Euroopan unionin neuvosto

Bryssel, 31. lokakuuta 2022
(OR. en)

14128/22

Toimielinten välinen asia:
2022/0085(COD)

CYBER 343
TELECOM 428
INST 396
CSC 472
CSCI 157
INF 176
FIN 1158
BUDGET 22
DATAPROTECT 294
CODEC 1617

ILMOITUS: I/A-KOHTA

Lähettäjä:	Neuvoston pääsihteeristö
Vastaanottaja:	Pysyvien edustajien komitea (Coreper II)/Neuvosto
Ed. asiak. nro:	10097/5/22 REV 5
Kom:n asiak. nro:	7474/22 + ADD 1
Asia:	Ehdotus Euroopan parlamentin ja neuvoston asetukseksi toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi unionin toimielimissä, elimissä ja laitoksissa – Yleisnäkemys

JOHDANTO

1. Komissio hyväksyi 22. maaliskuuta 2022 ehdotuksen asetukseksi toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi unionin toimielimissä, elimissä ja laitoksissa. Ehdotus oli yksi EU:n kyberturvallisuusstrategiassa digitaaliselle vuosikymmenelle[1] esitetyistä toimenpiteistä, ja sillä pyritään vahvistamaan unionin kollektiivista sietokykyä kyberuhkia vastaan.

[1] 14133/20.

Tästä strategiasta 22. maaliskuuta 2021 antamissaan päätelmissä[2] neuvosto korosti, että kyberturvallisuus on elintärkeää julkishallinnon ja instituutioiden toiminnalle niin kansallisella kuin EU:nkin tasolla sekä yhteiskunnallemme ja taloudellemme kokonaisuudessaan.

2. Euroopan unionin toiminnasta tehdyn sopimuksen 298 artiklaan perustuvalla komission ehdotuksella pyritään parantamaan kyberturvallisuuden tasoa unionin toimielimissä, elimissä ja laitoksissa vahvistamalla yhteinen kehys, jossa otetaan asianmukaisesti huomioon kunkin unionin toimijan itsenäisyys. Ehdotuksen tavoitteet ovat erityisesti seuraavat:

   – vahvistetaan CERT-EU:n (unionin toimijoille tarkoitettu toimielinten välinen itsenäinen tietotekniikan kriisiryhmä) toimeksiantoa ja rahoitusta;

   – perustetaan asetuksen asianmukaisen täytäntöönpanon varmistamiseksi toimielinten välinen rakenne (toimielinten välinen kyberturvallisuuslautakunta IICB), joka kokoaa yhteen kaikkien unionin toimijoiden edustajat;

   – otetaan käyttöön unionin toimijoiden velvoite jakaa (turvallisuusluokittelemattomia) tietoja poikkeamista CERT-EU:n kanssa ja ilmoittaa merkittävistä uhkista, haavoittuvuuksista ja poikkeamista; sekä

   – edistetään koordinointia ja yhteistyötä merkittäviin poikkeamiin reagoinnissa.

3. Euroopan parlamentti nimitti Henna Virkkusen (EPP) esittelijäksi käsittelyä johtavaan teollisuus-, tutkimus- ja energiavaliokuntaan. Mietintöluonnos julkaistiin 7. lokakuuta 2022.

4. Euroopan tietosuojavaltuutettu antoi lausuntonsa 17. toukokuuta 2022[3].

---

[2] 6722/21.
[3] 9252/22.

5. Neuvostossa ehdotuksen käsittely kyberkysymysten horisontaalisessa työryhmässä alkoi Ranskan puheenjohtajakaudella 29. maaliskuuta 2022. Puheenjohtajavaltio Ranska laati ensimmäisen kompromissitekstin, jota käsiteltiin kyberkysymysten horisontaalisessa työryhmässä kesäkuussa 2022, ja toimitti tilanneselvityksen[4] neuvostolle 21. kesäkuuta 2022.

6. Tšekin puheenjohtajakaudella kyberkysymysten horisontaalinen työryhmä käsitteli ehdotusta ja useita kompromissitekstejä kahdeksassa kokouksessa[5].

7. Puheenjohtajavaltio pyysi 23. toukokuuta 2022 neuvoston turvallisuuskomitealta lausuntoa ehdotuksen näkökohdista, jotka liittyvät tietoturvaan ja erityisesti turvallisuusluokiteltuihin tietoihin. Turvallisuuskomitea antoi lausuntonsa 19. syyskuuta 2022[6]. Turvallisuuskomitean ehdotuksen mukaisesti EU:n turvallisuusluokitellut tiedot on nimenomaisesti jätetty asetuksen soveltamisalan ulkopuolelle. Säännöksiä, jotka liittyvät muilta kuin unionin toimijoilta saatuihin tietoihin liittyviin poikkeuksiin jakamis- ja raportointivelvoitteista, on muutettu vastaavasti.

8. Kyberkysymysten horisontaalinen työryhmä pääsi 28. lokakuuta 2022 yhteisymmärrykseen liitteessä olevasta puheenjohtajavaltion kompromissiehdotuksesta.

---

4 9719/22.
5 6. ja 20. heinäkuuta, 13., 21. ja 28. syyskuuta sekä 5., 19. ja 28. lokakuuta 2022.
6 12603/22 + COR 1.

KESKEISET KYSYMYKSET

9. Jäsenvaltiot suhtautuivat myönteisesti ehdotukseen, koska se on oikea-aikainen ja täydentää tulevaa direktiiviä toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi koko unionissa, jäljempänä ’NIS 2 -direktiivi’, ja kannattivat sen yleisiä tavoitteita. Jäsenvaltiot kehottivat kuitenkin jatkamaan mukauttamista NIS 2 -direktiiviin, lisäämään vastavuoroisuutta unionin toimijoiden ja jäsenvaltioiden tietojenvaihdossa ja huomauttivat, että osa ehdotetuista toimenpiteistä perustuu liikaa vapaaehtoisuuteen. Jäsenvaltiot ilmaisivat myös pitävänsä parempana, että viittaus yhteiseen kyberturvallisuusyksikköön, jonka toimeksiantoa ja kokoonpanoa ei ole vielä määritelty, poistettaisiin.

10. Kyberkysymysten horisontaalisessa työryhmässä käytyjen keskustelujen perusteella seuraavat seikat on määritelty tärkeimmiksi poliittisiksi kysymyksiksi:

a) Mukauttaminen tulevaan NIS 2 -direktiiviin

Jäsenvaltioiden pyynnöstä ehdotusta on mukautettu edelleen tulevaan NIS 2 -direktiiviin, muun muassa

- mukauttamalla useita määritelmiä (3 artikla) NIS 2 -direktiivin määritelmiin;
- lisäämällä uusi 7 a artikla vapaaehtoisista vertaisarvioinneista NIS 2 -direktiivin mukaisesti ja unionin toimijoiden tarpeisiin mukautettuna;
- ehdotuksen 20 artiklan mukaiset raportointivelvoitteet on mukautettu NIS 2 -direktiivin mukaisiin raportointivelvoitteisiin.

b) Toimielinten välisen kyberturvallisuusneuvoston (IICB) kokoonpano (9 artikla)

Jäsenvaltioiden edustajien asianmukaisesta osallistumisesta IICB:n työhön käytyjen keskustelujen pohjalta kompromissiin päästiin pöytäkirjaan merkittävän neuvoston lausuman avulla.

c) Institutionaalinen autonomia

Jäsenvaltioiden halu vahvistaa noudattamisen valvontamekanismeja ja tarve noudattaa institutionaalisen autonomian periaatetta on saatu tasapainoon erityisesti tarkastusten ja kurinpitotoimien osalta (11 artikla).

Johdanto-osan 8 kappaleesta poistettiin viittaus tiettyyn prosenttiosuuteen, joka tietotekniikkabudjetista olisi varattava kyberturvallisuuteen.

PÄÄTELMÄ

11. Pysyvien edustajien komiteaa pyydetään

a) hyväksymään liitteessä oleva kompromissiteksti, joka toimii valtuutuksena Euroopan parlamentin kanssa käytäviä neuvotteluja varten,

b) ehdottamaan, että neuvosto hyväksyisi liitteessä olevan kompromissitekstin istunnossaan 18. marraskuuta 2022 ja merkitsisi tämän asiakirjan lisäyksessä olevan neuvoston lausuman pöytäkirjaan.

LIITE

2022/0085 (COD)

Ehdotus

EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS

toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi unionin toimielimissä, elimissä ja laitoksissa

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,

sekä katsovat seuraavaa:

(1) Tieto- ja viestintätekniikka on avoimen, tehokkaan ja riippumattoman unionin hallinnon kulmakivi digiaikakaudella. Alati kehittyvä teknologia sekä digitaalisten järjestelmien yhä suurempi monimutkaisuus ja keskinäinen riippuvuus lisäävät kyberturvallisuusriskejä, minkä seurauksena unionin hallinto on yhä haavoittuvampi kyberuhkille ja poikkeamille. Tämä puolestaan vaarantaa viime kädessä hallinnon toiminnan jatkuvuuden ja kyvyn suojata tietonsa. Vaikka pilvipalvelujen kasvava hyödyntäminen, tietotekniikan laajamittainen käyttö, korkea digitalisaatioaste, etätyö sekä kehittyvä teknologia ja verkkoyhteydet ovat nykyään keskeisiä piirteitä unionin hallinnollisten yksiköiden 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 heidän kampanjansa ovat yhä kehittyneempiä ja automaattisempia, ne kohdennetaan alttiina oleville, laajeneville hyökkäyspinnoille ja niissä käytetään nopeasti hyväksi haavoittuvuuksia.

(3) Unionin **toimijoiden** [...] tietoteknisillä ympäristöillä on keskinäisiä riippuvuussuhteita ja yhdistettyjä tietovirtoja, ja niiden käyttäjät tekevät tiivistä yhteistyötä. Tämä keskinäinen yhteys tarkoittaa, että vaikka häiriöt alun perin rajoittuisivatkin yhteen unionin **toimijaan** [...], niillä voi olla ketjureaktiovaikutuksia, jotka voivat aiheuttaa kauaskantoisia ja pitkäaikaisia kielteisiä vaikutuksia muihin. Lisäksi tiettyjen **unionin toimijoiden** [...] tietotekniset ympäristöt ovat yhteydessä jäsenvaltioiden tietoteknisiin ympäristöihin, minkä seurauksena yhdessä unionin toimijassa tapahtunut poikkeama aiheuttaa riskin jäsenvaltioiden tietoteknisten ympäristöjen kyberturvallisuudelle ja päinvastoin. **Unionin toimijat myös käsittelevät suuria määriä jäsenvaltioista peräisin olevia, usein arkaluonteisia tietoja, minkä vuoksi poikkeamat voivat vaikuttaa kielteisesti myös jäsenvaltioihin. Tästä syystä unionin toimijoiden kyberturvallisuus on erittäin tärkeää myös jäsenvaltioille. Poikkeamakohtaiset tiedot voivat myös 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 kyberuhkien sietokyvyssä ja sen kehitystasossa sekä kyvyssä havaita haitallinen kybertoiminta ja reagoida siihen. Eurooppalaisen hallinnon toimivuuden kannalta on siksi välttämätöntä, että unionin [...] **toimijat** saavuttavat yhteisen korkean kyberturvatason **toteuttamalla kyberturvallisuustoimenpiteitä,** [...] vaihtamalla tietoja ja tekemällä yhteistyötä.

(5) Toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi koko unionissa annetun direktiivin [ehdotus NIS 2 -direktiiviksi] tavoitteena on parantaa julkisten ja yksityisten toimijoiden, toimivaltaisten kansallisten viranomaisten ja elinten sekä koko unionin kyberuhkien sietokykyä ja kykyä reagoida poikkeamiin. Siksi on välttämätöntä, että unionin **toimijat** [...] seuraavat esimerkkiä varmistamalla, että niiden säännöt ovat yhdenmukaisia direktiivin [ehdotus NIS 2 -direktiiviksi] kanssa ja vastaavat sen vaatimustasoa.

(6) Yhteisen korkean kyberturvatason saavuttamiseksi unionin kunkin **toimijan** [...] on tarpeen laatia sisäinen kyberturvallisuusriskien hallinta- ja valvontakehys, jolla varmistetaan kaikkien kyberturvallisuusriskien tehokas ja järkevä hallinta [...]. **Kehyksessä olisi vahvistettava kyberturvallisuuspolitiikka, mukaan lukien menettelyt, joilla toteutettuja kyberturvallisuustoimenpiteitä arvioidaan. Kehyksen olisi perustuttava kaikki vaaratekijät huomioon ottavaan toimintatapaan, 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, lähetettävien, käsiteltävien tai saatavilla olevien tietojen saatavuuden, aitouden, eheyden tai luottamuksellisuuden. Kehyksessä olisi otettava huomioon riskianalyysin tulokset ja kaikki asiaankuuluvat tekniset, operatiiviset ja organisatoriset riskit asianomaisen unionin toimijan kyberturvallisuudelle.**

(6 a) Jotta kehyksessä yksilöityjä riskejä voidaan hallita, kunkin unionin toimijan olisi varmistettava, että asianmukaiset ja oikeasuhteiset tekniset, operatiiviset ja organisatoriset toimenpiteet toteutetaan. Ne olisi kohdistettava tässä asetuksessa vahvistettuihin aloihin, myös kyberturvallisuustoimenpiteiden osalta, kunkin unionin toimijan kyberturvallisuuden vahvistamiseksi.

(6 b) **Kehyksessä yksilöidyt resurssit ja riskit sekä säännöllisistä kehitystason arvioinneista tehdyt päätelmät olisi otettava huomioon kunkin unionin toimijan laatimassa kyberturvallisuussuunnitelmassa. Kyberturvallisuussuunnitelmaan olisi sisällytettävä hyväksytyt kyberturvallisuustoimenpiteet, joilla pyritään lisäämään asianomaisen unionin toimijan yleistä kyberturvallisuutta.**

(6 c) **Kyberturvallisuuden varmistaminen on jatkuva prosessi, joten kaikkien toimenpiteiden soveltuvuutta ja tehokkuutta olisi tarkasteltava säännöllisesti uudelleen unionin toimijoiden muuttuvien riskien, resurssien ja kehitystason valossa. Kehystä olisi tarkasteltava uudelleen säännöllisesti ja vähintään joka kolmas vuosi, ja kyberturvallisuussuunnitelmaa olisi tarkistettava vähintään kerran kahdessa vuodessa taikka kehyksen kunkin kehitystason arvioinnin tai uudelleentarkastelun jälkeen.**

(6 d) **Unionin toimijoiden olisi vaihdettava säännöllisesti asiaankuuluvia tietoja, myös asiaankuuluvista poikkeamista ja kyberuhkista, sekä varmistettava samalla raportoivan unionin toimijan toimittamien tietojen luottamuksellisuus ja asianmukainen suoja.**

(6 e) **Olisi otettava käyttöön mekanismi, jolla varmistetaan unionin toimijoiden tehokas tietojenvaihto, koordinointi ja yhteistyö merkittävien poikkeamien tapauksessa, mukaan lukien asianosaisten unionin toimijoiden tehtävien ja vastuiden selkeä määrittely. EU-CyCLONen nimetyn yhteyspisteen olisi otettava vaihdetut tiedot huomioon, kun se jakaa asiaankuuluvia tietoja EU-CyCLONen kanssa yhteisen tilannetietoisuuden edistämiseksi.**

(7) Unionin **toimijoiden** [...] välisten erojen vuoksi täytäntöönpanossa tarvitaan joustavuutta, koska yksi ratkaisu ei sovi kaikille. Toimenpiteisiin yhteisen korkean kyberturvatason varmistamiseksi ei pitäisi sisältyä velvoitteita, jotka heikentävät suoraan unionin **toimijoiden** [...] tehtävien hoitamista tai rajoittavat niiden hallinnollista riippumattomuutta. Näin ollen unionin **toimijoiden** [...] olisi laadittava omat kehyksensä kyberturvallisuusriskien hallintaa ja valvontaa varten **ja omat kyberturvallisuussuunnitelmansa** sekä hyväksyttävä [...] **kyberturvallisuustoimenpiteensä**. **Tällaisia toimenpiteitä toteutettaessa olisi otettava asianmukaisesti huomioon unionin toimijoiden väliset synergiat, jotta varmistetaan resurssien asianmukainen hallinnointi ja kustannusten optimointi. Olisi myös otettava asianmukaisesti huomioon, että toimenpiteet eivät vaikuta kielteisesti unionin yhteisöjen tehokkaaseen tietojenvaihtoon ja toimintaan muiden unionin yhteisöjen ja kansallisten toimivaltaisten viranomaisten kanssa.**

(8) Jotta unionin **toimijoille** [...] ei aiheutuisi kohtuutonta taloudellista ja hallinnollista rasitetta, kyberturvallisuusriskien hallintaa koskevien vaatimusten olisi oltava oikeassa suhteessa asianomaisen verkko- ja tietojärjestelmän aiheuttamaan riskiin, ottaen huomioon näiden toimenpiteiden viimeisin kehitys. Unionin kunkin **toimijan** [...] olisi pyrittävä osoittamaan oman kyberturvatasonsa parantamiseen riittävä prosenttiosuus tietotekniikkamenoistaan. **Kehitystason arvioinnissa olisi arvioitava myös sitä, ovatko unionin toimijan kyberturvallisuusmenot oikeassa suhteessa siihen kohdistuviin riskeihin.**

(9) Yhteinen korkea kyberturvataso edellyttää, että kyberturvallisuus on unionin kunkin **toimijan** [...] ylimmän johdon valvonnassa. [...] **Ylimmän johdon olisi valvottava tämän asetuksen täytäntöönpanoa, mukaan lukien riskien hallinta- ja valvontakehyksen sekä kyberturvallisuussuunnitelmien laatiminen, myös kyberturvallisuustoimenpiteiden osalta**. Kyberturvallisuuskulttuuriin eli kyberturvallisuuden käytännön harjoittamiseen puuttuminen on keskeinen osa **kaikkien unionin toimijoiden kyberturvallisuuskehystä** [...].

(10) [...] **Kyberturvallisuustoimenpiteiden** olisi muodostettava osa [...] **kyberturvallisuussuunnitelmaa**, ja niitä olisi tarkennettava CERT-EU:n julkaisemissa ohjeasiakirjoissa tai suosituksissa. Toimenpiteitä ja ohjeita määriteltäessä olisi otettava asianmukaisesti huomioon **kehittyneimmät asiaan liittyvät eurooppalaiset ja kansainväliset standardit sekä** asiaan liittyvä EU:n lainsäädäntö ja toimintapolitiikat, mukaan lukien NIS-yhteistyöryhmän julkaisemat riskinarvioinnit ja suositukset, kuten EU:n koordinoitu riskinarviointi ja 5G-kyberturvallisuutta koskeva EU:n välineistö. Lisäksi voitaisiin edellyttää asiaan liittyvien tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien sertifiointia asetuksen (EU) 2019/881 49 artiklan nojalla hyväksyttyjen erityisten eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien mukaisesti. **CERT-EU:n olisi tarvittaessa tehtävä yhteistyötä ENISAn kanssa.**

(11) Unionin toimielinten ja elinten pääsihteerit päättivät toukokuussa 2011 perustaa EU:n toimielinten, elinten ja virastojen tietotekniikan kriisiryhmän (CERT-EU) 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 Euroopan komission työryhmäksi, jonka toimeksianto kattaa useita toimielimiä. Joulukuussa 2017 unionin toimielimet ja elimet tekivät toimielinten välisen järjestelyn CERT-EU:n organisaatiosta ja toiminnasta[7]. 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**.

[...]

[7] EUVL C 12, 13.1.2018, s. 1–11.

(13) Monet kyberhyökkäykset ovat osa laajempia kampanjoita, jotka kohdistuvat unionin [...] **toimijoiden** ryhmiin tai etuyhteisöihin, joihin sisältyy unionin [...] **toimijoita**. Jotta voitaisiin havaita ongelmat etukäteen, reagoida poikkeamiin ja toteuttaa lieventäviä toimenpiteitä, unionin [...] **toimijoiden** olisi ilmoitettava CERT-EU:lle [...] kyberuhkista, haavoittuvuuksista**, läheltä piti -tilanteista** ja poikkeamista sekä jaettava sen kanssa asianmukaiset tekniset tiedot, jotka mahdollistavat samankaltaisen kyberuhkien, haavoittuvuuksien**, läheltä piti -tilanteiden** ja poikkeamien tunnistamisen tai lieventämisen sekä niihin reagoimisen [...] **muiden unionin toimijoiden toiminnassa**. Direktiivissä [ehdotus NIS 2 -direktiiviksi] määritetyn lähestymistavan mukaisesti silloin, kun **unionin** toimija saa tietoonsa merkittävän poikkeaman, sitä olisi vaadittava toimittamaan [...] **varhaisvaroitus** CERT-EU:lle 24 tunnin kuluessa. Tällaisen tietojenvaihdon olisi mahdollistettava se, että CERT-EU levittää tiedot muille unionin [...] **toimijoille** sekä asianmukaisille vastaavaa tehtävää hoitaville viranomaisille, jotta voidaan auttaa suojaamaan unionin tietoteknisiä järjestelmiä ja unionin kumppaneiden tietoteknisiä järjestelmiä samankaltaisilta poikkeamilta [...].

(13 a) Tässä asetuksessa säädetään merkittävien poikkeamien ilmoittamista koskevasta monivaiheisesta toimintatavasta, jotta löydetään oikea tasapaino toisaalta nopean raportoinnin, joka auttaa lieventämään merkittävien poikkeamien mahdollista leviämistä ja antaa unionin toimijoille mahdollisuuden hakea apua, ja toisaalta sellaisen syvällisemmän raportoinnin välillä, jossa otetaan tärkeää oppia yksittäisistä poikkeamista ja parannetaan ajan mittaan unionin toimijoiden kyberresilienssiä. Tätä varten tähän asetukseen olisi sisällytettävä raportointi poikkeamista, jotka unionin toimijan tekemän alustavan arvioinnin perusteella voisivat aiheuttaa vakavia häiriötilanteita unionin toimijan toiminnassa tai taloudellisia tappioita kyseiselle unionin toimijalle taikka vaikuttaa muihin luonnollisiin henkilöihin tai oikeushenkilöihin aiheuttamalla huomattavaa aineellista tai aineetonta vahinkoa. Tällaisessa alustavassa arvioinnissa olisi otettava huomioon muun muassa verkko- ja tietojärjestelmät, joihin vaikutukset kohdistuvat, ja erityisesti niiden merkitys unionin toimijan toiminnalle, kyberuhan vakavuus ja tekniset ominaisuudet ja siihen liittyvät hyödynnettävät haavoittuvuudet sekä unionin toimijan kokemus samankaltaisista poikkeamista. Indikaattorit, kuten se, miten laajat vaikutukset unionin toimijan toimintaan kohdistuvat, poikkeaman kesto tai niiden luonnollisten henkilöiden tai oikeushenkilöiden lukumäärä, joihin vaikutukset kohdistuvat, voisivat olla tärkeässä asemassa määritettäessä, onko häiriötilanne vakava.

(13 b) Koska asianomaisen unionin toimijan infrastruktuuri ja verkostot 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 asianomaisen unionin toimijan olisi ilmoitettava poikkeamista CERT-EU:n kansalliselle vastapuolelle, jonka jäsenvaltio on nimennyt direktiivin [ehdotus NIS 2 -direktiiviksi] mukaisesti, samassa määräajassa, jossa sen olisi ilmoitettava merkittävästä poikkeamasta CERT-EU:lle. CERT-EU:n olisi myös ilmoitettava kyseiselle kansalliselle vastapuolelle, kun se saa tiedon merkittävästä poikkeamasta jäsenvaltiossa, ellei asianomainen unionin toimija ole jo ilmoittanut siitä.

(14) Sen lisäksi, että CERT-EU:lle annetaan enemmän tehtäviä ja sen roolia laajennetaan, olisi perustettava toimielinten välinen kyberturvallisuuslautakunta (IICB). **Jotta voidaan edistää unionin toimijoiden yhteistä korkeaa kyberturvatasoa, IICB:llä** olisi **oltava yksinoikeutettu asema seurata** [...] tämän asetuksen täytäntöönpanoa unionin [...] **toimijoiden 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 toimielinten edustus ja otettava mukaan virastojen ja elinten edustajia unionin virastojen verkoston kautta. **IICB:n organisaatiota ja toimintaa olisi säänneltävä tarkemmin sen sisäisellä työjärjestyksellä, johon voi sisältyä IICB:n säännöllisten kokousten määrittely tarkemmin, myös sellaisten vuotuisten poliittisen tason kokousten osalta, joissa kunkin IICB:n jäsenen ylimmän johdon edustajat voisivat käydä strategista keskustelua ja antaa strategista ohjausta IICB:lle. IICB voi lisäksi perustaa toimeenpanevan komitean 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 yksityiskohtaisista säännöistä, unionin toimijoiden IICB:lle tämän asetuksen mukaisesti toimittamista asiakirjoista ja raporteista tai tehtävistä, jotka liittyvät vaatimusten noudattamista koskevia toimenpiteitä koskevien, IICB:n antamien päätösten valmisteluun ja niiden täytäntöönpanon seurantaan. IICB:n olisi vahvistettava toimeenpanevan komitean työjärjestys, mukaan lukien sen tehtävät ja valtuudet.**

(15) CERT-EU:n olisi tuettava toimenpiteiden toteuttamista yhteisen korkean kyberturvatason varmistamiseksi tekemällä IICB:lle ehdotuksia ohjeasiakirjoiksi ja suosituksiksi tai antamalla toimintakehotuksia. Tällaisten ohjeasiakirjojen ja suositusten hyväksymisestä vastaa IICB. Tarvittaessa CERT-EU:n olisi annettava toimintakehotuksia, jossa kuvaillaan kiireellisiä turvatoimenpiteitä, jotka unionin [...] **toimijoita** kehotetaan toteuttamaan tietyssä määräajassa**. IICB voi kehottaa CERT-EU:ta antamaan tai peruuttamaan toimintakehotuksen tai ehdotuksen ohjeasiakirjaksi tai suositukseksi taikka muokkaamaan niitä.**

(16) IICB:n olisi valvottava tämän asetuksen noudattamista, ohjeasiakirjojen ja suositusten jatkotoimien toteuttamista sekä [...] toimintakehotusten noudattamista. Teknisissä asioissa IICB:n tukena olisi oltava teknisiä neuvoa-antavia ryhmiä, joiden koostumuksesta päättää IICB. Niiden olisi tehtävä tiivistä yhteistyötä CERT-EU:n, unionin [...] **toimijoiden** sekä tarvittaessa muiden sidosryhmien kanssa. [...] **Jos IICB katsoo, että unionin toimijat eivät ole soveltaneet tai panneet täytäntöön tätä asetusta, mukaan lukien tämän asetuksen mukaisesti annetut ohjeasiakirjat, suositukset ja toimintakehotukset, se voi toteuttaa vaatimusten noudattamista koskevat toimenpiteet, sanotun kuitenkaan rajoittamatta asiaan liittyvän unionin toimijan sisäisten menettelyjen soveltamista. Vaatimusten noudattamista koskevien toimenpiteiden järjestelmää olisi käytettävä progressiivisesti. Tämä merkitsee sitä, että kun IICB hyväksyy vaatimusten noudattamista koskevat toimenpiteet, sen olisi aloitettava varoituksella vähiten ankarana toimenpiteenä ja tarvittaessa jatkettava kaikkein ankarimpaan toimenpiteeseen (kyseiselle unionin toimijalle toimitettavien tietovirtojen tilapäistä keskeyttämistä koskevan ohjeen antaminen), jota sovellettaisiin poikkeuksellisissa tapauksissa, joissa asianomainen toimija jättää noudattamatta tämän asetuksen mukaista velvoitettaan pitkäaikaisesti, tahallisesti tai vakavasti.**

(16 a) Varoitus on vähiten vakava vaatimusten noudattamista koskeva toimenpide, jolla puututaan unionin toimijan toiminnassa havaittuihin puutteisiin ja joka sisältää suosituksia sen kyberturvallisuusasiakirjojen muuttamiseksi tietyssä määräajassa. Varoituksen olisi oltava kaikkien unionin toimijoiden saatavilla, ellei sitä rajoiteta asianmukaisesti tämän asetuksen mukaisesti.

(16 b) IICB voi lisäksi suositella, että unionin toimijalle tehdään tarkastus. Unionin toimija voi käyttää tähän tarkoitukseen sisäisen tarkastuksen toimintoaan. IICB voisi myös pyytää, että tarkastuksen suorittaa kolmas osapuoli, mukaan lukien jokin yhteisesti sovituista yksityisen sektorin palveluntarjoajista.

(16 c) IICB voi suosituksestaan tai pyynnöstään suoritetun tarkastuksen tulosten perusteella pyytää lisäksi unionin toimijaa saattamaan kyberturvallisuusriskien hallinnan ja valvonnan tämän asetuksen säännösten mukaisiksi.

(16 d) Koska jäsenvaltiot jakavat asiaankuuluvien unionin toimijoiden kanssa tietoja, jotka voivat olla arkaluonteisia, tällaisten tietojen vastaanottajan kyberturvallisuus on ratkaisevan tärkeää jäsenvaltioille. Sen vuoksi poikkeustapauksissa, joissa unionin toimija laiminlyö velvoitteitaan pitkäaikaisesti, tahallisesti, toistuvasti tai vakavasti, IICB voi viimeisenä keinona antaa kaikille jäsenvaltioille ja unionin toimijoille ohjeen, jossa suositetaan asianosaiselle unionin toimijalle toimitettavien tietovirtojen tilapäistä keskeyttämistä siihen asti, kunnes kyseisen toimijan kyberturvallisuustilanne on korjattu. Tästä ohjeesta olisi ilmoitettava kaikille jäsenvaltioille ja unionin toimijoille asianmukaisten suojattujen viestintäkanavien kautta.

(16 e) **Jos IICB katsoo, että unionin toimija on jatkuvasti rikkonut tätä asetusta suoraan sen henkilöstön jäsenen toimien tai laiminlyöntien johdosta, myös ylimmällä johtotasolla, sen olisi tämän asetuksen asianmukaisen täytäntöönpanon varmistamiseksi pyydettävä asianomaista unionin toimijaa toteuttamaan asianmukaiset kyseistä henkilöstön jäsentä koskevat toimet henkilöstösääntöjen ja muiden tiettyihin unionin toimijoihin sovellettavien vastaavien sääntöjen mukaisesti. Näihin toimiin voivat kuulua esimerkiksi kurinpitomenettely ja tarvittaessa unionin virastojen tapauksessa toimivaltaiselle viranomaiselle esitetty pyyntö toteuttaa tarvittavat toimet, jotka liittyvät tämän asetuksen jatkuvasta rikkomisesta mahdollisesti vastuussa olevan henkilön mahdolliseen erottamiseen.**

(17) CERT-EU:n tarkoituksena olisi oltava edistää kaikkien unionin [...] **toimijoiden** tietoteknisen ympäristön turvallisuutta. **Kun CERT-EU harkitsee teknisen neuvonnan tai palautteen antamista asiaankuuluvissa toimintapoliittisissa kysymyksissä unionin toimijan pyynnöstä, sen olisi varmistettava, että tämä ei estä sitä hoitamasta muita tässä asetuksessa säädettyjä tehtäviään.**

(17 a) CERT-EU:n olisi toimittava vastaavassa tehtävässä kuin direktiivin [ehdotus NIS 2 -direktiiviksi] 6 artiklassa tarkoitettu Euroopan haavoittuvuusrekisteriin tehtävää koordinoitua haavoittuvuuksien ilmaisemista varten unionin [...] **toimijoille** nimetty koordinaattori**, ja sen olisi laadittava haavoittuvuuksien hallintaa koskeva politiikka, johon sisältyy vapaaehtoisen koordinoidun haavoittuvuuksien ilmaisemisen edistäminen ja helpottaminen.**

[...]

(19) CERT-EU:n olisi myös suoritettava sille direktiivissä [ehdotus NIS 2 -direktiiviksi] säädetty tehtävä, joka koskee yhteistyötä ja tietojen vaihtoa tietoturvaloukkauksiin reagoivien kansallisten yksiköiden (CSIRT-yksiköt) verkoston kanssa. Lisäksi CERT-EU:n olisi komission suosituksen (EU) 2017/1584[8] mukaisesti tehtävä yhteistyötä ja koordinoitava reagoiminen asiaan liittyvien sidosryhmien kanssa. Korkean kyberturvatason edistämiseksi koko unionissa CERT-EU:n olisi jaettava poikkeamakohtaista tietoa vastaavaa tehtävää hoitavien kansallisten elinten kanssa. CERT-EU:n olisi myös tehtävä yhteistyötä muiden vastaavaa tehtävää hoitavien julkisten ja yksityisten toimijoiden kanssa, myös Natossa, edellyttäen, että IICB on antanut sille etukäteisen hyväksynnän.

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

(20) CERT-EU:n olisi operatiivista kyberturvallisuutta tukiessaan hyödynnettävä saatavilla olevaa Euroopan unionin kyberturvallisuusviraston **(ENISA)** asiantuntemusta Euroopan parlamentin ja neuvoston asetuksessa (EU) 2019/881[9] tarkoitetun jäsennellyn yhteistyön kautta. Tarvittaessa tällaisen yhteistyön käytännön toteutus olisi määriteltävä erityisin järjestelyin näiden kahden toimijan välillä päällekkäisten tehtävien välttämiseksi. CERT-EU:n olisi tehtävä yhteistyötä [...] **ENISAn** kanssa uhka-analyysissa ja jaettava säännöllisesti uhkaympäristöä koskeva raporttinsa viraston kanssa.

[...]

(22) **Tämän asetuksen mukaisiin CERT-EU:n toimiin ja tietojen käsittelyyn voi sisältyä henkilötietojen käsittelyä.** Kaikessa tämän asetuksen nojalla toteutettavassa henkilötietojen käsittelyssä olisi noudatettava tietosuojalainsäädäntöä, myös Euroopan parlamentin ja neuvoston asetusta (EU) 2018/1725[11]. **Jos henkilötietoja siirretään tämän asetuksen nojalla muille unioniin sijoittautuneille vastaanottajille kuin unionin toimijoille, tämä olisi tehtävä asetuksen (EU) 2018/1725 9 artiklan mukaisesti.**

---

9 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).

11 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).

(23) CERT-EU:n sekä unionin [...] **toimijoiden** olisi noudatettava tietojen käsittelyssä [...] **sovellettavia tietoturvallisuutta koskevia** sääntöjä. [...]

(23 a) 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 tulee katsoa keinoksi antaa tietoa mahdollisista tiedon edelleen levittämistä koskevista rajoituksista. Sitä käytetään lähes kaikissa tietoturvaloukkauksiin reagoivissa ja niitä tutkivissa CSIRT-ryhmissä ja joissakin tiedon analysointi- ja jakamiskeskuksissa.

(24) **Tällä asetuksella ja CERT-EU:lle osoitetuilla uusilla tehtävillä ei ole vaikutusta monivuotisen rahoituskehyksen kokonaismenoihin.** Koska CERT-EU:n palvelut ja tehtävät ovat unionin kaikkien [...] **toimijoiden** edun mukaisia, unionin kunkin [...] **toimijan**, jolla on tietotekniikkamenoja, olisi osoitettava oikeudenmukainen rahoitusosuus näihin palveluihin ja tehtäviin. Nämä rahoitusosuudet eivät rajoita unionin [...] **toimijoiden** itsenäistä budjettivaltaa. **Kaikkien unionin toimijoiden ja niiden hallintojen olisi varmistettava resurssiensa optimointi nykyisellä tasolla ja vahvistettava tehokkuushyötyjä muun muassa syventämällä toimielinten välistä yhteistyötä kyberturvallisuuden alalla. Sen vuoksi unionin toimijoiden olisi mieluummin yhdistettävä hallintomenojaan kuin käytettävä varoja erikseen.**

(25) 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. **Lisäksi Euroopan tilintarkastustuomioistuinta pyydetään arvioimaan säännöllisesti CERT-EU:n toimintaa,**

OVAT HYVÄKSYNEET TÄMÄN ASETUKSEN:

I luku
YLEISET SÄÄNNÖKSET

1 artikla

Kohde

1. Tässä asetuksessa vahvistetaan **toimenpiteet, joilla pyritään saavuttamaan unionin toimijoiden yhteinen korkea kyberturvataso.** [...]

2. Tämän vuoksi asetuksessa vahvistetaan

c) **kullekin** [...] unionin [...] **toimijalle** velvoitteet perustaa [...] kyberturvallisuusriskien hallinta- ja valvontakehys;

d) unionin [...] **toimijoille asetettavat** kyberturvallisuusriskien hallinta- [...]**, raportointi- ja tiedonjakovelvoitteet**;

e) unionin [...] **toimijoille tarkoitetun toimielinten välisen itsenäisen tietotekniikan kriisiryhmän** (CERT-EU) organisaatioon ja toimintaan sekä toimielinten välisen kyberturvallisuuslautakunnan **(IICB)** organisaatioon ja toimintaan **sovellettavat säännöt;**

f) tämän asetuksen täytäntöönpanon seurantaa koskevat säännöt.

2 artikla

Soveltamisala

1. Tätä asetusta sovelletaan [...] kaikkiin unionin [...] **toimijoihin** sekä [...] **CERT-EU:hun** ja **IICB:hen** [...].

2. Tätä asetusta sovelletaan rajoittamatta perussopimusten mukaista institutionaalista riippumattomuutta.

3. Tätä asetusta ei sovelleta 12 artiklan 7 kohtaa lukuun ottamatta 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 ja laitoksia;

2) ’verkko- ja tietojärjestelmällä’ direktiivin [ehdotus NIS 2 -direktiiviksi] 4 artiklan 1 kohdassa [...] **määriteltyä** verkko- ja tietojärjestelmää;

3) ’verkko- ja tietojärjestelmien turvallisuudella’ direktiivin [ehdotus NIS 2 -direktiiviksi] 4 artiklan 2 kohdassa [...] **määriteltyä** verkko- ja tietojärjestelmien turvallisuutta;

4) ’kyberturvallisuudella’ ja ’kyberturvalla’ [...] **asetuksen (EU) 2019/881 2 artiklan 1 kohdassa määriteltyä kyberturvallisuutta**;

5) ’ylimmällä johdolla’ kaikkein ylimpään johtotasoon kuuluvaa johtajaa, hallinto- tai koordinointi- ja valvontaelintä**, jolla on päätäntävalta,** unionin kunkin [...] **toimijan** korkean tason hallintojärjestelyt huomioon ottaen;

5 a) ’läheltä piti -tilanteella’ direktiivin [ehdotus NIS 2 -direktiiviksi] 4 artiklan 4 a kohdassa määriteltyä läheltä piti -tilannetta;

6) ’poikkeamalla’ direktiivin [ehdotus NIS 2 -direktiiviksi] 4 artiklan 5 kohdassa [...] **määriteltyä** poikkeamaa;

[...]

8) ’[...] **merkittävällä 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) ’poikkeaman käsittelyllä’ direktiivin [ehdotus NIS 2 -direktiiviksi] 4 artiklan 6 kohdassa [...] **määriteltyä** poikkeaman käsittelyä;

10) ’kyberuhkalla’ asetuksen (EU) 2019/881 2 artiklan 8 kohdassa [...] **määriteltyä** kyberuhkaa;

[...]

12) ’haavoittuvuudella’ direktiivin [ehdotus NIS 2 -direktiiviksi] 4 artiklan 8 kohdassa tarkoitettua haavoittuvuutta;

[...]

14) ’[...] **riskillä**’ **direktiivin [ehdotus NIS 2 -direktiiviksi] 4 artiklan 7 b kohdassa tarkoitettua riskiä** [...];

[...]

[...]

3 a artikla

Henkilötietojen käsittely

1) CERT-EU:n, IICB:n tai unionin toimijoiden tämän asetuksen nojalla suorittamassa henkilötietojen käsittelyssä noudatetaan asetusta (EU) 2018/1725.

2) CERT-EU, IICB ja unionin toimijat käsittelevät ja vaihtavat henkilötietoja siinä määrin kuin on tarpeen ja yksinomaan tämän asetuksen mukaisten velvoitteidensa täyttämiseksi.

Luku II

TOIMENPITEET YHTEISEN KORKEAN KYBERTURVATASON VARMISTAMISEKSI

4 artikla

Riskien hallinta- ja valvontakehys

1. Unionin kukin [...] **toimija** laatii [...] kyberturvallisuusriskien hallinta- ja valvontakehyksen, jäljempänä ’kehys’, tukemaan kyseisen **toimijan** toimeksiantoa [...]**.** [...] **Kehystä** valvotaan kyseisen [...] **toimijan** ylimmällä hallintotasolla, jotta voidaan varmistaa kaikkien kyberturvallisuusriskien tehokas ja järkevä hallinta. Kehyksen on oltava käytössä viimeistään … päivänä …kuuta … [15 kuukauden kuluttua tämän asetuksen voimaantulosta].

2. Kehyksen on katettava asianomaisen [...] **unionin toimijan** koko turvallisuusluokittelematon tietotekninen ympäristö, mukaan lukien sen tiloissa oleva tietotekninen ympäristö, **operatiivinen teknologiaverkosto,** pilvipalveluympäristöissä olevat tai kolmansien osapuolten ylläpitämät ulkoistetut resurssit ja palvelut, mobiililaitteet, yritysverkot, internetiin liittämättömät liiketoiminnan verkot ja kaikki tietotekniseen ympäristöön liitetyt laitteet. **Kehyksen on perustuttava kaikki vaaratekijät huomioon ottavaan toimintatapaan ja 6 artiklan mukaiseen kehitystason arviointiin, joka kattaa kaikki asiaankuuluvat tekniset, operatiiviset ja organisatoriset riskit, jotka voisivat vaikuttaa kyseisen unionin toimijan kyberturvallisuuteen** [...].

2 a. **Kehyksessä on vahvistettava kyberturvallisuuspolitiikat, mukaan lukien verkko- ja tietojärjestelmien turvallisuutta koskevat tavoitteet ja painopisteet, sekä toimintatavat ja menettelyt, joilla arvioidaan toteutettujen kyberturvallisuusriskien hallintatoimenpiteiden tehokkuutta ja määritellään henkilöstön jäsenten tehtävät ja vastuut**.

2 b. Kehystä on tarkasteltava uudelleen säännöllisesti ja vähintään kerran kolmessa vuodessa unionin toimijan muuttuvien riskien, resurssien ja kehitystason perusteella.

3. Unionin kunkin [...] **toimijan** ylin johto valvoo, että sen organisaatiossa noudatetaan kyberturvallisuusriskien hallintaan ja valvontaan liittyviä velvoitteita, sanotun kuitenkaan rajoittamatta muiden hallintotasojen muodollisten vastuiden soveltamista vaatimusten noudattamisen ja riskinhallinnan osalta niiden omilla vastuualueilla.

3 a. **Kunkin unionin toimijan ylin johto voi tarvittaessa siirtää kyseisen toimijan muille johtaville virkamiehille tämän asetuksen mukaisen erityisvelvoitteen, sanotun kuitenkaan rajoittamatta toimijan vastuuta tämän asetuksen täytäntöönpanosta. Ylimmän johdon voidaan katsoa olevan vastuussa siitä, että toimija ei noudata tämän asetuksen mukaisia velvoitteita, riippumatta siitä, siirretäänkö erityisvelvoite.**

3 b. Kunkin unionin toimijan ylimmän johdon on varmistettava, että unionin toimijat hyväksyvät riskianalyysinsä mukaisesti kyberturvallisuusriskien hallintatoimenpiteitä sisältävän kyberturvallisuussuunnitelman, jotta kehys pannaan täytäntöön tämän asetuksen mukaisesti.

[...]

5. Unionin kukin [...] **toimija** nimittää paikallisen kyberturvallisuusvastaavan tai vastaavan toimenhaltijan, joka toimii keskitettynä yhteyspisteenä kyberturvallisuuden kaikissa näkökohdissa.

Paikallisen kyberturvallisuusvastaavan on helpotettava tämän asetuksen täytäntöönpanoa ja raportoitava 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, sanotun kuitenkaan rajoittamatta paikallisen kyberturvallisuusvastaavan toimimista kunkin unionin toimijan keskitettynä yhteyspisteenä. IICB päättää, onko tämän palvelun tarjoaminen osa CERT-EU:n peruspalveluja, ottaen huomioon asianomaisen unionin toimijan henkilöstö- ja rahoitusresurssit. Kunkin unionin toimijan on ilmoitettava nimetyt paikalliset kyberturvallisuusvastaavat ja heitä koskevat myöhemmin tehtävät muutokset CERT-EU:lle ilman aiheetonta viivytystä. CERT-EU ylläpitää säännöllisesti päivitettävää luetteloa nimetyistä paikallisista kyberturvallisuusvastaavista.

6. Unionin kunkin toimijan henkilöstösääntöjen[12] 29 artiklan 2 kohdassa tarkoitetut johtavat virkamiehet tai muut vastaavantasoiset virkamiehet osallistuvat säännöllisesti erityiskoulutukseen riittävien tietojen ja taitojen hankkimiseksi, jotta he voivat ymmärtää ja arvioida kyberturvallisuusriskejä ja -hallintakäytäntöjä sekä niiden vaikutusta organisaation toimintoihin.

12 Neuvoston asetus N:o 259/68, annettu 29 päivänä helmikuuta 1968, Euroopan yhteisöjen virkamiehiin sovellettavien henkilöstösääntöjen ja näiden yhteisöjen muuta henkilöstöä koskevien palvelussuhteen ehtojen vahvistamisesta, EYVL L 56, 4.3.1968.

7. Unionin kullakin toimijalla on oltava käytössä tehokkaat mekanismit sen varmistamiseksi, että riittävä prosenttiosuus tietotekniikkamenoista käytetään kyberturvallisuuteen. Kehys on otettava asianmukaisesti huomioon tätä prosenttiosuutta määriteltäessä.

5 artikla

Kyberturvallisuusriskien hallintatoimenpiteet [...]

1. [...] **Kukin unionin toimija varmistaa** ylimmän johtonsa [...] **valvonnassa, että 4 artiklan 1 kohdassa tarkoitetun kehyksen mukaisesti tunnistettujen riskien hallintaa varten ja poikkeamien vaikutusten ehkäisemiseksi tai minimoimiseksi toteutetaan asianmukaiset ja oikeasuhteiset tekniset, operatiiviset ja organisatoriset toimet. Näillä toimenpiteillä on varmistettava verkko- ja tietojärjestelmien turvallisuuden taso, joka on oikeassa suhteessa aiheutuneisiin riskeihin, ottaen huomioon uusin kehitys ja tapauksen mukaan asiaan liittyvät eurooppalaiset ja kansainväliset standardit sekä täytäntöönpanokustannukset. Näiden toimenpiteiden oikeasuhteisuutta arvioitaessa on otettava asianmukaisesti huomioon toimijan altistuminen riskeille, sen koko, poikkeamien toteutumisen todennäköisyys ja niiden vakavuus, mukaan lukien poikkeamien yhteiskunnalliset ja taloudelliset vaikutukset.**

[...]

3. Unionin toimijat ottavat IICB:n ohjeasiakirjojen ja suositusten mukaisesti kyberturvallisuussuunnitelmiinsa sisältyvien kyberturvallisuusriskien hallintatoimenpiteissä huomioon ainakin seuraavat erityiset osa-alueet:

a) kyberturvallisuuspolitiikka 4 artiklassa ja 5 artiklan 4 kohdassa tarkoitettujen tavoitteiden ja painopisteiden saavuttamiseksi tarvittavien välineiden ja toimenpiteiden määrittelyn osalta;

b) riskianalyysejä ja tietojärjestelmien turvallisuutta koskevat toimintaperiaatteet;

c) kyberturvallisuuden organisointi, mukaan lukien tehtävien ja vastuualueiden määrittely;

d) resurssien hallinta, mukaan lukien tietoteknisten resurssien inventointi ja tietoverkkojen kartoitus;

e) henkilöstöturvallisuus ja kulunvalvonta;

f) operatiivinen turvallisuus;

g) tietoliikenneturvallisuus;

h) järjestelmien hankinta, kehittäminen ja ylläpito, mukaan lukien haavoittuvuuksien käsittely ja julkistaminen;

i) toimitusketjun turvallisuus, mukaan lukien kunkin unionin toimijan ja sen suorien toimittajien tai palveluntarjoajien välisiä suhteita koskevat turvallisuusnäkökohdat. Unionin toimijoiden on otettava huomioon kullekin suoralle toimittajalle ja palveluntarjoajalle ominaiset haavoittuvuudet sekä tavarantoimittajiensa ja palveluntarjoajiensa tuotteiden ja kyberturvallisuuskäytäntöjen yleinen laatu, mukaan lukien niiden tuotekehityksen suojausmenettelyt;

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

k) toiminnan jatkuvuuden hallinta, kuten varmuuskopioiden hallinta ja toiminnan palauttaminen, ja kriisinhallinta; sekä

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

4. Unionin toimijat ottavat IICB:n ohjeasiakirjojen ja suositusten mukaisesti kyberturvallisuussuunnitelmiinsa sisältyvien kyberturvallisuusriskien hallintatoimenpiteissä huomioon ainakin seuraavat erityiset kyberturvallisuusriskien hallintatoimenpiteet:

a) tavoitteet ja painopisteet, jotka koskevat erityisesti direktiivin [ehdotus NIS 2 -direktiiviksi] 4 artiklan 19 kohdassa tarkoitettua pilvipalvelujen käyttöä sekä etätyön mahdollistamiseksi toteutettuja teknisiä järjestelyjä;

b) konkreettiset toimet nollaluottamusperiaatteen tulevaa käyttöä varten, mukaan lukien tietoturvamalli sekä koordinoitu kyberturvallisuus- ja järjestelmänhallintastrategia, jonka pohjana on se, että uhkia esiintyy sekä perinteisten verkkorajojen sisä- että ulkopuolella;

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

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

e) julkisia hankintoja koskevien sääntöjen parantaminen yhteisen korkean kyberturvatason edistämiseksi

i) sellaisten sopimuksista johtuvien esteiden poistaminen, jotka rajoittavat tietotekniikan palveluntarjoajien 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 on asianmukainen poikkeamiin reagoiminen ja seuranta;

f) salaustekniikoiden ja erityisesti päästä päähän -salauksen käyttö;

g) organisaation sisäiset suojatut viestintäjärjestelmät.

6 artikla

Kehitystason arvioinnit

1. Unionin kukin [...] **toimija** suorittaa **tarvittaessa erikoistuneen kolmannen osapuolen avustamana** vähintään kerran kolmessa vuodessa [...] kehitystason arvioinnin ja sisällyttää siihen kaikki 4 artiklassa tarkoitetut tietoteknisen ympäristönsä osatekijät ottaen huomioon 13 artiklan nojalla hyväksytyt asiaan liittyvät ohjeasiakirjat ja suositukset.

2. IICB hyväksyy CERT-EU:n suosituksesta ja Euroopan unionin kyberturvallisuusvirastoa (ENISA) kuultuaan neljän kuukauden kuluessa tämän asetuksen voimaantulosta kehitystason arviointien tekemistä koskevat menettelyohjeet.

3. Sen jälkeen, kun kehitystason arviointi [...] **on suoritettu, unionin toimija toimittaa sen IICB:lle. Ensimmäinen kehitystason arviointi on tehtävä viimeistään [12 kuukauden kuluttua tämän asetuksen voimaantulosta].**

7 artikla

Kyberturvallisuussuunnitelmat

1. Kehitystason arvioinnista saatujen johtopäätösten perusteella ja ottaen huomioon 4 artiklan nojalla tunnistetut resurssit ja riskit unionin kukin [...] **toimija** hyväksyy kyberturvallisuussuunnitelman ilman aiheetonta viivytystä sen jälkeen, kun [...] **kehys on laadittu,** [...] **kyberturvallisuusriskien hallintatoimenpiteet on hyväksytty ja kehitystason arviointi on suoritettu mutta kuitenkin viimeistään 21 kuukauden kuluttua tämän asetuksen voimaantulosta**. [...] **Kyberturvallisuussuunnitelman** tavoitteena on nostaa [...] **asianomaisen unionin** toimijan yleistä kyberturvallisuutta ja edistää siten yhteisen korkean kyberturvatason [...] parantamista unionin kaikkien [...] **toimijoiden** keskuudessa. [...] **Kyberturvallisuussuunnitelman** on sisällettävä vähintään **5 artiklan mukaiset kyberturvallisuusriskien hallintatoimenpiteet** [...]. [..] **Kyberturvallisuussuunnitelmaa** on tarkistettava vähintään [...] **kerran kahdessa vuodessa, kunkin** 6 artiklan mukaisesti [...] **tehdyn kehitystason arvioinnin** perusteella **tai jokaisen 4 artiklan mukaisesti suoritetun kehyksen uudelleentarkastelun perusteella.**

2. [...]

3. Kyberturvallisuussuunnitelmassa on otettava huomioon [...] **13 artiklan mukaisesti annetut** soveltuvat ohjeasiakirjat ja suositukset.

4. **Sen jälkeen, kun kyberturvallisuussuunnitelma on laadittu, unionin toimija toimittaa sen IICB:lle**.

7 a artikla

Vertaisarviointi

1. IICB hyväksyy CERT-EU:n suosituksesta ja ENISAa kuultuaan viimeistään ... [24 kuukauden kuluttua tämän asetuksen voimaantulosta] ja direktiivin [ehdotus NIS 2 -direktiiviksi] 16 artiklan mukaisia, unionin toimijoiden tarpeisiin tarvittaessa mukautettuja vertaisarviointi- ja itsearviointimenetelmiä noudattaen, vertaisarvioinnin menetelmät ja organisatoriset näkökohdat, jotta voidaan oppia yhteisistä kokemuksista, vahvistaa keskinäistä luottamusta, saavuttaa yhteinen korkea kyberturvataso sekä parantaa unionin toimijoiden kyberturvallisuusvalmiuksia ja -politiikkoja, joita tämän asetuksen täytäntöönpano edellyttää. Vertaisarviointiin osallistuminen on vapaaehtoista. Jäsenvaltioiden edustajat voivat osallistua vertaisarviointiin tarkkailijoina. Vertaisarviointeja suorittavat kyberturvallisuusasiantuntijat, joiden nimeäjänä on vähintään kaksi sellaista unionin toimijaa, jotka eivät ole arvioinnin kohteena, ja arvioinneissa on käsiteltävä vähintään yhtä seuraavista osa-alueista:

i) edellä 5 artiklassa ja jäljempänä 20 artiklassa tarkoitettujen kyberturvallisuusriskien hallintatoimenpiteiden ja raportointivelvoitteiden täytäntöönpano;

ii) valmiustaso, mukaan lukien käytettävissä olevat taloudelliset, tekniset ja henkilöresurssit;

iii) jäljempänä 19 artiklassa tarkoitetun tiedonvaihtojärjestelyn toteuttaminen;

iv) monialaiset erityiskysymykset.

2. Unionin toimijat voivat yksilöidä arvioitavaksi 1 kohdan iv alakohdassa mainittuja erityiskysymyksiä. Arvioinnin kohteet, mukaan lukien yksilöidyt kysymykset, on ilmoitettava osallistuville unionin toimijoille ennen vertaisarvioinnin aloittamista.

3. Unionin toimijat voivat ennen vertaisarviointia tehdä arvioitavista osa-alueista itsearvioinnin ja toimittaa sen nimetyille asiantuntijoille.

4. Vertaisarviointeihin sisältyy fyysisiä tai virtuaalisia kohdeselvityksiä sekä yleistä tiedonvaihtoa. Hyvän yhteistyön periaatteen mukaisesti vertaisarvioinnin kohteena olevien unionin toimijoiden on toimitettava nimetyille asiantuntijoille arviointia varten tarvittavat tiedot, sanotun kuitenkaan rajoittamatta arkaluonteisten tai turvallisuusluokiteltujen tietojen suojaamista koskevan kansallisen tai unionin lainsäädännön soveltamista. Vertaisarviointiprosessissa saatuja tietoja saa käyttää ainoastaan tähän tarkoitukseen. Vertaisarviointiin osallistuvat asiantuntijat eivät saa paljastaa arvioinnin aikana saatuja arkaluonteisia tai turvallisuusluokiteltuja tietoja ulkopuolisille.

5. Kun vertaisarviointi on tehty, samoista unionin toimijan arvioiduista osa-alueista ei tehdä uutta vertaisarviointia, ennen kuin vertaisarvioinnin päättymisestä on kulunut kaksi vuotta, ellei unionin toimija toisin pyydä tai sovi IICB:n ehdotuksesta.

6. Unionin toimijoiden on varmistettava, että nimettyihin asiantuntijoihin liittyvät mahdolliset eturistiriitariskit ilmoitetaan muille unionin toimijoille ja IICB:lle ennen vertaisarvioinnin aloittamista. Vertaisarvioinnin kohteena olevat unionin toimijat voivat vastustaa tiettyjen asiantuntijoiden nimeämistä asianmukaisesti perustelluista syistä, jotka ilmoitetaan asiantuntijat nimeäville unionin toimijoille.

7. Vertaisarviointeihin osallistuvien asiantuntijoiden on laadittava raportit arviointien tuloksista ja päätelmistä. Unionin toimijoiden on mahdollista esittää omista raporttiluonnoksistaan huomautuksia, jotka liitetään raporttiin. Raportteihin on sisällyttävä suosituksia, joiden avulla vertaisarvioinnissa arvioituja osa-alueita voidaan parantaa. Raportit on tarvittaessa esitettävä IICB:lle ja CSIRT-verkostolle. Arvioitavat unionin toimijat voivat päättää asettaa raporttinsa tai sen muokatun version julkisesti saataville.

8 artikla

Täytäntöönpano

1. [...]

2. Jäljempänä olevan 13 artiklan mukaisesti annetuilla ohjeasiakirjoilla ja suosituksilla tuetaan tässä luvussa vahvistettujen säännösten täytäntöönpanoa.

3. Unionin toimijat raportoivat tämän luvun erityisistä näkökohdista IICB:n pyynnöstä.

III luku

TOIMIELINTEN VÄLINEN KYBERTURVALLISUUSLAUTAKUNTA

9 artikla

Toimielinten välinen kyberturvallisuuslautakunta

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

2. IICB:n tehtävänä on

   a) seurata tämän asetuksen täytäntöönpanoa unionin [...] **toimijoiden toiminnassa**;

   b) valvoa sitä, miten CERT-EU panee täytäntöön yleiset painopisteet ja tavoitteet, ja antaa CERT-EU:lle strategista ohjausta.

3. IICB:hen kuuluvat

   a) yksi edustaja, jonka kukin seuraavista nimeää:

      i) Euroopan parlamentti;

      ii) Eurooppa-neuvosto;

      iii) Euroopan unionin neuvosto;

      iv) Euroopan komissio;

      v) Euroopan unionin tuomioistuin;

      vi) Euroopan keskuspankki;

vii) **Euroopan tilintarkastustuomioistuin;**

viii) **Euroopan ulkosuhdehallinto;**

ix) **Euroopan sosiaali- ja talouskomitea;**

x) **Euroopan alueiden komitea;**

xi) **Euroopan investointipankki;**

xii) **Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskus; sekä**

xiii) **Euroopan unionin kyberturvallisuusvirasto;**

b) **kolme edustajaa, jotka unionin virastojen verkoston (EUAN) nimittää** [...] tieto- ja viestintätekniikkaa käsittelevän neuvoa-antavan komiteansa ehdotuksesta ja jotka edustavat omaa tietoteknistä ympäristöään käyttävien virastojen ja elinten etuja. [...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

3 a. Jäseniä voi avustaa varajäsen. Puheenjohtaja voi kutsua muita edellä lueteltujen [...] **toimijoiden** tai muiden unionin [...] **toimijoiden** edustajia osallistumaan IICB:n kokouksiin ilman äänioikeutta.

4. IICB vahvistaa sisäisen työjärjestyksensä.

5. IICB nimeää sisäisen työjärjestyksensä mukaisesti jäsentensä keskuudesta puheenjohtajan [...] **kahden** vuoden ajaksi. Hänen sijaisestaan tulee IICB:n täysjäsen samaksi ajaksi.

6. IICB kokoontuu **vähintään kolme kertaa vuodessa** puheenjohtajan aloitteesta, CERT-EU:n pyynnöstä tai minkä tahansa jäsenensä pyynnöstä.

7. Kullakin IICB:n jäsenellä on yksi ääni. IICB tekee päätöksensä yksinkertaisella enemmistöllä, ellei tässä asetuksessa toisin säädetä. Puheenjohtaja ei äänestä, elleivät äänet mene tasan, jolloin hän voi antaa ratkaisevan äänen.

8. IICB voi toimia IICB:n sisäisen työjärjestyksen mukaisesti käynnistettyä yksinkertaistettua kirjallista menettelyä noudattaen. Kyseisessä menettelyssä asiaan liittyvää päätöstä pidetään hyväksyttynä puheenjohtajan asettaman määräajan päätyttyä, jollei joku jäsen esitä vastalausetta.

9. CERT-EU:n johtaja**, verkko- ja tietoturva-alan yhteistyöryhmän puheenjohtaja, EU-CyCLONen puheenjohtaja ja CSIRT-verkoston puheenjohtaja tai heidän** [...] sijaisensa [...] **voivat osallistua** IICB:n kokouksiin **tarkkailijoina**, ellei IICB toisin päätä.

10. **ENISA** [...] huolehtii IICB:n sihteeristötehtävistä**, ja sihteeristö on vastuussa IICB:n puheenjohtajalle**.

11. Edustajat, jotka unionin virastojen verkosto on nimittänyt tieto- ja viestintätekniikkaa käsittelevän neuvoa-antavan komitean ehdotuksesta, välittävät IICB:n päätökset [...] **unionin virastojen verkoston jäsenille**. Kaikilla unionin virastoilla ja elimillä on oikeus ottaa edustajien tai IICB:n puheenjohtajan kanssa esille mikä tahansa asia, joka niiden mielestä olisi saatettava IICB:n tietoon.

12. [...]

13. IICB voi **perustaa** [...] toimeenpanevan komitean avustamaan IICB:tä sen työssä ja siirtää komitealle osan tehtävistään ja valtuuksistaan**, erityisesti 10 artiklan c ja e kohdassa vahvistetuista tehtävistä ja valtuuksista**. IICB vahvistaa toimeenpanevan komitean työjärjestyksen, mukaan lukien sen tehtävät ja valtuudet sekä sen jäsenten toimikaudet.

14. IICB toimittaa neuvostolle 12 kuukauden välein kertomuksen, jossa esitetään yksityiskohtaisesti tämän asetuksen täytäntöönpanon edistyminen ja täsmennetään erityisesti, miten laajaa CERT-EU:n ja kunkin jäsenvaltion kansallisten vastapuolten yhteistyö on ollut. Kertomus sisällytetään asiaankuuluvan ajanjakson osalta kahden vuoden välein julkaistavaan kertomukseen kyberturvallisuuden tilasta unionissa direktiivin [ehdotus NIS 2 -direktiiviksi] 15 artiklan mukaisesti.

10 artikla

IICB:n tehtävät

Vastuitaan hoitaessaan IICB:n tehtävänä on erityisesti

(a) [...] **seurata ja valvoa tehokkaasti** tämän asetuksen [...] **soveltamista ja tukea** unionin [...] **toimijoita, kun ne vahvistavat kyberturvallisuuttaan**; **tätä varten IICB voi pyytää tapauskohtaisia kertomuksia CERT-EU:lta ja unionin toimijoilta;**

a a) **hyväksyä strategisen keskustelun pohjalta monivuotinen strategia unionin toimijoiden kyberturvallisuuden tason nostamiseksi ja arvioida sitä säännöllisesti vähintään kerran viidessä vuodessa sekä muuttaa sitä tarvittaessa;**

b) hyväksyä CERT-EU:n johtajan ehdotuksesta CERT-EU:n vuotuinen työohjelma ja seurata sen toteuttamista;

c) hyväksyä CERT-EU:n johtajan ehdotuksesta CERT-EU:n palvelujen luettelo **ja sen mahdolliset myöhemmät päivitykset**;

d) hyväksyä CERT-EU:n johtajan toimittaman ehdotuksen pohjalta vuotuinen rahoitussuunnitelma CERT-EU:n toimintaan liittyvistä tuloista ja menoista, henkilöstö mukaan luettuna;

e) hyväksyä CERT-EU:n johtajan ehdotuksen pohjalta palvelutasosopimusten yksityiskohdat;

f) tarkastaa ja hyväksyä CERT-EU:n johtajan laatima vuosikertomus, joka kattaa CERT-EU:n toiminnan ja varainhoidon;

g) hyväksyä ja seurata CERT-EU:ta koskevia keskeisiä tulosindikaattoreita, jotka on määritelty CERT-EU:n johtajan ehdotuksen pohjalta;

h) hyväksyä CERT-EU:n ja muiden toimijoiden välillä 17 artiklan nojalla tehdyt yhteistyöjärjestelyt, [...] **palvelutasosopimukset tai muut sopimukset**;

i) perustaa [...] teknisiä neuvoa-antavia ryhmiä avustamaan IICB:n työskentelyä, hyväksyä niiden tehtävänmääritykset ja nimetä niiden puheenjohtajat;

j) **hyväksyä ohjeasiakirjoja ja suosituksia CERT-EU:n ehdotusten perusteella 13 artiklan mukaisesti ja ohjeistaa CERT-EU:ta antamaan tai peruuttamaan toimintakehotuksen tai ehdotuksen ohjeasiakirjoiksi tai suosituksiksi taikka muuttamaan sellaista;**

k) vastaanottaa ja arvioida unionin toimijoiden tämän asetuksen nojalla toimittamia asiakirjoja ja raportteja;

l) tukea sellaisen epävirallisen ryhmän perustamista, joka kokoaa yhteen kaikkien toimijoiden paikalliset kyberturvallisuusvastaavat, ja helpottaa siten tämän asetuksen täytäntöönpanoon liittyvien parhaiden käytäntöjen ja tietojen vaihtoa;

m) laatia kyberturvallisuuskriisien hallintasuunnitelma, jolla tuetaan unionin toimijoihin vaikuttavien merkittävien poikkeamien koordinoitua hallintaa operatiivisella tasolla ja edistetään erityisesti merkittävien poikkeamien vaikutuksia ja vakavuutta sekä mahdollisia lieventämistapoja koskevien asiaankuuluvien tietojen säännöllistä vaihtoa.

11 artikla

Asetuksen noudattaminen

1. IICB seuraa **9 artiklan 2 kohdan ja 10 artiklan mukaisesti tehokkaasti** sitä, miten unionin [...] **toimijat** panevat tämän asetuksen sekä hyväksytyt ohjeasiakirjat, suositukset ja toimintakehotukset täytäntöön. **Tätä varten IICB voi pyytää tietoja tai asiakirjoja, joita tarvitaan sen arvioimiseksi, soveltavatko unionin toimijat asetuksen säännöksiä asianmukaisesti. Kun on kyse tämän artiklan mukaisten säännösten noudattamista koskevien toimenpiteiden hyväksymisestä, asianomaisella unionin toimijalla ei ole äänioikeutta.**

2. Jos IICB katsoo, että unionin [...] **toimijat** eivät ole soveltaneet tai panneet täytäntöön tehokkaasti tätä asetusta tai tämän asetuksen mukaisesti annettuja ohjeasiakirjoja, suosituksia ja toimintakehotuksia, se voi, sanotun rajoittamatta asiaan liittyvän unionin [...] **toimijan** sisäisten menettelyjen soveltamista **ja annettuaan asianomaiselle toimijalle tai henkilölle mahdollisuuden esittää näkemyksensä**

a) antaa varoituksen **havaittujen puutteiden korjaamiseksi tietyssä määräajassa, mukaan lukien suositukset unionin toimijoiden tämän asetuksen perusteella hyväksymien kyberturvallisuusasiakirjojen muuttamiseksi**; jos se on tarpeen huomattavan kyberturvallisuusriskin vuoksi, varoituksen kohderyhmä on rajattava asianmukaisesti;

a a) antaa perustellun ilmoituksen unionin toimijalle, jos aiemmin annetussa varoituksessa yksilöityihin puutteisiin ei ole puututtu riittävästi tietyssä määräajassa, ja antaa tämän ilmoituksen virallisesti tiedoksi neuvostolle, Euroopan parlamentille ja komissiolle;

b) **esittää erityisesti** [...]

i. suosituksen, että unionin toimijalle tehdään tarkastus;

ii. pyynnön siitä, että kolmas osapuoli suorittaa tarkastuksen.

c) pyytää unionin toimijaa saattamaan kyberturvallisuusriskien hallinta ja valvonta tämän asetuksen säännösten mukaisiksi, tarvittaessa määrätyllä tavalla ja määrätyn ajan kuluessa.

d) antaa kaikille jäsenvaltioille ja unionin toimijoille ohjeen, joissa suositetaan tietylle unionin toimijalle toimitettavien tietovirtojen tilapäistä keskeyttämistä.

3. Jos IICB on hyväksynyt 2 kohdan a–d alakohdan mukaisia toimenpiteitä, asianomaisen unionin toimijan on annettava yksityiskohtainen selvitys toimenpiteistä ja toimista, jotka on toteutettu IICB:n yksilöimien väitettyjen puutteiden korjaamiseksi. Unionin toimijan on toimitettava selvitys IICB:n kanssa sovittavan kohtuullisen ajan kuluessa.

4. **Jos IICB katsoo, että unionin toimija rikkoo jatkuvasti tämän asetuksen säännöksiä unionin virkamiehen tai muun henkilöstön jäsenen toimien tai laiminlyönnin seurauksena, myös ylimmällä johtotasolla, IICB pyytää asianomaista toimijaa toteuttamaan asianmukaiset toimet, myös kurinpitotoimet, erityisesti Euroopan unionin henkilöstösäännöissä ja muuhun henkilöstöön sovellettavissa palvelussuhteen ehdoissa vahvistettujen sääntöjen mukaisesti. Tätä varten IICB välittää tarvittavat tiedot asianomaiselle toimijalle.**

IV luku
CERT-EU

12 artikla

CERT-EU:n tarkoitus ja tehtävät

1. [...] **CERT-EU:n tarkoituksena on** parantaa kaikkien unionin [...] **toimijoiden** turvallisuusluokittelemattoman tietoteknisen ympäristön turvallisuutta tarjoamalla kyberturvallisuutta koskevaa neuvontaa, auttamalla ehkäisemään, havaitsemaan ja lieventämään poikkeamia ja reagoimaan niihin sekä toimimalla kyberturvallisuutta koskevan tietojenvaihdon ja poikkeamiin reagoimisen koordinointikeskuksena.

1 a. CERT-EU kerää, hallinnoi, analysoi ja jakaa unionin toimijoiden kanssa tietoja turvallisuusluokittelemattomiin tieto- ja viestintäteknisiin infrastruktuureihin kohdistuvista uhkista, niiden haavoittuvuuksista ja niihin liittyneistä poikkeamista. Se koordinoi poikkeamien käsittelyä toimielinten välisellä ja unionin toimijoiden tasolla muun muassa toimittamalla erikoistunutta operatiivista apua tai koordinoimalla sitä.

2. CERT-EU hoitaa seuraavia tehtäviä unionin [...] **toimijoille**:

a) niiden tukeminen tämän asetuksen täytäntöönpanossa ja tämän asetuksen soveltamisen koordinoinnin edistäminen 13 artiklan 1 kohdassa lueteltujen [...] **säännösten** tai IICB:n pyytämien tapauskohtaisten kertomusten avulla;

b) [...] **CSIRT-vakiopalvelujen tarjoaminen kaikille unionin toimijoille** palvelujen luettelossa kuvaillulla kyberturvallisuuspalvelujen paketilla (perustason palvelut);

c) vertais- ja kumppaniverkoston ylläpitäminen 16 ja 17 artiklassa tarkoitettujen palvelujen tukemiseksi;

d) mahdollisten tämän asetuksen täytäntöönpanoon sekä ohjeasiakirjojen, suositusten ja toimintakehotusten täytäntöönpanoon liittyvien ongelmien tuominen IICB:n tietoon;

e) [...] EU:n kyberturvallisuuden tilannekuvan parantaminen **1 a kohdassa tarkoitettujen tietojen pohjalta ja tiiviissä yhteistyössä ENISAn kanssa. Nämä tiedot jaetaan IICB:n sekä CSIRT-verkoston ja EU INTCENin kanssa;**

f) toimiminen direktiivin [ehdotus NIS 2 -direktiiviksi] 6 artiklassa tarkoitettua unionin elinten nimettyä koordinaattoria vastaavassa tehtävässä.

[...]

[...]

[...]

[...]

[...]

4. CERT-EU tekee **toimivaltakehyksen puitteissa** jäsenneltyä yhteistyötä [...] **ENISAn** kanssa kyberuhkien valmiuksien kehittämisessä, operatiivisessa yhteistyössä ja kyberuhkista tehtävissä pitkän aikavälin strategisissa analyyseissa Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/881 mukaisesti.

5. CERT-EU voi tarjota seuraavia palveluja, joita ei kuvata sen palvelujen luettelossa (veloitettavat palvelut):

   a) muut kuin 2 kohdassa tarkoitetut palvelut, joilla tuetaan unionin [...] **toimijoiden** tietoteknisen ympäristön kyberturvallisuutta, palvelutasosopimusten perusteella ja saatavilla olevien resurssien mukaan;

   b) palvelut, joilla tuetaan muita kuin [...] **unionin toimijoiden** tietoteknisen ympäristön suojaamiseksi toteutettavia kyberturvallisuustoimia tai -hankkeita, kirjallisten sopimusten perusteella ja IICB:n etukäteisellä hyväksynnällä;

   c) palvelut, joilla tuetaan sellaisten muiden kuin unionin [...] **toimijoiden** organisaatioiden, jotka tekevät tiivistä yhteistyötä unionin [...] **toimijoiden** kanssa esimerkiksi koska niille on annettu unionin lainsäädännön mukaisia tehtäviä tai vastuita, tietoteknisen ympäristön turvallisuutta, kirjallisten sopimusten perusteella ja IICB:n etukäteisellä hyväksynnällä.

6. CERT-EU voi tarvittaessa järjestää kyberturvallisuusharjoituksia**, osallistua niihin itse** tai suositella osallistumista jo käytössä oleviin harjoituksiin tiiviissä yhteistyössä [...] **ENISAn** kanssa unionin [...] **toimijoiden** kyberturvatason testaamiseksi.

7. CERT-EU voi avustaa unionin [...] **toimijoita** turvallisuusluokitelluissa tietoteknisissä ympäristöissä tapahtuvissa poikkeamissa, jos unionin asianomainen [...] **toimija** sitä nimenomaisesti pyytää **omien menetelmiensä mukaisesti. Tässä tapauksessa ei sovelleta tämän asetuksen 19–21 artiklan säännöksiä. CERT-EU:n tämän kohdan nojalla antama apu ei rajoita arkaluonteisten tai turvallisuusluokiteltujen tietojen suojaamista koskevien jäsenvaltioiden tai unionin sääntöjen soveltamista.**

8. CERT-EU ilmoittaa unionin toimijoille poikkeamien käsittelymenettelyistään ja -prosesseistaan.

9. CERT-EU voi seurata unionin toimijoiden verkkoliikennettä niiden suostumuksella.

10. Jos unionin toimijoiden poliittiset osastot sitä ovat nimenomaisesti pyytäneet, CERT-EU voi antaa asiaankuuluvia poliittisia kysymyksiä koskevaa teknistä neuvontaa tai lausuntoja.

11. CERT-EU tukee yhteistyössä Euroopan tietosuojavaltuutetun kanssa asianomaisia unionin toimijoita niiden käsitellessä henkilötietojen tietoturvaloukkauksiin johtaneita poikkeamia.

13 artikla

Ohjeasiakirjat, suositukset ja toimintakehotukset

1. CERT-EU tukee tämän asetuksen täytäntöönpanoa antamalla

   a) toimintakehotuksia, joissa kuvaillaan kiireellisiä turvatoimenpiteitä, jotka unionin [...] toimijoita kehotetaan toteuttamaan tietyssä määräajassa. Asianomaisen unionin toimijan on ilman aiheetonta viivytystä toimintakehotuksen vastaanottamisen jälkeen ilmoitettava CERT-EU:lle, miten kyseisiä toimenpiteitä on sovellettu;

   b) IICB:lle ehdotuksia ohjeasiakirjoiksi, jotka on suunnattu kaikille unionin [...] **toimijoille** tai tietylle unionin toimijoiden alaryhmälle;

   c) IICB:lle ehdotuksia suosituksiksi, jotka on suunnattu yksittäisille unionin [...] **toimijoille**.

2. Ohjeasiakirjat ja suositukset voivat sisältää

   a) yksityiskohtaisia sääntöjä kyberturvallisuusriskien hallinnasta ja [...] **kyberturvallisuusriskien hallintatoimenpiteistä** tai niiden parantamisesta;

   b) yksityiskohtaisia sääntöjä kehitystason arvioinneista ja kyberturvallisuussuunnitelmista; sekä

   c) tarvittaessa yhteisen teknologian, arkkitehtuurin ja niihin liittyvien parhaiden käytäntöjen käytöstä, jotta voidaan saavuttaa yhteentoimivuus ja [...] yhteiset standardit**, mukaan lukien toimitusketjun turvallisuutta koskeva koordinoitu toimintatapa**.

[...]

[...]

14 artikla

CERT-EU:n johtaja

1. Komissio nimittää CERT-EU:n johtajan saatuaan IICB:n hyväksynnän IICB:n jäsenten kahden kolmasosan enemmistöllä. IICB:tä kuullaan menettelyn kaikissa CERT-EU:n johtajan nimittämistä edeltävissä vaiheissa, erityisesti tähän tehtävään liittyvien avointa virkaa koskevien ilmoitusten laatimisen, hakemusten tarkastelun ja kilpailun valintalautakunnan nimittämisen yhteydessä.

2. CERT-EU:n johtaja vastaa CERT-EU:n moitteettomasta toiminnasta ja toimii valtuuksiensa puitteissa IICB:n alaisuudessa. Hän on vastuussa IICB:n asettamien strategisten suuntaviivojen, ohjeiden, tavoitteiden ja painopisteiden täytäntöönpanosta sekä CERT-EU:n hallinnoinnista, mukaan lukien sen taloudelliset ja henkilöresurssit. Hän raportoi säännöllisesti IICB:n puheenjohtajalle.

3. CERT-EU:n johtaja avustaa toimivaltaista valtuutettua tulojen ja menojen hyväksyjää varainhoitoasetuksen 74 artiklan 9 kohdan mukaisen, taloutta ja hallintoa koskevia tietoja, kuten tarkastustuloksia, sisältävän vuotuisen toimintakertomuksen laatimisessa ja raportoi tälle säännöllisesti niiden toimenpiteiden täytäntöönpanosta, joiden osalta hän on saanut edelleenvaltuutuksen.

4. CERT-EU:n johtaja laatii vuosittain CERT-EU:n toimintaan liittyviä hallintotuloja ja -menoja koskevan rahoitussuunnitelman, ehdotuksen vuotuiseksi työohjelmaksi, ehdotuksen CERT-EU:n palveluluetteloksi ja sen tarkistetun version, ehdotuksen palvelutasosopimuksia koskeviksi yksityiskohtaisiksi säännöiksi ja ehdotuksen CERT-EU:n keskeisiksi suorituskykyindikaattoreiksi, jotka IICB:n on hyväksyttävä 10 artiklan mukaisesti.

Tarkistettaessa CERT-EU:n palveluluetteloa CERT-EU:n johtaja ottaa huomioon CERT-EU:lle osoitetut resurssit.

5. CERT-EU:n johtaja toimittaa [...] **vuosittain** kertomuksia IICB:lle [...] CERT-EU:n toiminnasta, rahoitussuunnitelmasta, tuloista, talousarvion toteuttamisesta, tehdyistä palvelutasosopimuksista ja kirjallisista sopimuksista, yhteistyöstä vastaavaa tehtävää hoitavien elinten ja kumppanien kanssa sekä henkilöstön virkamatkoista, mukaan lukien 10 artiklan [...] **a** kohdassa tarkoitetut kertomukset.

15 artikla

Rahoitus- ja henkilöstöasiat

[...]

1 a. CERT-EU perustetaan riippumattomaksi toimielinten väliseksi palveluntarjoajaksi kaikkia unionin toimijoita varten, mutta se integroidaan kuitenkin jonkin komission pääosaston hallintorakenteeseen, jotta se voi hyödyntää komission hallinnon, varainhoidon ja kirjanpidon tukirakenteita. Komissio ilmoittaa IICB:lle CERT-EU:n hallinnollisesta sijainnista ja sen mahdollisista muutoksista. Tätä toimintatapaa arvioidaan säännöllisesti, viimeistään ennen kunkin SEUT-sopimuksen 312 artiklan mukaisesti vahvistetun monivuotisen rahoituskehyksen päättymistä, jotta asianmukaiset toimet voidaan toteuttaa.

2. Hallinto- ja rahoitusmenettelyjä soveltaessaan CERT-EU:n johtaja toimii komission valvonnassa.

3. CERT-EU:n tehtävät ja toimet, mukaan lukien CERT-EU:n 12 artiklan 2, [...] 4 ja 6 kohdan ja 13 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 virat esitetään komission henkilöstötaulukon alaviitteessä.

4. Muut kuin 3 kohdassa tarkoitetut unionin [...] **toimijat** suorittavat CERT-EU:lle vuotuisen rahoitusosuuden CERT-EU:n kyseisen 3 kohdan nojalla tarjoamien palvelujen kattamiseen. Kukin rahoitusosuus perustuu IICB:n toimittamiin ohjeisiin, ja kukin toimija ja CERT-EU sopivat niistä palvelutasosopimuksissa. Rahoitusosuuksien on vastattava oikeudenmukaista ja oikeasuhteista osuutta suoritettujen palvelujen kokonaiskustannuksista. Ne osoitetaan 3 kohdassa tarkoitettuun erilliseen budjettikohtaan Euroopan parlamentin ja neuvoston asetuksen (EU, Euratom) 2018/1046[13] 21 artiklan 3 kohdan c alakohdassa tarkoitettuina käyttötarkoitukseensa sidottuina tuloina.

5. Edellä 12 artiklan 5 kohdassa tarkoitettujen tehtävien kustannukset peritään CERT-EU:n palvelut vastaanottavilta unionin [...] **toimijoilta**. Tulot kohdennetaan kustannuksia tukeviin budjettikohtiin.

[13] 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).

16 artikla

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

1. CERT-EU tekee **ilman aiheetonta viivytystä** yhteistyötä ja vaihtaa tietoja jäsenvaltioissa vastaavaa tehtävää hoitavien kansallisten elinten, **erityisesti** [...] **direktiivin [ehdotus NIS 2 -direktiiviksi] 9 artiklassa tarkoitettujen** CSIRT-yksiköiden **ja tarvittaessa toimivaltaisten kansallisten viranomaisten sekä** [...] direktiivin [ehdotus NIS 2 -direktiiviksi] 8 artiklassa tarkoitettujen keskitettyjen yhteyspisteiden, kanssa kyberuhkista, haavoittuvuuksista ja poikkeamista, mahdollisista vastatoimista ja kaikista asioista, jotka ovat merkityksellisiä unionin [...] **toimijoiden** tietoteknisten ympäristöjen suojaamisen parantamisen kannalta, myös direktiivin [ehdotus NIS 2 -direktiiviksi] 13 artiklassa tarkoitetun CSIRT-verkoston kautta.

1 a. CERT-EU ilmoittaa ilman aiheetonta viivytystä 1 kohdassa tarkoitetuille asiaankuuluville vastaavaa tehtävää hoitaville jäsenvaltioiden kansallisille elimille, kun se saa tietoonsa merkittäviä poikkeamia kyseisen jäsenvaltion alueella, paitsi jos CERT-EU:lla on tietoja siitä, että asianomainen unionin toimija on jo ilmoittanut tällaisesta poikkeamasta 20 artiklan 2 a kohdan mukaisesti.

2. CERT-EU [...] vaihtaa **ilman aiheetonta viivytystä** poikkeamakohtaisia tietoja jäsenvaltioissa vastaavaa tehtävää hoitavien kansallisten elinten kanssa, jotta voidaan helpottaa samankaltaisten kyberuhkien tai -poikkeamien havaitsemista **taikka edistää poikkeaman analysointia**, ilman **sen** unionin **toimijan** [...] suostumusta**, johon uhka tai poikkeama kohdistuu**. CERT-EU [...] **ei saa** vaihtaa sellaisia poikkeamakohtaisia tietoja, joista käy ilmi kyberturvallisuuspoikkeaman kohteen identiteetti, [...] **paitsi jos**

a) asianomainen unionin toimija on antanut suostumuksensa;

b) asianomainen unionin toimija on jo julkisesti tiedottanut asiasta;

c) asianomainen unionin toimija ei ole antanut suostumustaan, mutta kyseisen unionin toimijan julkaiseminen lisäisi todennäköisyyttä, että poikkeamia voitaisiin välttää tai lieventää muualla. Tällaiset päätökset edellyttävät CERT-EU:n johtajan hyväksyntää. Asianomaiselle unionin toimijalle on ilmoitettava asiasta ennen julkaisemista.

17 artikla

CERT-EU:n yhteistyö [...] <u>muiden</u> vastaavaa tehtävää hoitavien elinten kanssa

1. CERT-EU voi tehdä yhteistyötä muiden [...] **Euroopan unionissa toimivien** vastaavien elinten **kuin 16 artiklassa mainittujen elinten** kanssa, mukaan lukien vastaavat toimialakohtaiset elimet, siltä osin kuin on kyse välineistä ja menetelmistä, kuten tekniikoista, taktiikoista, menettelyistä ja parhaista käytännöistä, tai kyberuhkista ja haavoittuvuuksista. CERT-EU hakee IICB:ltä etukäteen hyväksynnän **kaikelle** tällaisten [...] **vastaavaa tehtävää hoitavien elinten** kanssa tehtävälle [...] yhteistyölle **tapauskohtaisesti**. **CERT-EU ilmoittaa 16 artiklan 1 kohdassa tarkoitetuille asiaankuuluville vastaavaa tehtävää hoitaville elimille siinä jäsenvaltiossa, jossa tällaiset elimet sijaitsevat, kun CERT-EU aloittaa yhteistyön niiden kanssa.**

2. CERT-EU voi tehdä yhteistyötä muiden kumppaneiden, kuten kaupallisten toimijoiden, kansainvälisten järjestöjen, Euroopan unionin ulkopuolisten kansallisten yksikköjen tai yksittäisten asiantuntijoiden, kanssa kerätäkseen tietoa yleisistä ja erityisistä kyberuhkista, haavoittuvuuksista ja mahdollisista vastatoimista. CERT-EU hakee IICB:ltä **tapauskohtaisesti** etukäteen hyväksynnän tällaisten kumppanien kanssa tehtävälle laajemmalle yhteistyölle.

3. CERT-EU voi [...] **sellaisen** unionin [...] **toimijan** suostumuksella [...]**, johon poikkeama vaikuttaa,** antaa **kyseiseen** poikkeamaan liittyviä tietoja **1 ja 2 kohdassa tarkoitetuille** kumppaneille [...] **vain analysoinnin edistämiseksi ja edellyttäen, että asianomaisen kumppanin kanssa on voimassa salassapitojärjestely tai -sopimus**. **Tällaiset salassapitojärjestelyt tai -sopimukset on tarkistettava juridisesti komission asiaankuuluvien sisäisten menettelyjen mukaisesti. Salassapitojärjestelyt tai -sopimukset eivät edellytä IICB:n hyväksyntää etukäteen, mutta IICB:n puheenjohtajalle on ilmoitettava niistä.**

4. **CERT-EU voi poikkeuksellisesti IICB:n etukäteisellä hyväksynnällä tehdä palvelutasosopimuksia muiden kuin unionin toimijoiden kanssa.**

V luku
YHTEISTYÖ- JA RAPORTOINTIVELVOITTEET

18 artikla

Tietojen käsittely

1. CERT-EU sekä unionin [...] **toimijat** noudattavat salassapitovelvollisuutta Euroopan unionin toiminnasta tehdyn sopimuksen 339 artiklan tai vastaavien sovellettavien kehysten mukaisesti.

2. Pyyntöihin, jotka koskevat oikeutta tutustua CERT-EU:n hallussa oleviin asiakirjoihin, sovelletaan Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 1049/2001[14] säännöksiä, myös kyseisen asetuksen mukaista velvoitetta kuulla muita unionin [...] **toimijoita ja tarvittaessa jäsenvaltioita**, kun pyyntö koskee niiden asiakirjoja.

[...]

4. CERT-EU sekä [...] unionin [...] **toimijat** noudattavat tietojen käsittelyssä [...] **sovellettavia tietoturvallisuutta koskevia** sääntöjä.

[...]

19 artikla

[...] ***Kyberturvallisuustietojen vaihto***

-1. Unionin toimijat voivat vapaaehtoisesti toimittaa CERT-EU:lle tietoja niihin vaikuttavista kyberuhkista, poikkeamista, läheltä piti -tilanteista ja haavoittuvuuksista. CERT-EU varmistaa, että on käytössä tehokkaita viestintävälineitä tietojenvaihdon helpottamiseksi unionin toimijoiden kanssa. CERT-EU voi asettaa etusijalle pakollisten ilmoitusten käsittelyn vapaaehtoisten ilmoitusten käsittelyyn nähden.

[14] 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).

1. Jotta CERT-EU [...] **voi suorittaa 12 artiklassa määritellyn toimeksiantonsa ja tehtävänsä,** se voi pyytää unionin [...] **toimijoita** toimittamaan sille tietoa niiden tietoteknisiin järjestelmiin liittyvistä selvityksistä**, mukaan lukien tiedot kyberuhkista, läheltä piti -tilanteista, haavoittuvuuksista, vaarantumista kuvaavista indikaattoreista, kyberturvallisuushälytyksistä ja suosituksista, jotka koskevat kyberpoikkeamien havaitsemiseen käytettävien kyberturvallisuusvälineiden konfigurointia** [...]. Pyynnön kohteena olevan [...] **unionin toimijan** on toimitettava pyydetyt tiedot ja niihin myöhemmin tehtävät muutokset ilman aiheetonta viivytystä.

2. Unionin [...] **toimijat** toimittavat CERT-EU:n pyynnöstä ja ilman aiheetonta viivytystä digitaaliset tiedot, jotka niitä koskevissa poikkeamissa osallisina olleiden elektroniikkalaitteiden käyttö on luonut. CERT-EU voi selventää, minkä tyyppistä tällaista digitaalista tietoa se tarvitsee tilannekuvan muodostamista ja poikkeamiin reagoimista varten.

3. CERT-EU voi vaihtaa **unionin toimijoiden kanssa** sellaisia poikkeamakohtaisia tietoja, joista käy ilmi poikkeaman vaikutuksen kohteena olevan unionin [...] **toimijan** identiteetti, ainoastaan kyseisen [...] **toimijan** suostumuksella. **Jos suostumusta ei anneta, asianomaisen toimijan on esitettävä asianmukaisesti perustellut syyt CERT-EU:lle.** [...]

4. Tiedonjakovelvoitteet eivät koske EU:n turvallisuusluokiteltuja tietoja eivätkä tietoja, [...] **joiden jakamisen tiedot vastaanottaneen unionin toimijan ulkopuolelle tietojen lähde on kieltänyt näkyvin merkinnöin, ellei tietojen lähde erikseen salli niiden jakamista CERT-EU:lle.** [...]

20 artikla

[...] ***Raportointivelvoitteet***

-1. Poikkeama katsotaan merkittäväksi, jos

a) se on aiheuttanut tai voi aiheuttaa vakavia häiriötilanteita unionin toimijan toiminnassa tai taloudellisia tappioita kyseiselle unionin toimijalle;

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

1. Kaikki unionin [...] **toimijat toimittavat** [...] **CERT-EU:lle** [...]

[...].

(a) ilman aiheetonta viivytystä ja joka tapauksessa 24 tunnin kuluessa siitä, kun merkittävä poikkeama on tullut niiden tietoon, varhaisvaroituksen, jossa on tapauksen mukaan ilmoitettava, oletetaanko merkittävän poikkeaman johtuvan lainvastaisista tai vihamielisistä teoista tai voiko sillä olla rajatylittäviä vaikutuksia;

(b) ilman aiheetonta viivytystä ja joka tapauksessa 72 tunnin kuluessa siitä, kun merkittävä poikkeama on tullut niiden tietoon, poikkeamailmoituksen, jossa on tapauksen mukaan ajantasaistettava a alakohdassa tarkoitetut tiedot ja esitettävä ensimmäinen arvio merkittävästä poikkeamasta, sen vakavuudesta ja vaikutuksista sekä [...] **vaarantumista kuvaavat indikaattorit**, jos sellaisia on saatavilla;

(c) CERT-EU:n pyynnöstä väliraportin asiaankuuluvista tilannepäivityksistä;

(d) viimeistään kuukauden kuluttua b alakohdan mukaisesta merkittävää poikkeamaa koskevasta ilmoituksesta loppuraportin, joka sisältää vähintään seuraavat tiedot:

i) yksityiskohtainen kuvaus merkittävästä poikkeamasta, sen vakavuudesta ja vaikutuksista;

ii) merkittävän poikkeaman todennäköisesti aiheuttaneen uhan tai juurisyyn tyyppi;

iii) toteutetut ja meneillään olevat toimenpiteet vaikutusten lieventämiseksi;

iv) tapauksen mukaan merkittävän poikkeaman rajatylittävät vaikutukset;

(e) jos d alakohdassa tarkoitetun loppuraportin toimittamishetkellä on edelleen meneillään merkittäviä poikkeamia, edistymisraportti tuolla hetkellä ja loppuraportti kuukauden kuluessa siitä, kun poikkeama on käsitelty.

[...]

g) [...]

h) [...]

i) [...]

j) [...]

2 a. Kaikkien unionin toimijoiden on jaettava 1 kohdan mukaisesti raportoidut tiedot samassa määräajassa kaikkien 16 artiklan 1 kohdassa tarkoitettujen sen jäsenvaltion asiaankuuluvien vastaavaa tehtävää hoitavien kansallisten elinten kanssa, jossa ne sijaitsevat.

3. CERT-EU toimittaa [...] **IICB:lle, EU INTCENille ja CSIRT-verkostolle kolmen kuukauden välein** tiivistelmän, joka sisältää anonymisoidut koontitiedot [...] kyberuhkista, haavoittuvuuksista **19 artiklan mukaisesti, unionin toimijoiden vastauksista toimintakehotuksiin 13 artiklan 1 kohdan a alakohdan mukaisesti** sekä merkittävistä poikkeamista, joista on ilmoitettu 1 kohdan mukaisesti. **Kertomus sisällytetään kahden vuoden välein julkaistavaan kertomukseen kyberturvallisuuden tilasta unionissa direktiivin [ehdotus NIS 2 -direktiiviksi] 15 artiklan mukaisesti.**

4. IICB [...] antaa ... **[6 kuukautta tämän asetuksen voimaantulopäivästä] mennessä** ohjeasiakirjoja tai suosituksia**, joissa tarkennetaan raportointia koskevia sääntöjä sekä raportoinnin muotoa ja sisältöä** [...]. **Ohjeasiakirjoissa ja suosituksissa on otettava asianmukaisesti huomioon direktiivin [ehdotus NIS 2 -direktiiviksi] 20 artiklan 11 kohdan mukaisesti annetuilla täytäntöönpanosäädöksillä täytäntöön pannut säännökset**. CERT-EU levittää asianmukaiset tekniset tiedot, jotta unionin [...] **toimijat** voivat havaita ongelmat ennakolta, reagoida poikkeamiin tai toteuttaa lieventäviä toimenpiteitä.

5. **Raportointivelvoitteet** [...] eivät koske EU:n turvallisuusluokiteltuja tietoja eivätkä tietoja, [...] **joiden jakamisen tiedot vastaanottaneen unionin toimijan ulkopuolelle tietojen lähde on kieltänyt näkyvin merkinnöin, ellei tietojen lähde erikseen salli niiden jakamista CERT-EU:lle.** [...]

21 artikla

Poikkeamiin reagoimiseen liittyvä koordinointi ja yhteistyö[...]

1. Toimiessaan kyberturvallisuutta koskevan tietojenvaihdon ja poikkeamiin reagoimisen koordinointikeskuksena CERT-EU helpottaa kyberuhkia, haavoittuvuuksia ja poikkeamia koskevaa tietojenvaihtoa seuraavien kesken:

   a) unionin [...] **toimijat**;

   b) 16 ja 17 artiklassa tarkoitetut vastaavaa tehtävää hoitavat elimet.

2. CERT-EU edistää **tarvittaessa tiiviissä yhteistyössä ENISAn kanssa kyberturvallisuusasetuksen[15] 7 artiklan 7 kohdan d alakohdan mukaisesti** unionin [...] **toimijoiden** keskinäistä koordinointia poikkeamiin reagoimisen alalla muun muassa seuraavilla osa-alueilla:

   a) osallistuminen johdonmukaiseen ulkoiseen viestintään;

   [...]

   c) operatiivisten resurssien optimaalinen käyttö;

   d) koordinointi muiden unionin tason kriisinhallintamekanismien kanssa.

3. CERT-EU tukee **tiiviissä yhteistyössä ENISAn kanssa** unionin [...] **toimijoita** kyberuhkia, haavoittuvuuksia ja poikkeamia koskevan tilannekuvan muodostamisessa.

---

15 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).

4. IICB **hyväksyy viimeistään [12 kuukauden kuluttua tämän asetuksen voimaantulopäivästä] CERT-EU:n ehdotuksen perusteella ohjeasiakirjoja tai suosituksia** [...] poikkeamiin reagoimisen koordinoinnista ja yhteistyöstä merkittävien poikkeamien yhteydessä. Jos poikkeaman epäillään olevan luonteeltaan rikollinen, CERT-EU antaa ohjeita siitä, miten poikkeamasta ilmoitetaan lainvalvontaviranomaisille.

22 artikla

Merkittävien poikkeamien hallinta [...]

-1. Tukeakseen unionin toimijoihin vaikuttavien merkittävien poikkeamien koordinoitua hallintaa operatiivisella tasolla ja edistääkseen asiaankuuluvien tietojen säännöllistä vaihtoa unionin toimijoiden kesken ja jäsenvaltioiden kanssa IICB laatii tiiviissä yhteistyössä CERT-EU:n ja ENISAn kanssa 21 artiklan 2 kohdassa eriteltyihin toimiin perustuvan kyberturvallisuuskriisien hallintasuunnitelman, joka sisältää vähintään seuraavat osatekijät:

a) unionin toimijoiden välistä koordinointia ja tiedonkulkua koskevat säännöt merkittävien poikkeamien hallintaa varten operatiivisella tasolla;

b) yhteiset vakioidut toimintamenettelyt;

c) merkittävän poikkeaman vakavuuden ja kriisitilanteen kynnyspisteiden yhteinen luokitusjärjestelmä;

d) säännölliset harjoitukset;

e) käytettävät suojatut viestintäkanavat;

f) EU-CyCLONe-yhteyspiste, joka jakaa asiaankuuluvia tietoja EU-CyCLONen kanssa yhteisen tilannetietoisuuden edistämiseksi.

1. CERT-EU koordinoi unionin [...] **toimijoiden** kanssa reagoimista [...] **merkittäviin poikkeamiin**. Se ylläpitää luetteloa teknisestä asiantuntemuksesta, jota tarvitaan poikkeamiin reagoimiseksi [...] **merkittävien poikkeamien** yhteydessä.

2. Unionin [...] **toimijat** osallistuvat teknisen asiantuntemuksen luettelon kokoamiseen toimittamalla vuosittain päivitetyn luettelon organisaationsa käytettävissä olevista asiantuntijoista ja heidän teknisestä erityisosaamisestaan.

3. CERT-EU voi myös **sellaisen jäsenvaltion pyynnöstä, jossa asianomainen unionin toimija sijaitsee, ja** unionin asianomaisen [...] **toimijan** suostumuksella pyytää 2 kohdassa tarkoitettuihin luetteloihin sisältyviä asiantuntijoita osallistumaan [...] **merkittävään poikkeamaan** reagoimiseen [...] **kyseisen unionin toimijan osalta**.

VI luku
LOPPUSÄÄNNÖKSET

23 artikla

Ensimmäinen talousarvion uudelleen kohdentaminen

Komissio antaa ehdotuksen henkilöstöresurssien ja taloudellisten resurssien uudelleen kohdentamisesta asiaankuuluvista unionin [...] **toimijoista** komission talousarvioon. Uudelleen kohdentaminen tulee voimaan samaan aikaan kuin ensimmäinen talousarvio, joka hyväksytään tämän asetuksen voimaantulon jälkeen.

24 artikla

Uudelleentarkastelu

1. IICB raportoi CERT-EU:n avustuksella määräajoin komissiolle tämän asetuksen täytäntöönpanosta. IICB voi myös antaa komissiolle suosituksia [...] **tämän asetuksen uudelleentarkastelusta**.

2. Komissio antaa Euroopan parlamentille ja neuvostolle kertomuksen tämän asetuksen täytäntöönpanosta viimeistään [...] **36** kuukauden kuluttua tämän asetuksen voimaantulosta ja sen jälkeen kolmen vuoden välein.

3. Komissio arvioi tämän asetuksen toimivuutta ja antaa siitä kertomuksen Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle sekä alueiden komitealle **viimeistään** [...] viiden vuoden kuluttua asetuksen voimaantulopäivästä. **Kertomukseen liitetään tarvittaessa lainsäädäntöehdotus.**

25 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 Brysselissä

Euroopan parlamentin puolesta	*Neuvoston puolesta*
Puhemies	*Puheenjohtaja*

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

LIITE II

[...]

[...]

[...]

[...]

[...]

[...]

[...]