2023/2841

18.12.2023

EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS (EU, Euratom) 2023/2841,

annettu 13 päivänä joulukuuta 2023,

toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi unionin toimielimissä, elimissä, toimistoissa ja virastoissa

EUROOPAN PARLAMENTTI JA EUROOPAN UNIONIN NEUVOSTO, jotka

ottavat huomioon Euroopan unionin toiminnasta tehdyn sopimuksen ja erityisesti sen 298 artiklan,

ottavat huomioon Euroopan atomienergiayhteisön perustamissopimuksen ja erityisesti sen 106 A artiklan,

ottavat huomioon Euroopan komission ehdotuksen,

sen jälkeen kun esitys lainsäätämisjärjestyksessä hyväksyttäväksi säädökseksi on toimitettu kansallisille parlamenteille,

noudattavat tavallista lainsäätämisjärjestystä ([1]),

sekä katsovat seuraavaa:

(1) Tieto- ja viestintätekniikka on avoimen, tehokkaan ja riippumattoman eurooppalaisen hallinnon kulmakivi digiaikakaudella. Alati kehittyvä teknologia sekä digitaalisten järjestelmien yhä suurempi monimutkaisuus ja keskinäiset kytkökset lisäävät kyberturvallisuusriskejä, minkä seurauksena unionin toimijat ovat yhä alttiimpia kyberuhkille ja poikkeamille; tämä puolestaan aiheuttaa uhan viime kädessä niiden toiminnan jatkuvuudelle ja kyvylle suojata tietonsa. Vaikka pilvipalvelujen kasvava hyödyntäminen, tieto- ja viestintätekniikan (TVT) laajamittainen käyttö, korkea digitalisaatioaste, etätyö sekä kehittyvä teknologia ja verkkoyhteydet ovat keskeisiä piirteitä unionin toimijoiden kaikessa toiminnassa, digitaalinen häiriönsietokyky ei ole vielä riittävällä tavalla sisäänrakennettu.

(2) Unionin toimijoiden kyberuhkaympäristö muuttuu jatkuvasti. Uhkatoimijoiden käyttämät taktiikat, tekniikat ja menettelyt kehittyvät koko ajan, kun taas hyökkäysten perussyyt arvokkaiden julkistamattomien tietojen varastamisesta aina rahan hankkimiseen, yleisen mielipiteen manipuloimiseen tai digitaalisen infrastruktuurin heikentämiseen ovat pysyneet lähes ennallaan. Uhkatoimijat toteuttavat kyberhyökkäyksiään koko ajan nopeammalla tahdilla. Lisäksi uhkatoimijoiden kampanjat ovat yhä kehittyneempiä ja automaattisempia, ne kohdennetaan uhkille alttiille hyökkäyspinnoille, jotka laajenevat koko ajan, ja niissä käytetään nopeasti hyväksi haavoittuvuuksia.

(3) Unionin toimijoiden TVT-ympäristöillä on keskinäisiä riippuvuussuhteita ja yhdistettyjä tietovirtoja, ja niiden käyttäjät tekevät tiivistä yhteistyötä. Näiden keskinäisriippuvuuksien vuoksi kaikilla häiriöillä, vaikka ne alun perin rajoittuisivatkin yhteen unionin toimijaan, voi olla laajempi, ketjureaktiona etenevä vaikutus, joka saattaa johtaa kauaskantoisiin ja pitkäkestoisiin kielteisiin vaikutuksiin muihin unionin toimijoihin. Lisäksi tiettyjen unionin toimijoiden TVT-ympäristöt ovat yhteydessä jäsenvaltioiden TVT-ympäristöihin, minkä seurauksena jonkin unionin toimijan sisällä tapahtunut poikkeama aiheuttaa jäsenvaltioiden TVT-ympäristöihin kohdistuvan kyberturvallisuusriskin ja päinvastoin. Poikkeamakohtaisten tietojen jakaminen voi helpottaa jäsenvaltioihin vaikuttavien samankaltaisten kyberuhkien tai poikkeamien havaitsemista.

(4) Unionin toimijat ovat houkuttelevia kohteita erittäin taitaville uhkatoimijoille, joilla on käytössään paljon resursseja, ja niihin kohdistuu myös muita uhkia. Samalla kyseisten toimijoiden välillä on suuria eroja kyberresilienssissä ja sen kehitystasossa sekä kyvyssä havaita haitallinen kybertoiminta ja reagoida siihen. Unionin toimijoiden toiminnan kannalta on siksi välttämätöntä, että ne saavuttavat kyberturvallisuuden yhteisen korkean tason toteuttamalla tunnistettuihin kyberturvallisuusriskeihin suhteutettuja kyberturvallisuustoimenpiteitä, vaihtamalla tietoja ja tekemällä yhteistyötä.

([1]) Euroopan parlamentin kanta, vahvistettu 21. marraskuuta 2023 (ei vielä julkaistu virallisessa lehdessä), ja neuvoston päätös, tehty 8. joulukuuta 2023.

(5) Euroopan parlamentin ja neuvoston direktiivin (EU) 2022/2555 ([2]) tavoitteena on parantaa entisestään julkisten ja yksityisten toimijoiden, toimivaltaisten viranomaisten ja elinten sekä koko unionin kyberresilienssiä ja kykyä reagoida poikkeamiin. Siksi on tarpeen varmistaa, että unionin toimijat seuraavat esimerkkiä vahvistamalla säännöt, jotka ovat yhdenmukaisia direktiivin (EU) 2022/2555 kanssa ja vastaavat sen vaatimustasoa.

(6) Kyberturvallisuuden yhteisen korkean tason saavuttamiseksi kunkin unionin toimijan on tarpeen laatia sisäinen kyberturvallisuusriskien hallinta- ja valvontakehys, jäljempänä 'kehys', jolla varmistetaan kaikkien kyberturvallisuusriskien tehokas ja järkevä hallinta ja jossa otetaan huomioon toiminnan jatkuvuus ja kriisitilanteiden hallinta. Kehyksessä olisi vahvistettava verkko- ja tietojärjestelmien turvallisuutta koskevat kyberturvallisuusperiaatteet, joihin sisältyy tavoitteita ja painopisteitä ja jotka kattavat koko turvallisuusluokittelemattoman TVT-ympäristön. Kehyksen olisi perustuttava kaikki vaaratekijät huomioivaan toimintamalliin, jolla pyritään suojaamaan verkko- ja tietojärjestelmät ja näiden järjestelmien fyysinen ympäristö sellaisilta tapahtumilta kuin varkaus, tulipalo, tulva, televiestintä- tai sähkökatko sekä luvattomalta fyysiseltä pääsyltä unionin toimijan tietoihin tai tietojenkäsittely-ympäristöön ja niille aiheutuvalta vahingolta ja häirinnältä, jotka saattaisivat vaarantaa verkko- ja tietojärjestelmien välityksellä tallennettujen, siirrettyjen, käsiteltyjen tai saatavilla olevien tietojen saatavuuden, aitouden, eheyden tai luottamuksellisuuden.

(7) Jotta kehyksessä eriteltyjä kyberturvallisuusriskejä voidaan hallita, kunkin unionin toimijan olisi toteutettava asianmukaiset ja oikeasuhteiset tekniset, operatiiviset ja organisatoriset toimenpiteet. Toimenpiteiden olisi katettava tässä asetuksessa vahvistetut alat ja kyberturvallisuusriskien hallintatoimenpiteet kunkin unionin toimijan kyberturvallisuuden vahvistamiseksi.

(8) Kehyksessä eritellyt resurssit ja kyberturvallisuusriskit sekä säännöllisistä kyberturvallisuuden kehitystason arvioinneista tehdyt päätelmät olisi otettava huomioon kunkin unionin toimijan laatimassa kyberturvallisuussuunnitelmassa. Kyberturvallisuussuunnitelmaan olisi sisällyttävä käyttöön otetut kyberturvallisuusriskien hallintatoimenpiteet.

(9) Kyberturvallisuuden varmistaminen on jatkuva prosessi, joten tämän asetuksen nojalla toteutettujen toimenpiteiden soveltuvuutta ja tehokkuutta olisi tarkasteltava säännöllisesti unionin toimijoiden muuttuvien kyberturvallisuusriskien, resurssien ja kyberturvallisuuden kehitystason valossa. Kehystä olisi tarkasteltava uudelleen säännöllisesti ja vähintään neljän vuoden välein, ja kyberturvallisuussuunnitelmaa olisi tarkistettava kahden vuoden välein tai tarvittaessa useammin kyberturvallisuuden kehitystason arvioinnin tai kehyksen merkittävän uudelleentarkastelun jälkeen.

(10) Unionin toimijoiden käyttöön ottamiin kyberturvallisuusriskien hallintatoimenpiteisiin olisi sisällyttävä toimintaperiaatteita, joilla pyritään mahdollisuuksien mukaan tekemään lähdekoodista läpinäkyvä ottaen huomioon kolmansien osapuolten tai unionin toimijoiden oikeuksia koskevat suojatoimet. Kyseisten toimintaperiaatteiden olisi oltava oikeassa suhteessa kyberturvallisuusriskiin, ja niiden tarkoituksena on helpottaa kyberuhkien analysointia luomatta kuitenkaan sovellettavia sopimusehtoja pidemmälle meneviä velvoitteita luovuttaa tai oikeuksia käyttää kolmannen osapuolen koodia.

(11) Avoimen lähdekoodin kyberturvallisuustyökalut ja -sovellukset voivat osaltaan lisätä avoimuutta. Avoimet standardit helpottavat turvallisuustyökalujen yhteentoimivuutta, mikä edistää sidosryhmien turvallisuutta. Avoimen lähdekoodin kyberturvallisuustyökaluissa ja -sovelluksissa voidaan hyödyntää laajempaa kehittäjäyhteisöä, minkä ansiosta toimijat voivat monipuolistaa toimittajapohjaansa. Avoimen lähdekoodin käyttö voi tehdä kyberturvallisuuteen liittyvien työkalujen varmennusprosessista läpinäkyvämmän ja haavoittuvuuksien havaitsemisesta yhteisövetoista. Unionin toimijoiden olisi siksi voitava edistää avoimen lähdekoodin ohjelmistojen ja avointen standardien käyttöä toimintaperiaatteilla, jotka liittyvät avoimen datan ja avoimen lähdekoodin käyttöön osana avoimuuteen perustuvaa turvallisuutta.

([2]) Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555, annettu 14 päivänä joulukuuta 2022, toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta (NIS 2 -direktiivi) (EUVL L 333, 27.12.2022, s. 80).

(12) Unionin toimijoiden välisten erojen vuoksi tämän asetuksen täytäntöönpanossa tarvitaan joustavuutta. Tässä asetuksessa säädettyihin toimenpiteisiin kyberturvallisuuden yhteisen korkean tason varmistamiseksi ei pitäisi sisältyä velvoitteita, jotka heikentävät suoraan unionin toimijoiden tehtävien hoitamista tai rajoittavat niiden institutionaalista itsemääräämisoikeutta. Kyseisten toimijoiden olisi siksi laadittava omat kehyksensä sekä otettava käyttöön omat kyberturvallisuusriskien hallintatoimenpiteensä ja hyväksyttävä omat kyberturvallisuussuunnitelmansa. Tällaisia toimenpiteitä toteutettaessa olisi otettava asianmukaisesti huomioon unionin toimijoiden väliset nykyiset synergiat, jotta varmistetaan resurssien asianmukainen hallinnointi ja kustannusten optimointi. Olisi myös otettava asianmukaisesti huomioon, että toimenpiteet eivät vaikuta kielteisesti tehokkaaseen tietojenvaihtoon ja unionin toimijoiden väliseen sekä unionin toimijoiden ja jäsenvaltioiden vastaavaa tehtävää hoitavien elinten väliseen yhteistyöhön.

(13) Resurssien käytön optimoimiseksi tässä asetuksessa olisi säädettävä kahden tai useamman sellaisen unionin toimijan, joilla on samankaltaisia rakenteita, mahdollisuudesta tehdä yhteistyötä kutakin toimijaa koskevien kyberturvallisuuden kehitystason arviointien suorittamiseksi.

(14) Jotta unionin toimijoille ei aiheutuisi kohtuutonta taloudellista ja hallinnollista rasitetta, kyberturvallisuusriskien hallintaa koskevien vaatimusten olisi oltava oikeassa suhteessa asianomaisten verkko- ja tietojärjestelmien aiheuttamaan kyberturvallisuusriskiin ottaen huomioon näiden toimenpiteiden viimeisin kehitys. Kunkin unionin toimijan olisi pyrittävä osoittamaan riittävä prosenttiosuus TVT-menoistaan kyberturvallisuuden tasonsa parantamiseen. Pitkällä aikavälillä ohjeellisena tavoitteena olisi oltava vähintään 10 prosenttia. Kyberturvallisuuden kehitystason arvioinnissa olisi arvioitava, ovatko unionin toimijan kyberturvallisuusmenot oikeassa suhteessa siihen kohdistuviin kyberturvallisuusriskeihin. Komission olisi esityksessään ensimmäiseksi tämän asetuksen voimaantulon jälkeen hyväksyttäväksi unionin vuotuiseksi talousarvioksi otettava huomioon tästä asetuksesta johtuvat velvoitteet arvioidessaan unionin toimijoiden menoarvioiden mukaisia määräraha- ja henkilöstötarpeita, sanotun kuitenkaan rajoittamatta perussopimusten mukaisten unionin vuotuiseen talousarvioon liittyvien sääntöjen noudattamista.

(15) Kyberturvallisuuden yhteinen korkea taso edellyttää, että kyberturvallisuus on kunkin unionin toimijan ylimmän johdon valvonnassa. Unionin toimijan ylimmän johdon olisi vastattava tämän asetuksen täytäntöönpanosta, mukaan lukien kehyksen laatiminen, kyberturvallisuusriskien hallintatoimenpiteiden toteuttaminen ja kyberturvallisuussuunnitelman hyväksyminen. Kyberturvallisuuskulttuurin eli kyberturvallisuuden käytännön harjoittamisen parantaminen on keskeinen osa kaikkien unionin toimijoiden kehystä ja vastaavia kyberturvallisuusriskien hallintatoimenpiteitä.

(16) Sellaisten verkko- ja tietojärjestelmien turvallisuus, joissa käsitellään EU:n turvallisuusluokiteltuja tietoja, on olennaisen tärkeää. EU:n turvallisuusluokiteltuja tietoja käsittelevät unionin toimijat ovat velvollisia soveltamaan tällaisten tietojen suojaamiseksi käytössä olevia kattavia sääntelykehyksiä, mukaan lukien erityiset hallintotavat, toimintaperiaatteet ja riskinhallintamenettelyt. Verkko- ja tietojärjestelmiin, joissa käsitellään EU:n turvallisuusluokiteltuja tietoja, on tarpeen soveltaa tiukempia turvallisuusvaatimuksia kuin turvallisuusluokittelemattomiin verkko- ja tietojärjestelmiin. Tällaiset verkko- ja tietojärjestelmät sietävät siksi paremmin kyberuhkia ja poikkeamia. Näin ollen tätä asetusta ei pitäisi soveltaa verkko- ja tietojärjestelmiin, joissa käsitellään EU:n turvallisuusluokiteltuja tietoja, vaikka niitä varten tarvitaankin yhteinen kehys. Jos jokin unionin toimija sitä nimenomaisesti pyytää, EU:n toimielinten, elinten ja virastojen tietotekniikan kriisiryhmän (CERT-EU) olisi kuitenkin voitava avustaa kyseistä unionin toimijaa turvallisuusluokitelluissa TVT-ympäristöissä ilmenevien poikkeamien yhteydessä.

(17) Unionin toimijoiden olisi arvioitava toimittajien ja palveluntarjoajien, myös datan tallennus- ja käsittelypalvelujen tarjoajien tai tietoturvapalveluntarjoajien, kanssa solmittaviin suhteisiin liittyviä kyberturvallisuusriskejä ja toteutettava asianmukaiset toimenpiteet näiden riskien hallitsemiseksi. Kyberturvallisuustoimenpiteitä olisi tarkennettava CERT-EU:n antamissa ohjeissa tai suosituksissa. Toimenpiteitä vahvistettaessa ja ohjeita laadittaessa olisi otettava asianmukaisesti huomioon viimeisin kehitys ja tapauksen mukaan asiaan liittyvät eurooppalaiset ja kansainväliset standardit sekä asiaan liittyvät unionin säädökset ja toimintapolitiikat, mukaan lukien direktiivin (EU) 2022/2555 14 artiklalla perustetun yhteistyöryhmän julkaisemat kyberturvallisuutta koskevat riskinarvioinnit

ja suositukset, kuten 5G-verkkojen kyberturvallisuutta koskeva koordinoitu EU-tason riskinarviointi ja 5G-kyberturvallisuutta koskeva EU:n välineistö. Lisäksi, kun otetaan huomioon kyberuhkaympäristö ja unionin toimijoiden kyberresilienssin parantamisen merkitys, voitaisiin edellyttää asiaan liittyvien TVT-tuotteiden, TVT-palvelujen ja TVT-prosessien sertifiointia Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/881 ([3]) 49 artiklan nojalla hyväksyttyjen erityisten eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien mukaisesti.

(18) Unionin toimielinten ja elinten pääsihteerit päättivät toukokuussa 2011 perustaa CERT-EU:n kokoonpanon vahvistamista edeltävän ryhmän, jota valvoi toimielinten välinen johtokunta. Pääsihteerit vahvistivat heinäkuussa 2012 käytännön järjestelyt ja päättivät pitää CERT-EU:n pysyvänä yksikkönä, joka auttaisi edelleen parantamaan unionin toimielinten, elinten ja virastojen yleistä tietoteknistä turvallisuutta ja olisi näkyvä esimerkki toimielinten välisestä kyberturvallisuusyhteistyöstä. Syyskuussa 2012 perustettiin CERT-EU komission työryhmäksi, jonka toimeksianto kattaa useita toimielimiä. Joulukuussa 2017 unionin toimielimet ja elimet tekivät toimielinten välisen järjestelyn CERT-EU:n organisaatiosta ja toiminnasta ([4]). Tässä asetuksessa olisi vahvistettava kattava sääntökokonaisuus, joka koskee CERT-EU:n organisaatiota ja toimintaa. Tämän asetuksen säännökset ovat ensisijaisia joulukuussa 2017 tehdyn, CERT-EU:n organisaatiota ja toimintaa koskevan toimielinten välisen järjestelyn määräyksiin nähden.

(19) CERT-EU:n nimi olisi muutettava unionin toimielinten, elinten, toimistojen ja virastojen kyberturvallisuuspalveluksi. Lyhytnimi CERT-EU olisi säilytettävä nimen tunnettuuden vuoksi.

(20) Tällä asetuksella CERT-EU:lle annetaan enemmän tehtäviä ja sen roolia laajennetaan ja perustetaan lisäksi toimielinten välinen kyberturvallisuuslautakunta (IICB) unionin toimijoiden kyberturvallisuuden yhteisen korkean tason edistämiseksi. IICB:lle olisi annettava yksinoikeutetuksi tehtäväksi seurata sitä, miten unionin toimijat panevat tämän asetuksen täytäntöön, ja tukea sen täytäntöönpanoa niiden toiminnassa sekä valvoa sitä, miten CERT-EU panee täytäntöön yleiset painopisteet ja tavoitteet, ja antaa CERT-EU:lle strategista ohjausta. IICB:n olisi tämän vuoksi varmistettava unionin toimielinten edustus ja otettava mukaan unionin elinten, toimistojen ja virastojen edustajia EU:n virastojen verkoston (EUAN) kautta. IICB:n organisaatiota ja toimintaa olisi säänneltävä tarkemmin sen sisäisellä työjärjestyksellä, johon voi sisältyä IICB:n sääntömääräisten kokousten tarkempi määrittely, myös sellaisten vuotuisten poliittisen tason tapaamisten osalta, joissa kunkin IICB:n jäsenen ylimmän johdon edustajat voisivat käydä strategista keskustelua ja antaa strategista ohjausta IICB:lle. IICB:n olisi lisäksi voitava perustaa toimeenpaneva komitea avustamaan sen työssä ja siirtää sille joitakin tehtävistään ja valtuuksistaan, erityisesti kun on kyse tehtävistä, joissa tarvitaan sen jäsenten erityisasiantuntemusta, kuten palveluluettelon ja sen mahdollisten myöhempien päivitysten hyväksymisestä, palvelutasosopimuksia koskevista järjestelyistä, unionin toimijoiden IICB:lle tämän asetuksen nojalla toimittamien asiakirjojen ja raporttien arvioinnista tai tehtävistä, jotka liittyvät IICB:n vaatimusten noudattamista koskevista toimenpiteistä antamien päätösten valmisteluun ja niiden täytäntöönpanon seurantaan. IICB:n olisi vahvistettava toimeenpanevan komitean työjärjestys, mukaan lukien sen tehtävät ja valtuudet.

(21) IICB:n tavoitteena on tukea unionin toimijoita niiden kyberturvallisuuden tason parantamisessa panemalla täytäntöön tämän asetuksen. Unionin toimijoiden tukemiseksi IICB:n olisi annettava ohjausta CERT-EU:n päällikölle, hyväksyttävä monivuotinen strategia unionin toimijoiden kyberturvallisuuden tason nostamisesta, vahvistettava menetelmät ja muut näkökohdat vapaaehtoisten vertaisarviointien toteuttamiseksi sekä helpotettava paikallisten kyberturvallisuusvastaavien epävirallisen ryhmän perustamista Euroopan unionin kyberturvallisuusviraston (ENISA) tukemana siten, että tavoitteena on vaihtaa parhaita käytäntöjä ja tietoa tämän asetuksen täytäntöönpanosta.

([3]) Euroopan parlamentin ja neuvoston asetus (EU) 2019/881, annettu 17 päivänä huhtikuuta 2019, Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista sekä asetuksen (EU) N:o 526/2013 kumoamisesta (kyberturvallisuusasetus) (EUVL L 151, 7.6.2019, s. 15).

([4]) Euroopan parlamentin, Eurooppa-neuvoston, Euroopan unionin neuvoston, Euroopan komission, Euroopan unionin tuomioistuimen, Euroopan keskuspankin, Euroopan tilintarkastustuomioistuimen, Euroopan ulkosuhdehallinnon, Euroopan talous- ja sosiaalikomitean, Euroopan alueiden komitean ja Euroopan investointipankin välinen järjestely unionin toimielinten, elinten ja virastojen tietotekniikan kriisiryhmän (CERT-EU) organisaatiosta ja toiminnasta (EUVL C 12, 13.1.2018, s. 1).

(22) Jotta voidaan saavuttaa kyberturvallisuuden korkea taso kaikkien unionin toimijoiden toiminnassa, IICB:ssä olisi oltava kolme EUAN:n nimeämää edustajaa, jotka edustavat omaa TVT-ympäristöään käyttävien unionin elinten, toimistojen ja virastojen etuja. Henkilötietojen käsittelyn turvallisuus ja siten myös sen kyberturvallisuus on tietosuojan kulmakivi. Tietosuojan ja kyberturvallisuuden välisten synergioiden vuoksi Euroopan tietosuojavaltuutetun olisi oltava edustettuna IICB:ssä tämän asetuksen soveltamisalaan kuuluvana unionin toimijana, jolla on erityisasiantuntemusta tietosuojan alalla, mukaan lukien sähköisten viestintäverkkojen turvallisuus. Kun otetaan huomioon innovoinnin ja kilpailukyvyn merkitys kyberturvallisuuden alalla, Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksen olisi oltava edustettuna IICB:ssä. Kun otetaan huomioon ENISAn rooli kyberturvallisuuden asiantuntijakeskuksena ja ENISAn antama tuki sekä unionin avaruusinfrastruktuurin ja -palvelujen kyberturvallisuuden merkitys, ENISAn ja Euroopan unionin avaruusohjelmaviraston olisi oltava edustettuina IICB:ssä. Kun otetaan huomioon CERT-EU:lle tässä asetuksessa annettu tehtävä, IICB:n puheenjohtajan olisi kutsuttava CERT-EU:n päällikkö kaikkiin IICB:n kokouksiin, paitsi jos IICB keskustelee suoraan CERT-EU:n päällikköön liittyvistä asioista.

(23) IICB:n olisi valvottava tämän asetuksen noudattamista sekä ohjeiden ja suositusten jatkotoimien toteuttamista ja toimintakehotusten noudattamista. Teknisissä asioissa IICB:n tukena olisi oltava teknisiä neuvoa-antavia ryhmiä, joiden kokoonpanosta päättää IICB. Niiden olisi tehtävä tiivistä yhteistyötä CERT-EU:n, unionin toimijoiden sekä tarvittaessa muiden sidosryhmien kanssa.

(24) Jos IICB katsoo, että jokin unionin toimija ei ole tehokkaasti pannut täytäntöön tätä asetusta tai sen nojalla annettuja ohjeita, suosituksia ja toimintakehotuksia, sen olisi voitava toteuttaa vaatimusten noudattamista koskevia toimenpiteitä, sanotun kuitenkaan rajoittamatta asianomaisen unionin toimijan sisäisten menettelyjen soveltamista. IICB:n olisi sovellettava vaatimusten noudattamista koskevia toimenpiteitä asteittain, eli Siten, että sen olisi toisin sanoen ensin hyväksyttävä vähiten ankara toimenpide eli perusteltu lausunto ja ainoastaan tarvittaessa hyväksyttävä yhä ankarampia toimenpiteitä, joista kaikkein ankarin on asianomaiselle unionin toimijalle toimitettavien tietovirtojen tilapäistä keskeyttämistä koskeva suositus. Tällaista suositusta olisi sovellettava ainoastaan poikkeustapauksissa, joissa asianomainen unionin toimija rikkoo tätä asetusta pitkäaikaisesti, tahallisesti tai vakavasti.

(25) Perusteltu lausunto on vähiten ankara vaatimusten noudattamista koskeva toimenpide, jolla puututaan tämän asetuksen täytäntöönpanossa havaittuihin puutteisiin. IICB:n olisi voitava antaa perustellun lausunnon johdosta ohjausta, jolla autetaan unionin toimijaa varmistamaan, että sen kehys, kyberturvallisuusriskien hallintatoimenpiteet, kyberturvallisuussuunnitelma ja raportointi ovat tämän asetuksen mukaisia, ja tämän jälkeen varoitus, jonka mukaan unionin toimijan toiminnassa todettuihin puutteisiin on puututtava tietyn määräajan kuluessa. Jos varoituksessa yksilöityihin puutteisiin ei ole riittävästi puututtu, IICB:n olisi voitava antaa perusteltu ilmoitus.

(26) IICB:n olisi voitava suositella, että unionin toimijalle tehdään tarkastus. Unionin toimijan olisi voitava käyttää tähän tarkoitukseen sisäisen tarkastuksen toimintoaan. IICB:n olisi myös voitava pyytää, että tarkastuksen suorittaa ulkopuolinen tarkastuspalvelu, mukaan lukien jokin yhteisesti sovituista yksityisen sektorin palveluntarjoajista.

(27) Poikkeustapauksissa, joissa unionin toimija rikkoo tätä asetusta pitkäaikaisesti, tahallisesti, toistuvasti tai vakavasti, IICB:n olisi voitava viimeisenä keinona suositella kaikille jäsenvaltioille ja unionin toimijoille asianomaiselle unionin toimijalle toimitettavien tietovirtojen tilapäistä keskeyttämistä siihen asti, kun kyseinen toimija on lopettanut rikkomisen. Tällaisesta suosituksesta olisi ilmoitettava asianmukaisten suojattujen viestintäkanavien kautta.

(28) Tämän asetuksen moitteettoman täytäntöönpanon varmistamiseksi IICB:n olisi, jos se katsoo, että unionin toimijan tämän asetuksen jatkuva rikkominen johtuu suoraan sen henkilöstön jäsenen, myös ylimpään johtoon kuuluvan henkilöstön jäsenen, toimista tai laiminlyönneistä, pyydettävä asianomaista unionin toimijaa toteuttamaan asianmukaisia toimia, muun muassa pyytämällä sitä harkitsemaan kurinpitotoimien toteuttamista, neuvoston asetuksessa (ETY, Euratom, EHTY) N:o 259/68 ([5]) vahvistetuissa Euroopan unionin virkamiehiin sovellettavissa henkilöstösäännöissä ja unionin muuta henkilöstöä koskevissa palvelussuhteen ehdoissa, jäljempänä 'henkilöstösäännöt', vahvistettujen sääntöjen ja menettelyjen sekä muiden sovellettavien sääntöjen ja menettelyjen mukaisesti.

(29) CERT-EU:n olisi edistettävä kaikkien unionin toimijoiden TVT-ympäristön turvallisuutta. Kun CERT-EU harkitsee asiaankuuluvia toimintapoliittisia kysymyksiä koskevan teknisen neuvonnan tai palautteen antamista unionin toimijan pyynnöstä, sen olisi varmistettava, että tämä ei estä sitä hoitamasta muita sille tämän asetuksen nojalla annettuja tehtäviä. CERT-EU:n olisi toimittava unionin toimijoiden puolesta direktiivin (EU) 2022/2555 12 artiklan 1 kohdan nojalla haavoittuvuuksien koordinoitua julkistamista varten nimettyä koordinaattoria vastaavana tahona.

(30) CERT-EU:n olisi tuettava toimenpiteiden toteuttamista kyberturvallisuuden yhteisen korkean tason varmistamiseksi tekemällä IICB:lle ehdotuksia ohjeiksi ja suosituksiksi tai antamalla toimintakehotuksia. Tällaisten ohjeiden ja suositusten hyväksymisestä vastaa IICB. Tarvittaessa CERT-EU:n olisi annettava toimintakehotuksia, joissa kuvaillaan kiireellisiä turvallisuustoimenpiteitä, jotka unionin toimijoita kehotetaan toteuttamaan tietyssä määräajassa. IICB:n olisi ohjeistettava CERT-EU:ta antamaan ehdotuksen ohjeiksi tai suositukseksi taikka toimintakehotuksen, peruuttamaan sen tai muokkaamaan sitä.

(31) CERT-EU:n olisi myös suoritettava sille direktiivissä (EU) 2022/2555 säädetty tehtävä, joka koskee yhteistyötä ja tietojenvaihtoa mainitun direktiivin 15 artiklan nojalla perustetun tietoturvaloukkauksiin reagoivien ja niitä tutkivien kansallisten yksiköiden (CSIRT-yksiköt) verkoston kanssa. Lisäksi CERT-EU:n olisi komission suosituksen (EU) 2017/1584 ([6]) mukaisesti tehtävä yhteistyötä ja koordinoitava reagointi asiaan liittyvien sidosryhmien kanssa. Kyberturvallisuuden korkean tason edistämiseksi koko unionissa CERT-EU:n olisi jaettava poikkeamakohtaista tietoa vastaavaa tehtävää hoitavien jäsenvaltioiden elinten kanssa. CERT-EU:n olisi myös tehtävä yhteistyötä muiden vastaavaa tehtävää hoitavien julkisten ja yksityisten toimijoiden kanssa, myös Pohjois-Atlantin liitossa, edellyttäen, että IICB on antanut sille ennakkohyväksynnän.

(32) CERT-EU:n olisi operatiivista kyberturvallisuutta tukiessaan hyödynnettävä saatavilla olevaa ENISAn asiantuntemusta asetuksessa (EU) 2019/881 tarkoitetun jäsennellyn yhteistyön kautta. Tarvittaessa tällaisen yhteistyön käytännön toteutus olisi määriteltävä erityisin järjestelyin näiden kahden toimijan välillä päällekkäisiä tehtäviä välttäen. CERT-EU:n olisi tehtävä yhteistyötä ENISAn kanssa kyberuhka-analyysissa ja toimitettava uhkaympäristöä koskeva raporttinsa säännöllisesti ENISAlle.

(33) CERT-EU:n olisi voitava tehdä yhteistyötä ja vaihtaa tietoja asiaan liittyvien kyberturvallisuusyhteisöjen kanssa unionissa ja sen jäsenvaltioissa, jotta voidaan edistää operatiivista yhteistyötä ja antaa olemassa oleville verkostoille mahdollisuus hyödyntää koko potentiaalinsa unionin suojaamisessa.

(34) Koska CERT-EU:n palvelut ja tehtävät ovat kaikkien unionin toimijoiden edun mukaisia, kunkin unionin toimijan, jolla on TVT-menoja, olisi osoitettava kohtuullinen rahoitusosuus näihin palveluihin ja tehtäviin. Nämä rahoitusosuudet eivät rajoita unionin toimijoiden itsenäistä budjettivaltaa.

([5]) Neuvoston asetus (ETY, Euratom, EHTY) N:o 259/68, annettu 29 päivänä helmikuuta 1968, Euroopan yhteisöjen virkamiehiin sovellettavien henkilöstösääntöjen ja näiden yhteisöjen muuta henkilöstöä koskevien palvelussuhteen ehtojen vahvistamisesta sekä yhteisöjen virkamiehiin tilapäisesti sovellettavien erityisten toimenpiteiden laatimisesta (EYVL L 56, 4.3.1968, s. 1).

([6]) Komission suositus (EU) 2017/1584, annettu 13 päivänä syyskuuta 2017, koordinoidusta reagoinnista laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin (EUVL L 239, 19.9.2017, s. 36).

(35) Monet kyberhyökkäykset ovat osa laajempia kampanjoita, jotka kohdistuvat unionin toimijoiden ryhmiin tai etuyhteisöihin, joihin sisältyy unionin toimijoita. Jotta voitaisiin havaita ongelmat etukäteen, reagoida poikkeamiin tai toteuttaa lieventäviä toimenpiteitä sekä palautua poikkeamista, unionin toimijoiden olisi voitava ilmoittaa CERT-EU:lle poikkeamista, kyberuhkista, haavoittuvuuksista ja läheltä piti -tilanteista sekä jaettava sen kanssa asianmukaiset tekniset tiedot, jotka mahdollistavat samankaltaisen poikkeamien, kyberuhkien, haavoittuvuuksien ja läheltä piti -tilanteiden havaitsemisen tai lieventämisen sekä niihin reagoimisen muiden unionin toimijoiden toiminnassa. Direktiivissä (EU) 2022/2555 noudatetun lähestymistavan mukaisesti unionin toimijaa olisi vaadittava toimittamaan CERT-EU:lle ennakkovaroitus 24 tunnin kuluessa siitä, kun se on tullut tietoiseksi merkittävästä poikkeamasta. Tällaisen tietojenvaihdon olisi mahdollistettava se, että CERT-EU levittää tiedot muille unionin toimijoille sekä asianmukaisille vastaavaa tehtävää hoitaville elimille, jotta voidaan auttaa suojaamaan unionin toimijoiden TVT-ympäristöjä ja unionin toimijoiden vastaavaa tehtävää hoitavien kumppanien TVT-ympäristöjä samankaltaisilta poikkeamilta.

(36) Tässä asetuksessa säädetään merkittävien poikkeamien ilmoittamista koskevasta monivaiheisesta lähestymistavasta, jotta löydetään oikea tasapaino yhtäältä nopean ilmoittamisen, joka auttaa lieventämään merkittävien poikkeamien mahdollista leviämistä ja antaa unionin toimijoille mahdollisuuden pyytää apua, ja toisaalta sellaisen perusteellisemman raportoinnin välillä, jonka ansiosta saadaan arvokasta kokemusta yksittäisistä poikkeamista ja parannetaan ajan mittaan yksittäisten unionin toimijoiden kyberresilienssiä sekä edistetään niiden yleistä kyberturvallisuuden tasoa. Tätä varten tähän asetukseen olisi sisällytettävä sellaisista poikkeamista raportoiminen, jotka voivat asianomaisen unionin toimijan suorittaman alustavan arvioinnin perusteella johtaa vakaviin häiriöihin kyseisen unionin toimijan toiminnassa tai aiheuttaa sille suuria taloudellisia tappioita tai vaikuttaa muihin luonnollisiin henkilöihin tai oikeushenkilöihin aiheuttamalla huomattavaa aineellista tai aineetonta vahinkoa. Tällaisessa alustavassa arvioinnissa olisi otettava huomioon muun muassa verkko- ja tietojärjestelmät, joihin poikkeama vaikuttaa, ja erityisesti niiden merkitys unionin toimijan toiminnalle, kyberuhkan vakavuus ja tekniset ominaisuudet sekä mahdolliset taustalla olevat haavoittuvuudet, joita käytetään hyväksi, sekä unionin toimijan kokemukset samanlaisista poikkeamista. Indikaattorit, kuten se, miten laajat vaikutukset unionin toimijan toimintaan kohdistuvat, poikkeaman kesto tai niiden luonnollisten henkilöiden tai oikeushenkilöiden lukumäärä, joihin poikkeama vaikuttaa, voivat olla tärkeitä määritettäessä, onko toimintahäiriö vakava.

(37) Koska asianomaisen unionin toimijan infrastruktuuri ja verkko- ja tietojärjestelmät ja jäsenvaltio, jossa kyseinen unionin toimija sijaitsee, ovat kytköksissä toisiinsa, on ratkaisevan tärkeää, että kyseiselle jäsenvaltiolle ilmoitetaan ilman aiheetonta viivytystä merkittävistä poikkeamista, jotka koskevat kyseistä unionin toimijaa. Tätä varten unionin toimijan, johon poikkeuma vaikuttaa, olisi ilmoitettava direktiivin (EU) 2022/2555 8 ja 10 artiklan nojalla nimetyille tai perustetuille jäsenvaltioiden asiaankuuluville vastaavaa tehtävää hoitaville elimille sellaisen merkittävän poikkeaman esiintymisestä, josta se raportoi CERT-EU:lle. Jos CERT-EU saa tiedon merkittävästä poikkeamasta jäsenvaltiossa, sen olisi ilmoitettava asiasta mille tahansa asiaankuuluvalle kyseisen jäsenvaltion vastaavaa tehtävää hoitaville elimille.

(38) Olisi otettava käyttöön mekanismi, jolla varmistetaan unionin toimijoiden tehokas tietojenvaihto, koordinointi ja yhteistyö laajavaikutteisten poikkeamien tapauksessa ja jossa määritellään selkeästi asianomaisten unionin toimijoiden tehtävät ja vastuualueet. Jollei kyberkriisinhallintasuunnitelmasta muuta johdu, komission edustajan IICB:ssä olisi toimittava yhteyspisteenä, jonka välityksellä IICB voi helpommin jakaa laajavaikutteisia poikkeamia koskevia asiaankuuluvia tietoja Euroopan kyberkriisien yhteysorganisaatioiden verkoston (EU-CyCLONe) kanssa yhteisen tilannetietoisuuden edistämiseksi. Komission edustajan toimiminen IICB:ssä yhteyspisteenä ei saisi rajoittaa komission direktiivin (EU) 2022/2555 16 artiklan 2 kohdan mukaista itsenäistä ja erillistä roolia EU-CyCLONessa.

(39) Euroopan parlamentin ja neuvoston asetusta (EU) 2018/1725 ([7]) sovelletaan tämän asetuksen mukaisesti suoritettavaan henkilötietojen käsittelyyn. Henkilötietojen käsittelyä saattaa liittyä toimenpiteisiin, jotka on hyväksytty kyberturvallisuusriskien hallinnan, haavoittuvuuksien ja poikkeamien käsittelyn, poikkeamia, kyberuhkia ja haavoittuvuuksia koskevien tietojen jakamisen sekä poikkeamanhallintaa koskevan koordinoinnin ja yhteistyön yhteydessä. Tällaiset toimenpiteet saattavat edellyttää tiettyjen henkilötietoryhmien, kuten IP-osoitteiden, URL-osoitteiden, verkkotunnusten, sähköpostiosoitteiden, rekisteröidyn tehtävien organisaatiossa, aikaleimojen,

([7]) Euroopan parlamentin ja neuvoston asetus (EU) 2018/1725, annettu 23 päivänä lokakuuta 2018, luonnollisten henkilöiden suojelusta unionin toimielinten, elinten ja laitosten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta sekä asetuksen (EY) N:o 45/2001 ja päätöksen N:o 1247/2002/EY kumoamisesta (EUVL L 295, 21.11.2018, s. 39).

sähköpostiviestien aiheiden tai tiedostonimien, käsittelyä. Kaikkien tämän asetuksen nojalla toteutettavien toimenpiteiden olisi oltava tietosuojaa ja yksityisyyden suojaa koskevan kehyksen mukaisia, ja unionin toimijoiden, CERT-EU:n ja tarvittaessa IICB:n olisi toteutettava kaikki asiaankuuluvat tekniset ja organisatoriset suojatoimet, joilla varmistetaan, että kehyksen noudattaminen tapahtuu vastuullisesti.

(40) Tässä asetuksessa vahvistetaan oikeusperusta unionin toimijoiden, CERT-EU:n ja tarvittaessa IICB:n suorittamalle henkilötietojen käsittelylle niiden tämän asetuksen mukaisten tehtävien suorittamiseksi ja velvoitteiden täyttämiseksi asetuksen (EU) 2018/1725 5 artiklan 1 kohdan b alakohdan mukaisesti. CERT-EU voi toimia henkilötietojen käsittelijänä tai rekisterinpitäjänä sen mukaan, mitä tehtävää se suorittaa asetuksen (EU) 2018/1725 nojalla.

(41) Tietyissä tapauksissa voi olla tarpeen, että unionin toimijat ja CERT-EU käsittelevät asetuksen (EU) 2018/1725 10 artiklan 1 kohdassa tarkoitettuja erityisiä henkilötietoryhmiä täyttääkseen tämän asetuksen mukaiset velvoitteensa varmistaa kyberturvallisuuden korkea taso ja erityisesti haavoittuvuuksien ja poikkeamien käsittelyn yhteydessä. Tässä asetuksessa vahvistetaan oikeusperusta unionin toimijoiden ja CERT-EU:n suorittamalle erityisten henkilötietoryhmien käsittelylle asetuksen (EU) 2018/1725 10 artiklan 2 kohdan g alakohdan mukaisesti. Tämän asetuksen mukaisen erityisten henkilötietoryhmien käsittelyn olisi oltava ehdottoman oikeasuhteista tavoitteeseen nähden. Jollei mainitun asetuksen 10 artiklan 2 kohdan g alakohdassa säädetyistä edellytyksistä muuta johdu, unionin toimijoiden ja CERT-EU:n olisi voitava käsitellä tällaisia tietoja ainoastaan siinä laajuudessa kuin se on tarpeen ja jos siitä nimenomaisesti säädetään tässä asetuksessa. Unionin toimijoiden ja CERT-EU:n olisi erityisiä henkilötietoryhmiä käsitellessään noudatettava keskeisiltä osin oikeutta henkilötietojen suojaan ja huolehdittava asianmukaisista ja erityisistä toimenpiteistä rekisteröidyn perusoikeuksien ja etujen suojaamiseksi.

(42) Asetuksen (EU) 2018/1725 33 artiklan mukaan unionin toimijoiden ja CERT-EU:n olisi ottaen huomioon uusimman tekniikan ja toteuttamiskustannukset sekä käsittelyn luonteen, laajuuden, asiayhteyden ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit toteutettava henkilötietojen asianmukaisen turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet, kuten rajoitettujen käyttöoikeuksien tarjoaminen tiedonsaantitarpeen perusteella, jäljitysketjun periaatteiden soveltaminen, alkuperäketjun käyttöönotto, lepäävän datan säilyttäminen valvotussa ja tarkastettavissa olevassa ympäristössä, vakiotoimintamenettelyt ja yksityisyyden suojan säilyttävät toimenpiteet, kuten pseudonymisointi tai salaus. Näitä toimenpiteitä ei saisi toteuttaa tavalla, joka vaikuttaa poikkeamien käsittelyn tarkoituksiin ja todistusmateriaalin eheyteen. Kun unionin toimija tai CERT-EU siirtää poikkeamaan liittyviä henkilötietoja, myös erityisiä henkilötietoryhmiä, vastaavaa tehtävää hoitavalle elimelle tai kumppanille tämän asetuksen tarkoituksia varten, tällaisissa siirroissa olisi noudatettava asetusta (EU) 2018/1725. Kun erityisiä henkilötietoryhmiä siirretään kolmannelle osapuolelle, unionin toimijoiden ja CERT-EU:n olisi varmistettava, että kolmas osapuoli soveltaa asetuksen (EU) 2018/1725 tasoa vastaavia henkilötietojen suojaa koskevia toimenpiteitä.

(43) Tämän asetuksen tarkoituksia varten käsiteltäviä henkilötietoja olisi säilytettävä ainoastaan niin kauan kuin se on tarpeen asetuksen (EU) 2018/1725 mukaisesti. Unionin toimijoiden ja tapauksen mukaan rekisterinpitäjänä toimivan CERT-EU:n olisi vahvistettava säilytysajat, jotka olisi rajoitettava siihen, mikä on tarpeen tiettyjen erikseen määriteltyjen tarkoitusten saavuttamiseksi. Erityisesti poikkeamien käsittelyä varten kerättyjen henkilötietojen osalta unionin toimijoiden ja CERT-EU:n olisi erotettava toisistaan henkilötiedot, jotka kerätään kyberuhkan havaitsemiseksi niiden TVT-ympäristöissä, jotta voidaan ehkäistä poikkeama, ja henkilötiedot, jotka kerätään poikkeaman lieventämistä, siihen reagointia ja siitä palautumista varten. Kyberuhkan havaitsemiseksi on tärkeää ottaa huomioon se, kuinka pitkään uhkatoimija voi jäädä huomaamatta järjestelmässä. Poikkeaman lieventämiseksi, siihen reagoimiseksi ja siitä palautumiseksi on tärkeää harkita, ovatko henkilötiedot tarpeen toistuvan poikkeaman tai sellaisen vastaavanlaisen poikkeaman jäljittämiseksi ja käsittelemiseksi, jonka osalta voitaisiin osoittaa korrelaatio.

(44) Unionin toimijoiden ja CERT-EU:n suorittamassa tietojen käsittelyssä olisi noudatettava sovellettavia tietoturvallisuutta koskevia sääntöjä. Henkilöstöturvallisuuden sisällyttämisessä kyberturvallisuusriskien hallintatoimenpiteisiin olisi myös noudatettava sovellettavia sääntöjä.

(45) Tietoja jaettaessa käytetään näkyviä merkintöjä osoittamaan, että tietojen vastaanottajien on sovellettava tietojen jakamista koskevia rajoja, jotka perustuvat erityisesti salassapitosopimuksiin tai epävirallisiin salassapitosopimuksiin, kuten Traffic Light Protocol -käsittelyluokitukseen tai muihin lähteen selkeisiin merkintöihin. Traffic Light Protocol -käsittelyluokitus on keino tiedottaa mahdollisista tietojen levittämiseen liittyvistä rajoituksista. Sitä käytetään lähes kaikissa CSIRT-yksiköissä ja joissakin tietojen jakamisen ja analysoinnin keskuksissa.

(46) Tätä asetusta olisi arvioitava säännöllisesti monivuotisia rahoituskehyksiä koskevia tulevia neuvotteluja ajatellen, jotta voidaan tehdä lisäpäätöksiä CERT-EU:n toiminnasta ja institutionaalisesta roolista, mukaan lukien CERT-EU:n mahdollinen perustaminen unionin toimistoksi.

(47) IICB:n olisi tarkasteltava ja arvioitava tämän asetuksen täytäntöönpanoa CERT-EU:n avustuksella ja raportoitava havainnoistaan komissiolle. Komission olisi näiden tietojen perusteella annettava kertomus Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle. Kertomuksessa olisi IICB:n antamia tietoja hyödyntäen arvioitava, onko tämän asetuksen soveltamisalaan asianmukaista sisällyttää verkko- ja tietojärjestelmät, joissa käsitellään EU:n turvallisuusluokiteltuja tietoja, erityisesti jos unionin toimijoille yhteisiä tietoturvallisuutta koskevia sääntöjä ei ole.

(48) Suhteellisuusperiaatteen mukaisesti on tarpeen ja aiheellista kyberturvallisuuden yhteisen korkean tason saavuttamista unionin toimijoiden toiminnassa koskevan perustavoitteen toteuttamiseksi säätää unionin toimijoita koskevista kyberturvallisuussäännöistä. Euroopan unionista tehdyn sopimuksen 5 artiklan 4 kohdan mukaisesti tässä asetuksessa ei ylitetä sitä, mikä on tarpeen aiottujen tavoitteiden saavuttamiseksi.

(49) Tässä asetuksessa otetaan huomioon se, että unionin toimijoiden koko ja valmiudet vaihtelevat, myös taloudellisten ja henkilöresurssien osalta.

(50) Euroopan tietosuojavaltuutettua on kuultu asetuksen (EU) 2018/1725 42 artiklan 1 kohdan mukaisesti, ja hän on antanut lausunnon 17 päivänä toukokuuta 2022 ([8]),

OVAT HYVÄKSYNEET TÄMÄN ASETUKSEN:

I LUKU

YLEISET SÄÄNNÖKSET

1 artikla

Kohde

Tässä asetuksessa vahvistetaan toimenpiteet, joilla pyritään saavuttamaan kyberturvallisuuden yhteinen korkea taso unionin toimijoissa siltä osin kuin on kyse

a) kunkin unionin toimijan laatimasta sisäisestä kyberturvallisuusriskien hallinta- ja valvontakehyksestä, 6 artiklan nojalla;

b) kyberturvallisuusriskien hallinnasta, raportoinnista ja tietojen jakamisesta;

c) 10 artiklan nojalla perustetun toimielinten välisen kyberturvallisuuslautakunnan organisaatiosta ja toiminnasta sekä unionin toimielinten, elinten, toimistojen ja virastojen kyberturvallisuuspalvelun (CERT-EU) organisaatiosta ja toiminnasta;

d) tämän asetuksen täytäntöönpanon valvonnasta.

([8]) EUVL C 258, 5.7.2022, s. 10.

2 artikla

Soveltamisala

1. Tätä asetusta sovelletaan unionin toimijoihin, 10 artiklan nojalla perustettuun toimielinten väliseen kyberturvallisuuslautakuntaan ja CERT-EU:hun.

2. Tätä asetusta sovelletaan rajoittamatta perussopimusten mukaista institutionaalista itsemääräämisoikeutta.

3. Tätä asetusta ei 13 artiklan 8 kohtaa lukuun ottamatta sovelleta verkko- ja tietojärjestelmiin, joissa käsitellään EU:n turvallisuusluokiteltuja tietoja.

3 artikla

Määritelmät

Tässä asetuksessa tarkoitetaan:

1) ’unionin toimijoilla’ Euroopan unionista tehdyllä sopimuksella, Euroopan unionin toiminnasta tehdyllä sopimuksella tai Euroopan atomienergiayhteisön perustamissopimuksella taikka niiden nojalla perustettuja unionin toimielimiä, elimiä, toimistoja ja virastoja;

2) ’verkko- ja tietojärjestelmällä’ direktiivin (EU) 2022/2555 6 artiklan 1 alakohdassa määriteltyä verkko- ja tietojärjestelmää;

3) ’verkko- ja tietojärjestelmien turvallisuudella’ direktiivin (EU) 2022/2555 6 artiklan 2 alakohdassa määriteltyä verkko- ja tietojärjestelmien turvallisuutta;

4) ’kyberturvallisuudella’ asetuksen (EU) 2019/881 2 artiklan 1 alakohdassa määriteltyä kyberturvallisuutta;

5) ’ylimmällä johdolla’ unionin toimijan toiminnasta vastaavaa kaikkein ylimpään johtotasoon kuuluvaa johtajaa, hallintoelintä tai koordinointi- ja valvontaelintä, jolla on valtuudet tehdä tai valtuuttaa tekemään päätöksiä kyseisen unionin toimijan korkean tason hallintojärjestelyjen mukaisesti, sanotun kuitenkaan rajoittamatta muiden hallintotasojen muodollisten vastuiden soveltamista vaatimusten noudattamisen ja kyberturvallisuusriskien hallinnan osalta niiden omilla vastuualueilla;

6) ’läheltä piti -tilanteella’ direktiivin (EU) 2022/2555 6 artiklan 5 alakohdassa määriteltyä läheltä piti -tilannetta;

7) ’poikkeamalla’ direktiivin (EU) 2022/2555 6 artiklan 6 alakohdassa määriteltyä poikkeamaa;

8) ’laajavaikutteisella poikkeamalla’ mitä tahansa poikkeamaa, joka aiheuttaa niin laajan häiriön, ettei unionin toimijalla ja CERT-EU:lla ole valmiuksia hallita sitä, tai jolla on merkittävä vaikutus vähintään kahteen unionin toimijaan;

9) ’laajamittaisella kyberturvallisuuspoikkeamalla’ direktiivin (EU) 2022/2555 6 artiklan 7 alakohdassa määriteltyä laajamittaista kyberturvallisuuspoikkeamaa;

10) ’poikkeaman käsittelyllä’ direktiivin (EU) 2022/2555 6 artiklan 8 alakohdassa määriteltyä poikkeaman käsittelyä;

11) ’kyberuhkalla’ asetuksen (EU) 2019/881 2 artiklan 8 alakohdassa määriteltyä kyberuhkaa;

12) ’merkittävällä kyberuhkalla’ direktiivin (EU) 2022/2555 6 artiklan 11 alakohdassa määriteltyä merkittävää kyberuhkaa;

13) ’haavoittuvuudella’ direktiivin (EU) 2022/2555 6 artiklan 15 alakohdassa määriteltyä haavoittuvuutta;

14) ’kyberturvallisuusriskillä’ direktiivin (EU) 2022/2555 6 artiklan 9 alakohdassa määriteltyä riskiä;

15) ’pilvipalvelulla’ direktiivin (EU) 2022/2555 6 artiklan 30 alakohdassa määriteltyä pilvipalvelua.

4 artikla

Henkilötietojen käsittely

1. CERT-EU:n, 10 artiklan nojalla perustetun toimielinten välisen kyberturvallisuuslautakunnan ja unionin toimijoiden tämän asetuksen nojalla suorittamassa henkilötietojen käsittelyssä noudatetaan asetusta (EU) 2018/1725.

2. Tämän asetuksen mukaisia tehtäviä suorittaessaan tai velvoitteita täyttäessään CERT-EU, 10 artiklan nojalla perustettu toimielinten välinen kyberturvallisuuslautakunta ja unionin toimijat käsittelevät ja vaihtavat henkilötietoja vain siinä määrin kuin on tarpeen ja yksinomaan kyseisten tehtävien suorittamista tai kyseisten velvoitteiden täyttämistä varten.

3. Asetuksen (EU) 2018/1725 10 artiklan 1 kohdassa tarkoitettujen erityisten henkilötietoryhmien käsittelyn katsotaan olevan tarpeen kyseisen asetuksen 10 artiklan 2 kohdan g alakohdan mukaisesta tärkeää yleistä etua koskevasta syystä. Tällaisia tietoja voidaan käsitellä ainoastaan siinä määrin kuin on tarpeen tämän asetuksen 6 ja 8 artiklassa tarkoitettujen kyberturvallisuusriskien hallintatoimenpiteiden toteuttamista, 13 artiklan mukaista CERT-EU:n palvelujen tarjoamista, 17 artiklan 3 kohdan ja 18 artiklan 3 kohdan mukaista poikkeamakohtaisten tietojen jakamista, 20 artiklan mukaista tietojen jakamista, 21 artiklan mukaisia raportointivelvoitteita, 22 artiklan mukaista poikkeamanhallintaa koskevaa koordinointia ja yhteistyötä sekä 23 artiklan mukaista laajavaikutteisten poikkeamien hallintaa varten. Toimiessaan rekisterinpitäjinä unionin toimijat ja CERT-EU toteuttavat teknisiä toimenpiteitä estääkseen erityisten henkilötietoryhmien käsittelyn muita tarkoituksia varten ja huolehtivat asianmukaisista ja erityisistä toimenpiteistä rekisteröityjen perusoikeuksien ja etujen suojaamiseksi.

II LUKU

TOIMENPITEET KYBERTURVALLISUUDEN YHTEISEN KORKEAN TASON VARMISTAMISEKSI

5 artikla

Toimenpiteiden toteuttaminen

1. Jäljempänä olevan 10 artiklan nojalla perustettu toimielinten välinen kyberturvallisuuslautakunta antaa Euroopan unionin kyberturvallisuusvirastoa (ENISA) kuultuaan ja CERT-EU:lta ohjeistusta saatuaan viimeistään 8 päivänä syyskuuta 2024 unionin toimijoille ohjeet kyberturvallisuuden alustavan arvioinnin suorittamista ja 6 artiklan mukaisen sisäisen kyberturvallisuusriskien hallinta- ja valvontakehyksen laatimista, 7 artiklan mukaisten kyberturvallisuuden kehitystason arviointien suorittamista, 8 artiklan mukaisten kyberturvallisuusriskien hallintatoimenpiteiden toteuttamista ja 9 artiklan mukaisen kyberturvallisuussuunnitelman hyväksymistä varten.

2. Pannessaan täytäntöön 6, 7, 8 ja 9 artiklaa unionin toimijat ottavat huomioon tämän artiklan 1 kohdassa tarkoitetut ohjeet sekä 11 ja 14 artiklan nojalla annetut asiaankuuluvat ohjeet ja suositukset.

6 artikla

Kyberturvallisuusriskien hallinta- ja valvontakehys

1. Kukin unionin toimija laatii 8 päivään huhtikuuta 2025 mennessä sisäisen kyberturvallisuusriskien hallinta- ja valvontakehyksen, jäljempänä ’kehys’, suoritettuaan kyberturvallisuuden alustavan arvioinnin, kuten auditoinnin. Kehyksen laatimista valvotaan unionin toimijan ylimmässä johdossa ja sen vastuulla.

2. Kehyksen on katettava asianomaisen unionin toimijan koko turvallisuusluokittelematon TVT-ympäristö, mukaan lukien sen tiloissa oleva TVT-ympäristö ja operatiivinen teknologiaverkko, pilvipalveluympäristöissä olevat tai kolmansien osapuolten ylläpitämät ulkoistetut resurssit ja palvelut, mobiililaitteet, yritysverkot, internetiin liittämättömät liiketoimintaverkot ja kaikki kyseisiin ympäristöihin liitetyt laitteet, jäljempänä ’TVT-ympäristö’. Kehyksen on perustuttava kaikki vaaratekijät huomioivaan toimintamalliin.

3. Kehyksellä on varmistettava kyberturvallisuuden korkea taso. Kehyksessä on vahvistettava verkko- ja tietojärjestelmien turvallisuutta koskevat sisäiset kyberturvallisuusperiaatteet, joihin sisältyy tavoitteita ja painopisteitä, sekä unionin toimijan tämän asetuksen tehokkaan täytäntöönpanon varmistamisesta vastaavan henkilöstön tehtävät ja vastuualueet. Kehykseen on sisällyttävä myös mekanismeja täytäntöönpanon tehokkuuden mittaamiseksi.

4. Kehystä on tarkasteltava uudelleen säännöllisesti muuttuvien kyberturvallisuusriskien valossa ja vähintään neljän vuoden välein. Unionin toimijan kehystä voidaan päivittää tarvittaessa ja 10 artiklan nojalla perustetun toimielinten välisen kyberturvallisuuslautakunnan pyynnöstä todettujen poikkeamien tai tämän asetuksen täytäntöönpanossa havaittujen mahdollisten puutteiden johdosta annetun CERT EU:n ohjeistuksen perusteella

5. Kunkin unionin toimijan ylin johto on vastuussa tämän asetuksen täytäntöönpanosta ja valvoo, että sen organisaatiossa noudatetaan kehykseen liittyviä velvoitteita.

6. Kunkin unionin toimijan ylin johto voi tarvittaessa siirtää kyseisen unionin toimijan henkilöstösääntöjen 29 artiklan 2 kohdassa tarkoitetuille johtaville virkamiehille tai muille vastaavantasoisille virkamiehille tämän asetuksen mukaisia erityisiä velvoitteita, sanotun kuitenkaan rajoittamatta sen vastuuta tämän asetuksen täytäntöönpanosta. Ylimmän johdon voidaan erityisen velvoitteen mahdollisesta siirtämisestä riippumatta katsoa olevan vastuussa siitä, että asianomainen unionin toimija rikkoo tätä asetusta.

7. Kullakin unionin toimijalla on oltava käytössä tehokkaat mekanismit sen varmistamiseksi, että riittävä prosenttiosuus TVT-menoista käytetään kyberturvallisuuteen. Kehys on otettava asianmukaisesti huomioon kyseistä prosenttiosuutta vahvistettaessa.

8. Kukin unionin toimija nimittää paikallisen kyberturvallisuusvastaavan tai vastaavan vastuuhenkilön, joka toimii sen keskitettynä yhteyspisteenä kyberturvallisuuden kaikissa näkökohdissa. Paikallinen kyberturvallisuusvastaava helpottaa tämän asetuksen täytäntöönpanoa ja raportoi säännöllisesti suoraan ylimmälle johdolle täytäntöönpanon tilanteesta. Unionin toimija voi siirtää tiettyjä tämän asetuksen täytäntöönpanoon liittyviä paikallisen kyberturvallisuusvastaavan tehtäviä CERT-EU:lle kyseisen unionin toimijan ja CERT-EU:n välisen palvelutasosopimuksen perusteella tai kyseiset tehtävät voidaan jakaa usean unionin toimijan kesken, sanotun kuitenkaan rajoittamatta paikallisen kyberturvallisuusvastaavan toimimista kunkin unionin toimijan keskitettynä yhteyspisteenä. Jos kyseisiä tehtäviä siirretään CERT-EU:lle, 10 artiklan nojalla perustettu toimielinten välinen kyberturvallisuuslautakunta päättää, onko kyseisen palvelun tarjoaminen osa CERT-EU:n perustason palveluja, ottaen huomioon asianomaisen unionin toimijan henkilöstö- ja rahoitusresurssit. Kukin unionin toimija ilmoittaa nimitetyt paikalliset kyberturvallisuusvastaavat ja heitä koskevat myöhemmin tehtävät muutokset CERT-EU:lle ilman aiheetonta viivytystä.

CERT-EU laatii luettelon nimitetyistä paikallisista kyberturvallisuusvastaavista ja pitää sen ajan tasalla.

9. Kunkin unionin toimijan henkilöstösääntöjen 29 artiklan 2 kohdassa tarkoitetut johtavat virkamiehet tai muut vastaavantasoiset virkamiehet sekä kaikki asianomaiset henkilöstön jäsenet, joiden tehtävänä on tässä asetuksessa säädettyjen kyberturvallisuusriskien hallintaa koskevien toimenpiteiden ja velvoitteiden täyttäminen, osallistuvat säännöllisesti erityiskoulutukseen riittävien tietojen ja taitojen hankkimiseksi, jotta he voivat ymmärtää ja arvioida kyberturvallisuusriskejä ja kyberturvallisuusriskien hallintakäytäntöjä sekä niiden vaikutusta unionin toimijan toimintoihin.

7 artikla

Kyberturvallisuuden kehitystason arvioinnit

1. Kukin unionin toimija suorittaa viimeistään 8 päivänä heinäkuuta 2025 ja sen jälkeen vähintään kahden vuoden välein kyberturvallisuuden kehitystason arvioinnin ja sisällyttää siihen kaikki TVT-ympäristönsä osatekijät.

2. Kyberturvallisuuden kehitystason arvioinnit on tarvittaessa suoritettava erikoistuneen kolmannen osapuolen avustamana.

3. Unionin toimijat, joilla on samankaltaisia rakenteita, voivat tehdä yhteistyötä kutakin toimijaa koskevien kyberturvallisuuden kehitystason arviointien suorittamiseksi.

4. Jäljempänä olevan 10 artiklan nojalla perustetun toimielinten välisen kyberturvallisuuslautakunnan pyynnöstä ja asianomaisen unionin toimijan nimenomaisella suostumuksella kyberturvallisuuden kehitystason arvioinnin tuloksista voidaan keskustella kyseisessä kyberturvallisuuslautakunnassa tai paikallisten kyberturvallisuusvastaavien epävirallisessa ryhmässä, jotta voidaan ottaa oppia saaduista kokemuksista ja jakaa parhaita käytäntöjä.

8 artikla

Kyberturvallisuusriskien hallintatoimenpiteet

1. Kukin unionin toimija toteuttaa ilman aiheetonta viivytystä ja joka tapauksessa viimeistään 8 päivänä syyskuuta 2025 ylimmän johtonsa valvonnassa asianmukaisia ja oikeasuhteisia teknisiä, operatiivisia ja organisatorisia toimenpiteitä kehyksessä eriteltyjen kyberturvallisuusriskien hallitsemiseksi ja poikkeamien ehkäisemiseksi tai niiden vaikutusten minimoimiseksi. Kun otetaan huomioon viimeisin kehitys ja tapauksen mukaan asiaan liittyvät eurooppalaiset ja kansainväliset standardit, näillä toimenpiteillä on varmistettava, että koko TVT-ympäristön verkko- ja tietojärjestelmien turvallisuuden taso on oikeassa suhteessa kyberturvallisuusriskeihin. Näiden toimenpiteiden oikeasuhteisuutta arvioitaessa on otettava asianmukaisesti huomioon se, missä määrin unionin toimija altistuu kyberturvallisuusriskeille, toimijan koko sekä poikkeamien esiintymisen todennäköisyys ja niiden vakavuus, mukaan lukien niiden yhteiskunnalliset, taloudelliset ja toimielinten väliset vaikutukset.

2. Unionin toimijat käsittelevät kyberturvallisuusriskien hallintatoimenpiteiden täytäntöönpanossa ainakin seuraavia osa-alueita:

a) kyberturvallisuuspolitiikka, mukaan lukien 6 artiklassa ja tämän artiklan 3 kohdassa tarkoitettujen tavoitteiden ja painopisteiden saavuttamiseksi tarvittavat toimenpiteet;

b) kyberturvallisuutta koskevia riskianalyysejä ja tietojärjestelmien turvallisuutta koskevat politiikat;

c) pilvipalvelujen käyttöä koskevat politiikkatavoitteet;

d) tarvittaessa kyberturvallisuusauditointi, joka voi sisältää kyberturvallisuusriskien, haavoittuvuuksien ja kyberuhkien arvioinnin, sekä luotettavan yksityisen palveluntarjoajan säännöllisesti suorittama tunkeutumisenestotestaus;

e) d alakohdassa tarkoitetuista kyberturvallisuusauditoinneista johtuvien suositusten täytäntöönpano kyberturvallisuus-päivitysten ja toimintaperiaatteiden päivitysten avulla;

f) kyberturvallisuuden organisointi, mukaan lukien tehtävien ja vastuualueiden määrittäminen;

g) resurssien hallinta, mukaan lukien TVT-resurssien inventointi ja TVT-verkkojen kartoitus;

h) henkilöstöturvallisuus ja kulunvalvonta;

i) operatiivinen turvallisuus;

j) tietoliikenneturvallisuus;

k) järjestelmien hankinta, kehittäminen ja ylläpito, mukaan lukien haavoittuvuuksien käsittelyä ja julkistamista koskevat toimintaperiaatteet;

l) mahdollisuuksien mukaan lähdekoodin läpinäkyvyyttä koskevat toimintaperiaatteet;

m) toimitusketjun turvallisuus, mukaan lukien kunkin unionin toimijan ja sen välittömien toimittajien tai palveluntarjoajien välisten suhteiden turvallisuusnäkökohdat;

n) poikkeamien käsittely ja yhteistyö CERT-EU:n kanssa, kuten turvallisuuden seurannan ja kirjaamisen ylläpito;

o) toiminnan jatkuvuuden hallinta, esimerkiksi varmuuskopiointi ja palautumissuunnittelu, sekä kriisinhallinta; ja

p) kyberturvallisuuskoulutusta ja -taitoja, -tiedotusta ja -harjoituksia koskevien ohjelmien edistäminen ja kehittäminen.

Unionin toimijat ottavat ensimmäisen alakohdan m alakohdan tarkoituksia varten huomioon kullekin välittömälle toimittajalle ja palveluntarjoajalle ominaiset haavoittuvuudet, toimittajiensa ja palveluntarjoajiensa tuotteiden yleisen laadun sekä niiden kyberturvallisuuskäytännöt, mukaan lukien niiden tuotekehityksen suojausmenettelyt.

3. Unionin toimijat toteuttavat ainakin seuraavat erityiset kyberturvallisuusriskien hallintatoimenpiteet:

a) tekniset järjestelyt etätyön mahdollistamiseksi ja tukemiseksi;

b) konkreettiset toimet nollaluottamuksen periaatteiden noudattamiseen siirtymiseksi;

c) monivaiheisen tunnistuksen käyttö yleiskäytäntönä kaikissa verkko- ja tietojärjestelmissä;

d) kryptografian ja salaustekniikoiden käyttö, mukaan lukien erityisesti päästä päähän -salaus, sekä suojattu digitaalinen allekirjoitus;

e) tarvittaessa suojattu puhe-, video- ja tekstiviestintä sekä suojatut hätäviestintäjärjestelmät unionin toimijan toiminnassa;

f) ennakoivat toimenpiteet haitta- ja vakoiluohjelmien havaitsemiseksi ja poistamiseksi;

g) ohjelmistojen toimitusketjun turvallisuuden varmistaminen ohjelmistokehityksessä ja ohjelmistojen arvioinnissa sovellettavien turvallisuuskriteerien avulla;

h) sellaisten kyberturvallisuutta koskevien koulutusohjelmien laatiminen ja käyttöönotto, jotka ovat oikeassa suhteessa unionin toimijan ylimmälle johdolle ja tämän asetuksen tehokkaan täytäntöönpanon varmistamisesta vastaaville henkilöstön jäsenille asetettuihin tehtäviin ja näiltä odotettuihin valmiuksiin;

i) henkilöstön säännöllinen kyberturvallisuuskoulutus;

j) tarvittaessa osallistuminen unionin toimijoiden välisten yhteyksien riskianalyyseihin;

k) julkisia hankintoja koskevien sääntöjen parantaminen kyberturvallisuuden yhteisen korkean tason edistämiseksi seuraavien avulla:

   i) sellaisten sopimuksista johtuvien esteiden poistaminen, jotka rajoittavat TVT-palvelujen tarjoajien mahdollisuuksia jakaa tietoja poikkeamista, haavoittuvuuksista ja kyberuhkista CERT-EU:n kanssa;

   ii) sopimusehdot, jotka velvoittavat raportoimaan poikkeamista, haavoittuvuuksista ja kyberuhkista sekä huolehtimaan siitä, että käytössä ovat asianmukaiset mekanismit poikkeamanhallintaa ja seurantaa varten.

9 artikla

Kyberturvallisuussuunnitelmat

1. Edellä olevan 7 artiklan nojalla tehdyn kyberturvallisuuden kehitystason arvioinnin päättymisen jälkeen ja ottaen huomioon kehyksessä eritellyt resurssit ja kyberturvallisuusriskit sekä 8 artiklan nojalla toteutetut kyberturvallisuusriskien hallintatoimenpiteet kunkin unionin toimijan ylin johto hyväksyy kyberturvallisuussuunnitelman ilman aiheetonta viivytystä ja joka tapauksessa viimeistään 8 päivänä tammikuuta 2026. Kyberturvallisuussuunnitelman tavoitteena on nostaa unionin toimijan yleistä kyberturvallisuuden tasoa ja edistää siten kyberturvallisuuden yhteisen korkean tason parantamista unionin toimijoiden toiminnassa. Kyberturvallisuussuunnitelman on sisällettävä vähintään 8 artiklan nojalla toteutetut kyberturvallisuusriskien hallintatoimenpiteet. Kyberturvallisuussuunnitelmaa on tarkistettava kahden vuoden välein tai tarvittaessa useammin 7 artiklan nojalla tehtyjen kyberturvallisuuden kehitystason arviointien tai kehyksen merkittävän uudelleentarkastelun perusteella.

2. Kyberturvallisuussuunnitelman on sisällettävä laajavaikutteisia poikkeamia koskeva unionin toimijan kyberkriisinhallintasuunnitelma.

3. Unionin toimija toimittaa valmiin kyberturvallisuussuunnitelman 10 artiklan nojalla perustetulle toimielinten väliselle kyberturvallisuuslautakunnalle.

III LUKU

TOIMIELINTEN VÄLINEN KYBERTURVALLISUUSLAUTAKUNTA

10 artikla

Toimielinten välinen kyberturvallisuuslautakunta

1. Perustetaan toimielinten välinen kyberturvallisuuslautakunta, jäljempänä ’IICB’.

2. IICB:n tehtävänä on

a) seurata ja tukea tämän asetuksen täytäntöönpanoa unionin toimijoissa;

b) valvoa yleisten painopisteiden ja tavoitteiden täytäntöönpanoa CERT-EU:ssa ja antaa CERT-EU:lle strategista ohjausta.

3. IICB koostuu seuraavista:

a) yksi edustaja, jonka kukin seuraavista on nimennyt:
   i) Euroopan parlamentti;
   ii) Eurooppa-neuvosto;
   iii) Euroopan unionin neuvosto;
   iv) komissio;
   v) Euroopan unionin tuomioistuin;
   vi) Euroopan keskuspankki;
   vii) tilintarkastustuomioistuin;
   viii) Euroopan ulkosuhdehallinto;
   ix) Euroopan talous- ja sosiaalikomitea;
   x) Euroopan alueiden komitea;
   xi) Euroopan investointipankki;
   xii) Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskus;
   xiii) ENISA;
   xiv) Euroopan tietosuojavaltuutettu (EDPS);
   xv) Euroopan unionin avaruusohjelmavirasto;

b) kolme edustajaa, jotka EU:n virastojen verkosto (EUAN) on nimennyt TVT-alan neuvoa-antavan komiteansa ehdotuksesta edustamaan omaa TVT-ympäristöään käyttävien, muiden kuin a alakohdassa tarkoitettujen unionin elinten, toimistojen ja virastojen etuja.

IICB:ssä edustettuina olevat unionin toimijat pyrkivät saavuttamaan sukupuolten tasapuolisen edustuksen nimettyjen edustajiensa keskuudessa.

4. IICB:n jäseniä voi avustaa sijainen. Puheenjohtaja voi kutsua muita 3 kohdassa tarkoitettujen unionin toimijoiden tai muiden unionin toimijoiden edustajia osallistumaan IICB:n kokouksiin ilman äänioikeutta.

5. CERT-EU:n päällikkö sekä direktiivin (EU) 2022/2555 14 artiklan nojalla perustetun yhteistyöryhmän, sen 15 artiklan nojalla perustetun CSIRT-verkoston ja sen 16 artiklan nojalla perustetun EU-CyCLONen puheenjohtajat tai heidän sijaisensa voivat osallistua IICB:n kokouksiin tarkkailijoina. IICB voi poikkeustapauksissa työjärjestyksensä mukaisesti päättää toisin.

6. IICB vahvistaa työjärjestyksensä.

7. IICB nimeää työjärjestyksensä mukaisesti jäsentensä keskuudesta puheenjohtajan kolmen vuoden ajaksi. Puheenjohtajan sijaisesta tulee IICB:n täysjäsen samaksi ajaksi.

8. IICB kokoontuu vähintään kolme kertaa vuodessa puheenjohtajansa aloitteesta, CERT-EU:n pyynnöstä tai minkä tahansa jäsenensä pyynnöstä.

9. Kullakin IICB:n jäsenellä on yksi ääni. IICB:n päätökset tehdään yksinkertaisella enemmistöllä, jollei tässä asetuksessa toisin säädetä. IICB:n puheenjohtajalla ei ole äänivaltaa, paitsi äänten mennessä tasan, jolloin puheenjohtajan ääni ratkaisee.

10. IICB voi toimia työjärjestyksensä mukaisesti käynnistettyä yksinkertaistettua kirjallista menettelyä noudattaen. Kyseisessä menettelyssä asianomainen päätös katsotaan hyväksytyksi puheenjohtajan asettamassa määräajassa, jollei joku jäsen esitä vastalausetta.

11. Komissio huolehtii IICB:n sihteeristön tehtävistä, ja sihteeristö on vastuuvelvollinen IICB:n puheenjohtajalle.

12. EUAN:n nimittämät edustajat välittävät IICB:n päätökset EUAN:n jäsenille. Millä tahansa EUAN:n jäsenellä on oikeus ottaa näiden edustajien tai IICB:n puheenjohtajan kanssa esille mikä tahansa asia, joka sen mielestä olisi saatettava IICB:n tietoon.

13. IICB voi perustaa toimeenpanevan komitean avustamaan sitä sen työssä ja siirtää komitealle joitakin tehtävistään ja valtuuksistaan. IICB vahvistaa toimeenpanevan komitean työjärjestyksen, mukaan lukien sen tehtävät ja valtuudet, sekä sen jäsenten toimikauden.

14. IICB toimittaa 8 päivään tammikuuta 2025 mennessä ja sen jälkeen vuosittain Euroopan parlamentille ja neuvostolle raportin, jossa kuvataan yksityiskohtaisesti tämän asetuksen täytäntöönpanossa tapahtunutta edistymistä ja täsmennetään erityisesti CERT-EU:n jäsenvaltioiden vastaavaa tehtävää hoitavien elinten kanssa kussakin jäsenvaltiossa tekemän yhteistyön laajuutta. Raportti otetaan huomioon direktiivin (EU) 2022/2555 18 artiklan nojalla joka toinen vuosi annettavassa kyberturvallisuuden tilaa unionissa käsittelevässä kertomuksessa.

11 artikla

IICB:n tehtävät

Hoitaessaan tehtäviään IICB erityisesti

a) antaa CERT-EU:n päällikölle ohjausta;

b) seuraa ja valvoo tehokkaasti tämän asetuksen täytäntöönpanoa ja tukee unionin toimijoita niiden kyberturvallisuuden vahvistamisessa, tapauksen mukaan myös pyytämällä tapauskohtaisia raportteja unionin toimijoilta ja CERT-EU:lta;

c) hyväksyy strategisen keskustelun jälkeen monivuotisen strategian kyberturvallisuuden tason nostamisesta unionin toimijoissa, arvioi kyseistä strategiaa säännöllisesti ja joka tapauksessa viiden vuoden välein ja tarvittaessa muuttaa strategiaa;

d) vahvistaa menetelmät ja organisatoriset näkökohdat unionin toimijoiden suorittamien vapaaehtoisten vertaisarviointien toteuttamiseksi, jotta voidaan oppia yhteisistä kokemuksista, lujittaa keskinäistä luottamusta ja saavuttaa kyberturvallisuuden yhteinen korkea taso sekä kehittää unionin toimijoiden kyberturvallisuusvalmiuksia, varmistaen, että tällaisia vertaisarviointeja suorittavat muun kuin arvioitavana olevan unionin toimijan nimeämät kyberturvallisuusasiantuntijat ja että menetelmät perustuvat direktiivin (EU) 2022/2555 19 artiklaan ja ne mukautetaan tapauksen mukaan unionin toimijoihin;

e) hyväksyy CERT-EU:n päällikön ehdotuksesta CERT-EU:n vuotuisen työohjelman ja seuraa sen täytäntöönpanoa;

f) hyväksyy CERT-EU:n päällikön ehdotuksesta CERT-EU:n palveluluettelon ja sen mahdolliset päivitykset;

g) hyväksyy CERT-EU:n päällikön ehdotuksesta CERT-EU:n toimintaa koskevan vuotuisen rahoitussuunnitelman tuloista ja menoista, mukaan lukien henkilöstö;

h) hyväksyy CERT-EU:n päällikön ehdotuksesta palvelutasosopimuksia koskevat järjestelyt;

i) tarkastelee CERT-EU:n päällikön laatimaa vuosikertomusta, joka kattaa CERT-EU:n toiminnan ja varainhoidon, ja hyväksyy sen;

j) hyväksyy CERT-EU:n päällikön ehdotuksesta vahvistetut CERT-EU:n keskeiset tulosindikaattorit ja seuraa niitä;

k) hyväksyy yhteistyöjärjestelyt, palvelutasosopimukset tai sopimukset CERT-EU:n ja muiden toimijoiden välillä 18 artiklan nojalla;

l) hyväksyy ohjeita ja suosituksia CERT-EU:n ehdotuksesta 14 artiklan mukaisesti ja ohjeistaa CERT-EU:ta antamaan ehdotuksen ohjeiksi tai suosituksiksi taikka toimintakehotuksen, peruuttamaan sen tai muuttamaan sitä;

m) perustaa teknisiä neuvoa-antavia ryhmiä, joilla on erityistehtäviä, avustamaan IICB:tä sen työssä, hyväksyy niiden tehtävänmääritykset ja nimeää niiden puheenjohtajat;

n) vastaanottaa ja arvioi unionin toimijoiden tämän asetuksen nojalla toimittamia asiakirjoja ja raportteja, kuten kyberturvallisuuden kehitystason arviointeja;

o) helpottaa ENISAn tuella toimivan unionin toimijoiden paikallisten kyberturvallisuusvastaavien epävirallisen ryhmän perustamista tavoitteena vaihtaa parhaita käytäntöjä ja tietoja tämän asetuksen täytäntöönpanosta;

p) seuraa CERT-EU:n antamat tunnistettuja kyberturvallisuusriskejä ja saatuja kokemuksia koskevat tiedot huomioon ottaen unionin toimijoiden TVT-ympäristöjen kesken tehtyjen yhteenliitäntäjärjestelyjen riittävyyttä ja antaa neuvoja mahdollisista parannuksista;

q) laatii kyberkriisinhallintasuunnitelman, jotta voidaan tukea operatiivisella tasolla unionin toimijoihin vaikuttavien laajavaikutteisten poikkeamien koordinoitua hallintaa ja edistää asiaankuuluvien tietojen säännöllistä vaihtoa, erityisesti kun on kyse laajavaikutteisten poikkeamien vaikutuksista ja vakavuudesta sekä mahdollisista keinoista lieventää niiden vaikutuksia;

r) koordinoi 9 artiklan 2 kohdassa tarkoitettujen yksittäisten unionin toimijoiden kyberkriisinhallintasuunnitelmien hyväksymistä;

s) hyväksyy 8 artiklan 2 kohdan ensimmäisen alakohdan m alakohdassa tarkoitettuun toimitusketjun turvallisuuteen liittyviä suosituksia, ottaen huomioon direktiivin (EU) 2022/2555 22 artiklassa tarkoitettujen kriittisiä toimitusketjuja koskevien unionin tason koordinoitujen turvallisuusriskinarviointien tulokset, tukeakseen unionin toimijoita tehokkaiden ja oikeasuhteisten kyberturvallisuusriskien hallintatoimenpiteiden hyväksymisessä.

12 artikla

Vaatimusten noudattaminen

1. IICB seuraa 10 artiklan 2 kohdan ja 11 artiklan nojalla tehokkaasti tämän asetuksen sekä hyväksyttyjen ohjeiden, suositusten ja toimintakehotusten täytäntöönpanoa unionin toimijoissa. IICB voi pyytää unionin toimijoilta tätä tarkoitusta varten tarvittavia tietoja tai asiakirjoja. Hyväksyttäessä vaatimusten noudattamista koskevia toimenpiteitä tämän artiklan nojalla asianomaisella unionin toimijalla ei ole äänioikeutta, jos kyseinen unionin toimija on suoraan edustettuna IICB:ssä.

2. Jos IICB toteaa, että unionin toimija ei ole tehokkaasti pannut täytäntöön tätä asetusta tai sen nojalla annettuja ohjeita, suosituksia tai toimintakehotuksia, se voi, rajoittamatta asianomaisen unionin toimijan sisäisiä menettelyjä ja annettuaan asianomaiselle unionin toimijalle tilaisuuden esittää huomautuksensa,

a) toimittaa asianomaiselle unionin toimijalle perustellun lausunnon, jossa esitetään tämän asetuksen täytäntöönpanossa havaitut puutteet;

b) antaa CERT-EU:ta kuultuaan asianomaiselle unionin toimijalle ohjeita sen varmistamiseksi, että sen kehys, kyberturvallisuusriskien hallintatoimenpiteet, kyberturvallisuussuunnitelma ja raportointi ovat tämän asetuksen mukaisia tietyn määräajan kuluessa;

c) antaa varoituksen, jonka mukaan yksilöityihin puutteisiin on puututtava tietyn määräajan kuluessa, mukaan lukien suositukset asianomaisen unionin toimijan tämän asetuksen nojalla hyväksymien toimenpiteiden muuttamiseksi;

d) antaa asianomaiselle unionin toimijalle perustellun ilmoituksen siinä tapauksessa, että c alakohdan nojalla annetussa varoituksessa yksilöityihin puutteisiin ei ole riittävästi puututtu tietyn määräajan kuluessa;

e) antaa

i) suosituksen tarkastuksen toteuttamiseksi; tai

ii) pyynnön, että jokin ulkopuolinen tarkastuspalvelu suorittaa tarkastuksen;

f) ilmoittaa tapauksen mukaan tilintarkastustuomioistuimelle sen toimeksiannon piiriin kuuluvasta väitetystä vaatimusten noudattamatta jättämisestä;

g) antaa suosituksen, että kaikki jäsenvaltiot ja unionin toimijat panevat täytäntöön asianomaiselle unionin toimijalle toimitettavien tietovirtojen väliaikaisen keskeyttämisen.

Sovellettaessa ensimmäisen alakohdan c alakohtaa varoituksen yleisö on rajattava asianmukaisesti, tarpeen mukaan pakottavaa kyberturvallisuusriskiä silmällä pitäen.

Ensimmäisen alakohdan nojalla annetut varoitukset ja suositukset on osoitettava asianomaisen unionin toimijan ylimmälle johdolle.

3. Jos IICB on hyväksynyt toimenpiteitä 2 kohdan ensimmäisen alakohdan a–g alakohdan nojalla, asianomainen unionin toimija antaa yksityiskohtaiset tiedot IICB:n yksilöimien väitettyjen puutteiden korjaamiseksi toteutetuista toimenpiteistä ja toimista. Unionin toimija toimittaa nämä yksityiskohtaiset tiedot IICB:n kanssa sovittavan kohtuullisen määräajan kuluessa.

4. Jos IICB katsoo, että unionin toimija rikkoo jatkuvasti tätä asetusta unionin virkamiehen tai muun henkilöstön jäsenen, myös ylimpään johtoon kuuluvan, toimien tai laiminlyöntien välittömänä seurauksena, IICB pyytää asianomaista unionin toimijaa toteuttamaan asianmukaisia toimia, muun muassa harkitsemaan kurinpitotoimien toteuttamista, henkilöstösäännöissä vahvistettujen sääntöjen ja menettelyjen sekä muiden sovellettavien sääntöjen ja menettelyjen mukaisesti. Tätä varten IICB välittää tarvittavat tiedot asianomaiselle unionin toimijalle.

5. Jos unionin toimijat ilmoittavat, etteivät ne pysty noudattamaan 6 artiklan 1 kohdassa ja 8 artiklan 1 kohdassa säädettyjä määräaikoja, IICB voi asianmukaisesti perustelluissa tapauksissa toimijan koon huomioon ottaen antaa luvan kyseisten määräaikojen pidentämiseen.

IV LUKU

CERT-EU

13 artikla

CERT-EU:n toimeksianto ja tehtävät

1. CERT-EU:n toimeksiantona on edistää unionin toimijoiden turvallisuusluokittelemattoman TVT-ympäristön turvallisuutta neuvomalla niitä kyberturvallisuusasioissa, auttamalla niitä ehkäisemään, havaitsemaan, käsittelemään ja lieventämään poikkeamia, reagoimaan niihin ja palautumaan niistä sekä toimimalla niiden kyberturvallisuutta koskevan tietojenvaihdon ja poikkeamanhallinnan koordinointikeskuksena.

2. CERT-EU kerää, hallinnoi, analysoi ja jakaa unionin toimijoiden kanssa tietoja kyberuhkista, haavoittuvuuksista ja poikkeamista turvallisuusluokittelemattomassa TVT-infrastruktuurissa. Se koordinoi poikkeamiin liittyviä hallintatoimia toimielinten välisellä ja unionin toimijoiden tasolla, muun muassa tarjoamalla erikoistunutta operatiivista apua tai koordinoimalla sen tarjoamista.

3. CERT-EU hoitaa seuraavia tehtäviä unionin toimijoiden avustamiseksi:

a) se tukee niitä tämän asetuksen täytäntöönpanossa ja edistää tämän asetuksen täytäntöönpanon koordinointia 14 artiklan 1 kohdassa lueteltujen toimenpiteiden tai IICB:n pyytämien tapauskohtaisten raporttien kautta;

b) se tarjoaa unionin toimijoille vakioituja CSIRT-palveluja palveluluettelossaan kuvattujen kyberturvallisuuspalvelujen paketin avulla (perustason palvelut);

c) se ylläpitää vertais- ja kumppaniverkostoa 17 ja 18 artiklassa esitettyjen palvelujen tukemiseksi;

d) se tuo IICB:n tietoon tämän asetuksen täytäntöönpanoon sekä ohjeiden, suositusten ja toimintakehotusten täytäntöönpanoon liittyviä ongelmia;

e) se edistää 2 kohdassa tarkoitettujen tietojen pohjalta unionin kyberturvallisuuden tilannekuvan muodostamista tiiviissä yhteistyössä ENISAn kanssa;

f) se koordinoi laajavaikutteisten poikkeamien hallintaa;

g) se toimii unionin toimijoiden puolesta direktiivin (EU) 2022/2555 12 artiklan 1 kohdan nojalla koordinoitua haavoittuvuuksien julkistamista varten nimettyä koordinaattoria vastaavana tahona;

h) se tarjoaa unionin toimijan pyynnöstä kyseisen unionin toimijan yleisesti saatavilla olevien verkko- ja tietojärjestelmien ennakoivaa, ei-intrusiivista skannausta.

Ensimmäisen alakohdan e alakohdassa tarkoitetut tiedot on soveltuvin osin ja tapauksen mukaan, jollei asianmukaisista salassapitoehdoista muuta johdu, jaettava IICB:n, CSIRT-verkoston ja Euroopan unionin tiedusteluanalyysikeskuksen (EU INTCEN) kanssa.

4. CERT-EU voi tapauksen mukaan 17 tai 18 artiklan mukaisesti tehdä yhteistyötä asiaankuuluvien kyberturvallisuusyhteisöjen kanssa unionissa ja sen jäsenvaltioissa, myös seuraavilla aloilla:

a) varautuminen, poikkeamien koordinointi, tietojenvaihto ja kriisinhallinta teknisellä tasolla unionin toimijoihin liittyvissä tapauksissa;

b) CSIRT-verkostoa koskeva operatiivinen yhteistyö, myös keskinäisen avunannon osalta;

c) kyberuhkatiedustelutieto, mukaan lukien tilannetietoisuus;

d) mikä tahansa aihe, joka edellyttää CERT-EU:n teknistä kyberturvallisuusasiantuntemusta.

5. CERT-EU tekee toimivaltansa puitteissa jäsenneltyä yhteistyötä ENISAn kanssa valmiuksien kehittämisen, operatiivisen yhteistyön ja kyberuhkista tehtävien pitkän aikavälin strategisten analyysien alalla asetuksen (EU) 2019/881 mukaisesti. CERT-EU voi tehdä yhteistyötä ja vaihtaa tietoja Europolin Euroopan kyberrikostorjuntakeskuksen kanssa.

6. CERT-EU voi tarjota seuraavia, muita kuin sen palveluluettelossa kuvattuja palveluja (maksulliset palvelut):

a) palvelut, joilla tuetaan unionin toimijoiden TVT-ympäristön kyberturvallisuutta, lukuun ottamatta 3 kohdassa tarkoitettuja palveluja, palvelutasosopimusten perusteella ja saatavilla olevien resurssien mukaan, erityisesti laaja-alainen verkkoseuranta, mukaan lukien erittäin vakavien kyberuhkien ensivaiheen ympärivuorokautinen seuranta;

b) palvelut, joilla tuetaan unionin toimijoiden kyberturvallisuusoperaatioita tai -hankkeita, lukuun ottamatta operaatioita tai hankkeita niiden TVT-ympäristön suojaamiseksi, kirjallisten sopimusten perusteella ja IICB:n ennakkohyväksynnän pohjalta;

c) asianomaisen unionin toimijan verkko- ja tietojärjestelmien ennakoiva skannaus pyynnöstä sellaisten haavoittuvuuksien havaitsemiseksi, joilla voi olla merkittävä vaikutus;

d) palvelut, joilla tuetaan niiden TVT-ympäristön turvallisuutta, sellaisille muille organisaatioille kuin unionin toimijoille, jotka tekevät tiivistä yhteistyötä unionin toimijoiden kanssa esimerkiksi siksi, että niillä on unionin lainsäädännön nojalla siirrettyjä tehtäviä tai vastuita, kirjallisten sopimusten perusteella ja IICB:n ennakkohyväksynnän pohjalta.

Sovellettaessa ensimmäisen alakohdan d alakohtaa CERT-EU voi poikkeuksellisesti tehdä palvelutasosopimuksia muiden kuin unionin toimijoiden kanssa IICB:n ennakkohyväksynnän pohjalta.

7. CERT-EU järjestää kyberturvallisuusharjoituksia ja voi osallistua niihin tai suosittelee osallistumista olemassa oleviin harjoituksiin, tapauksen mukaan tiiviissä yhteistyössä ENISAn kanssa, unionin toimijoiden kyberturvallisuuden tason testaamiseksi.

8. CERT-EU voi tarjota unionin toimijoille apua sellaisissa verkko- ja tietojärjestelmissä esiintyvien poikkeamien osalta, joissa käsitellään EU:n turvallisuusluokiteltuja tietoja, jos asianomaiset unionin toimijat nimenomaisesti pyytävät sitä tekemään niin omien menettelyjensä mukaisesti. CERT-EU:n tämän kohdan nojalla tarjoaman avun tarjoaminen ei rajoita turvallisuusluokiteltujen tietojen suojaamista koskevien sovellettavien sääntöjen soveltamista.

9. CERT-EU ilmoittaa unionin toimijoille poikkeamien käsittelyä koskevista menettelyistään ja prosesseistaan.

10. CERT-EU tarjoaa asianmukaisten yhteistyömekanismien ja raportointisuhteiden kautta luottamuksellisuuden ja luotettavuuden korkean tason varmistaen asiaankuuluvia ja anonymisoituja tietoja laajavaikutteisista poikkeamista sekä tavasta, jolla ne on käsitelty. Nämä tiedot sisällytetään 10 artiklan 14 kohdassa tarkoitettuun raporttiin.

11. CERT-EU tukee yhteistyössä EDPS:n kanssa asianomaisia unionin toimijoita puututtaessa henkilötietojen tietoturvaloukkauksiin johtaneisiin poikkeamiin, sanotun kuitenkaan rajoittamatta EDPS:n toimivaltaa ja tehtäviä valvontaviranomaisena asetuksen (EU) 2018/1725 nojalla.

12. CERT-EU voi antaa teknistä neuvontaa tai lausuntoja asiaankuuluvista toimintapoliittisista kysymyksistä, jos unionin toimijoiden toimintapoliittiset osastot sitä nimenomaisesti pyytävät.

14 artikla

Ohjeet, suositukset ja toimintakehotukset

1. CERT-EU tukee tämän asetuksen täytäntöönpanoa antamalla

a) toimintakehotuksia, joissa kuvaillaan kiireellisiä turvallisuustoimenpiteitä, jotka unionin toimijoita kehotetaan toteuttamaan asetetussa määräajassa;

b) IICB:lle ehdotuksia ohjeiksi, jotka osoitetaan kaikille unionin toimijoille tai niiden alaryhmälle;

c) IICB:lle ehdotuksia suosituksiksi, jotka osoitetaan yksittäisille unionin toimijoille.

Sovellettaessa ensimmäisen alakohdan a alakohtaa asianomainen unionin toimija ilmoittaa CERT-EU:lle ilman aiheetonta viivytystä toimintakehotuksen vastaanotettuaan siitä, miten kiireellisiä turvallisuustoimenpiteitä on sovellettu.

2. Ohjeisiin ja suosituksiin voi sisältyä

a) yhteisiä menetelmiä sekä malli, joiden avulla arvioidaan unionin toimijoiden kyberturvallisuuden kehitystasoa, mukaan lukien vastaavat asteikot tai keskeiset tulosindikaattorit, ja jotka toimivat vertailukohtana kyberturvallisuuden jatkuvan parantamisen tukemiseksi unionin toimijoiden keskuudessa ja helpottavat kyberturvallisuusalojen ja -toimenpiteiden priorisointia toimijoiden kyberturvallisuuden taso huomioon ottaen;

b) järjestelyjä kyberturvallisuusriskien hallintaa ja kyberturvallisuusriskien hallintatoimenpiteitä varten tai parannuksia niihin;

c) järjestelyjä kyberturvallisuuden kehitystason arviointeja ja kyberturvallisuussuunnitelmia varten;

d) tapauksen mukaan yhteisen teknologian, arkkitehtuurin, avoimen lähdekoodin ja niihin liittyvien parhaiden käytäntöjen käyttö tavoitteena saavuttaa yhteentoimivuus ja yhteiset standardit, mukaan lukien toimitusketjun turvallisuutta koskeva koordinoitu toimintatapa;

e) tapauksen mukaan tietoja, joilla helpotetaan yhteishankintavälineiden käyttöä asiaankuuluvien kyberturvallisuuspalvelujen ja -tuotteiden ostamiseksi ulkopuolisilta toimittajilta;

f) tietojen jakamisjärjestelyjä 20 artiklan nojalla.

15 artikla

CERT-EU:n päällikkö

1. Komissio nimittää CERT-EU:n päällikön saatuaan IICB:n jäsenten kahden kolmasosan enemmistön hyväksynnän. IICB:tä kuullaan nimitysmenettelyn kaikissa vaiheissa, erityisesti tähän tehtävään liittyvien avoinna olevaa tointa koskevien ilmoitusten laatimisen, hakemusten tutkimisen ja valintalautakuntien nimittämisen osalta. Valintamenettelyssä, mukaan lukien lopullinen esivalintaluettelo ehdokkaista, joiden joukosta CERT-EU:n päällikkö on nimitettävä, on varmistettava kummankin sukupuolen tasapuolinen edustus ottaen huomioon jätetyt hakemukset.

2. CERT-EU:n päällikkö vastaa CERT-EU:n asianmukaisesta toiminnasta ja toimii roolinsa puitteissa ja IICB:n ohjauksessa. CERT-EU:n päällikkö raportoi säännöllisesti IICB:n puheenjohtajalle ja toimittaa IICB:lle tapauskohtaisia raportteja sen pyynnöstä.

3. CERT-EU:n päällikkö avustaa toimivaltaista valtuutettua tulojen ja menojen hyväksyjää laadittaessa Euroopan parlamentin ja neuvoston asetuksen (EU, Euratom) 2018/1046 ([9]) 74 artiklan 9 kohdan mukaisesti vuosittain toimintakertomus, joka sisältää taloutta ja hallinnointia koskevat tiedot, myös valvonnan tulokset, ja raportoi valtuutetulle tulojen ja menojen hyväksyjälle säännöllisesti niiden toimenpiteiden täytäntöönpanosta, joiden osalta CERT-EU:n päällikkö on saanut edelleenvaltuutuksen.

4. CERT-EU:n päällikkö laatii vuosittain sen toimintaa koskevan rahoitussuunnitelman hallinnollista tuloista ja menoista, ehdotetun vuotuisen työohjelman, CERT-EU:n ehdotetun palveluluettelon, ehdotetut palveluluettelon tarkistukset, ehdotetut palvelutasosopimuksia koskevat järjestelyt ja CERT-EU:n ehdotetut keskeiset tulosindikaattorit IICB:n hyväksyttäväksi 11 artiklan mukaisesti. Tarkistettaessa CERT-EU:n palveluluettelon palveluvalikoimaa CERT-EU:n päällikkö ottaa huomioon CERT-EU:lle osoitetut resurssit.

5. CERT-EU:n päällikkö toimittaa IICB:lle ja IICB:n puheenjohtajalle vähintään vuosittain raportteja CERT-EU:n toimista ja tuloksista viiteajanjakson aikana, muun muassa talousarvion toteuttamisesta, tehdyistä palvelutasosopimuksista ja kirjallisista sopimuksista, yhteistyöstä vastaavaa tehtävää hoitavien elinten ja kumppanien kanssa sekä henkilöstön tekemistä työmatkoista, mukaan lukien 11 artiklassa tarkoitetut raportit. Näihin raportteihin on sisällyttävä työohjelma seuraavaksi kaudeksi, rahoitussuunnitelma tuloista ja menoista, mukaan lukien henkilöstö, CERT-EU:n palveluluettelon suunnitellut päivitykset ja arvio odotetuista vaikutuksista, joita tällaisilla päivityksillä saattaa taloudellisten ja henkilöresurssien osalta olla.

16 artikla

Rahoitus- ja henkilöstöasiat

1. CERT-EU integroidaan komission jonkin pääosaston hallintorakenteeseen, jotta se voi hyötyä komission hallinnollisista, varainhoidon ja kirjanpidon tukirakenteista säilyttäen samalla asemansa itsenäisenä toimielinten välisenä palveluntarjoajana kaikille unionin toimijoille. Komissio ilmoittaa IICB:lle CERT-EU:n hallinnollisesta sijainnista ja sen mahdollisista muutoksista. Komissio tarkastelee uudelleen CERT-EU:hun liittyviä hallinnollisia järjestelyjä säännöllisesti ja joka tapauksessa ennen monivuotisen rahoituskehyksen vahvistamista Euroopan unionin toiminnasta tehdyn sopimuksen 312 artiklan nojalla, jotta on mahdollista toteuttaa asianmukaisia toimia. Uudelleentarkasteluun sisältyy mahdollisuus perustaa CERT-EU unionin toimistoksi.

2. Hallinto- ja rahoitusmenettelyjen soveltamiseksi CERT-EU:n päällikkö toimii komission alaisuudessa ja IICB:n valvonnassa.

([9]) Euroopan parlamentin ja neuvoston asetus (EU, Euratom) 2018/1046, annettu 18 päivänä heinäkuuta 2018, unionin yleiseen talousarvioon sovellettavista varainhoitosäännöistä, asetusten (EU) N:o 1296/2013, (EU) N:o 1301/2013, (EU) N:o 1303/2013, (EU) N:o 1304/2013, (EU) N:o 1309/2013, (EU) N:o 1316/2013, (EU) N:o 223/2014, (EU) N:o 283/2014 ja päätöksen N:o 541/2014/EU muuttamisesta sekä asetuksen (EU, Euratom) N:o 966/2012 kumoamisesta (EUVL L 193, 30.7.2018, s. 1).

3. CERT-EU:n tehtävät ja toimet, mukaan lukien CERT-EU:n 13 artiklan 3, 4, 5 ja 7 kohdan ja 14 artiklan 1 kohdan nojalla tarjoamat palvelut EU:n yleiseen hallintoon tarkoitetusta monivuotisen rahoituskehyksen otsakkeesta rahoitetuille unionin toimijoille, rahoitetaan komission talousarvion erillisestä budjettikohdasta. CERT-EU:lle varatut toimet esitetään komission henkilöstötaulukon alaviitteessä.

4. Muut kuin tämän artiklan 3 kohdassa tarkoitetut unionin toimijat suorittavat CERT-EU:lle vuotuisen rahoitusosuuden CERT-EU:n mainitun kohdan nojalla tarjoamien palvelujen kattamiseen. Asianomainen rahoitusosuus perustuu IICB:n esittämiin linjauksiin, ja siitä sovitaan kunkin unionin toimijan ja CERT-EU:n välillä palvelutasosopimuksissa. Rahoitusosuuksien on vastattava kohtuullista ja oikeasuhteista osuutta suoritettujen palvelujen kokonaiskustannuksista. Ne osoitetaan tämän artiklan 3 kohdassa tarkoitettuun erilliseen budjettikohtaan asetuksen (EU, Euratom) 2018/1046 21 artiklan 3 kohdan c alakohdassa tarkoitettuina sisäisinä käyttötarkoitukseensa sidottuina tuloina.

5. Edellä 13 artiklan 6 kohdassa säädettyjen palvelujen kustannukset peritään CERT-EU:n palveluja vastaanottavilta unionin toimijoilta. Tulot kohdennetaan kustannuksia tukeviin budjettikohtiin.

17 artikla

CERT-EU:n yhteistyö jäsenvaltioiden vastaavaa tehtävää hoitavien elinten kanssa

1. CERT-EU tekee yhteistyötä ja vaihtaa tietoja ilman aiheetonta viivytystä jäsenvaltioiden vastaavaa tehtävää hoitavien elinten, erityisesti direktiivin (EU) 2022/2555 10 artiklan nojalla nimettyjen tai perustettujen CSIRT-yksiköiden tai tapauksen mukaan toimivaltaisten viranomaisten ja mainitun direktiivin 8 artiklan nojalla nimettyjen tai perustettujen keskitettyjen yhteyspisteiden, kanssa, kun on kyse poikkeamista, kyberuhkista, haavoittuvuuksista, läheltä piti -tilanteista, mahdollisista vastatoimista sekä parhaista käytännöistä ja kaikista asioista, joilla on merkitystä unionin toimijoiden TVT-ympäristöjen suojaamisen parantamisen kannalta, myös direktiivin (EU) 2022/2555 15 artiklan nojalla perustetun CSIRT-verkoston avulla. CERT-EU tukee komissiota direktiivin (EU) 2022/2555 16 artiklan nojalla perustetussa EU-CyCLONessa laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien koordinoidussa hallinnassa.

2. Jos CERT-EU tulee tietoiseksi jäsenvaltion alueella esiintyvistä merkittävistä poikkeamista, se ilmoittaa asiasta 1 kohdan mukaisesti viipymättä mille tahansa asiaankuuluvalle kyseisen jäsenvaltion vastaavaa tehtävää hoitavalle elimelle.

3. Edellyttäen, että henkilötietoja suojataan sovellettavan unionin tietosuojalainsäädännön mukaisesti, CERT-EU vaihtaa ilman aiheetonta viivytystä jäsenvaltioiden vastaavaa tehtävää hoitavien elinten kanssa poikkeamakohtaisia tietoja, joilla on merkitystä vastaavien kyberuhkien tai poikkeamien havaitsemisen helpottamiseksi tai jonkin poikkeaman analysoinnissa auttamiseksi, ilman sen unionin toimijan lupaa, johon poikkeama vaikuttaa. CERT-EU vaihtaa poikkeamakohtaisia tietoja, joista paljastuu poikkeaman kohteen henkilöllisyys, vain jos jokin seuraavista tapahtuu:

a) unionin toimija, johon poikkeama vaikuttaa, antaa suostumuksensa;

b) unionin toimija, johon poikkeama vaikuttaa, ei anna suostumustaan a alakohdassa säädetyllä tavalla mutta sen unionin toimijan henkilöllisyyden julkistaminen, johon poikkeama vaikuttaa, lisäisi todennäköisyyttä siitä, että poikkeamia vältettäisiin tai lievennettäisiin muualla;

c) unionin toimija, johon poikkeama vaikuttaa, on jo ilmoittanut julkisesti, että poikkeama on vaikuttanut siihen.

CERT-EU:n päällikön on hyväksyttävä ensimmäisen alakohdan b alakohdan nojalla tehtävät päätökset sellaisten poikkeamakohtaisten tietojen vaihtamisesta, joista paljastuu poikkeaman kohteen henkilöllisyys. Ennen tällaisen päätöksen antamista CERT-EU ottaa kirjallisesti yhteyttä unionin toimijaan, johon poikkeama vaikuttaa, ja selittää selkeästi, miten sen henkilöllisyyden julkistaminen auttaisi välttämään tai lieventämään poikkeamia muualla. CERT-EU:n päällikön on annettava selitys ja nimenomaisesti pyydettävä unionin toimijaa ilmoittamaan asetetussa määräajassa, antaako se suostumuksensa. CERT-EU:n päällikön on myös ilmoitettava unionin toimijalle, että annetun selityksen valossa hän pidättää oikeuden julkistaa tiedot suostumuksen puuttuessakin. Unionin toimijalle, johon poikkeama vaikuttaa, on ilmoitettava, ennen kuin tiedot julkistetaan.

18 artikla

CERT-EU:n yhteistyö muiden vastaavaa tehtävää hoitavien elinten kanssa

1. CERT-EU voi tehdä yhteistyötä sellaisten muiden kuin 17 artiklassa tarkoitettujen vastaavaa tehtävää unionissa hoitavien elinten kanssa, joihin sovelletaan unionin kyberturvallisuusvaatimuksia, mukaan lukien toimialakohtaiset vastaavaa tehtävää hoitavat elimet, siltä osin kuin on kyse välineistä ja menetelmistä, kuten tekniikoista, taktiikoista, menettelyistä ja parhaista käytännöistä, tai kyberuhkista ja haavoittuvuuksista. Kaikkea tällaisten vastaavaa tehtävää hoitavien elinten kanssa tehtävää yhteistyötä varten CERT-EU pyytää IICB:ltä ennakkohyväksynnän tapauskohtaisesti. Jos CERT-EU aloittaa yhteistyön tällaisten vastaavaa tehtävää hoitavien elinten kanssa, se ilmoittaa asiasta 17 artiklan 1 kohdassa tarkoitetuille asiaankuuluville jäsenvaltioiden vastaavaa tehtävää hoitaville elimille siinä jäsenvaltiossa, jossa vastaavaa tehtävää hoitava elin sijaitsee. Tällainen yhteistyö ja sen ehdot, myös kyberturvallisuuden, tietosuojan ja tietojen käsittelyn osalta, on soveltuvin osin ja tapauksen mukaan vahvistettava erityisissä salassapitojärjestelyissä, kuten sopimuksissa tai hallinnollisissa järjestelyissä. Salassapitojärjestelyt eivät edellytä IICB:n ennakkohyväksyntää, mutta niistä on ilmoitettava IICB:n puheenjohtajalle. Jos on kiireellinen ja välitön tarve vaihtaa kyberturvallisuustietoja unionin toimijoiden tai muun osapuolen etujen mukaisesti, CERT-EU voi tehdä näin jonkin sellaisen toimijan kanssa, jonka erityistä pätevyyttä, kykyä ja asiantuntemusta perustellusti vaaditaan tällaisessa kiireellisessä ja välittömässä tarpeessa avustamista varten, silloinkin, kun CERT-EU:lla ei ole käytössä salassapitojärjestelyä kyseisen toimijan kanssa. Tällaisissa tapauksissa CERT-EU ilmoittaa asiasta välittömästi IICB:n puheenjohtajalle ja raportoi IICB:lle säännöllisten raporttien tai kokousten avulla.

2. CERT-EU voi tehdä yhteistyötä kumppanien, kuten kaupallisten toimijoiden, mukaan lukien toimialakohtaiset toimijat, kansainvälisten järjestöjen, unionin ulkopuolisten kansallisten toimijoiden tai yksittäisten asiantuntijoiden, kanssa kerätäkseen tietoja yleisistä ja erityisistä kyberuhkista, läheltä piti -tilanteista, haavoittuvuuksista ja mahdollisista vastatoimista. Tällaisten kumppanien kanssa tehtävää laajempaa yhteistyötä varten CERT-EU pyytää IICB:ltä ennakkohyväksynnän tapauskohtaisesti.

3. CERT-EU voi sen unionin toimijan suostumuksella, johon poikkeama vaikuttaa, ja edellyttäen, että asiaankuuluvan vastaavaa tehtävää hoitavan elimen tai kumppanin kanssa on käytössä salassapitojärjestely tai -sopimus, antaa kyseiseen poikkeamaan liittyviä tietoja 1 ja 2 kohdassa tarkoitetuille vastaavaa tehtävää hoitaville elimille tai kumppaneille yksinomaan sen analysoinnissa auttamiseksi.

V LUKU

YHTEISTYÖ- JA RAPORTOINTIVELVOITTEET

19 artikla

Tietojen käsittely

1. Unionin toimijat ja CERT-EU noudattavat salassapitovelvollisuutta Euroopan unionin toiminnasta tehdyn sopimuksen 339 artiklan tai vastaavien sovellettavien kehysten mukaisesti.

2. Euroopan parlamentin ja neuvoston asetusta (EY) N:o 1049/2001 ([10]) sovelletaan pyyntöihin, jotka koskevat yleisön oikeutta tutustua CERT-EU:n hallussa oleviin asiakirjoihin, mukaan lukien mainitun asetuksen mukainen velvoite kuulla muita unionin toimijoita tai tarvittaessa jäsenvaltioita aina, kun pyyntö koskee niiden asiakirjoja.

3. Unionin toimijoiden ja CERT-EU:n suorittamassa tietojen käsittelyssä on noudatettava sovellettavia tietoturvallisuutta koskevia sääntöjä.

([10]) Euroopan parlamentin ja neuvoston asetus (EY) N:o 1049/2001, annettu 30 päivänä toukokuuta 2001, Euroopan parlamentin, neuvoston ja komission asiakirjojen saamisesta yleisön tutustuttavaksi (EYVL L 145, 31.5.2001, s. 43).

20 artikla

Kyberturvallisuustietojen jakamisjärjestelyt

1. Unionin toimijat voivat vapaaehtoisesti ilmoittaa CERT-EU:lle ja antaa sille tietoja poikkeamista, kyberuhkista, läheltä piti -tilanteista ja haavoittuvuuksista, jotka vaikuttavat niihin. CERT-EU varmistaa, että saatavilla on tehokkaita viestintävälineitä, joissa varmistetaan jäljitettävyyden, luottamuksellisuuden ja luotettavuuden korkea taso, unionin toimijoiden kanssa toteutettavan tietojen jakamisen helpottamiseksi. Ilmoituksia käsitellessään CERT-EU voi asettaa etusijalle pakollisten ilmoitusten käsittelyn vapaaehtoisten ilmoitusten käsittelyyn nähden. Vapaaehtoinen ilmoittaminen ei saa johtaa sellaisten lisävelvoitteiden asettamiseen raportoivalle unionin toimijalle, joita siihen ei olisi sovellettu, jos se ei olisi antanut ilmoitusta, sanotun kuitenkaan rajoittamatta 12 artiklan soveltamista.

2. Suorittaakseen toimeksiantonsa ja tehtävänsä 13 artiklan nojalla CERT-EU voi pyytää unionin toimijoita antamaan sille tietoja niiden TVT-järjestelmien inventaareista, mukaan lukien tiedot kyberuhkista, läheltä piti -tilanteista, haavoittuvuuksista, vaarantumisindikaattoreista, kyberturvallisuushälytyksistä ja suosituksista, jotka koskevat poikkeamien havaitsemiseen käytettävien kyberturvallisuusvälineiden konfigurointia. Pyynnön kohteena oleva unionin toimija toimittaa pyydetyt tiedot ja niiden myöhemmät päivitykset ilman aiheetonta viivytystä.

3. CERT-EU voi vaihtaa unionin toimijoiden kanssa poikkeamakohtaisia tietoja, joista paljastuu sen unionin toimijan henkilöllisyys, johon poikkeama vaikuttaa, mutta ainoastaan unionin toimijan, johon poikkeama vaikuttaa, suostumuksella. Jos unionin toimija epää suostumuksensa, se antaa CERT-EU:lle perustelut tälle päätökselle.

4. Unionin toimijat jakavat pyynnöstä tietoja Euroopan parlamentin ja neuvoston kanssa kyberturvallisuussuunnitelmien valmistumisesta.

5. IICB tai tapauksen mukaan CERT-EU jakaa pyynnöstä ohjeita, suosituksia ja toimintakehotuksia Euroopan parlamentin ja neuvoston kanssa.

6. Tässä artiklassa säädetyt jakamisvelvoitteet eivät koske

a) EU:n turvallisuusluokiteltuja tietoja;

b) tietoja, joiden edelleenjakelu on suljettu pois näkyvällä merkinnällä, paitsi jos niiden jakaminen CERT-EU:n kanssa on nimenomaisesti sallittu.

21 artikla

Raportointivelvoitteet

1. Poikkeama katsotaan merkittäväksi, jos

a) se on aiheuttanut tai voi aiheuttaa asianomaisen unionin toimijan toiminnalle vakavan toimintahäiriön tai sille suuria taloudellisia tappioita;

b) se on vaikuttanut tai voi vaikuttaa muihin luonnollisiin henkilöihin tai oikeushenkilöihin aiheuttamalla huomattavaa aineellista tai aineetonta vahinkoa.

2. Unionin toimijat toimittavat CERT-EU:lle

a) ilman aiheetonta viivytystä ja joka tapauksessa 24 tunnin kuluessa siitä, kun ne ovat tulleet tietoisiksi merkittävästä poikkeamasta, ennakkovaroituksen, jossa on tapauksen mukaan ilmoitettava, epäilläänkö merkittävän poikkeaman johtuvan lainvastaisista tai vihamielisistä teoista tai voiko sillä olla toimijoiden välisiä tai rajatylittäviä vaikutuksia;

b) ilman aiheetonta viivytystä ja joka tapauksessa 72 tunnin kuluessa siitä, kun ne ovat tulleet tietoisiksi merkittävästä poikkeamasta, poikkeamailmoituksen, jossa on tapauksen mukaan ajantasaistettava a alakohdassa tarkoitetut tiedot ja esitettävä ensimmäinen arvio merkittävästä poikkeamasta, sen vakavuus ja vaikutukset mukaan lukien, sekä vaarantumisindikaattorit, jos sellaisia on saatavilla;

c) CERT-EU:n pyynnöstä väliraportin asiaan liittyvistä tilannepäivityksistä;

d) viimeistään kuukauden kuluttua b alakohdan mukaisen poikkeamailmoituksen toimittamisesta lopullisen raportin, joka sisältää seuraavat tiedot:

   i) yksityiskohtainen kuvaus poikkeamasta, sen vakavuus ja vaikutukset mukaan lukien;

   ii) poikkeaman todennäköisesti aiheuttaneen uhkan tai juurisyyn tyyppi;

   iii) toteutetut ja meneillään olevat toimenpiteet vaikutusten lieventämiseksi;

   iv) tapauksen mukaan poikkeaman rajatylittävät tai toimijoiden väliset vaikutukset;

e) jos poikkeama on edelleen meneillään silloin, kun d alakohdassa tarkoitettu lopullinen raportti pitäisi toimittaa, edistymisraportti tuolloin ja lopullinen raportti kuukauden kuluessa siitä, kun ne ovat käsitelleet poikkeaman.

3. Unionin toimija ilmoittaa ilman aiheetonta viivytystä ja joka tapauksessa 24 tunnin kuluessa siitä, kun se on tullut tietoiseksi merkittävästä poikkeamasta, asiaankuuluville 17 artiklan 1 kohdassa tarkoitetuille jäsenvaltioiden vastaavia tehtäviä hoitaville elimille siinä jäsenvaltiossa, jossa se sijaitsee, että on esiintynyt merkittävä poikkeama.

4. Unionin toimijat ilmoittavat muun muassa kaikki tiedot, joiden avulla CERT-EU voi määrittää mahdolliset toimijoiden väliset vaikutukset, vaikutukset isäntäjäsenvaltioon tai rajatylittävät vaikutukset merkittävän poikkeaman jälkeen. Ilmoittaminen ei itsessään lisää unionin toimijan vastuuta, sanotun kuitenkaan rajoittamatta 12 artiklan soveltamista.

5. Unionin toimijat tiedottavat soveltuvin osin ilman aiheetonta viivytystä niiden verkko- ja tietojärjestelmien, joihin merkittävä poikkeama tai merkittävä kyberuhka vaikuttaa, tai TVT-ympäristön muiden komponenttien käyttäjille, joihin poikkeama tai uhka saattaa vaikuttaa ja joiden on tapauksen mukaan tarpeen toteuttaa lieventäviä toimenpiteitä, kaikista toimenpiteistä tai korjaavista toimista, joita nämä voivat poikkeamaan tai kyseiseen uhkaan reagoimiseksi toteuttaa. Unionin toimijat tiedottavat tarvittaessa kyseisille käyttäjille merkittävästä kyberuhkasta itsestään.

6. Jos merkittävä poikkeama tai merkittävä kyberuhka vaikuttaa sellaiseen verkko- ja tietojärjestelmään tai unionin toimijan TVT-ympäristön sellaiseen komponenttiin, jonka tiedetään olevan yhteydessä toisen unionin toimijan TVT-ympäristöön, CERT-EU antaa asiaankuuluvan kyberturvallisuushälytyksen.

7. Unionin toimijat antavat CERT-EU:n pyynnöstä ilman aiheetonta viivytystä CERT-EU:lle niitä koskevissa poikkeamissa osallisina olleiden elektronisten laitteiden käytöllä luotuja digitaalisia tietoja. CERT-EU voi antaa yksityiskohtaisempia tietoja siitä, minkä tyyppisiä tietoja se tarvitsee tilannekuvan muodostamista ja poikkeamanhallintaa varten.

8. CERT-EU toimittaa IICB:lle, ENISAlle, EU INTCENille ja CSIRT-verkostolle kolmen kuukauden välein yhteenvetoraportin, joka sisältää anonymisoidut koontitiedot merkittävistä poikkeamista, poikkeamista, kyberuhkista, läheltä piti -tilanteista ja haavoittuvuuksista 20 artiklan nojalla sekä merkittävistä poikkeamista, joista on ilmoitettu tämän artiklan 2 kohdan nojalla. Yhteenvetoraportti otetaan huomioon direktiivin (EU) 2022/2555 18 artiklan nojalla joka toinen vuosi annettavassa kyberturvallisuuden tilaa unionissa käsittelevässä kertomuksessa.

9. IICB antaa 8 päivään heinäkuuta 2024 mennessä ohjeita tai suosituksia, joissa täsmennetään järjestelyt tämän artiklan nojalla tapahtuvaa raportointia varten sekä sen muoto ja sisältö. IICB ottaa tällaisia ohjeita tai suosituksia laatiessaan huomioon direktiivin (EU) 2022/2555 23 artiklan 11 kohdan nojalla hyväksytyt täytäntöönpanosäädökset, joissa täsmennetään tiedonannon tietosisältö, muoto ja ilmoitusmenettely. CERT-EU levittää asianmukaiset tekniset tiedot, jotta unionin toimijat voivat ennakoivasti havaita ongelmia, reagoida poikkeamiin tai toteuttaa lieventäviä toimenpiteitä.

10. Tässä artiklassa säädetyt raportointivelvoitteet eivät koske

a) EU:n turvallisuusluokiteltuja tietoja;

b) tietoja, joiden edelleenjakelu on suljettu pois näkyvällä merkinnällä, paitsi jos niiden jakaminen CERT-EU:n kanssa on nimenomaisesti sallittu.

22 artikla

Poikkeamanhallintaa koskeva koordinointi ja yhteistyö

1. Toimiessaan kyberturvallisuutta koskevan tietojenvaihdon ja poikkeamanhallinnan koordinointikeskuksena CERT-EU helpottaa poikkeamia, kyberuhkia, haavoittuvuuksia ja läheltä piti -tilanteita koskevaa tietojenvaihtoa seuraavien kesken:

a) unionin toimijat;

b) 17 ja 18 artiklassa tarkoitetut vastaavaa tehtävää hoitavat elimet.

2. CERT-EU helpottaa tarvittaessa tiiviissä yhteistyössä ENISAn kanssa poikkeamanhallintaa koskevaa koordinointia unionin toimijoiden kesken, mukaan lukien

a) osallistuminen johdonmukaiseen ulkoiseen viestintään;

b) keskinäinen tuki, kuten unionin toimijoille merkityksellisten tietojen jakaminen tai avun antaminen, tapauksen mukaan suoraan paikan päällä

c) operatiivisten resurssien optimaalinen käyttö;

d) koordinointi muiden unionin tason kriisinhallintamekanismien kanssa.

3. CERT-EU tukee tiiviissä yhteistyössä ENISAn kanssa unionin toimijoita poikkeamia, kyberuhkia, haavoittuvuuksia ja läheltä piti -tilanteita koskevan tilannetietoisuuden sekä kyberturvallisuuden alan merkityksellistä kehitystä koskevien tietojen jakamisen osalta.

4. IICB hyväksyy 8 päivään tammikuuta 2025 mennessä CERT-EU:n ehdotuksesta ohjeita tai suosituksia poikkeamanhallintaa koskevasta koordinoinnista ja yhteistyöstä merkittävien poikkeamien yhteydessä. Jos poikkeamaa epäillään rikokseksi, CERT-EU antaa ilman aiheetonta viivytystä neuvoja siitä, miten poikkeamasta ilmoitetaan lainvalvontaviranomaisille.

5. CERT-EU voi jäsenvaltion nimenomaisen pyynnön perusteella ja asianomaisten unionin toimijoiden hyväksynnän saatuaan pyytää asiantuntijoita 23 artiklan 4 kohdassa tarkoitetusta luettelosta osallistumaan sellaisen laajavaikutteisen poikkeaman hallintaan, jolla on vaikutusta tuossa jäsenvaltiossa, tai laajamittaisen kyberturvallisuuspoikkeaman hallintaan direktiivin (EU) 2022/2555 15 artiklan 3 kohdan g alakohdan mukaisesti. IICB hyväksyy CERT-EU:n ehdotuksesta erityissääntöjä, jotka koskevat unionin toimijoiden teknisten asiantuntijoiden saatavuutta ja käyttöä.

23 artikla

Laajavaikutteisten poikkeamien hallinta

1. Tukeakseen operatiivisella tasolla unionin toimijoihin vaikuttavien laajavaikutteisten poikkeamien koordinoitua hallintaa ja edistääkseen asiaankuuluvien tietojen säännöllistä vaihtoa unionin toimijoiden kesken ja jäsenvaltioiden kanssa IICB laatii 11 artiklan q alakohdan nojalla kyberkriisinhallintasuunnitelman 22 artiklan 2 kohdassa tarkoitettujen toimien perusteella tiiviissä yhteistyössä CERT-EU:n ja ENISAn kanssa. Kyberkriisinhallintasuunnitelma sisältää vähintään seuraavat osatekijät:

a) järjestelyt, jotka koskevat koordinointia ja tiedonkulkua unionin toimijoiden kesken laajavaikutteisten poikkeamien hallintaa varten operatiivisella tasolla;

b) yhteiset vakiotoimintamenettelyt;

c) yhteinen luokitus laajavaikutteisten poikkeamien vakavuutta ja kriisitilanteen kynnyspisteitä varten;

d) säännölliset harjoitukset;

e) suojatut viestintäkanavat, joita on tarkoitus käyttää.

2. Jollei tämän artiklan 1 kohdan nojalla laaditusta kyberkriisinhallintasuunnitelmasta muuta johdu, komission edustaja IICB:ssä on yhteyspiste laajavaikutteisia poikkeamia koskevien asiaankuuluvien tietojen jakamiseksi EU-CyCLONen kanssa, sanotun kuitenkaan rajoittamatta direktiivin (EU) 2022/2555 16 artiklan 2 kohdan ensimmäisen alakohdan soveltamista.

3. CERT-EU koordinoi laajavaikutteisten poikkeamien hallintaa unionin toimijoiden kesken. Se ylläpitää inventaaria saatavilla olevasta teknisestä asiantuntemuksesta, jota tarvittaisiin poikkeamanhallintaan laajavaikutteisten poikkeamien sattuessa, ja avustaa IICB:tä 9 artiklan 2 kohdassa tarkoitettujen, unionin toimijoiden laajavaikutteisia poikkeamia koskevien kyberkriisinhallintasuunnitelmien koordinoinnissa.

4. Unionin toimijat osallistuvat teknisen asiantuntemuksen inventaariin toimittamalla vuosittain päivitetyn luettelon organisaatiossaan käytettävissä olevista asiantuntijoista ja heidän teknisestä erityisosaamisestaan.

VI LUKU

LOPPUSÄÄNNÖKSET

24 artikla

Alustava talousarvion uudelleenkohdentaminen

CERT-EU:n asianmukaisen ja vakaan toiminnan varmistamiseksi komissio voi ehdottaa henkilöstöresurssien ja taloudellisten resurssien uudelleenkohdentamista komission talousarvioon käytettäviksi CERT-EU:n toiminnoissa. Uudelleenkohdentaminen tulee voimaan samaan aikaan kuin ensimmäinen tämän asetuksen voimaantulon jälkeen hyväksytty unionin vuotuinen talousarvio.

25 artikla

Uudelleentarkastelu

1. IICB raportoi CERT-EU:n avustuksella komissiolle tämän asetuksen täytäntöönpanosta 8 päivään tammikuuta 2025 mennessä ja sen jälkeen vuosittain. IICB voi esittää komissiolle suosituksia tämän asetuksen uudelleentarkastelusta.

2. Komissio arvioi tämän asetuksen täytäntöönpanoa sekä strategisella ja operatiivisella tasolla saatuja kokemuksia ja antaa Euroopan parlamentille ja neuvostolle kertomuksen niistä 8 päivään tammikuuta 2027 mennessä ja sen jälkeen kahden vuoden välein.

Tämän kohdan ensimmäisessä alakohdassa tarkoitettuun kertomukseen on sisällyttävä 16 artiklan 1 kohdassa tarkoitettu arviointi mahdollisuudesta perustaa CERT-EU unionin toimistoksi.

3. Komissio arvioi tämän asetuksen toimintaa ja toimittaa kertomuksen Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle sekä alueiden komitealle 8 päivään tammikuuta 2029 mennessä. Komissio arvioi myös, onko asianmukaista sisällyttää tämän asetuksen soveltamisalaan verkko- ja tietojärjestelmiä, joissa käsitellään EU:n turvallisuusluokiteltuja tietoja, ottaen huomioon muut näihin järjestelmiin sovellettavat unionin säädökset. Kertomukseen liitetään tarvittaessa lainsäädäntöehdotus.

26 artikla

Voimaantulo

Tämä asetus tulee voimaan kahdentenakymmenentenä päivänä sen jälkeen, kun se on julkaistu *Euroopan unionin virallisessa lehdessä*.

Tämä asetus on kaikilta osiltaan velvoittava, ja sitä sovelletaan sellaisenaan kaikissa jäsenvaltioissa.

Tehty Strasbourgissa 13 päivänä joulukuuta 2023.

Euroopan parlamentin puolesta	*Neuvoston puolesta*
Puhemies	*Puheenjohtaja*
R. METSOLA	P. NAVARRO RÍOS