi (EL) nr 1296/2013, (EL) nr 1301/2013, (EL) nr 1303/2013, (EL) nr 1304/2013, (EL) nr 1309/2013, (EL) nr 1316/2013, (EL) nr 223/2014, (EL) nr 283/2014 ja otsust nr 541/2014/EL ning tunnistatakse kehtetuks määrus (EL, Euratom) nr 966/2012 (ELT L 193, 30.7.2018, lk 1).

asutuste IT-keskkondade kaitse parandamiseks, sh direktiivi [küberturvalisuse 2. direktiivi ettepanek] artiklis 13 osutatud CSIRTide võrgustiku kaudu.

2. CERT-EU võib vahetada liikmesriikide samalaadsete asutustega teavet konkreetse intsidendi kohta, et hõlbustada samalaadsete küberohtude või intsidentide avastamist, ilma mõjutatud asjaosalise nõusolekuta. Sellist teavet, millest ilmneb küberturvalisuse intsidendi sihtmärgi identiteet, võib CERT-EU intsidendi kohta vahetada üksnes mõjutatud asjaosalise nõusolekul.

Artikkel 17
CERT-EU koostöö kolmandate riikide samalaadsete asutustega

1. CERT-EU võib teha töövahendite ja meetodite, nt tehnika, taktika, menetluste ja heade tavade, ning küberohtude ja nõrkuste alast koostööd kolmandate riikide samalaadsete asutustega, sh sektoripõhiste samalaadsete asutustega. CERT-EU taotleb IICB heakskiitu igasuguseks koostööks selliste samalaadsete asutustega, seda ka raamistikes, kus kolmandate riikide samalaadsed asutused teevad koostööd liikmesriikide samalaadsete asutustega.

2. CERT-EU võib teha koostööd muude partneritega, näiteks äriettevõtjate, rahvusvaheliste organisatsioonide, Euroopa Liidu väliste riiklike üksuste või üksikekspertidega, et koguda teavet üldiste või konkreetsete küberohtude, nõrkuste ja võimalike vastumeetmete kohta. Ulatuslikumaks koostööks selliste partneritega taotleb CERT-EU IICB eelnevat heakskiitu.

3. CERT-EU võib intsidendist mõjutatud asjaosalise nõusolekul esitada intsidendi kohta käivat teavet partneritele, kes võivad aidata seda intsidenti analüüsida.

V peatükk
KOOSTÖÖ- JA ARUANDEKOHUSTUSED

Artikkel 18
Teabe käitlemine

1. CERT-EU ning liidu institutsioonid, organid ja asutused järgivad ametisaladuse hoidmise kohustust kooskõlas Euroopa Liidu toimimise lepingu artikliga 339 või samaväärsete kohaldatavate raamistikega.

2. CERT-EU valduses olevatele dokumentidele üldsuse juurdepääsu taotluste suhtes kohaldatakse Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 1049/2001[9] sätteid, kaasa arvatud selle määruse kohast kohustust konsulteerida teiste liidu institutsioonide, organite ja asutustega alati, kui taotlus puudutab nende dokumente.

3. Käesoleva määruse alusel toimuva isikuandmete töötlemise suhtes kohaldatakse Euroopa Parlamendi ja nõukogu määrust (EL) 2018/1725.

4. CERT-EU ning temaga seotud liidu institutsioonid, organid ja asutused käitlevad teavet kooskõlas õigusnormidega, mis on sätestatud [kavandatud infoturbemääruses].

[9] Euroopa Parlamendi ja nõukogu 30. mai 2001. aasta määrus (EÜ) nr 1049/2001 üldsuse juurdepääsu kohta Euroopa Parlamendi, nõukogu ja komisjoni dokumentidele (EÜT L 145, 31.5.2001, lk 43).

5. Komisjoni julgeolekudirektoraadile ja IICB juhatajale tuleb põhjendamatute viivitusteta teatada kõigist juhtudest, kui riikide julgeoleku- ja luureteenistused algatavad või taotlevad kontaktivõttu CERT-EUga.

Artikkel 19
Jagamiskohustused

1. Et CERT-EU saaks koordineerida nõrkuste haldamist ja intsidentidele reageerimist, võib ta paluda liidu institutsioonidel, organitel ja asutustel esitada talle oma IT-süsteemide varade loendist teavet, mis on CERT-EU toetuse seisukohast asjakohane. Taotluse saanud institutsioon, organ või asutus edastab taotletud teabe ja kõik selle hilisemad ajakohastused põhjendamatu viivituseta.

2. Liidu institutsioonid, organid ja asutused esitavad CERT-EU taotluse peale CERT-EU-le põhjendamatu viivituseta digitaalse teabe, mis on tekkinud nende vastavate intsidentidega seotud elektrooniliste seadmete kasutamisel. CERT-EU võib täiendavalt selgitada, millist liiki digitaalset teavet tal on olukorrateadlikkuse ja intsidentidele reageerimise jaoks vaja.

3. Sellist teavet, millest ilmneb intsidendist mõjutatud liidu institutsiooni, organi või asutuse identiteet, võib CERT-EU intsidendi kohta vahetada üksnes selle üksuse nõusolekul. Sellist teavet, millest ilmneb küberturvalisuse intsidendi sihtmärgi identiteet, võib CERT-EU intsidendi kohta vahetada üksnes mõjutatud üksuse nõusolekul.

4. Jagamiskohustused ei laiene ELi salastatud teabele ega teabele, mille liidu institutsioon, organ või asutus on saanud liikmesriigi julgeoleku- või luureteenistuselt või õiguskaitseasutuselt selgesõnalisel tingimusel, et seda ei jagata CERT-EUga.

Artikkel 20
Teatamiskohustused

1. Kõik liidu institutsioonid, organid ja asutused esitavad CERT-EU-le esialgse teate oluliste küberohtude, oluliste nõrkuste ja oluliste intsidentide kohta ilma põhjendamatult viivitamata ja igal juhul hiljemalt 24 tunni jooksul pärast seda, kui on neist teada saanud.

   Nõuetekohaselt põhjendatud juhtudel ja kokkuleppel CERT-EUga võib asjaomane liidu institutsioon, organ või asutus kalduda kõrvale eelmises lõikes sätestatud tähtajast.

2. Liidu institutsioonid, organid ja asutused teatavad CERT-EU-le põhjendamatult viivitamata ka küberohtude, nõrkuste ja intsidentide asjakohased tehnilised üksikasjad, mis aitavad kaasa tuvastamisele, intsidentidele reageerimisele või leevendusmeetmetele. Teatatakse järgmistest asjaoludest, kui see teave on olemas:

   (a) asjakohased turvarikke indikaatorid;

   (b) asjakohased tuvastamismehhanismid;

   (c) võimalik mõju;

   (d) asjakohased leevendusmeetmed.

3. CERT-EU esitab ENISA-le kord kuus koondaruande, mis sisaldab anonüümitud ja koondatud andmeid oluliste küberohtude, oluliste nõrkuste ja oluliste intsidentide kohta, millest on teatatud vastavalt lõikele 1.

4. IICB võib anda välja juhenddokumente või soovitusi teadete esitamise korra ja sisu kohta. CERT-EU levitab asjakohaseid tehnilisi üksikasju, et liidu institutsioonid, organid ja asutused saaksid tegeleda ennetava avastamise, intsidentidele reageerimise või leevendusmeetmetega.

5. Teatamiskohustused ei laiene ELi salastatud teabele ega teabele, mille liidu institutsioon, organ või asutus on saanud liikmesriigi julgeoleku- või luureteenistuselt või õiguskaitseasutuselt selgesõnalisel tingimusel, et seda ei jagata CERT-EUga.

Artikkel 21

Intsidentidele reageerimise koordineerimine ja koostöö oluliste intsidentide korral

1. Küberturvalisuse alase teabevahetuse ja intsidentidele reageerimise koordineerimise keskusena hõlbustab CERT-EU küberohtude, nõrkuste ja intsidentidega seotud teabevahetust järgmiste isikute vahel:

   (a) liidu institutsioonid, organid ja asutused;

   (b) artiklites 16 ja 17 osutatud samalaadsed asutused.

2. CERT-EU hõlbustab intsidentidele reageerimise alast koordineerimist liidu institutsioonide, organite ja asutuste vahel, sh:

   (a) panustamist järjepidevasse välissuhtlusesse;

   (b) vastastikust abi;

   (c) operatiivressursside optimaalset kasutamist;

   (d) koordineerimist muude kriisidele reageerimise mehhanismidega liidu tasandil.

3. CERT-EU toetab liidu institutsioone, organeid ja asutusi küberohtude, nõrkuste ja intsidentide alase olukorrateadlikkuse vallas.

4. IICB annab välja juhendid intsidentidele reageerimise koordineerimise ja koostöö kohta oluliste intsidentide korral. Kui kahtlustatakse, et intsident on kuritegelik, annab CERT-EU nõu selle kohta, kuidas teatada intsidendist õiguskaitseasutustele.

Artikkel 22

Suured ründed

1. CERT-EU koordineerib suurtele rünnetele reageerimist liidu institutsioonide, organite ja asutuste vahel. CERT-EU peab loendit tehnilistest eksperditeadmistest, mida oleks vaja selliste rünnete korral intsidentidele reageerimiseks.

2. Liidu institutsioonid, organid ja asutused annavad oma panuse sellesse tehniliste eksperditeadmiste loendisse ning esitavad igal aastal ajakohastatava loetelu oma vastavates organisatsioonides tegutsevatest ekspertidest, märkides ära nende konkreetsed tehnilised oskused.

3. Asjaomaste liidu institutsioonide, organite ja asutuste nõusolekul võib CERT-EU pöörduda lõikes 2 osutatud loetelus nimetatud ekspertide poole ka selleks, et aidata

reageerida suurele ründele mõnes liikmesriigis kooskõlas ühise küberüksuse töökorraga.

VI peatükk
LÕPPSÄTTED

Artikkel 23
Eelarve esialgne ümberjaotamine

Komisjon teeb ettepaneku asjaomaste liidu institutsioonide, organite ja asutuste personali ja rahaliste vahendite ümberpaigutamiseks komisjoni eelarvesse. Ümberjaotamine jõustub samal ajal kui esimene pärast käesoleva määruse jõustumist vastu võetud eelarve.

Artikkel 24
Läbivaatamine

1. IICB esitab CERT-EU abiga komisjonile regulaarselt aruandeid käesoleva määruse rakendamise kohta. Samuti võib IICB anda komisjonile soovituse teha ettepaneku muuta käesolevat määrust.
2. Komisjon esitab Euroopa Parlamendile ja nõukogule aruande käesoleva määruse rakendamise kohta hiljemalt 48 kuud pärast määruse jõustumist ja seejärel iga kolme aasta tagant.
3. Komisjon hindab määruse toimimist ning esitab Euroopa Parlamendile, nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ja Regioonide Komiteele aruande mitte varem kui viis aastat pärast määruse jõustumist.

Artikkel 25
Jõustumine

Käesolev määrus jõustub kahekümnendal päeval pärast selle avaldamist *Euroopa Liidu Teatajas*.

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Brüssel,

Euroopa Parlamendi nimel	*Nõukogu nimel*
president	*eesistuja*

FINANTSSELGITUS

1. ETTEPANEKU/ALGATUSE RAAMISTIK

1.1. Ettepaneku/algatuse nimetus

1.2. Asjaomased poliitikavaldkonnad

1.3. Ettepanek/algatus käsitleb

1.4. Eesmärgid

1.4.1. Üldeesmärgid

1.4.2. Erieesmärgid

1.4.3. Oodatavad tulemused ja mõju

1.4.4. Tulemusnäitajad

1.5. Ettepaneku/algatuse põhjendused

1.5.1. Lühi- või pikaajalises perspektiivis täidetavad vajadused, sealhulgas algatuse rakendamise üksikasjalik ajakava

1.5.2. ELi meetme lisaväärtus (see võib tuleneda eri teguritest, nagu kooskõlastamisest saadav kasu, õiguskindlus, suurem tõhusus või vastastikune täiendavus). Käesoleva punkti kohaldamisel tähendab „ELi meetme lisaväärtus“ väärtust, mis tuleneb liidu sekkumisest ja lisandub väärtusele, mille liikmesriigid oleksid muidu üksi loonud.

1.5.3. Samalaadsetest kogemustest saadud õppetunnid

1.5.4. Kooskõla mitmeaastase finantsraamistikuga ja võimalik koostoime muude asjaomaste meetmetega

1.5.5. Erinevate kasutada olevate rahastamisvõimaluste, sealhulgas vahendite ümberpaigutamise võimaluste hinnang

1.6. Ettepaneku/algatuse kestus ja finantsmõju

1.7. Ettenähtud eelarve täitmise viisid

2. HALDUSMEETMED

2.1. Järelevalve ja aruandluse eeskirjad

2.2. Haldus- ja kontrollisüsteem(id)

2.2.1. Eelarve täitmise viisi(de), rahastamise rakendamise mehhanismi(de), maksete tegemise korra ja kavandatava kontrollistrateegia selgitus

2.2.2. Teave kindlakstehtud riskide ja nende vähendamiseks kasutusele võetud sisekontrollisüsteemi(de) kohta

2.2.3. Kontrollide kulutõhususe (kontrollikulude suhe hallatavate vahendite väärtusse) hinnang ja põhjendus ning prognoositav veariski tase (maksete tegemise ja sulgemise ajal).

2.3. Pettuse ja eeskirjade eiramise ärahoidmise meetmed

3. ETTEPANEKU/ALGATUSE HINNANGULINE FINANTSMÕJU

3.1. Mitmeaastase finantsraamistiku rubriigid ja kulude eelarveread, millele mõju avaldub

3.2. Ettepaneku hinnanguline finantsmõju assigneeringutele

3.2.1. Hinnanguline mõju tegevusassigneeringutele – ülevaade

3.2.2. Tegevusassigneeringutest rahastatav väljund (hinnang)

3.2.3. Hinnanguline mõju haldusassigneeringutele – ülevaade

3.2.4. Kooskõla kehtiva mitmeaastase finantsraamistikuga

3.2.5. Kolmandate isikute rahaline osalus

3.3. Hinnanguline mõju tuludele

FINANTSSELGITUS

1. ETTEPANEKU/ALGATUSE RAAMISTIK

1.1. Ettepaneku/algatuse nimetus

Ettepanek: Euroopa Parlamendi ja nõukogu määrus, milles sätestatakse meetmed küberturvalisuse ühtlaselt kõrge taseme tagamiseks liidu institutsioonides, organites ja asutustes

1.2. Asjaomased poliitikavaldkonnad

Euroopa avalik haldus

Ettepanek käsitleb meetmeid, millega tagatakse küberturvalisuse ühtlaselt kõrge tase liidu institutsioonides, organites ja asutustes

1.3. Ettepanek/algatus käsitleb

☑ **uut meedet**

☐ **uut meedet, mis tuleneb katseprojektist / ettevalmistavast meetmest**[10]

☐ **olemasoleva meetme pikendamist**

☑ **ühe või mitme meetme ümbersuunamist teise või uude meetmesse või ühendamist teise või uue meetmega**

1.4. Eesmärgid

1.4.1. Üldeesmärgid

– Luua raamistik küberturvalisuse ühtlaselt kõrge taseme tagamiseks liidu institutsioonides, organites ja asutustes

– Sätestada CERT-EU uus õiguslik alus, et suurendada tema volitusi ja rahastamist

1.4.2. Erieesmärgid

(1) Sätestada liidu institutsioonide, organite ja asutuste kohustus luua küberriskide sisejuhtimise, -haldamise ja -kontrolli raamistik

(2) Sätestada liidu institutsioonide, organite ja asutuste kohustus anda aru oma küberriskide sisejuhtimise, -haldamise ja -kontrolli raamistiku kohta ning teatada küberturvalisuse intsidentidest

(3) Sätestada liidu institutsioonide, organite ja asutuste küberturvalisuse keskuseks oleva ELi institutsioonide ja ametite infoturbeintsidentidega tegeleva rühma (CERT-EU) ning institutsioonidevahelise küberturvalisuse nõukogu (IICB) töökorralduse ja toimimise eeskirjad

(4) Toetada ühise küberüksuse tegevust

1.4.3. Oodatavad tulemused ja mõju

Märkige, milline peaks olema ettepaneku/algatuse oodatav mõju toetusesaajatele/sihtrühmale.

[10] Vastavalt finantsmääruse artikli 58 lõike 2 punktile a või b.

– Liidu institutsioonide, organite ja asutuste küberriskide sisejuhtimise, -haldamise ja -kontrolli raamistikud, küberturvalisuse ühtsed alamstandardid, korrapärased küpsuse hindamised ja küberturvalisuse kavad – Liidu institutsioonide, organite ja asutuste küberturvalisusalase vastupidavusvõime ja intsidentidele reageerimise suutlikkuse suurendamine – CERT-EU ajakohastamine – Ühise küberüksuse tegevuse toetamine

1.4.4. Tulemusnäitajad

Märkige, milliste näitajate abil jälgitakse edusamme ja saavutusi.

– Liidu institutsioonide, organite ja asutuste kehtestatud raamistikud ja ühtsed alamstandardid ning nende ellu viidud korrapärased küpsuse hindamised ja küberturvalisuse kavad – Intsidentide parem lahendamine – Liidu institutsioonide, organite ja asutuste kõrgema juhtkonna suurem teadlikkus küberriskidest – IKT turvalisusega seotud kulutuste (mida väljendatakse protsendina kõigist IKT valdkonda tehtavatest kulutustest) ühtlustumine – Institutsioonidevahelise küberturvalisuse nõukogu ja CERT-EU kindlakäeline juhtimine – Ulatuslikum teabevahetus liidu institutsioonide, organite ja asutuste vahel ning asjakohaste organite ja sidusrühmadega ELis – CERT-EU ja ENISA kaudu toimuv ulatuslikum küberturvalisusalane koostöö asjakohaste organite ja sidusrühmadega ELis

1.5. Ettepaneku/algatuse põhjendused

1.5.1. Lühi- või pikaajalises perspektiivis täidetavad vajadused, sealhulgas algatuse rakendamise üksikasjalik ajakava

Ettepaneku eesmärk on suurendada liidu institutsioonide, organite ja asutuste kübervastupidavusvõimet, vähendada nende üksuste vastupidavuse taseme ebaühtlust ning suurendada ühist olukorrateadlikkust, ühist valmisolekut ja ühist reageerimissuutlikkust. Ettepanek on täielikult kooskõlas muude seotud algatustega, eelkõige ettepanekuga võtta vastu direktiiv, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega tunnistatakse kehtetuks direktiiv 2016/1148 (küberturvalisuse 2. direktiivi ettepanek). Ettepanek on oluline osa ELi julgeolekuliidu strateegiast ja ELi küberturvalisuse strateegiast digikümnendi jaoks. Euroopa Komisjonil on kavas esitada määruse ettepanek 2021. aasta oktoobris, Euroopa Parlament ja nõukogu peaksid määruse vastu võtma 2022. aastal ja sätteid hakatakse kohaldama alates määruse jõustumisest. Selles finantsselgituses kirjeldatud finantsmõju ja mõju personalile peaksid hakkama avalduma 2023. aastal. Ettevalmistusperiood algas juba 2021. aastal, kuid 2021. ja 2022. aasta ettevalmistustegevusi ettepanek rahaliselt ei mõjuta.

1.5.2. ELi meetme lisaväärtus (see võib tuleneda eri teguritest, nagu kooskõlastamisest saadav kasu, õiguskindlus, suurem tõhusus või vastastikune täiendavus). Käesoleva punkti kohaldamisel tähendab „ELi meetme lisaväärtus“ väärtust, mis tuleneb liidu sekkumisest ja lisandub väärtusele, mille liikmesriigid oleksid muidu üksi loonud.

ELi tasandi meetme põhjused (*ex ante*)

2019.–2021. aastal on järsult suurenenud selliste liidu institutsioone, organeid ja asutusi mõjutavate oluliste intsidentide arv, mille on toime pannud kinnisründeohu (*advanced persistent threat*) subjektid. 2021. aasta esimesel poolel leidis aset sama palju olulisi intsidente kui kogu 2020. aastal. See kajastub ka nende ekspertiisitõmmiste (mõjutatud süsteemide või seadmete sisu hetktõmmis) arvus, mida CERT-EU 2020. aastal analüüsis ja mis 2019. aastaga võrreldes kolmekordistus, samal ajal kui oluliste intsidentide arv suurenes alates 2018. aastast rohkem kui kümme korda.

Üksuste küberturvalisuse küpsuse tase erineb märkimisväärselt[11]. See määrus tagab, et kõik liidu institutsioonid, organid ja asutused rakendavad turvameetmete ühtseid alamstandardeid ja teevad üksteisega koostööd, pidades silmas liidu halduse avatud ja tõhusat toimimist.

Säilitatavad süsteemid on liidu institutsioonide, organite ja asutuste otsustada ja juhtida ning liikmesriigid ei oleks saanud kavandatud meetmeid luua.

1.5.3. Samalaadsetest kogemustest saadud õppetunnid

Küberturvalisuse direktiiv on olnud esimene horisontaalne siseturu õigusvahend, mille eesmärk on parandada liidu võrkude ja süsteemide vastupanuvõimet küberriskide suhtes. See on pärast oma jõustumist 2016. aastal aidanud märkimisväärselt tõsta küberturvalisuse üldist taset liikmesriikides. Küberturvalisuse 2. direktiivi ettepaneku eesmärk on neid meetmeid veelgi tõhustada.

Määrusega soovitakse kehtestada samalaadsed meetmed liidu institutsioonidele, organitele ja asutustele.

1.5.4. Kooskõla mitmeaastase finantsraamistikuga ja võimalik koostoime muude asjaomaste meetmetega

Ettepanek on kooskõlas mitmeaastase finantsraamistikuga ning on oluline osa ELi julgeolekustrateegiast ja ELi küberturvalisuse strateegiast digikümnendi jaoks.

Ettepanekuga nähakse ette meetmete kohaldamine liidu institutsioonides, organites ja asutustes, et tagada seal küberturvalisuse ühtlaselt kõrge tase. Ettepanek on kooskõlas ettepanekuga võtta vastu direktiiv, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega tunnistatakse kehtetuks direktiiv (EL) 2016/1148 (küberturvalisuse 2. direktiivi ettepanek).

1.5.5. Erinevate kasutada olevate rahastamisvõimaluste, sealhulgas vahendite ümberpaigutamise võimaluste hinnang

Ülesannete täitmine eeldab CERT-EU-lt spetsiaalseid profiile ja tähendab täiendavat töökoormust, mida ei saa katta inim- ja rahalisi ressursse suurendamata.

[11] Viide: [Euroopa Kontrollikoja eriaruanne küberturvalisuse kohta liidu institutsioonides, organites ja asutustes].

1.6. Ettepaneku/algatuse kestus ja finantsmõju

☐ **Piiratud kestusega**

– ☐ hõlmab ajavahemikku [PP/KK]AAAA–[PP/KK]AAAA

– ☐ finantsmõju kulukohustuste assigneeringutele avaldub ajavahemikul AAAA–AAAA ja maksete assigneeringutele ajavahemikul AAAA–AAAA.

☑**Piiramatu kestusega**

– Finantsmõju peaks hakkama avalduma esimese eelarvega, mis võetakse vastu pärast määruse jõustumist. Esimesel aastal, mida käsitatakse üleminekuaastana, jaotatakse ressursid ümber liidu institutsioonidelt ja peamistelt organitelt komisjonile; see ja ressursside muu (ümber)jaotamine toimub aastaeelarvete raamistikus. Kui määrus võetakse vastu 2022. aastal, on üleminekuperiood 2023. eelarveaasta ja 2024. aastal algab täieulatuslik rakendamine.

1.7. Ettenähtud eelarve täitmise viisid[12]

☑ **Eelarve otsene täitmine** komisjoni ning iga liidu institutsiooni, organi ja asutuse poolt

– ☑ oma talituste kaudu, sealhulgas kasutades liidu delegatsioonides töötavat komisjoni personali;

– ☐ rakendusametite kaudu

☐ **Eelarve jagatud täitmine** koostöös liikmesriikidega

☐ **Eelarve kaudne täitmine**, mille puhul eelarve täitmise ülesanded on delegeeritud:

– ☐ kolmandatele riikidele või nende määratud asutustele;

– ☐ rahvusvahelistele organisatsioonidele ja nende allasutustele (nimetage);

– ☐ Euroopa Investeerimispangale ja Euroopa Investeerimisfondile;

– ☐ finantsmääruse artiklites 70 ja 71 osutatud asutustele;

– ☐ avalik-õiguslikele asutustele;

– ☐ avalikke teenuseid osutavatele eraõiguslikele asutustele, kuivõrd nad esitavad piisavad finantstagatised;

– ☐ liikmesriigi eraõigusega reguleeritud asutustele, kellele on delegeeritud avaliku ja erasektori partnerluse rakendamine ja kes esitavad piisavad finantstagatised;

– ☐ isikutele, kellele on delegeeritud Euroopa Liidu lepingu V jaotise kohaste ühise välis- ja julgeolekupoliitika erimeetmete rakendamine ja kes on kindlaks määratud asjaomases alusaktis.

– *Mitme eelarve täitmise viisi valimise korral esitage üksikasjad rubriigis „Märkused“.*

Märkused

Haldus- ja finantsmenetluste kohaldamisel tegutseb CERT-EU komisjoni järelevalve all. Määruse eelnõust tulenevad lisaressursid on järgmised.

[12] Eelarve täitmise viise koos viidetega finantsmäärusele on selgitatud veebisaidil https://myintracomm.ec.europa.eu/budgweb/ET/man/budgmanag/Pages/budgmanag.aspx

Määruse eelnõu artiklite 12 ja 13 rakendamine toob kaasa ulatuslikuma teenuste loetelu täiendavate põhiteenustega. Määruse täieulatuslikuks rakendamiseks on vaja järgmisi lisaressursse (kuni mitmeaastase finantsraamistiku kehtivuse lõpuni 2027. aasta lõpus): 21 täistööajale taandatud töötajat ja 14,05 miljonit eurot.

Eelarveliste lisaressursside jaotus eri ülesannete vahel on järgmine:

(a) artikli 12 lõike 2 punktides a, b, c ja e täpsustatud ülesannete täitmiseks liidu institutsioonide, organite ja asutuste heaks 13,75 täistööajale taandatud töötajat ja 11,275 miljonit eurot;

(b) artikli 12 lõikes 3 täpsustatud ülesannete täitmiseks (ühise küberüksuse tegevuse toetamine) 2 täistööajale taandatud töötajat ja 381 000 eurot;

(c) artikli 12 lõikes 4 täpsustatud ülesannete täitmiseks (struktureeritud koostöö ENISAga) 0,25 täistööajale taandatud töötajat ja 236 000 eurot;

(d) artikli 12 lõikes 6 täpsustatud ülesannete täitmiseks (küberturvalisuse õppused) 0,25 täistööajale taandatud töötajat ja 79 000 eurot;

(e) artikli 12 lõike 2 punktis d ja artiklis 13 täpsustatud ülesannete täitmiseks (määruse rakendamise analüüsimine ja aruandlus, juhenddokumentide, soovituste ja üleskutsete koostamine) 3,75 täistööajale taandatud töötajat ja 2,079 miljonit eurot.

(f) institutsioonidevahelise küberturvalisuse nõukogu toetamise ülesannete täitmiseks 1 täistööajale taandatud töötaja.

Ülevaade praegustest ressurssidest ja üleminekust täieulatuslikule rakendamisele:

2021. aasta septembris olid CERT-EU käsutuses järgmised ressursid:

– alalised ja lähetatud riiklike ekspertidega täidetud ametikohad: 14 täistööajale taandatud töötajat,

– teenustaseme kokkulepete alusel rahastatavad lepingulised töötajad: 24 täistööajale taandatud töötajat,

– kokku 38 täistööajale taandatud töötajat.

CERT-EU 2020. aasta eelarve oli 250 000 eurot komisjoni eelarvest ja 3,5 miljonit eurot teenustaseme kokkulepete sihtotstarbelistest tuludest. Kokku 3,75 miljonit eurot. See oli kogu CERT-EU eelarve, mis hõlmas koolitust, riistvara, tarkvara, lähetusi, tuge, lepingulisi töötajaid ja konverentse.

Pärast määruse jõustumist peaksid CERT-EU tulevased ressursid olema järgmised:

– alalised ametikohad: 34 täistööajale taandatud töötajat,

– lepingulised töötajad: 15 täistööajale taandatud töötajat,

– kokku 49 täistööajale taandatud töötajat, mis tähendab 11 täistööajale taandatud töötaja suurust netokasvu.

Alaliste ametikohtade ja lepinguliste töötajate suhte muutmisega kõrvaldatakse pidevad probleemid küberturvalisuse vanemspetsialistide värbamisel ja enda juures hoidmisel, kuna neid on tööturul vähe.

Lisaks on komisjoni informaatika peadirektoraati vaja ühte täistööajale taandatud lepingulist töötajat, et toetada institutsioonidevahelist küberturvalisuse nõukogu.

Seega on määruse rakendamiseks vaja kokku 21 täiendavat täistööajale taandatud töötajat (20 täistööajale taandatud töötajat CERT-EU ja 1 komisjoni informaatika peadirektoraadi jaoks).

Selle kompenseerimiseks vähendatakse CERT-EU personali samal ajal 9 sellise täistööajale taandatud lepingulise töötaja võrra, keda enne rahastati teenustaseme kokkulepete sihtotstarbelistest tuludest.

CERT-EU üleminekuperioodijärgsetest 2024. aasta eelarvevahenditest, mis on ette nähtud muudeks kui personalikuludeks, kaetakse eespool punktides a–e loetletud ülesanded ja neid on kavas rahastada järgmiselt:

– 8,921 miljonit eurot aastas liidu institutsioonidelt, keda rahastatakse liidu eelarve rubriigist 7,

– 2,459 miljonit eurot liidu institutsioonidelt, organitelt ja asutustelt, keda rahastatakse liidu eelarve rubriikidest 1–6,

– 2,670 miljonit eurot isemajandavatelt liidu institutsioonidelt, organitelt ja asutustelt.

– CERT-EU kogueelarve on 14,05 miljonit eurot.

Artikli 12 lõikes 5 loetletud ülesandeid ei ole tema teenuste loetelus kirjeldatud, vaid need on tasulised teenused. Need on lisateenused, hõlmavad suhteliselt väikeseid summasid, on peamiselt ajutised ja nende teenuste kulud nõutakse teenustaseme kokkulepete või kirjalike kokkulepete alusel tagasi teenuste saajatelt.

Mis puudutab osalemist CERT-EU personali tagamises, siis liidu institutsioonid ja peamised organid annavad oma õiglase panuse, mis on proportsionaalne organisatsiooni alaliste AD ametikohtade osakaaluga. Tuleks vaadata, kas EKP ja EIP saavad samuti anda õiglase panuse alaliste töötajate lähetamise kaudu.

2. HALDUSMEETMED

2.1. Järelevalve ja aruandluse eeskirjad

Märkige sagedus ja tingimused.

Komisjon vaatab määruse selle toimivuse hindamiseks institutsioonidevahelise küberturvalisuse nõukogu ja CERT-EU abil korrapäraselt läbi ning esitab sellekohase aruande Euroopa Parlamendile ja nõukogule esimest korda hiljemalt 48 kuud pärast käesoleva määruse jõustumist ja seejärel iga kolme aasta tagant.

Läbivaatamiseks kasutatavad andmed saadakse peamiselt institutsioonidevaheliselt küberturvalisuse nõukogult ja CERT-EU-lt. Lisaks võidakse vajaduse korral kasutada andmekogumise erivahendeid, nt liidu institutsioonide, organite ja asutuste, ENISA või CSIRTi võrgustiku uuringuid.

2.2. Haldus- ja kontrollisüsteem(id)

2.2.1. Eelarve täitmise viisi(de), rahastamise rakendamise mehhanismi(de), maksete tegemise korra ja kavandatava kontrollistrateegia selgitus

Määrusest tulenevaid meetmeid juhitakse igas liidu institutsioonis, organis ja asutuses vastavalt nende suhtes kohaldatavatele asjakohastele õigusnormidele.

CERT-EU tegevuse haldus- ja finantsjuhtimine toimub komisjoni halduse raames ning järgib sellele kohaldatavaid eelarve täitmise ja rakendusmehhanisme, maksete tegemise korda ja kontrollimehhanisme.

Komisjoni siseaudiitoril on CERT-EU suhtes samad volitused nagu komisjoni talituste suhtes.

2.2.2. Teave kindlakstehtud riskide ja nende vähendamiseks kasutusele võetud sisekontrollisüsteemi(de) kohta

Väga väike risk, kuna CERT-EU juba tegutseb halduslikult informaatika peadirektorile alluva komisjoni rakkerühmana ja institutsioonidevaheline küberturvalisuse nõukogu on kujundatud praeguse CERT-EU juhtnõukogu eeskujul. Finantsjuhtimise ja sisekontrolli süsteem on seega juba paigas.

2.2.3. Kontrollide kulutõhususe (kontrollikulude suhe hallatavate vahendite väärtusse) hinnang ja põhjendus ning prognoositav veariski tase (maksete tegemise ja sulgemise ajal).

Hanke-, finantsjuhtimise ja kontrollimenetlused on juba kehtestatud ja edukalt katsetatud. Kontrollide kulutõhusus ja veariski tase vastavad iga liidu institutsiooni, organi või asutuse ja CERT-EU tegevuse puhul komisjoni kontrollide kulutõhususele ja veariski tasemele.

2.3. Pettuse ja eeskirjade eiramise ärahoidmise meetmed

Nimetage rakendatavad või kavandatud ennetus- ja kaitsemeetmed, nt pettustevastase võitluse strateegias esitatud meetmed.

CERT-EU tegevuse suhtes kohaldatakse komisjoni finantsjuhtimis- ja sisekontrollisüsteemi.

Pettuse, korruptsiooni ja muu ebaseadusliku tegevuse vastu võitlemiseks kohaldatakse piiranguteta Euroopa Parlamendi ja nõukogu 11. septembri 2013. aasta

määrust (EL, Euratom) nr 883/2013, mis käsitleb Euroopa Pettustevastase Ameti (OLAF) juurdlusi.

3. ETTEPANEKU/ALGATUSE HINNANGULINE FINANTSMÕJU

3.1. Mitmeaastase finantsraamistiku rubriigid ja kulude eelarveread, millele mõju avaldub

- Olemasolevad eelarveread

Järjestage mitmeaastase finantsraamistiku rubriigiti ja iga rubriigi sees eelarveridade kaupa

Mitmeaastase finantsraamistiku rubriik	Eelarverida	Kulu liik	Rahaline osalus			
	Nr	Liigendatud/liigendamata[13]	EFTA riigid[14]	kandidaatriigid[15]	kolmandad riigid	finantsmääruse artikli 21 lõike 2 punkti b tähenduses
1–6	Eelarveread, mis hõlmavad liidu toetusi detsentraliseeritud asutustele ja organitele	Liigendatud	EI	EI	EI	EI
7	Eelarveread, mis hõlmavad töötasu, IT-kulusid ja muid halduskulusid ELi eelarve eri jaotistes	Liigendamata	EI	EI	EI	EI

- Uued eelarveread, mille loomist taotletakse

Järjestage mitmeaastase finantsraamistiku rubriigiti ja iga rubriigi sees eelarveridade kaupa

Mitmeaastase finantsraamistiku rubriik	Eelarverida	Kulu liik	Rahaline osalus			
	Nr	Liigendatud/liigendamata	EFTA riigid	kandidaatriigid	kolmandad riigid	finantsmääruse artikli 21 lõike 2 punkti b tähenduses
	Puudub		JAH/EI	JAH/EI	JAH/EI	JAH/EI

[13] Liigendatud = Liigendatud assigneeringud / liigendamata = liigendamata assigneeringud.
[14] EFTA: Euroopa Vabakaubanduse Assotsiatsioon.
[15] Kandidaatriigid ja vajaduse korral Lääne-Balkani potentsiaalsed kandidaatriigid.

3.2. Ettepaneku hinnanguline finantsmõju assigneeringutele

3.2.1. Hinnanguline mõju tegevusassigneeringutele – ülevaade

– ☐ Ettepanek/algatus ei hõlma tegevusassigneeringute kasutamist

– ☑ Ettepanek/algatus hõlmab tegevusassigneeringute kasutamist, mis toimub järgmiselt:

miljonites eurodes (kolm kohta pärast koma)

Mitmeaastase finantsraamistiku rubriik	1–6	Rubriigid, mis hõlmavad toetusi detsentraliseeritud asutustele ja organitele

DG: mitu			Aasta **2023**	Aasta **2024**	Aasta **2025**	Aasta **2026**	Aasta **2027**	**KOKKU**
○Tegevusassigneeringud								
Eelarveread, mis hõlmavad liidu toetusi detsentraliseeritud asutustele (xx 10 xx xx)[16]	Kulukohustused	(1a)	2,459	2,459	2,459	2,459	2,459	12,293
	Maksed	(2a)	2,459	2,459	2,459	2,459	2,459	12,293
Eriprogrammide vahenditest rahastatavad haldusassigneeringud[17]								
Eelarverida		(3)						
Mitme peadirektoraadi assigneeringud KOKKU	Kulukohustused	= 1a + 1b + 3	2,459	2,459	2,459	2,459	2,459	12,293
	Maksed	= 2a + 2b +3	2,459	2,459	2,459	2,459	2,459	12,293

[16] Eelarve ametliku liigenduse kohaselt.

[17] Tehniline ja/või haldusabi ning ELi programmide ja/või meetmete rakendamiseks antava toetusega seotud kulud (endised BA read), kaudne teadustegevus, otsene teadustegevus.

○Tegevusassigneeringud KOKKU	Kulukohustused	(4)	2,459	2,459	2,459	2,459	2,459	12,293
	Maksed	(5)	2,459	2,459	2,459	2,459	2,459	12,293
○Eriprogrammide vahenditest rahastatavad haldusassigneeringud KOKKU		(6)						
Mitmeaastase finantsraamistiku **RUBRIIKIDE 1–6 assigneeringud KOKKU**	Kulukohustused	= 4 + 6	2,459	2,459	2,459	2,459	2,459	12,293
	Maksed	= 5 + 6	2,459	2,459	2,459	2,459	2,459	12,293

Juhul kui ettepanek/algatus mõjutab mitut rubriiki, tuleb eelmist jaotist korrata

○Tegevusassigneeringud KOKKU (kõik rubriigid)	Kulukohustused	(4)	2,459	2,459	2,459	2,459	2,459	12,293
	Maksed	(5)	2,459	2,459	2,459	2,459	2,459	12,293
Eriprogrammide vahenditest rahastatavad haldusassigneeringud KOKKU (kõik rubriigid)		(6)						
Mitmeaastase finantsraamistiku **RUBRIIKIDE 1–6 assigneeringud KOKKU** (võrdlussumma)	Kulukohustused	= 4 + 6	2,459	2,459	2,459	2,459	2,459	12,293
	Maksed	= 5 + 6	2,459	2,459	2,459	2,459	2,459	12,293

Mitmeaastase finantsraamistiku rubriik	**7**	„Halduskulud“

Selle punkti täitmisel tuleks kasutada haldusalaste eelarveandmete tabelit, mis on esitatud õigusaktile lisatava finantsselgituse lisas (sisekorraeeskirjade V lisa), ja laadida see üles DECIDE'i talitustevahelise konsulteerimise eesmärgil.

miljonites eurodes (kolm kohta pärast koma)

		Aasta **2023**	Aasta **2024**	Aasta **2025**	Aasta **2026**	**Aasta 2027**	**KOKKU**
DG: DIGIT (CERT-EU)							
○Personalikulud		1,184	2,126	2,754	3,225	3,225	12,514
○Muud halduskulud		7,938	8,921	8,921	8,921	8,921	43,622
DG DIGIT (CERT-EU) KOKKU	Assigneeringud	9,122	11,047	11,675	12,146	12,146	56,136

Mitmeaastase finantsraamistiku **RUBRIIGI 7 assigneeringud KOKKU**	(Kulukohustuste kogusumma = maksete kogusumma)	9,122	11,047	11,675	12,146	12,146	**56,136**

miljonites eurodes (kolm kohta pärast koma)

		Aasta 2023	Aasta 2024	Aasta 2025	Aasta 2026	Aasta 2027	**KOKKU**
Mitmeaastase finantsraamistiku **RUBRIIKIDE 1–7 assigneeringud KOKKU (*)**	Kulukohustused	11,581	13,506	14,134	14,605	14,605	68,429
	Maksed	11,581	13,506	14,134	14,605	14,605	68,429

(*) Isemajandavate liidu institutsioonide, organite ja asutuste toetused on hinnangute järgi 2,670 miljonit eurot aastas (viie aasta jooksul kokku 13,350 miljonit eurot). Toetused on CERT-EU sihtotstarbelised tulud. Eeltoodud tabelid sisaldavad üksnes hinnangulist kogumõju liidu eelarvele ega hõlma neid toetusi.

3.2.2. Tegevusassigneeringutest rahastatav väljund (hinnang)

kulukohustuste assigneeringud miljonites eurodes (kolm kohta pärast koma)

Märkige eesmärgid ja väljundid ⇩			Aasta **N**		Aasta **N+1**		Aasta **N+2**		Aasta **N+3**		Lisage vajalik arv aastaid, et kajastada kogu finantsmõju kestust (vt punkt 1.6)						**KOKKU**	
	VÄLJUNDID																	
	Väljundi liik[18]	Keskmine kulu	Arv	Kulu	Arv	Kulu	Arv	Kulu	Arv	Kulu	Arv	Kulu	Arv	Kulu	Arv	Kulu	Väljundite arv kokku	Kulud kokku
ERIEESMÄRK nr 1[19]...																		
- Väljund																		
- Väljund																		
- Väljund																		
Erieesmärk nr 1 kokku																		
ERIEESMÄRK nr 2 ...																		
- Väljund																		
Erieesmärk nr 2 kokku																		
KOKKU																		

[18] Väljunditena käsitatakse tarnitud tooteid ja osutatud teenuseid (rahastatud üliõpilasvahetuste arv, ehitatud teede pikkus kilomeetrites jms).

[19] Vastavalt punktile 1.4.2 „Erieesmärgid ...“

3.2.3. Hinnanguline mõju haldusassigneeringutele – ülevaade

– ☐ Ettepanek/algatus ei hõlma haldusassigneeringute kasutamist

– ☑ Ettepanek/algatus hõlmab haldusassigneeringute kasutamist, mis toimub järgmiselt:

miljonites eurodes (kolm kohta pärast koma)

	Aasta 2023	Aasta 2024	Aasta 2025	Aasta 2026	Aasta 2027	**KOKKU**
Mitmeaastase finantsraamistiku RUBRIIK 7						
Personalikulud						
Alalised töötajad (AD palgaastmed)	1,099	2,041	2,669	3,14	3,14	12,089
Lepingulised töötajad	0,085	0,085	0,085	0,085	0,085	0,425
Muud halduskulud	7,938	8,921	8,921	8,921	8,921	43,622
Mitmeaastase finantsraamistiku RUBRIIGI 7 kulud kokku	9,122	11,047	11,675	12,146	12,146	56,136

Mitmeaastase finantsraamistiku RUBRIIGIST 7[20] välja jäävad kulud						
Personalikulud						
Muud halduskulud						
Mitmeaastase finantsraamistiku RUBRIIGIST 7 välja jäävad kulud kokku						

KOKKU	9,122	11,047	11,675	12,146	12,146	56,136

Personali ja muude halduskuludega seotud assigneeringute vajadused kaetakse asjaomase peadirektoraadi poolt kõnealuse meetme haldamiseks juba antud ja/või peadirektoraadi siseselt ümberpaigutatud assigneeringutest, mida vajaduse korral võidakse täiendada nendest lisaassigneeringutest, mis haldavale peadirektoraadile eraldatakse iga-aastase vahendite eraldamise menetluse käigus, arvestades eelarvepiirangutega.

[20] Tehniline ja/või haldusabi ning ELi programmide ja/või meetmete rakendamiseks antava toetusega seotud kulud (endised BA read), kaudne teadustegevus, otsene teadustegevus.

3.2.3.1. Hinnanguline personalivajadus

– ☐ Ettepanek/algatus ei hõlma personali kasutamist

– ☑ Ettepanek/algatus hõlmab personali kasutamist, mis toimub järgmiselt:

Hinnanguline väärtus täistööaja ekvivalendina

		Aasta 2023	Aasta 2024	Aasta 2025	Aasta 2026	Aasta 2027		
O Ametikohtade loeteluga ette nähtud ametikohad (ametnikud ja ajutised töötajad)								
20 01 02 01 (komisjoni peakorteris ja esindustes)		7	13	17	20	20		
20 01 02 03 (delegatsioonides)								
01 01 01 01 (kaudne teadustegevus)								
01 01 01 11 (otsene teadustegevus)								
Muud eelarveread (märkige)								
O Koosseisuväline personal (täistööajale taandatud töötajad)[21]								
20 02 01 (üldvahenditest rahastatavad lepingulised töötajad, riikide lähetatud eksperdid ja renditööjõud)		1	1	1	1	1		
20 02 03 (lepingulised töötajad, kohalikud töötajad, riikide lähetatud eksperdid, renditööjõud ja noored eksperdid delegatsioonides)								
XX 01 xx **yy zz**[22]	- peakorteris							
	- delegatsioonides							
01 01 01 02 (lepingulised töötajad, riikide lähetatud eksperdid ja renditööjõud kaudse teadustegevuse valdkonnas)								
01 01 01 12 (lepingulised töötajad, riikide lähetatud eksperdid ja renditööjõud otsese teadustegevuse valdkonnas)								
Muud eelarveread (märkige)								
KOKKU		**8**	**14**	**18**	**21**	**21**		

XX tähistab asjaomast poliitikavaldkonda või eelarvejaotist.

Personalivajadused kaetakse juba meedet haldavate peadirektoraadi töötajatega ja/või töötajate peadirektoraadisisese ümberpaigutamise teel. Vajaduse korral võidakse personali täiendada iga-aastase vahendite eraldamise menetluse käigus, arvestades olemasolevate eelarvepiirangutega.

Ülesannete kirjeldus:

Ametnikud ja ajutised töötajad	Ametnikud täidavad CERT-EU ülesandeid ja viivad ellu CERT-EU tegevusi vastavalt määrusele, eelkõige IV ja V peatükile.
Koosseisuvälised töötajad	Lepinguline töötaja abistab institutsioonidevahelise küberturvalisuse nõukogu sekretäritöös.

[21] Lepingulised töötajad, kohalikud töötajad, riikide lähetatud eksperdid, renditööjõud, noored spetsialistid delegatsioonides.

[22] Tegevusassigneeringutest rahastatavate koosseisuväliste töötajate ülempiiri arvestades (endised BA read).

3.2.4. Kooskõla kehtiva mitmeaastase finantsraamistikuga

Ettepanek/algatus:

– ☑ on täielikult rahastatav mitmeaastase finantsraamistiku asjaomase rubriigi sisese vahendite ümberpaigutamise kaudu.

Selgitage ümberplaneerimist, osutades asjaomastele eelarveridadele ja summadele. Põhjaliku ümberplaneerimise korral tuleb esitada Exceli tabel.

– ☐ tingib mitmeaastase finantsraamistiku asjaomases rubriigi mittesihtotstarbelise varu ja/või mitmeaastase finantsraamistiku määruses sätestatud erivahendite kasutuselevõtu.

Selgitage, millised toimingud on vajalikud, osutades asjaomastele rubriikidele, eelarveridadele ja summadele ning nimetades kasutatavad rahastamisvahendid.

– ☐ nõuab mitmeaastase finantsraamistiku muutmist.

Selgitage, millised toimingud on vajalikud, osutades asjaomastele rubriikidele, eelarveridadele ja summadele.

3.2.5. Kolmandate isikute rahaline osalus

Ettepanek/algatus:

– ☑ ei hõlma kolmandate isikute poolset kaasrahastamist[23]

– ☐ hõlmab kaasrahastamist, mille hinnanguline summa on järgmine:

assigneeringud miljonites eurodes (kolm kohta pärast koma)

	Aasta **N**[24]	Aasta **N+1**	Aasta **N+2**	Aasta **N+3**	Lisage vajalik arv aastaid, et kajastada kogu finantsmõju kestust (vt punkt 1.6)			Kokku
Nimetage kaasrahastav asutus								
Kaasrahastatavad assigneeringud KOKKU								

[23] Sihtotstarbelisi tulusid, mis tulenevad artikli 12 lõike 5 punktis c ette nähtud teenuste juhuslikust osutamisest välisorganisatsioonidele, ei ole arvestatud, sest need peaksid olema marginaalsed.

[24] N on aasta, mil alustatakse ettepaneku/algatuse rakendamist. „N“ asemel tuleb märkida esimene eeldatav rakendamise aasta (näiteks 2021). Sama tuleb teha ka järgnevate aastate puhul.

3.3. Hinnanguline mõju tuludele

– ☑ Ettepanekul/algatusel puudub finantsmõju tuludele

– ☐ Ettepanekul/algatusel on järgmine finantsmõju:

  – ☐ omavahenditele

  – ☐ muudele tuludele

  – palun märkige, kas see on kulude eelarveridasid mõjutav sihtotstarbeline tulu ☐

miljonites eurodes (kolm kohta pärast koma)

Tulude eelarverida	Jooksva aasta eelarves kättesaadavad assigneeringud	Ettepaneku/algatuse mõju[25]						
		Aasta **N**	Aasta **N+1**	Aasta **N+2**	Aasta **N+3**	Lisage vajalik arv aastaid, et kajastada kogu finantsmõju kestust (vt punkt 1.6)		
Artikkel ….								

Sihtotstarbeliste tulude puhul märkige, milliseid kulude eelarveridasid ettepanek mõjutab.

Muud märkused (nt tuludele avaldatava mõju arvutamise meetod/valem või muu teave).

[25] Traditsiooniliste omavahendite (tollimaksud ja suhkrumaksud) korral tuleb märkida netosummad, st brutosumma pärast 20 % sissenõudmiskulude mahaarvamist.