Euroopa Liidu
Teataja

ET
L-seeria

2023/2841

18.12.2023

EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS (EL, Euratom) 2023/2841,

13. detsember 2023,

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 ([1])

ning arvestades järgmist:

(1) Digiajastul on info- ja kommunikatsioonitehnoloogia avatud, tõhusa ja sõltumatu Euroopa halduskorralduse alustala. Tehnoloogia areng ning digisüsteemide kasvav keerukus ja omavaheline seotus võimendavad küberturvalisusriske ja suurendavad liidu üksuste vastuvõtlikkust küberohtudele ja -intsidentidele, mis seab ohtu nende toimepidevuse ja võime tagada oma andmete turvalisus. Pilveteenuste kasutamise kasv, info- ja kommunikatsioonitehnoloogia (IKT) kasutamine kõikjal, digitaliseerituse kõrge tase, kaugtöö ning tehnoloogia ja ühenduvuse areng on liidu üksuste kõigi tegevuste põhielemendid, kuid digivastupidavusvõime ei ole sellesse veel piisavalt sisse ehitatud.

(2) Liidu üksusi ümbritsevad küberohud arenevad pidevalt. Ohusubjektide taktika, metoodika ja töövõtted arenevad pidevalt, kuid selliste rünnete peamised ajendid on üldjoones samad, alates väärtusliku avalikustamata teabe varastamisest kuni raha teenimiseni, avaliku arvamusega manipuleerimiseni või digitaristu kahjustamiseni. Ohusubjektid korraldavad küberründe aina sagedamini ning ründed ise muutuvad keerukamaks ja automatiseeritumaks; sihikule võetakse ohtudele avatud ja üha suurenevad ründepinnad ning nõrkusi kasutatakse kiiresti ära.

(3) Liidu üksuste IKT-keskkonnad on omavahel seotud, nende andmevood on integreeritud ja nende keskkondade kasutajad teevad tihedat koostööd. See omavaheline seotus tähendab, et isegi kui mõni häire piirdub esialgu ühe liidu üksusega, võib see kaasa tuua laiema ahelreaktsiooni, millel võib olla kaugeleulatuv ja pikaajaline negatiivne mõju teistele liidu üksustele. Lisaks on teatavate liidu üksuste IKT-keskkonnad seotud liikmesriikide IKT-keskkondadega, mistõttu intsident liidu üksuses võib tekitada küberturvalisuse riski liikmesriikide IKT-keskkondadele ja vastupidi. Intsidenti käsitleva teabe jagamine võib hõlbustada liikmesriike mõjutavate samalaadsete küberohtude või intsidentide avastamist.

(4) Liidu üksused on atraktiivsed sihtmärgid, mida ähvardavad heade oskuste ja korralike ressurssidega ohusubjektid, aga ka muud ohud. Samas on kübervastupidavuse tase ning pahatahtliku kübertegevuse avastamise ja sellele reageerimise võime liidu üksustes väga erinev. Seepärast on liidu üksuste toimimiseks vaja, et nad saavutaksid küberturvalisuse ühtlaselt kõrge taseme tuvastatud küberturvalisusriskidele vastavate küberturvalisuse meetmete rakendamise, teabevahetuse ja koostöö kaudu.

([1]) Euroopa Parlamendi 21. novembri 2023. aasta seisukoht (*Euroopa Liidu Teatajas* seni avaldamata) ja nõukogu 8. detsembri 2023. aasta otsus.

(5) Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 ([2]) eesmärk on parandada veelgi avaliku ja erasektori üksuste, pädevate asutuste ja organite ning kogu liidu kübervastupidavusvõimet ja intsidentidele reageerimise suutlikkust. Seepärast on vaja tagada, et liidu üksused toimiksid samade põhimõtete alusel, nähes ette normid, mis on kooskõlas direktiiviga (EL) 2022/2555 ja mille eesmärgid on sama ulatuslikud.

(6) Küberturvalisuse ühtlaselt kõrge taseme saavutamiseks on vaja, et iga liidu üksus kehtestaks sisemise küberturvalisusriskide juhtimis-, haldamis- ja kontrollraamistiku (edaspidi „raamistik“), mis tagab kõigi küberturvalisusriskide tulemusliku ja aruka juhtimise ning võtab arvesse toimepidevust ja kriisijuhtimist. Raamistikuga tuleks kehtestada küberturvalisuse põhimõtted, sealhulgas eesmärgid ja prioriteedid, seoses selliste võrgu- ja infosüsteemide turvalisusega, mis hõlmavad kogu salastamata IKT-keskkonda. Raamistik peaks põhinema kõiki ohte hõlmaval lähenemisviisil, mille eesmärk on kaitsta võrgu- ja infosüsteeme ning nende süsteemide füüsilist keskkonda selliste sündmuste eest nagu vargus, tulekahju, üleujutus, telekommunikatsiooni- või elektrikatkestus või loata füüsiline juurdepääs liidu üksuse teabe- ja teabetöötlusrajatistele ning nende kahjustamine ja häirimine, mis võib ohustada võrgu- ja infosüsteemides salvestatud, edastatud või töödeldud või nende süsteemide kaudu juurdepääsetavate andmete kättesaadavust, autentsust, terviklust või konfidentsiaalsust.

(7) Raamistiku alusel kindlaks tehtud küberturvalisusriskide juhtimiseks peaks iga liidu üksus võtma asjakohaseid ja proportsionaalseid tehnilisi, tegevuslikke ja korralduslikke meetmeid. Need meetmed peaksid käsitlema käesolevas määruses sätestatud valdkondi ja küberturvalisuse riskijuhtimismeetmeid, et tugevdada iga liidu üksuse küberturvalisust.

(8) Raamistikus kindlaks tehtud varasid ja küberturvalisusriske ning korrapäraste küberturvalisuse küpsustaseme hindamiste põhjal tehtud järeldusi tuleks arvesse võtta iga liidu üksuse koostatud küberturvalisuse kavas. Küberturvalisuse kava peaks sisaldama vastuvõetud küberturvalisuse riskijuhtimismeetmeid.

(9) Kuna küberturvalisuse tagamine on pidev protsess, tuleks käesoleva määruse kohaselt võetud meetmete sobivus ja mõjusus korrapäraselt läbi vaadata, võttes arvesse liidu üksuste muutuvaid küberturvalisusriske, varasid ja küberturvalisuse küpsustaset. Raamistik tuleks läbi vaadata korrapäraselt, ent vähemalt iga nelja aasta järel, samas kui küberturvalisuse kava tuleks läbi vaadata iga kahe aasta tagant või vajaduse korral tihemini pärast küberturvalisuse küpsustaseme hindamisi või raamistiku põhjalikku läbivaatamist.

(10) Liidu üksuste kehtestatud küberturvalisuse riskijuhtimismeetmed peaksid hõlmama põhimõtteid, mille eesmärk on muuta lähtekood võimaluse korral läbipaistvaks, võttes arvesse kaitsemeetmeid kolmandate isikute või liidu üksuste õiguste kaitseks. Need põhimõtted peaksid olema proportsionaalsed küberturvalisuse riskiga ja nende eesmärk peaks olema lihtsustada küberohtude analüüsimist, ilma et nendega kaasneksid kohustused avalikustada kolmanda isiku kood või õigused pääseda sellele juurde suuremas ulatuses, kui see on kehtivates lepingutingimustes ette nähtud.

(11) Tänu avatud lähtekoodiga küberturbevahenditele ja -rakendustele võib tõusta avatuse tase. Avatud standardid soodustavad turbevahendite koostalitlusvõimet, mis on kasulik sidusrühmade turvalisuse seisukohast. Avatud lähtekoodiga küberturbevahendid ja -rakendused võivad võimendada laiemat arendajate kogukonda, võimaldades tarnijate mitmekesistamist. Avatud lähtekoodiga võib kaasneda küberturvalisusega seotud vahendite kontrolliprotsessi suurem läbipaistvus ning kogukonna juhitav nõrkuste tuvastamise protsess. Seetõttu peaks liidu üksustel olema võimalik edendada avatud lähtekoodiga tarkvara ja avatud standardite kasutamist, järgides poliitikat, mis on seotud avatud andmete ja avatud lähtekoodi kasutamisega läbipaistvusel põhineva turvalisuse osana.

([2]) Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta direktiiv (EL) 2022/2555, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega muudetakse määrust (EL) nr 910/2014 ja direktiivi (EL) 2018/1972 ning tunnistatakse kehtetuks direktiiv (EL) 2016/1148 (küberturvalisuse 2. direktiiv) (ELT L 333, 27.12.2022, lk 80).

(12) Erinevused liidu üksuste vahel eeldavad käesoleva määruse paindlikku rakendamist. Käesolevas määruses sätestatud küberturvalisuse ühtlaselt kõrge taseme tagamise meetmed ei tohiks sisaldada kohustusi, mis sekkuvad otseselt liidu üksuste ülesannete täitmisse või piiravad nende institutsioonilist autonoomiat. Seetõttu peaksid liidu üksused koostama oma raamistiku ning võtma vastu oma küberturvalisuse riskijuhtimismeetmed ja küberturvalisuse kavad. Selliste meetmete rakendamisel tuleks hoolikalt arvesse võtta liidu üksuste vahelist koostoimet, et ressursse nõuetekohaselt hallata ja kulusid optimeerida. Samuti tuleks hoolikalt jälgida, et need meetmed ei mõjutaks negatiivselt tõhusat teabevahetust ega koostööd liidu üksuste vahel ning liidu üksuste ja liikmesriikide samalaadsete asutuste vahel.

(13) Ressursikasutuse optimeerimiseks tuleks käesoleva määrusega näha ette võimalus, et kaks või enam sarnase struktuuriga liidu üksust võivad oma asjaomaste üksuste küberturvalisuse küpsustaseme hindamisel teha koostööd.

(14) Vältimaks liidu üksustele ebaproportsionaalse finants- ja halduskoormuse tekitamist, peaksid küberturvalisuse riskijuhtimisnõuded olema proportsionaalsed asjaomaste võrgu- ja infosüsteemide puhul esineva küberturvalisuse riskiga, võttes seejuures arvesse tehnika taset selliste meetmete osas. Iga liidu üksus peaks püüdma eraldada oma IKT eelarvest piisava osa oma küberturvalisuse taseme tõstmiseks. Pikemas perspektiivis tuleks soovituslikuks eesmärgiks seada vähemalt 10 %. Küberturvalisuse küpsustaseme hindamisel tuleks hinnata, kas liidu üksuse küberturvalisuse kulutused on proportsionaalsed teda ohustavate küberturvalisusriskidega. Ilma et see piiraks aluslepingutest tulenevate liidu aastaeelarvega seotud reeglite kohaldamist, peaks komisjon oma ettepanekus esimese aastaeelarve kohta, mis võetakse vastu pärast käesoleva määruse jõustumist, võtma liidu üksuste kuluprognoosidest tulenevate eelarvestamise ja personalivajaduste hindamisel arvesse käesolevast määrusest tulenevaid kohustusi.

(15) Küberturvalisuse ühtlaselt kõrge taseme saavutamiseks peab küberturvalisus kuuluma iga liidu üksuse kõrgeima juhtimistasandi järelevalve alla. Liidu üksuse kõrgeim juhtimistasand peaks vastutama käesoleva määruse rakendamise eest, sealhulgas raamistiku kehtestamise, küberturvalisuse riskijuhtimismeetmete võtmise ja küberturvalisuse kava heakskiitmise eest. Tegelemine küberturvalisuse kultuuriga, st igapäevase küberturvalisusega, on kõigis liidu üksustes raamistiku ning vastavate küberturvalisuse riskijuhtimismeetmete lahutamatu osa.

(16) ELi salastatud teavet käitlevate võrgu- ja infosüsteemide turvalisus on ülioluline. ELi salastatud teavet käitlevad liidu üksused peavad kohaldama sellise teabe kaitsmiseks kehtestatud põhjalikke õigusraamistikke, sealhulgas konkreetset juhtimist, poliitikat ja riskijuhtimismenetlusi. ELi salastatud teavet käitlevad võrgu- ja infosüsteemid peavad vastama rangematele turvastandarditele kui salastamata võrgu- ja infosüsteemid. Seetõttu on ELi salastatud teavet käitlevad võrgu- ja infosüsteemid küberohtudele ja -intsidentidele vastupidavamad. Seetõttu, tunnistades samas vajadust ühise raamistiku järele selles valdkonnas, ei tuleks käesolevat määrust kohaldada ELi salastatud teavet käitlevate võrgu- ja infosüsteemide suhtes. Kui liidu üksus seda sõnaselgelt taotleb, peaks Euroopa Liidu institutsioonide, organite ja asutuste infoturbeintsidentidega tegeleval rühmal (CERT-EU) olema siiski võimalik anda kõnealusele liidu üksusele abi seoses salastatud IKT-keskkondades esinevate intsidentidega.

(17) Liidu üksused peaksid hindama küberturvalisusriske, mis tulenevad suhetest tarnijate ja teenuseosutajatega, sh andmetalletuse ja andmetöötlusteenuste pakkujate või hallatavate turbeteenuste pakkujatega, ning võtma asjakohaseid meetmeid nende riskide vähendamiseks. Küberturvalisuse meetmeid tuleks CERT-EU välja antavates suunistes või soovitustes täpsemalt kirjeldada. Meetmete ja suuniste kehtestamisel tuleks hoolikalt arvesse võtta tehnika taset, ning kui see on kohaldatav, vastavaid Euroopa ja rahvusvahelisi standardeid, samuti asjakohaseid liidu õigusakte ja põhimõtteid, sh direktiivi (EL) 2022/2555 artikli 14 kohaselt loodud koostöörühma tehtud küberturvalisuse riskide hindamisi ja soovitusi, näiteks 5G-võrkude küberturvalisuse ELi kooskõlastatud

riskihindamist ja ELi meetmepaketti 5G-võrkude turvalisuse tagamiseks. Lisaks võiks ümbritsevaid küberohtusid ning liidu üksuste kübervastupidavusvõime suurendamise tähtsust arvesse võttes nõuda asjaomaste IKT-toodete, IKT-teenuste ja IKT-protsesside sertifitseerimist vastavalt konkreetsetele Euroopa küberturvalisuse sertifitseerimise kavadele, mis on vastu võetud Euroopa Parlamendi ja nõukogu määruse (EL) 2019/881 ([3]) artikli 49 kohaselt.

(18) Liidu institutsioonide ja organite peasekretärid otsustasid mais 2011 luua CERT-EU eelrühma, mille tegevuse üle teostab järelevalvet institutsioonidevaheline juhtnõukogu. Juulis 2012 kinnitasid peasekretärid praktilise korra ja leppisid kokku CERT-EU tegutsemises alalise üksusena, et aidata institutsioonidevahelise küberturvalisuse alase koostöö ühe selge näitena jätkuvalt parandada liidu institutsioonide, organite ja asutuste infotehnoloogia turvalisuse üldist taset. Septembris 2012 loodi komisjoni rakkerühmana institutsioonidevaheliste volitustega CERT-EU. Detsembris 2017 sõlmisid liidu institutsioonid, organid ja asutused institutsioonidevahelise kokkuleppe CERT-EU töökorralduse ja toimimise kohta ([4]). Käesolevas määruses tuleks sätestada põhjalikud normid CERT-EU ülesehituse, toimimise ja töökorralduse kohta. Käesoleva määruse sätted on ülimuslikud 2017. aasta detsembris sõlmitud CERT-EU ülesehitust ja töökorraldust käsitleva institutsioonidevahelise kokkuleppe suhtes.

(19) CERT-EU tuleks nimetada ümber liidu institutsioonide, organite ja asutuste küberturvalisuse teenistuseks, kuid alles peaks jääma selle nime tuntuks saanud lühivorm „CERT-EU“.

(20) Lisaks sellele, et CERT-EU-le antakse rohkem ülesandeid ja laiem tegevusulatus, luuakse käesoleva määrusega institutsioonidevaheline küberturvalisuse nõukoda (IICB), et edendada liidu üksustes küberturvalisuse ühtlaselt kõrget taset. IICB-l peaks olema ainupädevus seirata, kuidas liidu üksused käesolevat määrust rakendavad ja seda toetada ning teha järelevalvet CERT-EU üldiste prioriteetide ja eesmärkide rakendamise üle ning anda CERT-EU-le strateegilisi suuniseid. Seetõttu peaks IICB tagama liidu institutsioonide esindatuse ning kaasama liidu organite ja asutuste esindajad läbi ELi asutuste võrgustiku (EUAN). IICB töökorraldust ja toimimist tuleks lisaks reguleerida kodukorraga, milles võib täiendavalt täpsustada IICB korrapäraste koosolekute, sealhulgas selliste iga-aastaste poliitilise tasandi kohtumiste toimumist, kus IICB iga liikme kõrgeima juhtimistasandi esindajate osavõtt võimaldaks IICB-l pidada strateegilisi arutelusid ja anda IICB-le strateegilisi juhiseid. Lisaks peaks IICB-l olema võimalik luua täitevkomitee, mis aitaks teda tema töös, ning delegeerida sellele osa oma ülesandeid ja volitusi, eelkõige need, mis nõuavad selle liikmete eriteadmisi, näiteks teenuste kataloogi ja kõigi selle hilisemate ajakohastuste ning teenustaseme kokkulepete tingimuste heakskiitmine, liidu üksuste poolt IICB-le käesoleva määruse kohaselt esitatavate dokumentide ja aruannete hindamine või ülesanded, mis on seotud IICB poolt välja antavate nõuete järgimise meetmeid käsitlevate otsuste ettevalmistamisega ja nende rakendamise seirega. IICB peaks kehtestama täitevkomitee kodukorra, kaasa arvatud selle ülesanded ja volitused.

(21) IICB eesmärk on toetada liidu üksusi nende vastava turvaoleku taseme tõstmisel kübervaldkonnas käesoleva määruse rakendamise kaudu. Selleks et toetada liidu üksusi, peaks IICB andma CERT-EU juhile juhiseid, võtma vastu mitmeaastase strateegia liidu üksustes küberturvalisuse taseme tõstmiseks, kehtestama metoodika ja muud aspektid vabatahtlike vastastikuste hindamiste tegemiseks ning hõlbustama Euroopa Liidu Küberturvalisuse Ameti (ENISA) toetatava kohalikke küberturvalisuse ametnikke koondava mitteametliku rühma loomist, et vahetada käesoleva määruse rakendamisega seotud parimaid tavasid ja teavet.

([3]) 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).

([4]) Kokkulepe Euroopa Parlamendi, Euroopa Ülemkogu, Euroopa Liidu Nõukogu, Euroopa Komisjoni, Euroopa Liidu Kohtu, Euroopa Keskpanga, Euroopa Kontrollikoja, Euroopa välisteenistuse, Euroopa Majandus- ja Sotsiaalkomitee, Euroopa Regioonide Komitee ja Euroopa Investeerimispanga vahel liidu institutsioonide, organite ja asutuste infoturbeintsidentidega tegeleva rühma (CERT-EU) töökorralduse ja toimimise kohta (ELT C 12, 13.1.2018, lk 1).

(22) Selleks et saavutada kõigis liidu üksustes küberturvalisuse kõrge tase, peaksid oma IKT-keskkonda haldavate liidu organite ja asutuste huve esindama IICBs kolm EUANi määratud esindajat. Isikuandmete töötlemise turvalisus ja seega ka selle küberturvalisus on andmekaitse nurgakivi. Võttes arvesse andmekaitse ja küberturvalisuse vahelist koostoimet, peaks Euroopa Andmekaitseinspektor olema IICBs esindatud käesoleva määruse kohaldamisalasse kuuluva liidu üksusena, kellel on eriteadmised andmekaitse, sealhulgas elektroonilise side võrkude turvalisuse valdkonnas. Pidades silmas innovatsiooni ja konkurentsivõime olulisust küberturvalisuse valdkonnas, peaks IICB-s olema esindatud küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskus. Võttes arvesse ENISA rolli küberturvalisuse eksperdikeskusena ja ENISA pakutavat tuge ning liidu kosmosetaristu ja -teenuste küberturvalisuse tähtsust, peaksid IICBs olema esindatud ENISA ja Euroopa Liidu Kosmoseprogrammi Amet. Võttes arvesse CERT-EU-le käesoleva määruse alusel määratud rolli, peaks IICB juhataja kutsuma CERT-EU juhi kõigile IICB koosolekutele, välja arvatud juhul, kui IICB arutab küsimusi, mis on otseselt seotud CERT-EU juhiga.

(23) IICB peaks seirama nii käesoleva määruse järgimist kui ka suuniste ja soovituste ning üleskutsete rakendamist. Tehnilistes küsimustes peaks IICBd toetama tehnilised nõuanderühmad, mille koosseis vastab IICB äranägemisele. Tehnilised nõuanderühmad peaksid vastavalt vajadusele tegema tihedat koostööd CERT-EU, liidu üksuste ja muude sidusrühmadega.

(24) Kui IICB leiab, et liidu üksus ei ole käesolevat määrust või käesoleva määruse alusel esitatud suuniseid, soovitusi või üleskutseid tulemuslikult rakendanud, peaks IICB-l olema võimalik võtta nõuete järgimise meetmeid, ilma et see piiraks asjaomase liidu üksuse sisemenetlusi. IICB peaks kohaldama nõuete järgimise meetmeid järk-järgult, ehk teiste sõnadega peaks IICB võtma esmalt vastu kõige leebema meetme ehk põhjendatud arvamuse ning üksnes vajaduse korral võtma vastu järjest rangemaid meetmeid, lõpetades kõige rangema meetmega, milleks on soovitus peatada ajutiselt andmevood asjaomasele liidu üksusele. Sellist soovitust tuleks kohaldada ainult erandjuhtudel, kui asjaomane liidu üksus rikub käesolevat määrust pikaajaliselt, tahtlikult, korduvalt või oluliselt.

(25) Põhjendatud arvamus kujutab endast kõige leebemat nõuete järgimise meedet, millega käsitletakse käesoleva määruse rakendamisel täheldatud puudusi. IICB-l peaks olema võimalik esitada põhjendatud arvamuse järel juhised, et aidata liidu üksusel tagada, et tema raamistik, küberturvalisuse riskijuhtimismeetmed, küberturvalisuse kava ja aruandlus oleksid kooskõlas käesoleva määrusega, ning seejärel esitada hoiatus liidu üksuses tuvastatud puuduste kõrvaldamiseks kindlaksmääratud aja jooksul. Kui hoiatuses tuvastatud puudusi ei ole piisavalt käsitletud, peaks IICB-l olema võimalik esitada põhjendatud teade.

(26) IICB-l peaks olema võimalik soovitada teha liidu üksuse audit. Liidu üksusel peaks olema võimalik kasutada sel eesmärgil oma siseauditi funktsiooni. IICB-l peaks olema võimalik samuti nõuda, et auditi teeks kolmandast isikust audiitor, sealhulgas vastastikku kokku lepitud erasektori teenuseosutaja.

(27) Erandjuhtudel, kui liidu üksus rikub käesolevat määrust pikaajaliselt, tahtlikult, korduvalt või oluliselt, peaks IICB-l olema võimalik viimase abinõuna soovitada kõigil liikmesriikidel ja liidu üksustel ajutiselt peatada andmevood asjaomasele liidu üksusele, kuni liidu üksus on rikkumise kõrvaldanud. Selline soovitus tuleks edastada asjakohaste ja turvaliste sidekanalite kaudu.

(28) Käesoleva määruse nõuetekohase rakendamise tagamiseks peaks IICB juhul, kui ta leiab, et liidu üksus rikub pidevalt käesolevat määrust, tingituna otseselt tema töötaja tegevusest või tegevusetusest, sealhulgas kõrgeimal juhtimistasandil, nõudma, et asjaomane liidu üksus võtaks asjakohaseid meetmeid, sealhulgas nõudes, et üksus kaaluks distsiplinaarmeetmete võtmist kooskõlas nõukogu määrusega (EMÜ, Euratom, ESTÜ) nr 259/68 ([5]) kehtestatud Euroopa Liidu ametnike personalieeskirjades ja liidu muude teenistujate teenistustingimustes (edaspidi „personalieeskirjad“) sätestatud normide ja menetlustega ning muude kohaldatavate normide ja menetlustega.

(29) CERT-EU peaks aitama kaasa kõigi liidu üksuste IKT-keskkonna turvalisusele. Kui CERT-EU kaalub, kas anda liidu üksuse taotlusel asjakohastes poliitikaküsimustes tehnilist nõu või omapoolne sisend, peaks ta tagama, et see ei takista muude talle käesoleva määruse kohaselt antud muude ülesannete täitmist. CERT-EU peaks tegutsema liidu üksuste nimel samaväärsena koordinaatoriga, kes on määratud nõrkuste koordineeritud avalikustamise jaoks vastavalt direktiivi (EL) 2022/2555 artikli 12 lõikele 1.

(30) CERT-EU peaks toetama küberturvalisuse ühtlaselt kõrge taseme tagamise meetmete rakendamist IICB-le tehtavate ettepanekutega suuniste ja soovituste kohta või üleskutsete esitamisega. IICB peaks sellised suunised ja soovitused heaks kiitma. Vajaduse korral peaks CERT-EU esitama üleskutseid, milles kirjeldatakse kiireloomulisi turbemeetmeid, mida liidu üksused peaksid võtma kindlaksmääratud aja jooksul. IICB peaks andma CERT-EU-le korralduse esitada suuniste või soovituse ettepanek või üleskutse või see tagasi võtta või seda muuta.

(31) Samuti peaks CERT-EU täitma rolli, mis on talle direktiiviga (EL) 2022/2555 ette nähtud kõnealuse direktiivi artikli 15 kohaselt loodud küberturbe intsidentide lahendamise üksuste (CSIRTide) võrgustikuga tehtavas koostöös ja teabevahetuses. Ühtlasi peaks CERT-EU kooskõlas komisjoni soovitusega (EL) 2017/1584 ([6]) tegema koostööd ja koordineerima reageerimist asjaomaste sidusrühmadega. Küberturvalisuse kõrge taseme saavutamiseks kogu liidus peaks CERT-EU jagama intsidentide kohta käivat teavet liikmesriikide samalaadsete asutustega. Samuti peaks CERT-EU tegema koostööd muude avaliku ja erasektori samalaadsete asutustega, sh Põhja-Atlandi Lepingu Organisatsiooniga, kui IICB on selle eelnevalt heaks kiitnud.

(32) Operatiivse küberturvalisuse toetamisel peaks CERT-EU kasutama ENISA olemasolevaid oskusteadmisi struktureeritud koostöö kaudu, nagu on sätestatud määruses (EL) 2019/881. Asjakohasel juhul tuleks nende kahe üksuse vahel kehtestada erikord, et määrata kindlaks sellise koostöö elluviimine praktikas ja vältida tegevuse dubleerimist. CERT-EU peaks tegema ENISAga küberohtude analüüsi alast koostööd ning jagama ENISAga regulaarselt oma ohtude kaardistamise aruannet.

(33) CERT-EU-l peaks olema võimalik teha koostööd ja vahetada teavet asjaomaste küberturvalisuse kogukondadega liidus ja selle liikmesriikides, et edendada operatiivkoostööd ja võimaldada olemasolevatel võrgustikel realiseerida liidu kaitsmisel kogu oma potentsiaali.

(34) CERT-EU teenused ja ülesanded on liidu üksuste huvides ning seega peaks iga IKT eelarvega liidu üksus andma nende teenuste ja ülesannete jaoks oma õiglase panuse. Selline panus ei piira liidu üksuste eelarveautonoomiat.

([5]) Nõukogu 29. veebruari 1968. aasta määrus (EMÜ, Euratom, ESTÜ) nr 259/68, millega kehtestatakse Euroopa ühenduste ametnike personalieeskirjad ja muude teenistujate teenistustingimused ning komisjoni ametnike suhtes ajutiselt kohaldatavad erimeetmed (EÜT L 56, 4.3.1968, lk 1).

([6]) 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).

(35) Paljud küberründed on osa laiematest rünnakutest, mis on suunatud liidu üksuste rühmade vastu või huviringkondade vastu, kuhu kuuluvad ka liidu üksused. Ettevaatava tuvastamise, intsidentidele reageerimise ja leevendusmeetmete ning intsidentidest taastumise võimaldamiseks peaks liidu üksustel olema võimalik teatada CERT-EU-le intsidentidest, küberohtudest, nõrkustest ja intsidendiohtudest ning jagada asjakohaseid tehnilisi üksikasju, et teistel liidu üksustel oleks võimalik samalaadseid intsidente, küberohte, nõrkusi ja intsidendiohtusid tuvastada või leevendada ja neile reageerida. Järgides samasugust lähenemisviisi nagu direktiivis (EL) 2022/2555, peaks liidu üksustel olema kohustus esitada CERT-EU-le varajane hoiatus 24 tunni jooksul pärast seda, kui nad saavad teada olulisest intsidendist. Selline teabevahetus peaks andma CERT-EU-le võimaluse levitada teavet teistele liidu üksustele ning asjaomastele samalaadsetele asutustele, et aidata kaitsta liidu üksuste IKT-keskkondi ja liidu üksuste samalaadsete asutuste IKT-keskkondi samalaadsete intsidentide eest.

(36) Käesolevas määruses sätestatakse olulistest intsidentidest teatamise mitmeetapiline lähenemisviis, et saavutada õige tasakaal kahe ülesande vahel: ühelt poolt kiire teatamine, mis aitab vähendada oluliste intsidentide võimalikku levikut ja võimaldab liidu üksustel abi otsida, ning teiselt poolt põhjalik aruandlus, mis võimaldab saada üksikintsidentidest väärtuslikke kogemusi ja suurendada aja jooksul konkreetsete liidu üksuste kübervastupidavusvõimet ning aitab tõsta nende üldist turvaoleku taset kübervaldkonnas. Sellega seoses peaks käesolev määrus hõlmama teatamist intsidentidest, mis asjaomase liidu üksuse esialgse hinnangu kohaselt võivad põhjustada asjaomase liidu üksuse toimimises tõsiseid häireid või sellele liidu üksusele rahalist kahju või mõjutada teisi füüsilisi või juriidilisi isikuid, põhjustades märkimisväärset varalist või mittevaralist kahju. Esialgses hinnangus tuleks muu hulgas arvesse võtta mõjutatud võrgu- ja infosüsteeme, eelkõige nende tähtsust liidu üksuse toimimise jaoks, küberohu tõsidust ja tehnilisi tunnuseid ning kõiki sellega seotud ärakasutatavaid nõrkusi, samuti liidu üksuse kogemusi samalaadsete intsidentidega. Sellised näitajad nagu liidu üksuse toimimise mõjutamise ulatus, intsidendi kestus või mõjutatud füüsiliste või juriidiliste isikute arv, võivad olla olulised selle kindlakstegemisel, kas tegevushäire on tõsine.

(37) Kuna asjaomase liidu üksuse ja liidu üksuse asukohaliikmesriigi taristu ja võrgu- ja infosüsteemid on omavahel seotud, on kõnealuse liikmesriigi jaoks väga oluline, et teda teavitataks põhjendamatu viivituseta olulisest intsidendist asjaomases liidu üksuses. Selleks peaks mõjutatud liidu üksus teavitama kõiki direktiivi (EL) 2022/2555 artiklite 8 ja 10 kohaselt määratud või asutatud asjaomaseid liikmesriikide samalaadseid asutusi olulisest intsidendist, millest ta CERT-EU-le teatab. Kui CERT-EU saab teada liikmesriigis aset leidnud olulisest intsidendist, peaks ta teavitama kõiki kõnealuse liikmesriigi asjaomaseid samalaadseid asutusi.

(38) Tuleks rakendada mehhanismi, millega tagatakse liidu üksuste tulemuslik teabevahetus, koordineerimine ja koostöö tõsiste intsidentide korral, sealhulgas asjaomaste liidu üksuste ülesannete ja kohustuste selge kindlaksmääramine. Kui küberkriiside haldamise kavast ei tulene teisiti, peaks komisjoni esindaja IICBs olema kontaktpunkt, et hõlbustada IICB-l tõsiste intsidentidega seotud asjakohase teabe jagamist Euroopa küberkriisiga tegelevate kontaktasutuste võrgustikuga (EU-CyCLONe), et aidata kaasa ühisele olukorrateadlikkusele. Komisjoni esindaja roll IICBs kontaktpunktina ei tohiks piirata komisjoni eraldiseisvat ja eristatavat rolli EU-CyCLONes vastavalt direktiivi (EL) 2022/2555 artikli 16 lõikele 2.

(39) Käesoleva määruse kohase isikuandmete töötlemise suhtes kohaldatakse Euroopa Parlamendi ja nõukogu määrust (EL) 2018/1725 ([7]). Isikuandmete töötlemine võib toimuda seoses meetmetega, mis on võetud küberturvalisuse riskijuhtimise, nõrkuste ja intsidentide käsitlemise, intsidentide, küberohtude ja nõrkuste kohta teabe jagamise ning intsidentidele reageerimise koordineerimise ja koostöö raames. Sellised meetmed võivad nõuda teatavat liiki isikuandmete töötlemist, nagu IP-aadressid, ühtsed ressursilokaatorid (URLid), domeeninimed, e-posti aadressid,

([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).

andmesubjekti organisatsioonilised rollid, ajatemplid, e-posti teemad või failinimed. Kõik käesoleva määruse kohaselt võetud meetmed peaksid olema kooskõlas andmekaitse- ja eraelu puutumatuse raamistikuga ning liidu üksused, CERT-EU ja asjakohasel juhul IICB peaksid võtma kõik asjakohased tehnilised ja korralduslikud kaitsemeetmed, et tagada nõuete järgimine vastutustundlikul viisil.

(40) Käesoleva määrusega luuakse õiguslik alus isikuandmete töötlemiseks liidu üksuste, CERT-EU ja asjakohasel juhul IICB poolt nende käesolevast määrusest tulenevate ülesannete ja kohustuste täitmiseks kooskõlas määruse (EL) 2018/1725 artikli 5 lõike 1 punktiga b. Vastavalt määrusele (EL) 2018/1725 võib CERT-EU tegutseda volitatud töötleja või vastutava töötlejana, sõltuvalt ülesandest, mida ta täidab.

(41) Teatavatel juhtudel võib liidu üksustel ja CERT-EU-l olla vaja töödelda määruse (EL) 2018/1725 artikli 10 lõikes 1 osutatud isikuandmete eriliike, et täita käesolevast määrusest tulenevaid kohustusi tagada küberturvalisuse kõrge tase ning eelkõige seoses nõrkuste ja intsidentide käsitlemisega. Käesoleva määrusega luuakse õiguslik alus isikuandmete eriliikide töötlemiseks liidu üksuste ja CERT-EU poolt kooskõlas määruse (EL) 2018/1725 artikli 10 lõike 2 punktiga g. Isikuandmete eriliikide töötlemine käesoleva määruse alusel peaks olema rangelt proportsionaalne taotletava eesmärgiga. Vastavalt kõnealuse määruse artikli 10 lõike 2 punktis g sätestatud tingimustele peaks liidu üksustel ja CERT-EU-l olema võimalik selliseid andmeid töödelda üksnes vajalikus ulatuses ja juhul, kui see on käesolevas määruses sõnaselgelt ette nähtud. Isikuandmete eriliikide töötlemisel peaksid liidu üksused ja CERT-EU austama isikuandmete kaitse õiguse olemust ja nägema ette sobivad ja konkreetsed meetmed andmesubjektide põhiõiguste ja huvide kaitseks.

(42) Määruse (EL) 2018/1725 artikli 33 kohaselt peaksid liidu üksused ja CERT-EU, võttes arvesse tehnika taset, rakendamise kulusid ning töötlemise laadi, ulatust, konteksti ja eesmärke, samuti erineva tõenäosuse ja suurusega ohte füüsiliste isikute õigustele ja vabadustele, rakendama asjakohaseid tehnilisi ja korralduslikke meetmeid, et tagada isikuandmete asjakohane turvalisuse tase, näiteks piiratud juurdepääsuõiguste andmine teadmisvajaduse alusel, kontrolljälje põhimõtete kohaldamine, järelevalveahela vastuvõtmine, jõudeolekus andmete säilitamine kontrollitud ja auditeeritavas keskkonnas, standardne töökord ja eraelu puutumatuse tagamise meetmed, nagu pseudonüümimine või krüpteerimine. Neid meetmeid ei tohiks rakendada viisil, mis mõjutab intsidentide käsitlemise ja tõendite tervikluse eesmärke. Kui liidu üksus või CERT-EU edastab käesoleva määruse kohaldamisel intsidendiga seotud isikuandmeid, sealhulgas isikuandmete eriliike, samalaadsele asutusele või partnerile, peaks selline edastamine toimuma kooskõlas määrusega (EL) 2018/1725. Isikuandmete eriliikide edastamisel kolmandale isikule peaksid liidu üksused ja CERT-EU tagama, et kolmas isik kohaldab isikuandmete kaitse meetmeid tasemel, mis on samaväärne määrusega (EL) 2018/1725.

(43) Käesoleva määruse otstarbel töödeldavaid isikuandmeid tuleks säilitada üksnes nii kaua, kui see on määruse (EL) 2018/1725 kohaselt vajalik. Liidu üksused, ja kui see on kohaldatav, vastutava töötlejana tegutsev CERT-EU, peaksid kehtestama säilitamistähtajad, mis piirduvad kindlaksmääratud eesmärkide saavutamiseks vajalikuga. Eelkõige seoses intsidentide käsitlemiseks kogutud isikuandmetega peaksid liidu üksused ja CERT-EU tegema vahet isikuandmetel, mida kogutakse küberohu tuvastamiseks nende IKT-keskkonnas, et intsidenti ennetada, ning isikuandmetel, mida kogutakse intsidendi leevendamiseks, sellele reageerimiseks ja sellest taastumiseks. Küberohu tuvastamiseks on oluline võtta arvesse aega, mille vältel ohusubjekt võib süsteemis tuvastamata jääda. Intsidendi leevendamiseks, sellele reageerimiseks ja sellest taastumiseks on oluline kaaluda, kas isikuandmed on vajalikud sellise korduva intsidendi või sarnase intsidendi jälgimiseks ja käsitlemiseks, mille puhul oleks võimalik tõendada korrelatsiooni.

(44) Liidu üksused ja CERT-EU peaksid teavet käitlema kooskõlas kohaldatavate infoturvet käsitlevate õigusnormidega. Personali turvalisuse lisamine küberturvalisuse riskijuhtimismeetmena peaks samuti olema kooskõlas kohaldatavate õigusnormidega.

(45) Teabe jagamiseks kasutatakse nähtavaid märgiseid, mis näitavad, et teabe saajad peavad kohaldama teabe jagamisel piiranguid, mis põhinevad eelkõige ametlikel või mitteametlikel mitteavalikustamise kokkulepetel, näiteks fooritulede analoogial põhineval protokollil teabe tundlikkuse märgistamiseks või muudel teabeallika poolt antud selgetel viidetel. Kõnealust protokolli tuleb mõista kui vahendit, millega antakse teavet teabe edasise levitamisega seotud piirangute kohta. Seda kasutatakse peaaegu kõigis CSIRTides ning mõnes teabeanalüüsi- ja -jagamiskeskuses.

(46) Käesolevat määrust tuleks korrapäraselt hinnata, pidades silmas tulevasi läbirääkimisi mitmeaastaste finantsraamistike üle, et oleks võimalik teha edasisi otsuseid CERT-EU toimimise ja institutsioonilise rolli kohta, sealhulgas CERT-EU võimaliku liidu ametina loomise kohta.

(47) IICB peaks CERT-EU abiga läbi vaatama ja hindama käesoleva määruse rakendamist ja teatama oma järeldustest komisjonile. Sellele teabele toetudes peaks komisjon esitama aruande Euroopa Parlamendile, nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ning Regioonide Komiteele. Kõnealuses aruandes, mille koostamisse annab oma panuse IICB, tuleks hinnata, kas ELi salastatud teavet käitlevate võrgu- ja infosüsteemide lisamine käesoleva määruse kohaldamisalasse on asjakohane, eelkõige juhul, kui liidu üksustel puuduvad ühised infoturbenormid.

(48) Vastavalt proportsionaalsuse põhimõttele on vajalik ja asjakohane selleks, et saavutada põhieesmärk, st küberturvalisuse ühtlaselt kõrge taseme saavutamine liidu üksustes, kehtestada küberturvalisust käsitlevad normid liidu üksuste jaoks. Euroopa Liidu lepingu (ELi leping) artikli 5 lõike 4 kohaselt ei lähe käesolev määrus seatud eesmärgi saavutamiseks vajalikust kaugemale.

(49) Käesolev määrus kajastab asjaolu, et liidu üksuste suurus ja suutlikkus on erinev, sealhulgas rahaliste vahendite ja inimressursside osas.

(50) Euroopa Andmekaitseinspektoriga konsulteeriti kooskõlas määruse (EL) 2018/1725 artikli 42 lõikega 1 ning ta esitas arvamuse 17. mail 2022 ([8]),

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

I PEATÜKK

ÜLDSÄTTED

Artikkel 1

Reguleerimisese

Käesolevas määruses sätestatakse meetmed, mille eesmärk on saavutada küberturvalisuse ühtlaselt kõrge tase liidu üksustes seoses järgmisega:

a) artikli 6 kohase sisemise küberturvalisusriskide juhtimis-, haldamis- ja kontrollraamistiku kehtestamine igas liidu üksuses;

b) küberturvalisuse riskijuhtimine, küberturvalisusriskidest teatamine ja teabevahetus;

c) artikli 10 kohaselt loodud institutsioonidevahelise küberturvalisuse nõukoja ülesehitus, toimimine ja töökorraldus ning liidu institutsioonide, organite ja asutuste küberturvalisuse teenistuse (CERT-EU) ülesehitus, toimimine ja töökorraldus;

d) käesoleva määruse rakendamise seire.

([8]) ELT C 258, 5.7.2022, lk 10.

Artikkel 2

Kohaldamisala

1. Käesolevat määrust kohaldatakse liidu üksuste, artikli 10 kohaselt loodud institutsioonidevahelise küberturvalisuse nõukoja ning CERT-EU suhtes.

2. Käesoleva määruse kohaldamine ei piira aluslepingute kohast institutsioonilist autonoomiat.

3. Käesolevat määrust, välja arvatud artikli 13 lõige 8, ei kohaldata ELi salastatud teavet käitlevate võrgu- ja infosüsteemide suhtes.

Artikkel 3

Mõisted

Käesolevas määruses kasutatakse järgmisi mõisteid:

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

2) „võrgu- ja infosüsteem“ – direktiivi (EL) 2022/2555 artikli 6 punktis 1 määratletud võrgu- ja infosüsteem;

3) „võrgu- ja infosüsteemide turvalisus“ – direktiivi (EL) 2022/2555 artikli 6 punktis 2 määratletud võrgu- ja infosüsteemide turvalisus;

4) „küberturvalisus“ – määruse (EL) 2019/881 artikli 2 punktis 1 määratletud küberturvalisus;

5) „kõrgeim juhtimistasand“ – liidu üksuse toimimise eest vastutav halduslikult kõige kõrgema tasandi juht, juhtkond või koordineerimise ja järelevalvega tegelev organ, kellel on volitus võtta vastu otsuseid või anda otsuste vastuvõtmiseks luba kooskõlas kõnealuse liidu üksuse kõrgema taseme juhtimise korraga, ilma et see piiraks muude juhtimistasandite ametlikke kohustusi nõuete järgimisel ja küberturvalisuse riskijuhtimisel oma vastutusalas;

6) „intsidendioht“ – direktiivi (EL) 2022/2555 artikli 6 punktis 5 määratletud intsidendioht;

7) „intsident“ – direktiivi (EL) 2022/2555 artikli 6 punktis 6 määratletud intsident;

8) „tõsine intsident“ – intsident, mis põhjustab häireid, mis ületavad liidu üksuse ja CERT-EU suutlikkust neile reageerida või millel on oluline mõju vähemalt kahele liidu üksusele;

9) „ulatuslik küberturbeintsident“ – direktiivi (EL) 2022/2555 artikli 6 punktis 7 määratletud ulatuslik küberturbeintsident;

10) „intsidendi käsitlemine“ – direktiivi (EL) 2022/2555 artikli 6 punktis 8 määratletud intsidendi käsitlemine;

11) „küberoht“ – määruse (EL) 2019/881 artikli 2 punktis 8 määratletud küberoht;

12) „oluline küberoht“ – direktiivi (EL) 2022/2555 artikli 6 punktis 11 määratletud oluline küberoht;

13) „nõrkus“ – direktiivi (EL) 2022/2555 artikli 6 punktis 15 määratletud nõrkus;

14) „küberturvalisuse risk“ – direktiivi (EL) 2022/2555 artikli 6 punktis 9 määratletud risk;

15) „pilvandmetöötlusteenus“ – direktiivi (EL) 2022/2555 artikli 6 punktis 30 määratletud pilvandmetöötlusteenus.

Artikkel 4

Isikuandmete töötlemine

1. CERT-EU, artikli 10 kohaselt loodud institutsioonidevaheline küberturvalisuse nõukoda ja liidu üksused töötlevad käesoleva määruse alusel isikuandmeid kooskõlas määrusega (EL) 2018/1725.

2. CERT-EU, artikli 10 kohaselt loodud institutsioonidevaheline küberturvalisuse nõukoda ja liidu üksused töötlevad ja vahetavad isikuandmeid käesoleva määruse kohaste ülesannete või kohustuste täitmisel üksnes kõnealuste ülesannete või kohustuste täitmise eesmärgil ja ulatuses, mis on selleks vajalik.

3. Määruse (EL) 2018/1725 artikli 10 lõikes 1 osutatud isikuandmete eriliikide töötlemist peetakse vajalikuks olulise avaliku huviga seotud põhjustel vastavalt kõnealuse määruse artikli 10 lõike 2 punktile g. Selliseid andmeid võib töödelda üksnes ulatuses, mis on vajalik käesoleva määruse artiklites 6 ja 8 osutatud küberturvalisuse riskijuhtimismeetmete rakendamiseks, CERT-EU teenuste osutamiseks vastavalt artiklile 13, konkreetse intsidendiga seotud teabe jagamiseks vastavalt artikli 17 lõikele 3 ja artikli 18 lõikele 3, teabe jagamiseks vastavalt artiklile 20, aruandekohustuste täitmiseks vastavalt artiklile 21, intsidentidele reageerimise koordineerimiseks ja koostööks vastavalt artiklile 22 ning tõsiste intsidentide haldamiseks vastavalt artiklile 23. Vastutava töötlejana kohaldavad liidu üksused ja CERT-EU tehnilisi meetmeid, et takistada isikuandmete eriliikide töötlemist muudel eesmärkidel, ning näevad ette sobivad erimeetmed andmesubjektide põhiõiguste ja huvide kaitseks.

II PEATÜKK

KÜBERTURVALISUSE ÜHTLASELT KÕRGE TASEME TAGAMISE MEETMED

Artikkel 5

Meetmete rakendamine

1. Hiljemalt 8. septembriks 2024 annab artikli 10 kohaselt loodud institutsioonidevaheline küberturvalisuse nõukoda pärast Euroopa Liidu Küberturvalisuse Ametiga (ENISA) konsulteerimist ja CERT-EU-lt juhiste saamist liidu üksustele suunised, et viia läbi esialgne küberturvalisuse alane läbivaatamine ning luua sisemise küberturvalisusriskide juhtimis-, haldamis- ja kontrollraamistik vastavalt artiklile 6, hinnata küberturvalisuse küpsustaset vastavalt artiklile 7, võtta küberturvalisuse riskijuhtimismeetmeid vastavalt artiklile 8 ja võtta vastu küberturvalisuse kava vastavalt artiklile 9.

2. Artiklite 6–9 rakendamisel võtavad liidu üksused arvesse käesoleva artikli lõikes 1 osutatud suuniseid ning vastavalt artiklitele 11 ja 14 vastu võetud asjakohaseid suuniseid ja soovitusi.

Artikkel 6

Küberturvalisusriskide juhtimis-, haldamis- ja kontrollraamistik

1. Hiljemalt 8. aprilliks 2025 kehtestab iga liidu üksus pärast küberturvalisuse alast esialgset läbivaatamist, näiteks auditit, sisemise küberturvalisusriskide juhtimis-, haldamis- ja kontrollraamistiku (edaspidi „raamistik“). Raamistiku kehtestamise üle teeb järelevalvet ja selle eest vastutab liidu üksuse kõrgeim juhtimistasand.

2. Raamistik peab hõlmama asjaomase liidu üksuse kogu salastamata IKT-keskkonda, sealhulgas ruumides kohapeal olev IKT-keskkond, käidutehnoloogia võrk, 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 nende keskkondadega (edaspidi „IKT-keskkond“). Raamistik põhineb kõiki ohte hõlmaval lähenemisviisil.

3. Raamistikuga tagatakse küberturvalisuse kõrge tase. Raamistikuga kehtestatakse võrgu- ja infosüsteemide turvalisusega seotud sisemised küberturvalisuse põhimõtted, sealhulgas eesmärgid ja prioriteedid, ning liidu üksuse nende töötajate roll ja kohustused, kelle ülesanne on tagada käesoleva määruse tulemuslik rakendamine. Raamistik sisaldab ka rakendamise tulemuslikkuse mõõtmise mehhanisme.

4. Raamistik vaadatakse läbi korrapäraselt, ent vähemalt iga nelja aasta tagant, võttes arvesse küberturvalisusriskide muutumist. Asjakohasel juhul ja artikli 10 kohaselt loodud institutsioonidevahelise küberturvalisuse nõukoja taotlusel võib liidu üksuse raamistikku ajakohastada vastavalt CERT-EU juhistele, mis käsitlevad kindlaks tehtud intsidente või käesoleva määruse rakendamisel täheldatud võimalikke lünki.

5. Iga liidu üksuse kõrgeim juhtimistasand vastutab käesoleva määruse rakendamise eest ja teeb järelevalvet selle üle, kuidas tema organisatsioon täidab raamistikuga seotud kohustusi.

6. Asjakohasel juhul ja ilma et see piiraks liidu üksuse kõrgeima juhtimistasandi vastutust käesoleva määruse rakendamise eest, võib iga liidu üksuse kõrgeim juhtimistasand delegeerida käesolevast määrusest tulenevad teatavad kohustused asjaomase liidu üksuse kõrgematele ametnikele personalieeskirjade artikli 29 lõike 2 tähenduses või muudele samaväärse tasandi ametnikele. Olenemata delegeerimisest võib kõrgeimat juhtimistasandit pidada vastutavaks käesoleva määruse rikkumise eest asjaomases liidu üksuses.

7. Igas liidu üksuses peavad olema toimivad mehhanismid, millega tagatakse, et küberturvalisusele kulutatakse piisav osa IKT eelarvest. Selle osa kindlaksmääramisel võetakse nõuetekohaselt arvesse raamistikku.

8. Iga liidu üksus nimetab ametisse kohaliku küberturvalisuse ametniku või samaväärseid ülesandeid täitva töötaja, kes on ühtne kontaktpunkt kõigis küberturvalisuse aspektides. Kohalik küberturvalisuse ametnik hõlbustab käesoleva määruse rakendamist ja annab otse kõrgeimale juhtimistasandile rakendamise seisust korrapäraselt aru. Ilma et see piiraks kohaliku küberturvalisuse ametniku tegutsemist igas liidu üksuses ühtse kontaktpunktina, võib liidu üksus delegeerida kohaliku küberturvalisuse ametniku teatavad käesoleva määruse rakendamisega seotud ülesanded CERT-EU-le kõnealuse liidu üksuse ja CERT-EU vahel sõlmitud teenustaseme kokkuleppe alusel või võib need ülesanded jagada mitme liidu üksuse vahel. Kui need ülesanded delegeeritakse CERT-EU-le, otsustab artikli 10 alusel loodud institutsioonidevaheline küberturvalisuse nõukoda, kas seda teenust osutatakse CERT-EU põhiteenuste osana, võttes arvesse asjaomase liidu üksuse inim- ja rahalisi ressursse. Iga liidu üksus teavitab põhjendamatu viivituseta CERT-EUd kohaliku küberturvalisuse ametniku ametisse nimetamisest ja sellega seotud hilisematest muudatustest.

CERT-EU koostab ametisse nimetatud kohalike küberturvalisuse ametnike nimekirja ja ajakohastab seda.

9. Iga liidu üksuse kõrgemad ametnikud personalieeskirjade artikli 29 lõike 2 tähenduses või muud samaväärse tasandi ametnikud ning kõik töötajad, kelle ülesanne on rakendada käesolevas määruses sätestatud küberturvalisuse riskijuhtimismeetmeid ja täita käesolevas määruses sätestatud kohustusi, osalevad korrapäraselt erikoolitustel, et omandada piisavad teadmised ja oskused küberturvalisuse riskide ja nende juhtimise tavade ning nende liidu üksuse tegevusele avalduva mõju mõistmiseks ja hindamiseks.

Artikkel 7

Küberturvalisuse küpsustaseme hindamine

1. Hiljemalt 8. juuliks 2025 ja seejärel vähemalt iga kahe aasta tagant viib iga liidu üksus läbi küberturvalisuse küpsustaseme hindamise, mis hõlmab kõiki tema IKT-keskkonna elemente.

2. Küberturvalisuse küpsustaseme hindamine viiakse asjakohasel juhul läbi valdkonnale spetsialiseerunud kolmanda isiku abiga.

3. Sarnase struktuuriga liidu üksused võivad oma asjaomaste üksuste küberturvalisuse küpsustaseme hindamisel teha koostööd.

4. Artikli 10 kohaselt loodud institutsioonidevahelise küberturvalisuse nõukoja taotlusel ja asjaomase liidu üksuse sõnaselgel nõusolekul võib küberturvalisuse küpsustaseme hindamise tulemusi arutada nimetatud nõukojas või kohalike küberturvalisuse ametnike mitteametlikus rühmas, et õppida kogemustest ja jagada parimaid tavasid.

Artikkel 8

Küberturvalisuse riskijuhtimismeetmed

1. Iga liidu üksus võtab põhjendamatu viivituseta ja igal juhul hiljemalt 8. septembriks 2025 oma kõrgeima juhtimistasandi järelevalve all asjakohased ja proportsionaalsed tehnilised, tegevuslikud ja korralduslikud meetmed, et juhtida raamistiku alusel kindlaks tehtud küberturvalisusriske ning hoida ära või minimeerida intsidentide mõju. Kõnealuste meetmetega tagatakse kogu IKT-keskkonnas võrgu- ja infosüsteemide turvalisuse tase, mis vastab asjakohastele küberturvalisusriskidele, võttes arvesse tehnika taset, ja kui see on kohaldatav, asjakohaseid Euroopa ja rahvusvahelisi standardeid. Kõnealuste meetmete proportsionaalsuse hindamisel võetakse igakülgselt arvesse liidu üksuse küberturvalisusriskidele avatuse määra, tema suurust ning intsidentide esinemise tõenäosust ja nende raskust, sealhulgas nende ühiskondlikku, majanduslikku ja institutsioonidevahelist mõju.

2. Liidu üksused käsitlevad küberturvalisuse riskijuhtimismeetmete rakendamisel vähemalt järgmisi valdkondi:

a) küberturvalisuse põhimõtted, sealhulgas artiklis 6 ja käesoleva artikli lõikes 3 osutatud eesmärkide ja prioriteetide saavutamiseks vajalikud meetmed;

b) küberturvalisuse riskide analüüsi ja infosüsteemide turvalisuse põhimõtted;

c) pilvandmetöötlusteenuste kasutamisega seotud põhimõtete eesmärgid;

d) asjakohasel juhul küberturvalisuse audit, mis võib hõlmata küberturvalisuse riskide, nõrkuste ja küberohtude hindamist, ning läbistustestimine, mida teeb korrapäraselt usaldusväärne erasektori teenuseosutaja;

e) punktis d osutatud küberturvalisuse audititest tulenevate soovituste rakendamine küberturvalisuse ja põhimõtete ajakohastamise kaudu;

f) küberturvalisuse korraldamine, sealhulgas ülesannete ja kohustuste kindlaksmääramine;

g) varade haldamine, sealhulgas IKT-varade inventeerimine ja IKT-võrgu kaardistamine;

h) personali turvalisus ja juurdepääsu kontroll;

i) tegevuse turvalisus;

j) teabeedastuse turvalisus;

k) süsteemide soetamine, arendamine ja hooldamine, sealhulgas nõrkuste käsitlemise ja avalikustamise põhimõtted;

l) võimaluse korral lähtekoodi läbipaistvuse põhimõtted;

m) tarneahela turvalisus, sealhulgas turvalisusega seotud aspektid iga liidu üksuse ja tema otseste tarnijate või teenuseosutajate vahelistes suhetes;

n) intsidentide käsitlemine ja koostöö CERT-EUga, näiteks pidev turvalisuse seire ja logipidamine;

o) talitluspidevuse juhtimine, näiteks varundushaldus ja avariitaaste, ning kriisiohje, ning

p) küberturvalisuse alase õppe, oskuste, teadlikkuse suurendamise, õppuste ja koolitusega seotud programmide edendamine ja arendamine.

Esimese lõigu punkti m kohaldamisel võtavad liidu üksused arvesse igale otsesele tarnijale ja teenuseosutajale omaseid nõrkusi ning oma tarnijate ja teenuseosutajate toodete üldist kvaliteeti ja küberturvalisuse tavasid, sealhulgas nende turvalise arenduse korda.

3. Liidu üksused võtavad vähemalt järgmisi küberturvalisuse riskijuhtimiserimeetmeid:

a) kaugtöö võimaldamise ja jätkamise tehniline kord;

b) konkreetsed sammud usaldamatuse põhimõtete järgimiseks;

c) võrgu- ja infosüsteemides mitmikautentimise kohustuslik kasutamine;

d) krüptograafia ja krüpteerimise, eelkõige otspunktkrüpteerimise ja turvalise digiallkirjastamise kasutamine;

e) asjakohasel juhul turvalise hääl-, video- ja tekstiside ning turvaliste hädaolukorra sidesüsteemide kasutamine liidu üksuses;

f) ennetavad meetmed paha- ja nuhkvara tuvastamiseks ja kõrvaldamiseks;

g) tarkvara tarneahela turvalisuse tagamine tarkvara arendamise ja hindamise turvalisuse kriteeriumide abil;

h) selliste küberturvalisuse alaste koolitusprogrammide koostamine ja vastuvõtmine, mis on vastavuses ülesannetega, mis on antud käesoleva määruse tulemusliku rakendamise tagamise eest vastutavale liidu üksuse kõrgeimale juhtimistasandile ja töötajatele, ja neilt eeldatava suutlikkusega;

i) töötajate korrapärane koolitamine küberturvalisuse teemal;

j) liidu üksuste omavahelise ühendatuse riskianalüüsides osalemine, kui see on asjakohane;

k) hankereeglite tõhustamine, et toetada küberturvalisuse ühtlaselt kõrget taset järgmiste vahenditega:

   i) selliste lepinguliste tõkete kõrvaldamine, mis piiravad IKT-teenuste osutajate võimalust jagada CERT-EUga teavet intsidentide, nõrkuste ja küberohtude kohta;

   ii) lepingulised kohustused teatada intsidentidest, nõrkustest ja küberohtudest ning luua asjakohased intsidentidele reageerimise ja nende seire mehhanismid.

Artikkel 9

Küberturvalisuse kavad

1. Lähtudes artikli 7 kohaselt tehtud küberturvalisuse küpsustaseme hindamise põhjal tehtud järeldustest ning võttes arvesse raamistikus kindlaks tehtud varasid ja küberturvalisusriske ning artikli 8 kohaselt võetud küberturvalisuse riskijuhtimismeetmeid, kiidab iga liidu üksuse kõrgeim juhtimistasand küberturvalisuse kava heaks ilma põhjendamatu viivituseta, ent igal juhul hiljemalt 8. jaanuariks 2026. Küberturvalisuse kava eesmärk on suurendada asjaomase liidu üksuse üldist küberturvalisust ja aidata seeläbi tõsta küberturvalisuse ühtlaselt kõrget taset liidu üksustes. Küberturvalisuse kava hõlmab vähemalt artikli 8 kohaselt võetud küberturvalisuse riskijuhtimismeetmeid. Küberturvalisuse kava vaadatakse läbi iga kahe aasta tagant või vajaduse korral tihemini pärast artikli 7 kohaselt tehtud küberturvalisuse küpsustaseme hindamist või raamistiku põhjalikku läbivaatamist.

2. Küberturvalisuse kava hõlmab liidu üksuse küberkriiside haldamise kava tõsiste intsidentide käsitlemiseks.

3. Liidu üksus esitab oma küberturvalisuse tervikkava artikli 10 kohaselt loodud institutsioonidevahelisele küberturvalisuse nõukojale.

III PEATÜKK

INSTITUTSIOONIDEVAHELINE KÜBERTURVALISUSE NÕUKODA

Artikkel 10

Institutsioonidevaheline küberturvalisuse nõukoda

1. Luuakse institutsioonidevaheline küberturvalisuse nõukoda (IICB).

2. IICB kohustused on järgmised:

a) seirata, kuidas liidu üksused käesolevat määrust rakendavad, ja toetada seda;

b) teha järelevalvet CERT-EU üldiste prioriteetide ja eesmärkide rakendamise üle ning anda CERT-EU-le strateegilisi suuniseid.

3. IICB-sse kuuluvad järgmised isikud:

a) üks esindaja, kelle määrab iga järgnevalt nimetatud üksus:

   i) Euroopa Parlament;

   ii) Euroopa Ülemkogu;

   iii) Euroopa Liidu Nõukogu;

   iv) komisjon;

   v) Euroopa Liidu Kohus;

   vi) Euroopa Keskpank;

   vii) Euroopa Kontrollikoda;

   viii) Euroopa välisteenistus;

   ix) Euroopa Majandus- ja Sotsiaalkomitee;

   x) Euroopa Regioonide Komitee;

   xi) Euroopa Investeerimispank;

   xii) küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskus;

   xiii) ENISA;

   xiv) Euroopa Andmekaitseinspektor;

   xv) Euroopa Liidu Kosmoseprogrammi Amet;

b) kolm esindajat, kelle määrab ELi asutuste võrgustik (EUAN) oma IKT nõuandekomitee ettepanekul ja kes esindavad oma IKT-keskkonda haldavate liidu organite ja asutuste huve, välja arvatud punktis a osutatud esindajad.

IICBs esindatud liidu üksused püüavad saavutada määratud esindajate seas soolise tasakaalu.

4. IICB liikmeid võivad abistada asendusliikmed. Juhataja võib IICB koosolekule osalema kutsuda lõikes 3 osutatud liidu üksuste või muude liidu üksuste muid esindajaid, kuid neil ei ole hääleõigust.

5. CERT-EU juht ja direktiivi (EL) 2022/2555 artikli 14 kohaselt loodud koostöörühma, artikli 15 kohaselt loodud CSIRTide võrgustiku ja artikli 16 kohaselt loodud EU-CyCLONe juhatajad või nende asendusliikmed võivad IICB koosolekul osaleda vaatlejana. Erandjuhtudel ja kooskõlas IICB kodukorraga võib IICB otsustada teisiti.

6. IICB võtab vastu oma kodukorra.

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

8. IICB kohtub vähemalt kolm korda aastas juhataja algatusel või CERT-EU või mõne oma liikme taotlusel.

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

10. IICB võib tegutseda oma kodukorra kohaselt algatatud lihtsustatud kirjaliku menetluse teel. Kõnealuse menetluse kohaselt loetakse asjaomane otsus juhataja määratud aja jooksul heakskiidetuks, kui mõni liige ei esita vastuväidet.

11. IICB sekretariaaditeenuseid osutab komisjon ja sekretariaat on vastutav IICB juhataja ees.

12. ELi asutuste võrgustiku poolt nimetatud esindajad edastavad IICB otsused ELi asutuste võrgustiku liikmetele. Igal ELi asutuste võrgustiku liikmel on õigus juhtida nende esindajate või IICB juhataja tähelepanu teemale, mis tema arvates peaks pälvima IICB tähelepanu.

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

14. IICB esitab hiljemalt 8. jaanuariks 2025 ja seejärel igal aastal Euroopa Parlamendile ja nõukogule aruande, milles kirjeldatakse üksikasjalikult käesoleva määruse rakendamisel tehtud edusamme ning täpsustatakse eelkõige, mil määral teeb CERT-EU koostööd iga liikmesriigi samalaadsete asutustega. Aruannet võetakse arvesse direktiivi (EL) 2022/2555 artikli 18 kohaselt iga kahe aasta tagant vastu võetavas aruandes, mis käsitleb küberturvalisuse olukorda liidus.

Artikkel 11

IICB ülesanded

Oma kohustuste täitmisel teeb IICB eeskätt järgmist:

a) annab CERT-EU juhile juhiseid;

b) seirab tõhusalt käesoleva määruse rakendamist ja teeb selle üle järelevalvet ning toetab liidu üksusi nende küberturvalisuse parandamisel, sealhulgas nõuab asjakohasel juhul liidu üksustelt ja CERT-EU-lt *ad hoc* aruandeid;

c) võtab pärast strateegilist arutelu vastu mitmeaastase strateegia liidu üksustes küberturvalisuse taseme tõstmiseks, hindab seda strateegiat korrapäraselt, ent vähemalt iga viie aasta tagant, ning muudab seda vajaduse korral;

d) töötab välja metoodika ja korralduslikud aspektid liidu üksuste vabatahtlike vastastikuste hindamiste tegemiseks, et õppida jagatud kogemustest, tugevdada vastastikust usaldust, saavutada küberturvalisuse ühtlaselt kõrge tase ja suurendada liidu üksuste küberturvalisuse alast suutlikkust, tagades, et selliseid vastastikuseid hindamisi teevad küberturvalisuse valdkonna eksperdid, kelle on määranud liidu üksus, mis ei ole hinnatav liidu üksus, ning et metoodika põhineb direktiivi (EL) 2022/2555 artiklil 19 ja on asjakohasel juhul kohandatud liidu üksustele;

e) kiidab CERT-EU juhi ettepaneku põhjal heaks CERT-EU iga-aastase tööprogrammi ja seirab selle rakendamist;

f) kiidab CERT-EU juhi ettepaneku põhjal heaks CERT-EU teenuste kataloogi ja kõik selle ajakohastused;

g) kiidab CERT-EU juhi ettepaneku põhjal heaks CERT-EU tegevuse iga-aastase tulude ja kulude finantskalkulatsiooni, sealhulgas seoses personaliga;

h) kiidab CERT-EU juhi ettepaneku põhjal heaks CERT-EU teenustaseme kokkulepete korra;

i) vaatab läbi ja kiidab heaks CERT-EU juhi koostatud aastaaruande, milles käsitletakse CERT-EU tegevust ja rahaliste vahendite haldamist;

j) kiidab heaks CERT-EU juhi ettepaneku põhjal kehtestatud CERT-EU põhilised tulemusnäitajad ja seirab neid;

k) kiidab heaks CERT-EU ja muude üksuste vahelised artikli 18 kohaselt sõlmitud koostöökokkulepped, teenustaseme kokkulepped ja lepingud;

l) võtab CERT-EU artikli 14 kohase ettepaneku alusel vastu suuniseid ja soovitusi ning annab CERT-EU-le korralduse esitada suuniste või soovituste ettepanek või üleskutse, see tagasi võtta või seda muuta;

m) loob spetsiifilisi ülesandeid täitvaid tehnilisi nõuanderühmi, et abistada IICBd tema töös, kiidab heaks nende pädevuse ja määrab nende juhatajad;

n) võtab vastu ja hindab liidu üksuste poolt käesoleva määruse alusel esitatud dokumente ja aruandeid, näiteks küberturvalisuse küpsustaseme hinnanguid;

o) hõlbustab ENISA toetatava, liidu üksuste kohalike küberturvalisuse ametnike mitteametliku rühma loomist, et vahetada käesoleva määruse rakendamisega seotud parimaid tavasid ja teavet;

p) seirab liidu üksuste IKT-keskkondade omavahelise ühendatuse korra asjakohasust ja annab nõuandeid võimalike paranduste tegemiseks, võttes arvesse CERT-EU esitatud teavet kindlaks tehtud küberturvalisusriskide ja saadud kogemuste kohta;

q) töötab välja küberkriiside haldamise kava, et toetada tegevuse tasandil liidu üksusi mõjutavate tõsiste intsidentide koordineeritud haldamist ja aidata kaasa asjakohase teabe korrapärasele vahetamisele, eelkõige seoses tõsiste intsidentide mõju ja raskusega ning nende mõju vähendamise võimalike viisidega;

r) koordineerib liidu eri üksuste artikli 9 lõikes 2 osutatud küberkriiside haldamise kavade vastuvõtmist;

s) võtab vastu artikli 8 lõike 2 esimese lõigu punkti m kohase tarneahela turvalisusega seotud soovitused, võttes arvesse direktiivi (EL) 2022/2555 artiklis 22 osutatud liidu tasandil kriitilise tähtsusega tarneahelate koordineeritud turberiski hindamise tulemusi, et toetada liidu üksusi tulemuslike ja proportsionaalsete küberturvalisuse riskijuhtimismeetmete vastuvõtmisel.

Artikkel 12

Nõuete järgimine

1. IICB teeb kooskõlas artikli 10 lõikega 2 ja artikliga 11 tulemuslikku seiret selle üle, kuidas liidu üksused rakendavad käesolevat määrust ning vastuvõetud suuniseid, soovitusi ja üleskutseid. IICB võib nõuda liidu üksustelt selleks vajalikku teavet või dokumente. Käesoleva artikli kohaste nõuete järgimise meetmete vastuvõtmisel ei ole liidu üksusel hääleõigust, kui asjaomane liidu üksus on otseselt esindatud IICBs.

2. Kui IICB leiab, et liidu üksus ei ole käesolevat määrust või käesoleva määruse alusel esitatud suuniseid, soovitusi või üleskutseid tulemuslikult järginud, võib ta pärast asjaomasele liidu üksusele võimaluse andmist tähelepanekute esitamiseks ja ilma, et see piiraks asjaomase liidu üksuse sisemenetlusi, teha järgmist:

a) edastada asjaomasele liidu üksusele põhjendatud arvamuse, milles juhitakse tähelepanu käesoleva määruse rakendamisel täheldatud puudustele;

b) anda pärast CERT-EUga konsulteerimist asjaomasele liidu üksusele suuniseid, tagamaks et selle raamistik, küberturvalisuse riskijuhtimismeetmed, küberturvalisuse kava ja aruandlus oleksid kindlaksmääratud aja jooksul käesoleva määrusega kooskõlas;

c) anda hoiatuse tuvastatud puuduste käsitlemiseks kindlaksmääratud aja jooksul, sealhulgas soovitused muuta asjaomase liidu üksuse poolt käesoleva määruse kohaselt vastu võetud meetmeid;

d) esitada asjaomasele liidu üksusele põhjendatud teate, kui punkti c kohaselt antud hoiatuses tuvastatud puudusi ei ole kindlaksmääratud aja jooksul piisavalt käsitletud;

e) esitada

i) soovituse viia läbi audit või

ii) nõude, et auditi teeks kolmandast isikust audiitor;

f) teavitada oma volituste piires kontrollikoda väidetavast nõuetele mittevastavusest, kui see on asjakohane;

g) esitada kõigile liikmesriikidele ja liidu üksustele soovituse peatada ajutiselt asjaomasele liidu üksusele suunatud andmevood.

Esimese lõigu punkti c kohaldamisel piiratakse hoiatuse sihtrühma asjakohaselt, kui see on vajalik küberturvalisusriski tõttu.

Esimese lõigu kohaselt esitatud hoiatused ja soovitused suunatakse asjaomase liidu üksuse kõrgeimale juhtimistasandile.

3. Kui IICB on võtnud lõike 2 esimese lõigu punktide a–g kohaseid meetmeid, esitab asjaomane liidu üksus IICB tuvastatud väidetavate puuduste kõrvaldamiseks võetud meetmete üksikasjad. Liidu üksus esitab need üksikasjad IICBga kokku lepitud mõistliku aja jooksul.

4. Kui IICB leiab, et liidu üksus rikub järjepidevalt käesolevat määrust, tingituna otseselt liidu ametniku või muu teenistuja tegevusest või tegevusetusest, sealhulgas kõrgeimal juhtimistasandil, nõuab IICB, et asjaomane liidu üksus võtaks asjakohased meetmed, sealhulgas nõuab, et üksus kaaluks distsiplinaarmeetmete võtmist kooskõlas personalieeskirjades sätestatud normide ja menetlustega ning muude kohaldatavate normide ja menetlustega. Selleks edastab IICB asjaomasele liidu üksusele vajaliku teabe.

5. Kui liidu üksus teatab, et ta ei suuda artikli 6 lõikes 1 ja artikli 8 lõikes 1 sätestatud tähtaegadest kinni pidada, võib IICB anda igakülgselt põhjendatud juhtudel ja liidu üksuse suurust arvesse võttes loa tähtaegu pikendada.

IV PEATÜKK

CERT-EU

Artikkel 13

CERT-EU missioon ja ülesanded

1. CERT-EU missioon on aidata kaasa kõigi liidu üksuste salastamata IKT-keskkonna turvalisusele, andes neile küberturvalisuse alast nõu, aidates neil intsidente ära hoida, tuvastada, neid käsitleda ja leevendada, intsidentidele reageerida ja neist taastuda ning tegutsedes nende küberturvalisuse alase teabevahetuse ja intsidentidele reageerimise koordineerimise keskusena.

2. CERT-EU kogub, haldab, analüüsib ja jagab liidu üksustega teavet, mis käsitleb salastamata IKT-taristu küberohte, nõrkusi ja sellega seotud intsidente. CERT-EU koordineerib intsidentidele reageerimist institutsioonidevahelisel ja liidu üksuste tasandil, andes muu hulgas operatiivset eriabi või koordineerides seda.

3. CERT-EU täidab liidu üksuste jaoks järgmisi ülesandeid:

a) toetab neid käesoleva määruse rakendamisel ja aitab seda koordineerida artikli 14 lõikes 1 loetletud meetmetega või IICB nõutud *ad hoc* aruannetega;

b) pakub kõigile liidu üksustele standardseid CSIRT-teenuseid teenustekataloogis kirjeldatud küberturvalisuse teenuste paketiga (edaspidi „baasteenused“);

c) hoiab alal samalaadsete organisatsioonide ja partnerite võrgustikku, et toetada teenuseid, nagu on kirjeldatud artiklites 17 ja 18;

d) juhib IICB tähelepanu probleemidele, mis on seotud käesoleva määruse rakendamisega ning suuniste, soovituste ja üleskutsete rakendamisega;

e) aitab lõikes 2 osutatud teabe põhjal ja tihedas koostöös ENISAga suurendada liidu küberolukorrateadlikkust;

f) koordineerib tõsiste intsidentide haldamist;

g) tegutseb liidu üksuste nimel samaväärsena koordinaatoriga, kes on määratud nõrkuste koordineeritud avalikustamise koordinaatoriks vastavalt direktiivi (EL) 2022/2555 artikli 12 lõikele 1;

h) tagab liidu üksuse taotlusel kõnealuse liidu üksuse üldkasutatavate võrgu- ja infosüsteemide ennetava välise kontrollimise.

Kui see on kohaldatav ja asjakohane, jagatakse esimese lõigu punktis e osutatud teavet IICB, CSIRTide võrgustiku ning Euroopa Liidu luure- ja situatsioonikeskusega (EU INTCEN), järgides seejuures asjakohaseid konfidentsiaalsusnõudeid.

4. CERT-EU võib asjakohasel juhul teha liidus ja selle liikmesriikides koostööd asjaomaste küberturvalisuse kogukondadega vastavalt artiklile 17 või 18, muuhulgas järgmistes valdkondades:

a) valmisolek, intsidentide koordineerimine, teabevahetus ja kriisidele reageerimine tehnilisel tasandil liidu üksustega seotud juhtumite puhul;

b) operatiivkoostöö seoses CSIRTide võrgustikuga, k.a vastastikuse abi valdkonnas;

c) küberohuteadmus, sh olukorrateadlikkus;

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

5. CERT-EU teeb enda pädevusse kuuluvates küsimustes struktureeritud koostööd ENISAga suutlikkuse suurendamise, operatiivkoostöö ja küberohtude pikaajalise strateegilise analüüsi vallas kooskõlas määrusega (EL) 2019/881. CERT-EU võib teha koostööd ja vahetada teavet Europoli küberkuritegevuse vastase võitluse Euroopa keskusega.

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

a) muud kui lõikes 3 osutatud teenused, mis toetavad liidu üksuste IKT-keskkonna küberturvalisust, teenustaseme kokkulepete põhjal ja vastavalt olemasolevatele ressurssidele, eelkõige ulatuslik võrkude seire, sealhulgas tõsiste küberohtude esmatasandi pidev seire;

b) teenused, mis toetavad liidu üksuste küberturvalisuse toiminguid või projekte, välja arvatud nende IKT-keskkonna kaitsmiseks mõeldud teenused, kirjaliku lepingu põhjal ja IICB eelneval heakskiidul;

c) taotluse korral asjaomase liidu üksuse võrgu- ja infosüsteemide ennetav kontrollimine, et tuvastada võimalikke olulise mõjuga nõrkusi;

d) teenused, mis toetavad selliste organisatsioonide IKT-keskkonna turvalisust, mis ei ole liidu üksused, kuid teevad liidu üksustega tihedat koostööd, näiteks kui neile on liidu õiguse alusel määratud ülesandeid või kohustusi, kirjaliku lepingu põhjal ja IICB eelneval heakskiidul.

Võttes arvesse esimese lõigu punkti d, võib CERT-EU erandkorras sõlmida teenustaseme kokkuleppeid muude üksustega kui liidu üksused, kui IICB on selle eelnevalt heaks kiitnud.

7. CERT-EU korraldab küberturvalisuse õppusi ja võib neil osaleda või soovitada osaleda olemasolevatel õppustel, tehes seda tihedas koostöös ENISAga alati, kui see on asjakohane, et kontrollida liidu üksuste küberturvalisuse taset.

8. CERT-EU võib pakkuda liidu üksustele abi ELi salastatud teavet käitlevate võrgu- ja infosüsteemide intsidentide puhul, kui asjaomased liidu üksused seda temalt oma vastavate menetluste kohaselt sõnaselgelt taotlevad. CERT-EU poolt käesoleva lõike alusel abi osutamine ei piira salastatud teabe kaitseks kehtestatud reeglite järgimist.

9. CERT-EU teavitab liidu üksusi oma intsidendi käsitlemise menetlustest ja protsessidest.

10. CERT-EU edastab asjakohaste koostöömehhanismide ja aruandlusahelate kaudu olulise ja anonüümitud teabe tõsiste intsidentide ja nende käsitlemisviisi kohta, tagades seejuures konfidentsiaalsuse ja usaldusväärsuse kõrge taseme. See teave lisatakse artikli 10 lõikes 14 osutatud aruandesse.

11. CERT-EU toetab koostöös Euroopa Andmekaitseinspektoriga liidu üksusi selliste intsidentide käsitlemisel, millega kaasneb isikuandmetega seotud rikkumine, ilma et see piiraks Euroopa Andmekaitseinspektori kui järelevalveasutuse ülesandeid ja pädevust määruse (EL) 2018/1725 alusel.

12. CERT-EU võib asjakohastes poliitikaküsimustes anda tehnilist nõu või sisendit, kui liidu üksuste poliitikaosakonnad on seda sõnaselgelt taotlenud.

Artikkel 14

Suunised, soovitused ja üleskutsed

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

a) üleskutsed, milles kirjeldatakse kiireloomulisi turbemeetmeid, mida liidu üksused peaksid võtma kindlaksmääratud aja jooksul;

b) ettepanekud IICB-le suuniste kohta, mis on adresseeritud kõigile liidu üksustele või mõnedele nende hulgast;

c) ettepanekud IICB-le soovituste kohta, mis on adresseeritud konkreetsetele liidu üksustele.

Võttes arvesse esimese lõigu punkti a, annab asjaomane liidu üksus põhjendamatu viivituseta pärast üleskutse saamist CERT-EU-le teada, kuidas kiireloomulisi turbemeetmeid rakendati.

2. Suunised ja soovitused võivad sisaldada:

a) ühtset metoodikat ja mudelit liidu üksuste küberturvalisuse küpsustaseme hindamiseks, sealhulgas vastavaid skaalasid või peamisi tulemusnäitajaid, mida kasutatakse võrdlusalusena küberturvalisuse pideva suurendamise toetamisel kõigis liidu üksustes ning küberturvalisuse valdkondade ja meetmete prioriseerimise hõlbustamisel, võttes arvesse üksuste turvaoleku taset kübervaldkonnas;

b) küberturvalisuse riskijuhtimise ja küberturvalisuse riskijuhtimismeetmete üksikasju või parendusi;

c) küberturvalisuse küpsustaseme hindamise ja küberturvalisuse kavade üksikasju;

d) kui see on asjakohane, ühise tehnoloogia, arhitektuuri, avatud lähtekoodi ja nendega seotud heade tavade kasutamist, et saavutada koostalitlusvõime ja ühised standardid, sealhulgas koordineeritud lähenemisviis tarneahela turvalisusele;

e) kui see on asjakohane, teavet, mis hõlbustaks ühishankevahendite kasutamist asjaomaste küberturvalisuse teenuste ja toodete ostmiseks kolmandast isikust tarnijatelt;

f) artikli 20 kohast teabevahetuskorda.

Artikkel 15

CERT-EU juht

1. Pärast kahe kolmandiku IICB liikmete heakskiidu saamist nimetab komisjon ametisse CERT-EU juhi. IICBga konsulteeritakse kõigis ametisse nimetamise menetluse etappides, eeskätt vaba ametikoha teadete koostamise, avalduste läbivaatamise ja selle ametikohaga seotud valikukomisjonide ametisse nimetamise käigus. Kogu valikumenetluse jooksul, sealhulgas lõpliku nimekirja koostamisel kandidaatidest, kelle hulgast CERT-EU juht ametisse nimetatakse, tagatakse esitatud taotlusi arvesse võttes sugude õiglane esindatus.

2. CERT-EU juht vastutab CERT-EU sujuva toimimise eest, tegutsedes oma pädevusvaldkonna piires ja IICB juhtimisel. CERT-EU juht annab korrapäraselt aru IICB juhatajale ja esitab IICB-le *ad hoc* aruandeid, kui IICB on seda taotlenud.

3. CERT-EU juht aitab vastutaval volitatud eelarvevahendite käsutajal koostada iga-aastast tegevusaruannet, mis sisaldab finants- ja haldusteavet, sh kontrollide tulemusi, ning mis koostatakse vastavalt Euroopa Parlamendi ja nõukogu määruse (EL, Euratom) 2018/1046 ([9]) artikli 74 lõikele 9, ning ta annab volitatud eelarvevahendite käsutajale korrapäraselt aru nende meetmete rakendamisest, millega seoses volitused CERT-EU juhile delegeeriti.

4. CERT-EU juht töötab igal aastal välja oma tegevuse haldustulude ja -kulude finantskalkulatsiooni, iga-aastase tööprogrammi ettepaneku, CERT-EU teenuste kataloogi ettepaneku, CERT-EU teenuste kataloogi muudatuste ettepanekud, teenustaseme kokkulepete korra ettepanekud ning CERT-EU peamiste tulemusnäitajate ettepaneku, mille peab heaks kiitma IICB kooskõlas artikliga 11. CERT-EU teenuste kataloogi teenuste loendi läbivaatamisel võtab CERT-EU juht arvesse CERT-EU-le eraldatud vahendeid.

5. CERT-EU juht esitab vähemalt kord aastas IICB-le ja IICB juhatajale aruanded CERT-EU tulemuslikkuse ja tegevuse kohta aruandeperioodil, sealhulgas eelarve täitmise, teenustaseme kokkulepete ja sõlmitud kirjalike lepingute, samalaadsete asutuste ja partneritega tehtava koostöö ning töötajate lähetuste kohta, sh artiklis 11 osutatud aruanded. Need aruanded sisaldavad järgmise perioodi tööprogrammi, tulude ja kulude finantskalkulatsiooni, sh seoses personaliga, CERT-EU teenuste kataloogi kavandatud ajakohastamisi ning hinnangut selle kohta, kuidas sellised ajakohastamised võivad eeldatavalt mõjutada rahalisi ja inimressursse.

Artikkel 16

Personali- ja finantsküsimused

1. CERT-EU integreeritakse komisjoni ühe peadirektoraadi haldusstruktuuri, et kasutada ära komisjoni haldus- ja finantsjuhtimis- ning raamatupidamisalaste tugistruktuuride eeliseid, kuid samal ajal säilitatakse selle staatus autonoomse institutsioonidevahelise teenuseosutajana kõigile liidu üksustele. Komisjon teavitab IICBd CERT-EU halduslikust asukohast ja selle mis tahes muudatustest. Komisjon vaatab CERT-EUga seotud halduskokkulepped korrapäraselt ja igal juhul enne ELi toimimise lepingu artikli 312 kohase mitmeaastase finantsraamistiku kehtestamist läbi, et võimaldada asjakohaste meetmete võtmist. Läbivaatamine käsitleb ka võimalust muuta CERT-EU liidu ametiks.

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

([9]) 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).

3. CERT-EU ülesandeid ja tegevusi, sh teenuseid, mida CERT-EU osutab artikli 13 lõigete 3, 4, 5 ja 7 ning artikli 14 lõike 1 alusel liidu üksustele, 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. Muud kui käesoleva artikli lõikes 3 osutatud liidu üksused teevad CERT-EU-le igal aastal rahalise eraldise teenuste eest, mida CERT-EU osutab vastavalt nimetatud lõikele. Eraldised põhinevad orientiiridel, mille on andnud IICB ja milles iga liidu üksus ja CERT-EU on kokku leppinud teenustaseme kokkulepetes. Eraldised peavad moodustama õiglase ja proportsionaalse osa osutatud teenuste kogukuludest. Need kantakse käesoleva artikli lõikes 3 osutatud eraldi eelarvereale sihtotstarbelise sisetuluna vastavalt määruse (EL, Euratom) 2018/1046 artikli 21 lõike 3 punktile c.

5. Artikli 13 lõikes 6 määratletud teenustega seotud kulud katavad liidu üksused, kes CERT-EU teenuseid tarbivad. Tulu kantakse eelarvereale, millelt kulusid kaetakse.

Artikkel 17

CERT-EU koostöö liikmesriikide samalaadsete asutustega

1. CERT-EU teeb liikmesriikide samalaadsete asutustega, sh direktiivi (EL) 2022/2555 artikli 10 kohaselt määratud või asutatud CSIRTidega või asjakohasel juhul pädevate asutustega ja sama direktiivi artikli 8 kohaselt määratud või asutatud ühtsete kontaktpunktidega põhjendamatu viivituseta koostööd ja vahetab nendega teavet küsimustes, mis puudutavad intsidente, küberohte, nõrkusi, ohuolukordi, võimalikke vastumeetmeid ja häid tavasid, ning kõigis küsimustes, mis on asjakohased liidu üksuste IKT-keskkondade kaitse parandamiseks, sh direktiivi (EL) 2022/2555 artiklis 15 osutatud CSIRTide võrgustiku kaudu. CERT-EU toetab komisjoni direktiivi (EL) 2022/2555 artikli 16 kohaselt loodud EU-CyCLONe töös ulatuslike küberturbeintsidentide ja kriiside koordineeritud haldamisel.

2. Kui CERT-EU saab teada liikmesriigi territooriumil aset leidnud olulisest intsidendist. teavitab ta vastavalt lõikele 1 viivitamata kõiki kõnealuse liikmesriigi asjaomaseid samalaadseid asutusi.

3. CERT-EU vahetab põhjendamatu viivituseta ja tingimusel, et isikuandmeid kaitstakse kohaldatava liidu andmekaitsealase õiguse kohaselt, liikmesriikide samalaadsete asutustega asjakohast teavet konkreetse intsidendi kohta, et hõlbustada samalaadsete küberohtude või intsidentide avastamist või aidata intsidenti analüüsida, ilma mõjutatud liidu üksuse loata. CERT-EU vahetab konkreetse intsidendi kohta sellist teavet, millest ilmneb intsidendi sihtmärgi identiteet, üksnes juhul, kui:

a) mõjutatud liidu üksus annab selleks oma nõusoleku;

b) mõjutatud liidu üksus ei ole punktis a sätestatu kohaselt oma nõusolekut andnud, kuid mõjutatud liidu üksuse identiteedi avaldamine suurendaks tõenäosust, et seeläbi välditakse või leevendatakse intsidente mujal;

c) mõjutatud liidu üksus on juba avalikustanud, et see intsident on teda mõjutanud.

Otsused konkreetse intsidendi kohta sellise teabe vahetamiseks, millest ilmneb intsidendi sihtmärgi identiteet vastavalt esimese lõigu punktile b, kiidab heaks CERT-EU juht. Enne sellise otsuse tegemist võtab CERT-EU mõjutatud liidu üksusega kirjalikult ühendust ja selgitab, kuidas tema identiteedi avalikustamine aitaks vältida või leevendada intsidente mujal. CERT-EU juht esitab omapoolse selgituse ja palub sõnaselgelt, et liidu üksus teataks, kas ta annab oma nõusoleku kindlaksmääratud ajavahemiku jooksul. CERT-EU juht teavitab liidu üksust ka sellest, et esitatud selgitust arvesse võttes jätab ta endale õiguse avaldada teave isegi juhul, kui üksus selleks oma nõusolekut ei anna. Enne kui teave avalikustatakse, teavitatakse sellest mõjutatud liidu üksust.

Artikkel 18

CERT-EU koostöö teiste samalaadsete asutustega

1. CERT-EU võib teha töövahendite ja meetodite, nt tehnika, taktika, menetluste ja heade tavade, ning küberohtude ja nõrkuste alast koostööd liidus asuvate teiste samalaadsete asutustega, v.a artiklis 17 osutatud asutused, kelle suhtes kehtivad liidu küberturvalisuse nõuded, sh sektoripõhiste samalaadsete asutustega. Igasuguseks koostööks selliste samalaadsete asutustega taotleb CERT-EU igal üksikjuhul eraldi eelnevat IICB heakskiitu. Kui CERT-EU alustab sellise samalaadse asutusega koostööd, teavitab ta sellest kõiki asjaomaseid artikli 17 lõikes 1 osutatud samalaadseid asutusi liikmesriigis, kus kõnealune samalaadne asutus asub. Kui see on kohaldatav ja asjakohane, reguleeritakse selline koostöö ja selle tingimused, sealhulgas seoses küberturvalisuse, andmekaitse ja teabe käitlemisega, konkreetsete konfidentsiaalsuskokkulepetega, näiteks lepingute või halduskokkulepetega. Konfidentsiaalsuskokkuleppeid ei pea IICB eelnevalt heaks kiitma, kuid neist tuleb IICB juhatajale teada anda. Kui tekib kiireloomuline ja otsene vajadus vahetada küberturvalisuse alast teavet liidu üksuste või mõne muu poole huvides, võib CERT-EU seda teha sellise üksuse kaasabil, kelle spetsiifiline pädevus, suutlikkus ja eksperditeadmised on põhjendatult vajalikud niisuguse kiireloomulise ja otsese vajaduse korral isegi juhul, kui CERT-EU-l ei ole selle üksusega konfidentsiaalsuskokkulepet. Sellisel juhul teavitab CERT-EU viivitamata IICB juhatajat ja annab IICB-le aru korrapäraste aruannete või kohtumiste kaudu.

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

3. CERT-EU võib intsidendist mõjutatud liidu üksuse nõusolekul ja tingimusel, et asjaomase samalaadse asutuse või partneriga on sõlmitud mitteavalikustamise kokkulepe või leping, esitada lõigetes 1 ja 2 osutatud samalaadsetele asutustele või partneritele konkreetse intsidendi kohta käivat teavet üksnes selle analüüsimisse panustamise eesmärgil.

V PEATÜKK

KOOSTÖÖ- JA ARUANDEKOHUSTUSED

Artikkel 19

Teabe käitlemine

1. Liidu üksused ja CERT-EU järgivad ametisaladuse hoidmise kohustust kooskõlas ELi toimimise lepingu artikliga 339 või samaväärsete kohaldatavate raamistikega.

2. CERT-EU valduses olevatele dokumentidele üldsuse juurdepääsu taotluste suhtes kohaldatakse Euroopa Parlamendi ja nõukogu määrust (EÜ) nr 1049/2001 ([10]), kaasa arvatud nimetatud määruse kohast kohustust konsulteerida teiste liidu üksuste ning asjakohasel juhul liikmesriikidega alati, kui taotlus puudutab nende dokumente.

3. Liidu üksused ja CERT-EU käitlevad teavet kooskõlas kohaldatavate infoturvet käsitlevate õigusnormidega.

([10]) 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).

Artikkel 20

Küberturvalisuse alase teabe jagamise kord

1. Liidu üksused võivad vabatahtlikult teatada CERT-EU-le neid mõjutavatest intsidentidest, küberohtudest, ohuolukordadest ja nõrkustest ning anda sellekohast teavet. CERT-EU tagab selliste tõhusate sidevahendite olemasolu, mis kindlustavad kõrgel tasemel jälgitavuse, konfidentsiaalsuse ja usaldusväärsuse, et hõlbustada liidu üksustega teabe jagamist. Teadete töötlemisel võib CERT-EU seada kohustuslike teadete menetlemise vabatahtlike teadete menetlemisest tähtsamale kohale. Ilma et see piiraks artikli 12 kohaldamist, ei too vabatahtlik teatamine teadet esitavale liidu üksusele kaasa lisakohustusi, mida tal ei oleks olnud, kui ta ei oleks teadet esitanud.

2. Selleks et täita oma artiklist 13 tulenevat missiooni ja ülesandeid, võib CERT-EU taotleda, et liidu üksused esitaksid talle oma IKT-süsteemide varade loendist teavet, sealhulgas teavet, mis käsitleb küberohtusid, ohuolukordi, nõrkusi, rikkeindikaatoreid, küberturvalisuse hoiatusi ning soovitusi seoses intsidentide tuvastamiseks vajalike küberturvalisuse vahendite konfiguratsiooniga. Taotluse saanud liidu üksus edastab taotletud teabe ja kõik selle hilisemad ajakohastused põhjendamatu viivituseta.

3. Sellist teavet, millest ilmneb intsidendist mõjutatud liidu üksuse identiteet, võib CERT-EU intsidendi kohta vahetada liidu üksustega tingimusel, et mõjutatud liidu üksus annab selleks nõusoleku. Nõusoleku andmisest keeldumise korral esitab liidu üksus CERT-EU-le oma otsuse põhjendused.

4. Liidu üksused jagavad taotluse korral Euroopa Parlamendi ja nõukoguga teavet küberturvalisuse kavade lõpuleviimise kohta.

5. IICB või CERT-EU, nagu on asjakohane, jagab taotluse korral suuniseid, soovitusi ja üleskutseid Euroopa Parlamendi ja nõukoguga.

6. Käesolevas artiklis sätestatud jagamiskohustused ei laiene

a) ELi salastatud teabele;

b) teabele, mille edasine levitamine on nähtava märgistuse abil välistatud, välja arvatud juhul, kui selle jagamiseks CERT-EUga on antud sõnaselge luba.

Artikkel 21

Aruandekohustused

1. Intsidenti käsitatakse olulisena, kui:

a) see on põhjustanud või võib põhjustada tõsiseid häireid asjaomase liidu üksuse toimimises või rahalist kahju sellele üksusele;

b) see on mõjutanud või võib mõjutada teisi füüsilisi või juriidilisi isikuid, põhjustades märkimisväärset materiaalset või mittemateriaalset kahju.

2. Liidu üksused esitavad CERT-EU-le:

a) põhjendamatu viivituseta, ent igal juhul 24 tunni jooksul pärast olulisest intsidendist teadasaamist varajase hoiatuse, milles asjakohasel juhul märgitakse, et olulise intsidendi põhjuseks on eeldatavasti ebaseaduslik või pahatahtlik tegevus või et sellel võib olla üksuseülene või piiriülene mõju;

b) põhjendamatu viivituseta, ent igal juhul 72 tunni jooksul pärast olulisest intsidendist teadasaamist intsidenditeate, millega asjakohasel juhul ajakohastatakse punktis a osutatud teavet ning antakse esialgne hinnang olulisele intsidendile, sealhulgas selle raskusastmele ja mõjule ning võimaluse korral ka rikkeindikaatoritele;

c) CERT-EU taotlusel vahearuande vaatlusaluste asjade seisu kohta;

d) hiljemalt üks kuu pärast punkti b kohase intsidenditeate edastamist lõpparuande, mis sisaldab järgmist:

i) intsidendi, sealhulgas selle raskusastme ja mõju üksikasjalik kirjeldus;

ii) intsidendi tõenäoliselt põhjustanud ohu liik või algpõhjus;

iii) kohaldatud ja kohaldamisel olevad leevendusmeetmed;

iv) asjakohasel juhul intsidendi piiriülene või üksuseülene mõju;

e) kui intsident punktis d osutatud lõpparuande esitamise ajal veel kestab, hetkeseisu kajastava eduaruande ja ühe kuu jooksul pärast intsidendi käsitlemist üksuste poolt lõpparuande.

3. Liidu üksus teavitab põhjendamatu viivituseta, ent igal juhul 24 tunni jooksul pärast olulisest intsidendist teadasaamist artikli 17 lõikes 1 osutatud liikmesriikide samalaadseid asutusi liikmesriigis, kus ta asub, olulise intsidendi ilmnemisest.

4. Liidu üksused esitavad muu hulgas mis tahes teabe, mis võimaldab CERT-EU-l teha kindlaks sellest olulisest intsidendist lähtuva üksuseülese mõju, vastuvõtvale liikmesriigile avalduva mõju või piiriülese mõju. Ilma et see piiraks artikli 12 kohaldamist, ei suurene teavitava üksuse vastutus üksnes teavitamise tõttu.

5. Kui see on kohaldatav, teavitavad liidu üksused mõjutatud võrgu- ja infosüsteemide või muude selliste IKT-keskkonna komponentide kasutajaid, mida oluline intsident või oluline küberoht võib mõjutada, ja kes peavad asjakohasel juhul võtma leevendusmeetmeid, põhjendamatu viivituseta meetmetest või parandusmeetmetest, mida nad saavad sellele intsidendile või ohule reageerimiseks võtta. Kui see on asjakohane, teavitavad liidu üksused kõnealuseid kasutajaid ka olulisest küberohust endast.

6. Kui oluline intsident või oluline küberoht mõjutab võrgu- ja infosüsteemi või liidu üksuse IKT-keskkonna sellist komponenti, mis on teadlikult ühendatud mõne teise liidu üksuse IKT-keskkonnaga, väljastab CERT-EU asjakohase küberturvalisuse hoiatuse.

7. Liidu üksused esitavad CERT-EU taotlusel CERT-EU-le põhjendamatu viivituseta digitaalse teabe, mis on tekkinud nende vastavate intsidentidega seotud elektrooniliste seadmete kasutamisel. CERT-EU võib esitada täiendavaid üksikasju sellise teabe liigi kohta, mida ta vajab olukorrateadlikkuse ja intsidentidele reageerimise jaoks.

8. CERT-EU esitab IICB-le, ENISA-le, EU INTCENile ja CSIRTide võrgustikule iga kolme kuu tagant koondaruande, mis sisaldab anonüümitud ja koondatud andmeid oluliste intsidentide, intsidentide, küberohtude, ohuolukordade ja nõrkuste kohta vastavalt artiklile 20 ning käesoleva artikli lõike 2 kohaselt teatatud oluliste intsidentide kohta. Koondaruannet võetakse arvesse direktiivi (EL) 2022/2555 artikli 18 kohaselt iga kahe aasta järel vastu võetavas aruandes, mis käsitleb küberturvalisuse olukorda liidus.

9. Hiljemalt 8. juuliks 2024 annab IICB välja suunised või soovitused, milles täpsustatakse käesoleva artikli alusel aruandmise täiendavad üksikasjad, vorming ja sisu. Selliste suuniste või soovituste koostamisel võtab IICB arvesse kõiki direktiivi (EL) 2022/2555 artikli 23 lõike 11 kohaselt vastu võetud rakendusakte, milles täpsustatakse teavituse teabeliik, vorming ja esitamise kord. CERT-EU levitab asjakohaseid tehnilisi üksikasju, et liidu üksused saaksid tegeleda ennetava tuvastamise, intsidentidele reageerimise või leevendusmeetmetega.

10. Käesolevas artiklis sätestatud aruandekohustused ei laiene

a) ELi salastatud teabele;

b) teabele, mille edasine levitamine on nähtava märgistuse abil välistatud, välja arvatud juhul, kui selle jagamiseks CERT-EUga on antud sõnaselge luba.

Artikkel 22

Intsidentidele reageerimise koordineerimine ja koostöö

1. Küberturvalisuse alase teabevahetuse ja intsidentidele reageerimise koordineerimise keskusena hõlbustab CERT-EU intsidentide, küberohtude, nõrkuste ja ohuolukordadega seotud teabevahetust järgnevalt nimetatute vahel:

a) liidu üksused;

b) artiklites 17 ja 18 osutatud samalaadsed asutused.

2. CERT-EU hõlbustab asjakohasel juhul ja tihedas koostöös ENISAga intsidentidele reageerimise alast koordineerimist liidu üksuste vahel, sealhulgas:

a) panustamist järjepidevasse välissuhtlusesse;

b) vastastikust toetust, nagu liidu üksustele olulise teabe jagamine või abistamine vahetult kohapeal, kui see on asjakohane;

c) operatiivressursside optimaalset kasutamist;

d) koordineerimist muude kriisidele reageerimise mehhanismidega liidu tasandil.

3. CERT-EU toetab tihedas koostöös ENISAga liidu üksusi intsidentide, küberohtude, nõrkuste ja ohuolukordade alase olukorrateadlikkuse vallas, samuti küberturvalisuse valdkonna asjakohaste arengusuundumuste alase teabe jagamise vallas.

4. Hiljemalt 8. jaanuariks 2025 võtab IICB CERT-EU ettepaneku alusel vastu suunised või soovitused intsidentidele reageerimise koordineerimise ja koostöö kohta oluliste intsidentide korral. Kui kahtlustatakse, et intsident on kuritegelik, annab CERT-EU nõu selle kohta, kuidas teatada intsidendist põhjendamatu viivituseta õiguskaitseasutustele.

5. Liikmesriigi konkreetse taotluse alusel ja asjaomaste liidu üksuste nõusolekul võib CERT-EU kutsuda artikli 23 lõikes 4 osutatud nimekirjast eksperte, et aidata reageerida kõnealust liikmesriiki mõjutavale tõsisele intsidendile või ulatuslikule küberturbeintsidendile kooskõlas direktiivi (EL) 2022/2555 artikli 15 lõike 3 punktiga g. Konkreetsed reeglid, mille alusel saab liidu üksustest tehnilisi eksperte kutsuda ja nende teadmisi kasutada, kiidab CERT-EU ettepaneku alusel heaks IICB.

Artikkel 23

Tõsiste intsidentide haldamine

1. Selleks et toetada liidu üksusi mõjutavate tõsiste intsidentide koordineeritud haldamist operatiivtasandil ning aidata kaasa asjakohase teabe korrapärasele vahetamisele liidu üksuste vahel ja liikmesriikidega, töötab IICB vastavalt artikli 11 punktile q ning tihedas koostöös CERT-EU ja ENISAga välja artikli 22 lõikes 2 osutatud tegevustel põhineva küberkriiside haldamise kava. Küberkriiside haldamise kava sisaldab vähemalt järgmist:

a) liidu üksuste vahelise koordineerimise ja teabevoo kord tõsiste intsidentide haldamiseks operatiivtasandil;

b) ühtne standardne töökord;

c) tõsiste intsidentide raskusastme ja kriisi käivitavate tegurite ühtne taksonoomia;

d) korrapärased õppused;

e) kasutatavad turvalised sidekanalid.

2. Käesoleva artikli lõike 1 alusel välja töötatud küberkriiside haldamise kava kohaldamisel ja ilma et see piiraks direktiivi (EL) 2022/2555 artikli 16 lõike 2 esimese lõigu kohaldamist, toimib IICB tegevuses osalev komisjoni esindaja kontaktpunktina tõsiste intsidentidega seotud asjakohase teabe jagamisel EU-CyCLONega.

3. CERT-EU koordineerib tõsiste intsidentide haldamist liidu üksuste vahel. CERT-EU peab loendit olemasolevatest tehnilistest eksperditeadmistest, mida oleks vaja tõsiste intsidentide korral intsidentidele reageerimiseks, ning aitab IICB-l koordineerida artikli 9 lõikes 2 osutatud liidu üksuste küberkriiside haldamise kavasid tõsiste intsidentide käsitlemiseks.

4. Liidu üksused annavad oma panuse tehniliste eksperditeadmiste loendisse ning esitavad igal aastal ajakohastatava nimekirja oma vastavates organisatsioonides tegutsevatest ekspertidest, märkides ära nende konkreetsed tehnilised oskused.

VI PEATÜKK

LÕPPSÄTTED

Artikkel 24

Eelarve esialgne ümberjaotamine

Et tagada CERT-EU nõuetekohane ja stabiilne toimimine, võib komisjon teha ettepaneku personali ja rahaliste vahendite ümberpaigutamiseks komisjoni eelarvesse, et kasutada neid CERT-EU tegevuseks. Ümberjaotamine jõustub samal ajal kui esimene pärast käesoleva määruse jõustumist vastu võetud liidu aastaeelarve.

Artikkel 25

Läbivaatamine

1. Hiljemalt 8. jaanuariks 2025 ja seejärel igal aastal esitab IICB CERT-EU abiga komisjonile aruande käesoleva määruse rakendamise kohta. IICB võib anda komisjonile soovituse käesolev määrus läbi vaadata.

2. Hiljemalt 8. jaanuariks 2027 ja seejärel iga kahe aasta tagant hindab komisjon käesoleva määruse rakendamist ning strateegilisel ja operatiivtasandil saadud kogemusi ning esitab Euroopa Parlamendile ja nõukogule selle kohta aruande.

Käesoleva lõike esimeses lõigus osutatud aruanne hõlmab artikli 16 lõikes 1 osutatud läbivaatamist, mis käsitleb võimalust muuta CERT-EU liidu ametiks.

3. Hiljemalt 8. jaanuariks 2029 hindab komisjon käesoleva määruse toimimist ja esitab Euroopa Parlamendile, nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ning Regioonide Komiteele aruande. Komisjon hindab ka ELi salastatud teavet käitlevate võrgu- ja infosüsteemide käesoleva määruse kohaldamisalasse lisamise asjakohasust, võttes arvesse ka teisi nende süsteemide suhtes kohaldatavaid liidu õigusakte. Vajaduse korral lisatakse aruandele seadusandlik ettepanek.

Artikkel 26

Jõustumine

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

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Strasbourg, 13. detsember 2023

Euroopa Parlamendi nimel	*Nõukogu nimel*
president	*eesistuja*
R. METSOLA	P. NAVARRO RÍOS