Euroopan unionin neuvosto

Bryssel, 22. maaliskuuta 2022
(OR. en)

7474/22

Toimielinten välinen asia:
2022/0085 (COD)

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

EHDOTUS

Lähettäjä:	Euroopan komission pääsihteeri, allekirjoittajana johtaja Martine DEPREZ
Saapunut:	22. maaliskuuta 2022
Vastaanottaja:	Jeppe TRANHOLM-MIKKELSEN, Euroopan unionin neuvoston pääsihteeri
Kom:n asiak. nro:	COM(2022) 122 final
Asia:	Ehdotus EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUKSEKSI toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi unionin toimielimissä, elimissä ja laitoksissa

Valtuuskunnille toimitetaan oheisena asiakirja COM(2022) 122 final.

Liite: COM(2022) 122 final

EUROOPAN
KOMISSIO

Bryssel 22.3.2022
COM(2022) 122 final

2022/0085 (COD)

Ehdotus

EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS

toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi unionin toimielimissä, elimissä ja laitoksissa

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

PERUSTELUT

1. EHDOTUKSEN TAUSTA

• Ehdotuksen perustelut ja tavoitteet

Tällä ehdotetulla asetuksella perustetaan kehys, jonka tarkoituksena on varmistaa, että unionin toimielimillä, elimillä ja virastoilla on yhteiset kyberturvallisuussäännöt ja -toimenpiteet. Tavoitteena on parantaa entisestään kaikkien yksiköiden kyberuhkien sietokykyä ja valmiuksia reagoida niihin. Ehdotettu asetus auttaa osaltaan saavuttamaan komission päätavoitteita eli kehittämään Euroopan digitaalista valmiutta ja rakentamaan tulevaisuuden taloutta, joka toimii ihmisten hyväksi. Lisäksi turvallisen ja häiriönsietokykyisen julkishallinnon varmistaminen on koko yhteiskunnan digitalisaation kulmakivi.

Tämä ehdotus perustuu EU:n turvallisuusunionistrategiaan (COM(2020) 605 final) sekä EU:n kyberturvallisuusstrategiaan digitaaliselle vuosikymmenelle (JOIN(2020) 18 final).

Ehdotetulla asetuksella nykyaikaistetaan CERT-EU:n oikeudellista kehystä ottaen huomioon toimielinten, elinten ja virastojen digitalisaatiossa viime vuosina tapahtuneet muutokset ja edistyminen sekä alati muuttuva kyberuhkaympäristö. Covid-19-kriisi on entisestään vahvistanut molempia kehityskulkuja. Samaan aikaan kyberturvallisuuspoikkeamien määrä on edelleen kasvussa, hyökkäykset ovat yhä sofistikoituneempia ja ne tulevat monista eri lähteistä.

Ehdotuksella muutetaan CERT-EU:n nimi tietotekniikan kriisiryhmästä unionin toimielinten, elinten ja virastojen kyberturvallisuuskeskukseksi. Tämä noudattaa jäsenvaltioissa tapahtunutta ja kansainvälistä kehitystä, sillä useat CERT-yksiköt on nimetty uudelleen kyberturvallisuuskeskuksiksi. Lyhytnimi CERT-EU säilytetään nimen tunnettuuden vuoksi.

• Yhdenmukaisuus muiden alaa koskevien politiikkojen säännösten kanssa

Tämän ehdotuksen tavoitteena on parantaa unionin toimielinten, elinten ja virastojen kyberuhkien sietokykyä sekä yhdenmukaistaa säännöksiä seuraavien säädösten kanssa:

- direktiivi (EU) 2016/1148 toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa; ehdotus on yhdenmukainen myös ehdotuksen direktiiviksi (EU) XXXX/XXXX toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi koko unionissa ja direktiivin (EU) 2016/1148 kumoamisesta [ehdotus tarkistetuksi verkko- ja tietoturvadirektiiviksi] kanssa
- asetus (EU) 2019/881 Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista (kyberturvallisuusasetus)
- ehdotus asetukseksi (EU) XXXX/XXXX tietoturvallisuudesta unionin toimielimissä, elimissä ja laitoksissa
- yhteisen kyberturvallisuusyksikön perustamisesta 23 päivänä kesäkuuta 2021 annettu komission suositus
- koordinoidusta reagoinnista laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin 13 päivänä syyskuuta 2017 annettu komission suositus (EU) 2017/1584.

Koordinoidusta reagoinnista laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin 13 päivänä syyskuuta 2017 annetun komission suosituksen (EU) 2017/1584 liitteessä esitetään suunnitelma koordinoidusta reagoinnista laajamittaisiin rajat ylittäviin kyberturvallisuuspoikkeamiin ja -kriiseihin.

Maaliskuun 9 päivänä 2021 annetussa Euroopan unionin neuvoston päätöslauselmassa korostettiin, että kyberturvallisuus on olennaisen tärkeää kansallisen ja EU-tason julkishallinnon toiminnan sekä koko yhteiskunnan ja talouden toiminnan kannalta. Lisäksi siinä painotettiin vankan ja johdonmukaisen turvallisuuskehyksen käyttöönoton merkitystä koko EU:n henkilöstön, datan, viestintäverkkojen, tietojärjestelmien ja päätöksentekoprosessien turvaamiseksi. Tämä on tarkoitus saavuttaa erityisesti parantamalla unionin toimielinten, elinten ja virastojen häiriönsietokykyä ja turvallisuuskulttuuria. Tähän on tarkoitus osoittaa riittävät resurssit ja valmiudet muun muassa CERT-EU:n toimeksiannon laajentamisen yhteydessä.

2. OIKEUSPERUSTA, TOISSIJAISUUSPERIAATE JA SUHTEELLISUUSPERIAATE

- **Oikeusperusta**

Tämän asetuksen oikeusperusta on Euroopan unionin toiminnasta tehdyn sopimuksen, jäljempänä ’SEUT-sopimus’, 298 artikla, jossa määrätään, että ”unionin toimielimet, elimet ja laitokset tukeutuvat tehtäviään hoitaessaan avoimeen, tehokkaaseen ja riippumattomaan eurooppalaiseen hallintoon”. Tätä varten Euroopan parlamentti ja neuvosto antavat tavallista lainsäätämisjärjestystä noudattaen asetuksilla säännökset, joissa kunnioitetaan 336 artiklan nojalla vahvistettuja henkilöstösääntöjä ja palvelussuhteen ehtoja.

Tietotekniikka on tarjonnut unionin toimielimille, elimille ja virastoille uusia tapoja työskennellä, olla vuorovaikutuksessa kansalaisten kanssa ja parantaa toimintaa yleisesti. Teknologian kehittyessä myös kyberuhkaympäristö kehittyy. Unionin toimielimistä, elimistä ja virastoista on tullut erittäin houkuttelevia kohteita sofistikoituneille kyberhyökkäyksille. Kyberturvallisuuden varmistamiseen liittyvien järjestelmien ja vaatimusten käyttöönottaminen näyttää edistävän eurooppalaisen hallinnon tehokkuutta ja riippumattomuutta. Tämän seurauksena unionin toimielimet, elimet, toimistot ja virastot voivat hoitaa tehtäviään entistä tehokkaammin digitaalisessa maailmassa.

Lisäksi unionin toimielinten, elinten ja virastojen kyberturvatasossa sekä kyberturvallisuutta koskevassa lähestymistavassa olevat nykyiset erot, joita kuvaillaan jäljempänä 3 jaksossa, ovat esteenä avoimelle, tehokkaalle ja riippumattomalle eurooppalaiselle hallinnolle. Ilman yhteistä lähestymistapaa unionin toimielinten, elinten ja virastojen kyberturvatasot jatkaisivat kehittymistään eri suuntiin. Tämä oikeusperusta on näin ollen asianmukainen, kun otetaan huomioon, että asetuksen tavoitteena on luoda yhteinen oikeudellinen kehys kyberturvallisuudelle unionin toimielimissä, elimissä, toimistoissa ja virastoissa.

- **Toissijaisuusperiaate**

Asetus toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi unionin toimielimissä, elimissä ja laitoksissa kuuluu unionin yksinomaiseen toimivaltaan.

- **Suhteellisuusperiaate**

Ehdotetun asetuksen säännöt eivät ylitä sitä, mikä on tarpeen sen erityistavoitteiden saavuttamiseksi tyydyttävällä tavalla. Suunnitellut toimenpiteet edistävät yhteisen korkean kyberturvatason saavuttamista ilman, että ne ylittävät sitä, mikä on tarpeen kyseisen tavoitteen saavuttamiseksi, kun otetaan huomioon kasvavat riskit.

- **Toimintatavan valinta**

Asetusta, jota sovelletaan sellaisenaan, pidetään asianmukaisena oikeudellisena välineenä unionin toimielimille, elimille ja virastoille asetettavien velvoitteiden määrittelemiseksi ja

selkeyttämiseksi. Asetus on asianmukaisin oikeudellinen väline kohdennettujen parannusten toteuttamiseksi.

3. ENNAKKOARVIOINTIEN, SIDOSRYHMIEN KUULEMISTEN JA VAIKUTUSTENARVIOINTIEN TULOKSET

- **Ennakkoarvioinnit**

CERT-EU on suorittanut arvioinnin tärkeimmistä kyberuhkista, joille unionin toimielimet, elimet ja virastot altistuvat parhaillaan tai todennäköisesti altistuvat ennakoitavissa olevassa tulevaisuudessa.

Arvioinnissa käytettiin kolmea havaintoluokkaa:

- yritykset tunkeutua unionin toimielinten, elinten ja virastojen tietotekniseen infrastruktuuriin (jos tunkeutuminen onnistuu, sitä käsitellään poikkeamana, muut tapaukset kirjataan havaittuina yrityksinä)
- unionin toimielinten, elinten ja virastojen läheisyydessä havaitut uhkat (esimerkiksi niihin liittyvillä toimialoilla, niiden sidosryhmäyhteisöissä tai Euroopassa)
- maailmanlaajuisesti havaitut merkittävät uhkiin liittyvät kehityssuuntaukset.

Lisäksi arvioinnissa otettiin huomioon, miten merkittävät käynnissä olevat muutokset vaikuttavat tapoihin, joilla unionin toimielimet hallinnoivat ja käyttävät tietoteknistä infrastruktuuriaan ja tietotekniikkapalvelujaan. Tällaisia muutoksia ovat muun muassa

- etätyön lisääntyminen
- järjestelmien siirtäminen pilveen
- tietotekniikkapalvelujen yhä suurempi ulkoistaminen.

Kohdistettuja hyökkäyksiä (APT) suorittavien toimijoiden toteuttamien, unionin toimielimiin, elimiin ja virastoihin vaikuttaneiden merkittävien poikkeamien[1] määrä kasvoi merkittävästi vuodesta 2019 vuoteen 2021. Vuoden 2021 ensimmäisellä puoliskolla havaittiin yhtä paljon merkittäviä poikkeamia kuin koko vuoden 2020 aikana. Tämä näkyi myös CERT-EU:n vuonna 2020 analysoimien forensisten peilikuvatiedostojen (kopiot hyökkäysten kohteena olevien järjestelmien tai laitteiden sisällöstä) määrässä, joka kolminkertaistui vuodesta 2019. Samalla merkittävien poikkeamien määrä yli kymmenkertaistui vuodesta 2018.

CERT-EU:n johtoryhmä asetti CERT-EU:lle vuonna 2020 uuden strategisen tavoitteen, joka on perusteellisen, laajuudeltaan ja syvyydeltään asianmukaisen kyberpuolustustason varmistaminen kaikissa unionin toimielimissä, elimissä ja virastoissa sekä sen jatkuva mukauttaminen nykyisiin tai tuleviin uhkiin, kuten mobiililaitteisiin, pilviympäristöihin ja esineiden internetiä käyttäviin laitteisiin kohdistuviin hyökkäyksiin.

Komissio on tehnyt CERT-EU:n uhka-analyysin täydentämiseksi arvioinnin kyberturvallisuuden toiminnasta 20:ssä unionin toimielimessä, elimessä ja virastossa. Arvioinnista saatiin tietoa vakiintuneista kyberturvallisuuskäytännöistä ja kyberturvallisuuden hallinnointiin liittyvistä valmiuksista. Lisäksi joistakin teknisistä turvallisuusvalvontatoimista saatiin ulkoista vertailutietoa.

[1] ’Merkittävällä poikkeamalla’ tarkoitetaan mitä tahansa poikkeamaa, lukuun ottamatta sellaisia, joilla on vähäinen vaikutus ja joihin ei todennäköisesti liity juurikaan epäselvyyksiä menetelmän tai teknologian osalta.

Arviointi perustui kyselylomakkeisiin, joihin nämä toimielimet, elimet ja virastot vastasivat, sekä julkisesti saatavilla oleviin ja unionin toimielinten, elinten ja virastojen suoraan toimittamiin tietoihin. Se tarjoaa riittävästi tietoa nykytilanteesta, jotta voidaan tehdä seuraavat päätelmät:

- Arvioinnin kohteena olleiden unionin toimielinten, elinten ja virastojen välillä on huomattavia eroja kyberturvallisuuden kehitystasossa, tietoteknisen infrastruktuurin koossa ja valmiustasoissa.
- Vaikka monissa unionin toimielimissä, elimissä ja virastoissa on yleisesti ottaen kehitystasoltaan hyvät havaitsemista ja reagointia koskevat valmiudet, niiden kyberturvallisuuden hallintoa koskevien valmiuksien integroidun riskinhallinnan tasoissa on eroja.
- Arvioinnin kohteena olleiden unionin toimielinten, elinten ja virastojen kyberturvallisuuskehykset (strategia, toimintapolitiikka ja sääntöpohja) olivat yleisesti ottaen vakiintuneita asetuksen liitteessä I luetelluilla keskeisillä kyberturvallisuuden osa-alueilla. Joillakin unionin toimielimillä, elimillä ja virastoilla on kuitenkin puutteita toiminnan jatkuvuuden hallinnassa, vaatimusten noudattamisessa, tarkastuksissa ja jatkuvassa parantamisessa.
- Arvioinnissa havaittiin, että parhaina käytäntöinä pidettyjä teknisiä toimenpiteitä ei sovellettu yhtenäisesti arvioinnin kohteena olleissa unionin toimielimissä, elimissä ja virastoissa.

Yhteenvetona voidaan todeta, että 20 unionin toimielimen, elimen ja viraston analyysi osoittaa, että niiden hallinnossa, kyberhygieniassa, yleisissä valmiuksissa ja kehitystasossa on suurta vaihtelua. Näiden kehitystasossa olevien erojen korjaamiseksi ja sen varmistamiseksi, että kaikissa unionin toimielimissä, elimissä ja virastoissa noudatetaan yhteistä korkeaa kyberturvatasoa, on ratkaisevan tärkeää, että kaikkia unionin toimielimiä, elimiä ja virastoja edellytetään panemaan täytäntöön kyberturvallisuustoimenpiteiden perustaso.

Tähän mennessä unionin lainsäädännössä ei ole käsitelty unionin toimielinten, elinten ja virastojen kyberturvallisuutta eikä puututtu kattavasti kyberuhkaympäristöön ja digitalisaation aiheuttamiin uusiin tietoteknisiin riskeihin.

- **Sidosryhmien kuuleminen**

Komissio on kuullut sidosryhmiä kaikista unionin toimielimistä, elimistä ja virastoista sekä jäsenvaltioiden edustajia neuvostossa ja sidosryhmiä Euroopan parlamentissa. Jäsenvaltioiden edustajat ja asiaan liittyvät sidosryhmät unionin toimielimistä, elimistä ja virastoista osallistuivat 25. kesäkuuta 2021 komission järjestämään työpajaan, jossa keskusteltiin tulevan asetusehdotuksen sisällöstä.

- **Vaikutustenarviointi**

Tämän ehdotuksen vaikutus kohdistuu unionin toimielimiin, elimiin ja virastoihin. Erityistä vaikutustenarviointia ei siis tarvita, koska ehdotus ei koske jäsenvaltioita.

- **Perusoikeudet**

Euroopan unioni on sitoutunut varmistamaan perusoikeuksien korkeatasoisen suojelun. Kaikki tähän asetukseen perustuva tietojen jakaminen toteutettaisiin luotettavissa ympäristöissä noudattaen täysimääräisesti Euroopan unionin perusoikeuskirjan 8 artiklassa vahvistettua oikeutta henkilötietojen suojaan sekä asiaan liittyvää tietosuojalainsäädäntöä, erityisesti Euroopan parlamentin ja neuvoston asetusta (EU) 2018/1725.

4. TALOUSARVIOVAIKUTUKSET

Markkinaviitearvoista ja tutkimuksista[2] käy ilmi, että suorat kyberturvallisuusmenot ovat yleensä olleet 4–7 prosenttia organisaatioiden yhteenlasketuista tietotekniikkamenoista. CERT-EU:n tämän lainsäädäntöehdotuksen tueksi tekemä uhka-analyysi viittaa kuitenkin siihen, että kansainväliset elimet ja poliittiset organisaatiot kohtaavat yhä suurempia riskejä. Siksi vaikuttaisi asianmukaisemmalta tavoitteelta ohjata kyberturvallisuuteen 10 prosenttia tietotekniikkamenoista. Tällaisten toimien tarkkoja kustannuksia ei voida määrittää, koska unionin toimielinten, elinten ja virastojen tietotekniikkamenoista ja kyberturvallisuusmenojen osuudesta ei ole yksityiskohtaista tietoa.

Vaikka on näin ollen todennäköistä, että useat unionin toimielimet, elimet ja virastot investoivat kyberturvallisuuteen vähemmän kuin niiden pitäisi, tämä asetus ei sinällään aiheuta lisäystä nykyisiin menoihin. Myös ilman asetusta kunkin yksikön olisi varmistettava riittävä kyberturvallisuuden taso. Tällä asetuksella jatketaan aiempaa yhteistyötä CERT-EU:n johtokunnassa ja virallistetaan tietojenvaihtotaso, joka on jo tällä hetkellä osittain käytössä. Kuten säädösehdotukseen liittyvässä rahoitusselvityksessä todetaan, CERT-EU tarvitsee lisävaroja laajennetun tehtävänsä suorittamiseksi ja nämä varat olisi kohdennettava uudelleen CERT-EU:n palveluja hyödyntäviltä unionin toimielimiltä, elimiltä ja virastoilta.

5. LISÄTIEDOT

- **Täytäntöönpano, seuranta, arviointi ja raportointijärjestelyt**

Toimielinten välisen kyberturvallisuuslautakunnan (IICB) olisi CERT-EU:n avustuksella tarkasteltava tämän asetuksen toimintaa, tehtävä arviointeja ja toimitettava komissiolle kertomus havainnoistaan. Komission olisi varmistettava, että Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle raportoidaan säännöllisesti.

CERT-EU voi laatia ehdotuksen ohjeasiakirjaksi tai suositukseksi, ja IICB tekee päätöksen ehdotuksen hyväksymisestä. Ohjeasiakirja on kaikille unionin toimielimille, elimille ja virastoille tai tietylle unionin toimielinten, elinten ja virastojen alaryhmälle suunnattu tiedote, kun taas suositus on osoitettu yksittäisille unionin toimielimille, elimille ja virastoille. Toimintakehotus on CERT-EU:n tiedote, jossa kuvaillaan kiireellisiä turvatoimenpiteitä, jotka unionin toimielimiä, elimiä ja virastoja kehotetaan toteuttamaan tietyssä määräajassa.

- **Ehdotukseen sisältyvien säännösten yksityiskohtaiset selitykset**

Yleiset säännökset

Tässä asetuksessa säädetään toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi, ja sitä sovelletaan unionin toimielimiin, elimiin ja virastoihin, jotta ne voivat hoitaa tehtävänsä avoimella, tehokkaalla ja riippumattomalla tavalla. (1–3 ja 23–25 artikla)

Toimenpiteet yhteisen korkean kyberturvatason varmistamiseksi

Unionin toimielimet, elimet ja virastot velvoitetaan laatimaan sisäinen kyberturvallisuusriskien hallinta- ja valvontakehys, jolla varmistetaan kaikkien

[2] Lähde: Gartner, ”Identifying the Real Information Security Budget” (2016). Tämän lisäksi tietotekniikan turvallisuuteen kytkeytyy epäsuoria menoja, kuten verkkoturvallisuuteen (esimerkiksi palomuurit ja virustorjunta) ja järjestelmävastaavan vastuualueisiin (esimerkiksi riskinarviointi ja turvallisuusvalvontatoimien toteuttaminen) liittyvät menot. Vuonna 2020 julkaistun artikkelin mukaan kyberturvallisuusmenot ovat rahoituslaitoksissa 10–11 prosenttia tietotekniikkamenoista. Lähde: DI_2020-FS-ISAC-Cybersecurity.pdf (deloitte.com).

kyberturvallisuusriskien tehokas ja järkevä hallinta. Unionin toimielinten, elinten ja virastojen on lisäksi otettava käyttöön kyberturvallisuuden perustaso hallinta- ja valvontakehyksen mukaisesti tunnistettujen riskien torjumiseksi, tehtävä säännöllisiä kyberturvallisuuden kehitystason arviointeja sekä hyväksyttävä kyberturvallisuussuunnitelma. (4–8 artikla)

Toimielinten välinen kyberturvallisuuslautakunta

Asetuksella perustetaan toimielinten välinen kyberturvallisuuslautakunta, jonka tehtävänä on seurata asetuksen täytäntöönpanoa unionin toimielimissä, elimissä ja virastoissa, valvoa sitä, miten CERT-EU panee täytäntöön yleiset painopisteet ja tavoitteet, sekä antaa CERT-EU:lle strategista ohjausta. (9–11 artikla)

CERT-EU

CERT-EU parantaa kaikkien unionin toimielinten, elinten ja virastojen tietoteknisen ympäristön turvallisuutta tarjoamalla neuvontaa, auttamalla ehkäisemään, havaitsemaan ja lieventämään poikkeamia ja reagoimaan niihin sekä toimimalla kyberturvallisuutta koskevan tietojenvaihdon ja poikkeamiin reagoimisen koordinointikeskuksena. (12–17 artikla)

Yhteistyö- ja raportointivelvoitteet

Asetuksella varmistetaan yhteistyö ja tietojenvaihto CERT-EU:n sekä unionin toimielinten, elinten ja virastojen kesken luottamuksen lisäämiseksi ja luotettavuuden parantamiseksi. Tätä varten CERT-EU voi pyytää unionin toimielimiä, elimiä ja virastoja toimittamaan sille asiaankuuluvia tietoja. Se voi myös vaihtaa poikkeamakohtaisia tietoja unionin toimielinten, elinten ja virastojen kanssa helpottaakseen samankaltaisten kyberuhkien tai poikkeamien havaitsemista ilman poikkeaman kohteena olleen tahon suostumusta. CERT-EU voi vaihtaa sellaisia poikkeamakohtaisia tietoja, joista käy ilmi kyberturvallisuuspoikkeaman kohteen identiteetti, ainoastaan poikkeaman kohteena olleen tahon suostumuksella.

Kaikki unionin toimielimet, elimet ja virastot ilmoittavat CERT-EU:lle merkittävistä kyberuhkista, haavoittuvuuksista ja poikkeamista ilman aiheetonta viivytystä ja joka tapauksessa viimeistään 24 tunnin kuluessa siitä, kun tällainen uhka, haavoittuvuus tai poikkeama on tullut niiden tietoon. (18–22 artikla)

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 toimielinten, elinten ja virastojen 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 toimielinten, elinten ja virastojen 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 toimielimeen, elimeen tai virastoon, niillä voi olla ketjureaktiovaikutuksia, jotka voivat aiheuttaa kauaskantoisia ja pitkäaikaisia kielteisiä vaikutuksia muihin. Lisäksi tiettyjen toimielinten, elinten ja virastojen tietotekniset ympäristöt ovat yhteydessä jäsenvaltioiden tietoteknisiin ympäristöihin, minkä

seurauksena yhdessä unionin yksikössä tapahtunut poikkeama aiheuttaa riskin jäsenvaltioiden tietoteknisten ympäristöjen kyberturvallisuudelle ja päinvastoin.

(4) Unionin toimielimet, elimet ja virastot ovat houkuttelevia kohteita erittäin taitaville uhkatoimijoille, joilla on käytössään paljon resursseja, ja niihin kohdistuu myös muita uhkia. Samalla kyseisten yksikköjen 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 toimielimet, elimet ja virastot saavuttavat yhteisen korkean kyberturvatason ottamalla käyttöön kyberturvallisuuden perustason (kyberturvallisuutta koskevat vähimmäissäännöt, joita verkko- ja tietojärjestelmien sekä niiden tarjoajien ja käyttäjien on noudatettava kyberturvallisuusriskien minimoimiseksi), vaihtamalla tietoja ja tekemällä yhteistyötä.

(5) Toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi koko unionissa annetun direktiivin [ehdotus tarkistetuksi verkko- ja tietoturvadirektiiviksi] 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 toimielimet, elimet ja virastot 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 toimielimen, elimen ja viraston on tarpeen laatia sisäinen kyberturvallisuusriskien hallinta- ja valvontakehys, jolla varmistetaan kaikkien kyberturvallisuusriskien tehokas ja järkevä hallinta ja jossa otetaan huomioon toiminnan jatkuvuus ja kriisitilanteiden hallinta.

(7) Unionin toimielinten, elinten ja virastojen 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 toimielinten, elinten ja virastojen tehtävien hoitamista tai rajoittavat niiden hallinnollista riippumattomuutta. Näin ollen unionin toimielinten, elinten ja virastojen olisi laadittava omat kehyksensä kyberturvallisuusriskien hallintaa ja valvontaa varten sekä hyväksyttävä oma perustasonsa ja kyberturvallisuussuunnitelmansa.

(8) Jotta unionin toimielimille, elimille ja virastoille 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 toimielimen, elimen ja viraston olisi pyrittävä osoittamaan oman kyberturvatasonsa parantamiseen riittävä prosenttiosuus tietotekniikkamenoistaan. Pitkällä aikavälillä tavoitteena olisi oltava noin 10 prosenttia.

(9) Yhteinen korkea kyberturvataso edellyttää, että kyberturvallisuus on unionin kunkin toimielimen, elimen ja viraston ylimmän johdon valvonnassa. Ylimmän johdon olisi hyväksyttävä kyberturvallisuuden perustaso, jonka olisi torjuttava kunkin toimielimen, elimen ja viraston perustaman kehyksen mukaisesti tunnistettuja riskejä. Kyberturvallisuuskulttuuriin eli kyberturvallisuuden käytännön harjoittamiseen puuttuminen on keskeinen osa kyberturvallisuuden perustasoa kaikissa unionin toimielimissä, elimissä ja virastoissa.

(10) Unionin toimielinten, elinten ja virastojen olisi arvioitava toimittajien ja palveluntarjoajien, myös datatallennus- ja -käsittelypalvelujen tai

tietoturvapalveluntarjoajien (MSSP), kanssa solmittaviin suhteisiin liittyviä riskejä ja toteutettava asianmukaiset toimet näiden riskien hallitsemiseksi. Näiden toimenpiteiden olisi muodostettava osa kyberturvallisuuden perustasoa, ja niitä olisi tarkennettava CERT-EU:n julkaisemissa ohjeasiakirjoissa tai suosituksissa. Toimenpiteitä ja ohjeita määriteltäessä olisi otettava asianmukaisesti huomioon 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.

(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[3]. Tämän järjestelyn kehittämistä olisi jatkettava tämän asetuksen täytäntöönpanon tukemiseksi.

(12) CERT-EU:n nimi olisi muutettava tietotekniikan kriisiryhmästä unionin toimielinten, elinten ja virastojen kyberturvallisuuskeskukseksi. Tämä noudattaa jäsenvaltioissa tapahtunutta ja kansainvälistä kehitystä, sillä useat CERT-yksiköt on nimetty uudelleen kyberturvallisuuskeskuksiksi. Lyhytnimi CERT-EU olisi säilytettävä nimen tunnettuuden vuoksi.

(13) Monet kyberhyökkäykset ovat osa laajempia kampanjoita, jotka kohdistuvat unionin toimielinten, elinten ja virastojen ryhmiin tai etuyhteisöihin, joihin sisältyy unionin toimielimiä, elimiä ja virastoja. Jotta voitaisiin havaita ongelmat etukäteen, reagoida poikkeamiin tai toteuttaa lieventäviä toimenpiteitä, unionin toimielinten, elinten ja virastojen olisi ilmoitettava CERT-EU:lle merkittävistä kyberuhkista, haavoittuvuuksista ja poikkeamista sekä jaettava sen kanssa asianmukaiset tekniset tiedot, jotka mahdollistavat samankaltaisen kyberuhkien, haavoittuvuuksien ja poikkeamien tunnistamisen tai lieventämisen sekä niihin reagoimisen muissa unionin toimielimissä, elimissä ja virastoissa. Direktiivissä [ehdotus tarkistetuksi verkko- ja tietoturvadirektiiviksi] määritetyn lähestymistavan mukaisesti silloin, kun toimija saa tietoonsa merkittävän poikkeaman, sitä olisi vaadittava toimittamaan ensimmäinen ilmoitus CERT-EU:lle 24 tunnin kuluessa. Tällaisen tietojenvaihdon olisi mahdollistettava se, että CERT-EU levittää tiedot muille unionin toimielimille, elimille ja virastoille sekä asianmukaisille vastaavaa tehtävää hoitaville viranomaisille, jotta voidaan auttaa suojaamaan unionin tietoteknisiä järjestelmiä ja unionin kumppaneiden tietoteknisiä järjestelmiä samankaltaisilta poikkeamilta, uhkilta ja haavoittuvuuksilta.

(14) Sen lisäksi, että CERT-EU:lle annetaan enemmän tehtäviä ja sen roolia laajennetaan, olisi perustettava toimielinten välinen kyberturvallisuuslautakunta (IICB). Sen olisi

[3] EUVL C 12, 13.1.2018, s. 1–11.

edistettävä yhteistä korkeaa kyberturvatasoa unionin toimielimissä, elimissä ja virastoissa seuraamalla tämän asetuksen täytäntöönpanoa unionin toimielimissä, elimissä ja virastoissa, valvomalla sitä, miten CERT-EU panee täytäntöön yleiset painopisteet ja tavoitteet, ja antamalla CERT-EU:lle strategista ohjausta. IICB:n olisi varmistettava toimielinten edustus ja otettava mukaan virastojen ja elinten edustajia unionin virastojen verkoston kautta.

(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 toimielimiä, elimiä ja virastoja kehotetaan toteuttamaan tietyssä määräajassa.

(16) IICB:n olisi valvottava tämän asetuksen noudattamista, ohjeasiakirjojen ja suositusten jatkotoimien toteuttamista sekä CERT-EU:n antamien 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 toimielinten, elinten ja virastojen sekä tarvittaessa muiden sidosryhmien kanssa. Tarvittaessa IICB:n olisi annettava ei-sitovia varoituksia ja suositeltava tarkastuksia.

(17) CERT-EU:n tarkoituksena olisi oltava edistää kaikkien unionin toimielinten, elinten ja virastojen tietoteknisen ympäristön turvallisuutta. CERT-EU:n olisi toimittava vastaavassa tehtävässä kuin direktiivin [ehdotus tarkistetuksi verkko- ja tietoturvadirektiiviksi] 6 artiklassa tarkoitettu Euroopan haavoittuvuusrekisteriin tehtävää koordinoitua haavoittuvuuksien ilmaisemista varten unionin toimielimille, elimille ja virastoille nimetty koordinaattori.

(18) CERT-EU:n johtoryhmä asetti CERT-EU:lle vuonna 2020 uuden strategisen tavoitteen, joka on perusteellisen, soveltuvan laajuisen ja syvällisen kyberpuolustustason varmistaminen kaikissa unionin toimielimissä, elimissä ja virastoissa ja sen jatkuva mukauttaminen nykyisiin tai tuleviin uhkiin, kuten mobiililaitteisiin, pilviympäristöihin ja esineiden internetiä käyttäviin laitteisiin kohdistuviin hyökkäyksiin. Tämä strateginen tavoite sisältää myös laaja-alaiset turvaoperaatiokeskukset, jotka seuraavat verkkoja, sekä erittäin vakavien uhkien ympärivuorokautisen seurannan. CERT-EU:n olisi tuettava unionin suurten toimielinten, elinten ja virastojen tietotekniikan turvallisuudesta vastaavia ryhmiä, myös ympärivuorokautisessa ensivaiheen seurannassa. Lisäksi CERT-EU:n olisi tarjottava kaikki palvelut pienille ja joillekin keskikokoisille unionin toimielimille, elimille ja virastoille.

(19) CERT-EU:n olisi myös suoritettava sille direktiivissä [ehdotus tarkistetuksi verkko- ja tietoturvadirektiiviksi] 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[4] 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

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

hoitavien julkisten ja yksityisten toimijoiden kanssa, myös Natossa, edellyttäen, että IICB on antanut sille etukäteisen hyväksynnän.

(20) CERT-EU:n olisi operatiivista kyberturvallisuutta tukiessaan hyödynnettävä saatavilla olevaa Euroopan unionin kyberturvallisuusviraston asiantuntemusta Euroopan parlamentin ja neuvoston asetuksessa (EU) 2019/881[5] tarkoitetun jäsennellyn yhteistyön kautta. Tarvittaessa tällaisen yhteistyön käytännön toteutus olisi määriteltävä erityisin järjestelyin näiden kahden yksikön välillä päällekkäisten tehtävien välttämiseksi. CERT-EU:n olisi tehtävä yhteistyötä Euroopan unionin kyberturvallisuusviraston kanssa uhka-analyysissa ja jaettava säännöllisesti uhkaympäristöä koskeva raporttinsa viraston kanssa.

(21) CERT-EU:n olisi tuettava 23 päivänä kesäkuuta 2021 annetun komission suosituksen[6] mukaisesti perustettua yhteistä kyberturvallisuusyksikköä tekemällä yhteistyötä ja vaihtamalla tietoja sidosryhmien kanssa, jotta voidaan edistää operatiivista yhteistyötä ja hyödyntää olemassa olevien verkostojen koko potentiaali unionin suojaamisessa.

(22) Kaikessa tämän asetuksen nojalla toteutettavassa henkilötietojen käsittelyssä olisi noudatettava tietosuojalainsäädäntöä, myös Euroopan parlamentin ja neuvoston asetusta (EU) 2018/1725[7].

(23) CERT-EU:n sekä unionin toimielinten, elinten ja virastojen olisi noudatettava tietojen käsittelyssä asetuksessa [ehdotus asetukseksi tietoturvallisuudesta] vahvistettuja sääntöjä. Turvallisuusasioiden koordinoinnin varmistamiseksi kaikki yhteydenotot, joita kansalliset turvallisuus- tai tiedustelupalvelut toteuttavat tai pyrkivät toteuttamaan CERT-EU:n kanssa, olisi ilman aiheetonta viivytystä annettava tiedoksi komission turvallisuusosastolle ja IICB:n puheenjohtajalle.

(24) Koska CERT-EU:n palvelut ja tehtävät ovat unionin kaikkien toimielinten, elinten ja virastojen edun mukaisia, unionin kunkin toimielimen, elimen ja viraston, jolla on tietotekniikkamenoja, olisi osoitettava oikeudenmukainen rahoitusosuus näihin palveluihin ja tehtäviin. Nämä rahoitusosuudet eivät rajoita unionin toimielinten, elinten ja virastojen itsenäistä budjettivaltaa.

(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,

---

5 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).

6 Komission suositus C(2021) 4520, annettu 23 päivänä kesäkuuta 2021, yhteisen kyberturvallisuusyksikön perustamisesta.

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).

OVAT HYVÄKSYNEET TÄMÄN ASETUKSEN:

I luku
YLEISET SÄÄNNÖKSET

1 artikla
Kohde

Tässä asetuksessa säädetään

a) unionin toimielimille, elimille ja virastoille asetettavista sisäisen kyberturvallisuusriskien hallinta- ja valvontakehyksen perustamisvelvoitteista;

b) unionin toimielimille, elimille ja virastoille asetettavista kyberturvallisuusriskien hallinta- ja raportointivelvoitteista;

c) unionin toimielinten, elinten ja virastojen kyberturvallisuuskeskuksen (CERT-EU) organisaatioon ja toimintaan sekä toimielinten välisen kyberturvallisuuslautakunnan organisaatioon ja toimintaan sovellettavista säännöistä.

2 artikla
Soveltamisala

Tätä asetusta sovelletaan kyberturvallisuusriskien hallintaan ja valvontaan kaikissa unionin toimielimissä, elimissä ja virastoissa sekä CERT-EU:n ja toimielinten välisen kyberturvallisuuslautakunnan organisaatioon ja toimintaan.

3 artikla
Määritelmät

Tässä asetuksessa tarkoitetaan:

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

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

3) ’verkko- ja tietojärjestelmien turvallisuudella’ direktiivin [ehdotus tarkistetuksi verkko- ja tietoturvadirektiiviksi] 4 artiklan 2 kohdassa tarkoitettua verkko- ja tietojärjestelmien turvallisuutta;

4) ’kyberturvallisuudella’ ja ’kyberturvalla’ direktiivin [ehdotus tarkistetuksi verkko- ja tietoturva -direktiiviksi] 4 artiklan 3 kohdassa tarkoitettua kyberturvallisuutta ja kyberturvaa;

5) ’ylimmällä johdolla’ kaikkein ylimpään johtotasoon kuuluvaa johtajaa, hallinto- tai koordinointi- ja valvontaelintä unionin kunkin toimielimen, elimen tai viraston korkean tason hallintojärjestelyt huomioon ottaen;

6) ’poikkeamalla’ direktiivin [ehdotus tarkistetuksi verkko- ja tietoturvadirektiiviksi] 4 artiklan 5 kohdassa tarkoitettua poikkeamaa;

7) ’merkittävällä poikkeamalla’ mitä tahansa poikkeamaa, lukuun ottamatta sellaisia, joilla on vähäinen vaikutus ja joihin ei todennäköisesti liity juurikaan epäselvyyksiä menetelmän tai teknologian osalta;

8) ’laajalla hyökkäyksellä’ mitä tahansa poikkeamaa, joka edellyttää enemmän resursseja kuin vaikutuksen kohteena olevalla unionin toimielimellä, elimellä tai virastolla taikka CERT-EU:lla on käytössään;

9) ’poikkeaman käsittelyllä’ direktiivin [ehdotus tarkistetuksi verkko- ja tietoturvadirektiiviksi] 4 artiklan 6 kohdassa tarkoitettua poikkeaman käsittelyä;

10) ’kyberuhkalla’ asetuksen (EU) 2019/881 2 artiklan 8 kohdassa tarkoitettua kyberuhkaa;

11) ’merkittävällä kyberuhkalla’ kyberuhkaa, jonka tarkoituksena on aiheuttaa, jolla saatetaan aiheuttaa tai jolla kyetään aiheuttamaan merkittävä poikkeama;

12) ’haavoittuvuudella’ direktiivin [ehdotus tarkistetuksi verkko- ja tietoturvadirektiiviksi] 4 artiklan 8 kohdassa tarkoitettua haavoittuvuutta;

13) ’merkittävällä haavoittuvuudella’ haavoittuvuutta, joka todennäköisesti johtaa merkittävään poikkeamaan, jos sitä käytetään hyväksi;

14) ’kyberturvallisuusriskillä’ mitä tahansa kohtuullisesti tunnistettavissa olevaa tilannetta tai tapahtumaa, joka saattaa vaikuttaa haitallisesti verkko- ja tietojärjestelmien turvallisuuteen;

15) ’yhteisellä kyberturvallisuusyksiköllä’ unionissa toimivien eri kyberturvallisuusyhteisöjen yhteistyötä varten perustettua virtuaalista ja fyysistä alustaa, jossa keskitytään toimien operatiiviseen ja tekniseen koordinointiin 23 päivänä kesäkuuta 2021 annetussa komission suosituksessa tarkoitetuissa suurissa rajat ylittävissä kyberturvallisuusuhkissa ja -poikkeamissa;

16) ’kyberturvallisuuden perustasolla’ kyberturvallisuussääntöjen vähimmäisjoukkoa, jota verkko- ja tietojärjestelmien sekä niiden tarjoajien ja käyttäjien on noudatettava kyberturvallisuusriskien minimoimiseksi.

II luku
TOIMENPITEET YHTEISEN KORKEAN KYBERTURVATASON VARMISTAMISEKSI

4 artikla
Riskien hallinta ja valvonta

1. Unionin kukin toimielin, elin ja virasto laatii ylimmän johtonsa valvonnassa sisäisen kyberturvallisuusriskien hallinta- ja valvontakehyksen, jäljempänä ’kehys’, tukemaan kyseisen yksikön toimeksiantoa ja käyttäen institutionaalista itsemääräämisoikeuttaan. Tätä työtä valvotaan kyseisen yksikön 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 toimielimen, elimen tai viraston koko tietotekninen ympäristö, mukaan lukien sen tiloissa oleva tietotekninen ympäristö, pilvipalveluympäristöissä olevat tai kolmansien osapuolten ylläpitämät ulkoistetut resurssit ja palvelut, mobiililaitteet, yritysverkot, internetiin liittämättömät

liiketoiminnan verkot ja kaikki tietotekniseen ympäristöön liitetyt laitteet. Kehyksessä on otettava huomioon toiminnan jatkuvuus ja kriisitilanteiden hallinta, toimitusketjun turvallisuus sekä sellaisten inhimillisten riskien hallinta, jotka voisivat vaikuttaa unionin asianomaisen toimielimen, elimen tai viraston kyberturvallisuuteen.

3. Unionin kunkin toimielimen, elimen ja viraston 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.

4. Unionin kullakin toimielimellä, elimellä ja virastolla on oltava käytössä tehokkaat mekanismit sen varmistamiseksi, että riittävä prosenttiosuus tietotekniikkamenoista käytetään kyberturvallisuuteen.

5. Unionin kukin toimielin, elin ja virasto nimittää paikallisen kyberturvallisuusvastaavan tai vastaavan toimenhaltijan, joka toimii keskitettynä yhteyspisteenä kyberturvallisuuden kaikissa näkökohdissa.

5 artikla
Kyberturvallisuuden perustaso

1. Unionin kunkin toimielimen, elimen ja viraston ylin johto hyväksyy kyberturvallisuuden perustason 4 artiklan 1 kohdassa tarkoitetussa kehyksessä eriteltyjen riskien torjumiseksi. Se tekee tämän tukeakseen toimeksiantoaan ja käyttäen institutionaalista itsemääräämisoikeuttaan. Kyberturvallisuuden perustason on oltava käytössä viimeistään … päivänä …kuuta … [18 kuukauden kuluttua tämän asetuksen voimaantulosta], ja sen on katettava liitteessä I luetellut osa-alueet ja liitteessä II luetellut toimenpiteet.

2. Unionin kunkin toimielimen, elimen ja viraston ylempi johto osallistuu säännöllisesti erityiskoulutukseen riittävien tietojen ja taitojen hankkimiseksi, jotta he voivat ymmärtää ja arvioida kyberturvallisuusriskejä ja -hallintakäytäntöjä sekä niiden vaikutusta organisaation toimintoihin.

6 artikla
Kehitystason arvioinnit

Unionin kukin toimielin, elin tai virasto suorittaa vähintään joka kolmas vuosi kyberturvallisuuden kehitystason arvioinnin ja sisällyttää siihen kaikki 4 artiklassa tarkoitetut tietoteknisen ympäristönsä osatekijät ottaen huomioon 13 artiklan nojalla hyväksytyt asiaan liittyvät ohjeasiakirjat ja suositukset.

7 artikla
Kyberturvallisuussuunnitelmat

1. Kehitystason arvioinnista saatujen johtopäätösten perusteella ja ottaen huomioon 4 artiklan nojalla tunnistetut resurssit ja riskit unionin kukin toimielin, elin ja virasto hyväksyy kyberturvallisuussuunnitelman ilman aiheetonta viivytystä sen jälkeen, kun riskien hallinta- ja valvontakehys sekä kyberturvallisuuden perustaso on määritetty. Suunnitelman tavoitteena on nostaa asianomaisen yksikön yleistä kyberturvallisuutta ja edistää siten yhteisen korkean kyberturvatason saavuttamista tai parantamista unionin kaikissa toimielimissä, elimissä ja virastoissa. Yksikön toimeksiannon

tukemiseksi sen institutionaalisen itsemääräämisoikeuden pohjalta suunnitelman on sisällettävä vähintään liitteessä I luetellut osa-alueet, liitteessä II luetellut toimenpiteet sekä poikkeamiin varautumiseen ja reagoimiseen ja niistä toipumiseen liittyvät toimenpiteet, kuten turvallisuuden seuranta ja kirjaaminen. Suunnitelmaa on tarkistettava vähintään joka kolmas vuosi 6 artiklan mukaisesti tehtyjen kehitystason arviointien perusteella.

2. Kyberturvallisuussuunnitelman on sisällettävä henkilöstön jäsenten tehtävät ja vastuut sen täytäntöönpanossa.

3. Kyberturvallisuussuunnitelmassa on otettava huomioon CERT-EU:n julkaisemat soveltuvat ohjeasiakirjat ja suositukset.

8 artikla
Täytäntöönpano

1. Sen jälkeen, kun kehitystason arvioinnit on suoritettu, unionin toimielimet, elimet ja virastot toimittavat ne toimielinten väliselle kyberturvallisuuslautakunnalle. Sen jälkeen, kun kyberturvallisuussuunnitelmat on tehty, unionin toimielimet, elimet ja virastot ilmoittavat niiden valmistumisesta toimielinten väliselle kyberturvallisuuslautakunnalle. Kyberturvallisuuslautakunnan pyynnöstä ne raportoivat tämän luvun erityisistä näkökohdista.

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

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 toimielimissä, elimissä ja virastoissa;

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

3. IICB koostuu kolmesta unionin virastojen verkoston (EUAN) nimittämästä edustajasta, jotka nimitetään tieto- ja viestintätekniikkaa käsittelevän neuvoa-antavan komitean ehdotuksesta ja edustavat omaa tietoteknistä ympäristöään käyttävien virastojen ja elinten etuja, sekä yhdestä kunkin seuraavan nimeämästä edustajasta:

   a) Euroopan parlamentti;

   b) Euroopan unionin neuvosto;

   c) Euroopan komissio;

   d) Euroopan unionin tuomioistuin;

   e) Euroopan keskuspankki;

   f) Euroopan tilintarkastustuomioistuin;

g) Euroopan ulkosuhdehallinto;

h) Euroopan sosiaali- ja talouskomitea;

i) Euroopan alueiden komitea;

j) Euroopan investointipankki;

k) Euroopan unionin kyberturvallisuusvirasto.

Jäseniä voi avustaa varajäsen. Puheenjohtaja voi kutsua muita edellä lueteltujen organisaatioiden tai muiden unionin toimielinten, elinten ja virastojen edustajia osallistumaan IICB:n kokouksiin ilman äänioikeutta.

4. IICB vahvistaa sisäisen työjärjestyksensä.

5. IICB nimeää sisäisen työjärjestyksensä mukaisesti jäsentensä keskuudesta puheenjohtajan neljän vuoden ajaksi. Hänen sijaisestaan tulee IICB:n täysjäsen samaksi ajaksi.

6. IICB kokoontuu 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 tai hänen sijaisensa osallistuu IICB:n kokouksiin, ellei IICB toisin päätä.

10. Komissio huolehtii IICB:n sihteeristötehtävistä.

11. Edustajat, jotka unionin virastojen verkosto on nimittänyt tieto- ja viestintätekniikkaa käsittelevän neuvoa-antavan komitean ehdotuksesta, välittävät IICB:n päätökset unionin virastoille ja yhteisyrityksille. 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. IICB voi toimia yksinkertaistettua kirjallista menettelyä noudattaen puheenjohtajan aloitteesta, jolloin asianomainen päätös katsotaan hyväksytyksi puheenjohtajan asettamassa määräajassa, jollei joku jäsenistä vastusta sitä.

13. IICB voi nimetä toimeenpanevan komitean avustamaan IICB:tä sen työssä ja siirtää komitealle osan tehtävistään ja valtuuksistaan. IICB vahvistaa toimeenpanevan komitean työjärjestyksen, mukaan lukien sen tehtävät ja valtuudet sekä sen jäsenten toimikaudet.

10 artikla
IICB:n tehtävät

Vastuitaan hoitaessaan IICB:n tehtävänä on erityisesti

a) tarkastella CERT-EU:lta pyydettyjä kertomuksia, jotka koskevan tämän asetuksen täytäntöönpanon tilaa unionin toimielimissä, elimissä ja virastoissa;

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;

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 yksikköjen välillä 17 artiklan nojalla tehdyt yhteistyöjärjestelyt, palvelutasojärjestelyt tai palvelutasosopimukset;

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

11 artikla
Vaatimusten noudattaminen

IICB seuraa tämän asetuksen sekä hyväksyttyjen ohjeasiakirjojen, suositusten ja toimintakehotusten täytäntöönpanoa unionin toimielimissä, elimissä ja virastoissa. Jos IICB katsoo, että unionin toimielimet, elimet tai virastot 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 toimielimen, elimen tai viraston sisäisten menettelyjen soveltamista

a) antaa varoituksen; jos se on tarpeen huomattavan kyberturvallisuusriskin vuoksi, varoituksen yleisö on rajattava asianmukaisesti;

b) suositella, että asiaankuuluva tarkastusyksikkö tekee tarkastuksen.

IV luku
CERT-EU

12 artikla
CERT-EU:n tarkoitus ja tehtävät

1. CERT-EU:n, joka on unionin kaikkien toimielinten, elinten ja virastojen itsenäinen toimielinten välinen kyberturvallisuuskeskus, tarkoituksena on edistää unionin kaikkien toimielinten, elinten ja virastojen turvallisuusluokittelemattoman tietoteknisen ympäristön turvallisuutta neuvomalla niitä kyberturvallisuusasioissa, auttamalla niitä ehkäisemään, havaitsemaan ja lieventämään poikkeamia ja reagoimaan niihin sekä toimimalla niiden kyberturvallisuutta koskevan tietojenvaihdon ja poikkeamiin reagoimisen koordinointikeskuksena.

2. CERT-EU hoitaa seuraavia tehtäviä unionin toimielimille, elimille ja virastoille:

a) niiden tukeminen tämän asetuksen täytäntöönpanossa ja tämän asetuksen soveltamisen koordinoinnin edistäminen 13 artiklan 1 kohdassa lueteltujen toimenpiteiden tai IICB:n pyytämien lisäkertomusten avulla;

b) niiden tukeminen 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) unionin toimielinten, elinten ja virastojen kohtaamista kyberuhkista raportointi ja EU:n kyberturvallisuuden tilannekuvan parantaminen.

3. CERT-EU tukee 23 päivänä kesäkuuta 2021 annetun komission suosituksen mukaisesti perustettua yhteistä kyberturvallisuusyksikköä muun muassa seuraavilla osa-alueilla:

a) varautuminen, poikkeamien koordinointi, tiedonvaihto ja kriisinhallinta teknisellä tasolla unionin toimielimiin, elimiin ja virastoihin liittyvissä tapauksissa;

b) operatiivinen yhteistyö tietoturvaloukkauksiin reagoivien kansallisten yksiköiden (CSIRT-yksiköt) verkostoa, myös keskinäistä avunantoa, ja laajempaa kyberturvallisuusyhteisöä koskevissa asioissa;

c) uhkatiedustelutieto, mukaan lukien tilannekuva;

d) kaikki aihepiirit, joilla tarvitaan CERT-EU:n kyberturvallisuuteen liittyvää teknistä asiantuntemusta.

4. CERT-EU tekee jäsenneltyä yhteistyötä Euroopan unionin kyberturvallisuusviraston 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 toimielinten, elinten ja virastojen tietoteknisen ympäristön kyberturvallisuutta, palvelutasosopimusten perusteella ja saatavilla olevien resurssien mukaan;

b) palvelut, joilla tuetaan muita kuin toimielinten, elinten ja virastojen tietoteknisen ympäristön suojaamiseksi toteutettavia kyberturvallisuustoimia tai -hankkeita, kirjallisten sopimusten perusteella ja IICB:n etukäteisellä hyväksynnällä;

c) palvelut, joilla tuetaan sellaisten muiden kuin unionin toimielinten, elinten ja virastojen organisaatioiden, jotka tekevät tiivistä yhteistyötä unionin toimielinten, elinten ja virastojen 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 tai suositella osallistumista jo käytössä oleviin harjoituksiin tiiviissä yhteistyössä Euroopan unionin kyberturvallisuusviraston kanssa unionin toimielinten, elinten ja virastojen kyberturvatason testaamiseksi.

7. CERT-EU voi avustaa unionin toimielimiä, elimiä ja virastoja turvallisuusluokitelluissa tietoteknisissä ympäristöissä tapahtuvissa poikkeamissa, jos unionin asianomainen toimielin, elin tai virasto sitä nimenomaisesti pyytää.

13 artikla
Ohjeasiakirjat, suositukset ja toimintakehotukset

1. CERT-EU tukee tämän asetuksen täytäntöönpanoa antamalla

   a) toimintakehotuksia, joissa kuvaillaan kiireellisiä turvatoimenpiteitä, jotka unionin toimielimiä, elimiä ja virastoja kehotetaan toteuttamaan tietyssä määräajassa;

   b) IICB:lle ehdotuksia ohjeasiakirjoiksi, jotka on suunnattu kaikille unionin toimielimille, elimille ja virastoille tai tietylle unionin toimielinten, elinten ja virastojen alaryhmälle;

   c) IICB:lle ehdotuksia suosituksiksi, jotka on suunnattu yksittäisille unionin toimielimille, elimille ja virastoille.

2. Ohjeasiakirjat ja suositukset voivat sisältää

   a) yksityiskohtaisia sääntöjä kyberturvallisuusriskien hallinnasta ja kyberturvallisuuden perustasosta tai niiden parantamisesta;

   b) yksityiskohtaisia sääntöjä kehitystason arvioinneista ja kyberturvallisuussuunnitelmista; ja

   c) tarvittaessa yhteisen teknologian, arkkitehtuurin ja niihin liittyvien parhaiden käytäntöjen käytöstä, jotta voidaan saavuttaa yhteentoimivuus ja direktiivin [ehdotus tarkistetuksi verkko- ja tietoturvadirektiiviksi] 4 artiklan 10 kohdassa tarkoitetut yhteiset standardit.

3. IICB voi hyväksyä ohjeasiakirjoja tai suosituksia CERT-EU:n ehdotuksesta.

4. IICB voi kehottaa CERT-EU:ta antamaan tai peruuttamaan toimintakehotuksen tai ehdotuksen ohjeasiakirjoiksi tai suosituksiksi taikka muokkaamaan niitä.

14 artikla
CERT-EU:n johtaja

CERT-EU:n johtaja toimittaa säännöllisesti kertomuksia IICB:lle ja IICB:n puheenjohtajalle 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 1 kohdassa tarkoitetut kertomukset.

15 artikla
Rahoitus- ja henkilöstöasiat

1. Komissio nimittää CERT-EU:n johtajan saatuaan IICB:n yksimielisen hyväksynnän. 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. 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, 3, 4 ja 6 kohdan ja 13 artiklan 1 kohdan nojalla tarjoamat palvelut EU:n yleiseen hallintoon tarkoitetusta monivuotisen rahoituskehyksen otsakkeesta rahoitetuille unionin toimielimille, elimille ja virastoille, rahoitetaan komission talousarvion erillisestä budjettikohdasta. CERT-EU:lle varatut virat esitetään komission henkilöstötaulukon alaviitteessä.

4. Muut kuin 3 kohdassa tarkoitetut unionin toimielimet, elimet ja virastot 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 yksikkö 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[8] 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 toimielimiltä, elimiltä ja virastoilta. Tulot kohdennetaan kustannuksia tukeviin budjettikohtiin.

16 artikla

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

1. CERT-EU tekee yhteistyötä ja vaihtaa tietoja jäsenvaltioissa vastaavaa tehtävää hoitavien kansallisten elinten, muun muassa CERT-yksiköiden, kansallisten kyberturvallisuuskeskusten, CSIRT-yksiköiden ja direktiivin [ehdotus NIS 2 -direktiiviksi] 8 artiklassa tarkoitettujen keskitettyjen yhteyspisteiden, kanssa kyberuhkista, haavoittuvuuksista ja poikkeamista, mahdollisista vastatoimista ja kaikista asioista, jotka ovat merkityksellisiä unionin toimielinten, elinten ja virastojen tietoteknisten ympäristöjen suojaamisen parantamisen kannalta, myös direktiivin [ehdotus tarkistetuksi verkko- ja tietoturvadirektiiviksi] 13 artiklassa tarkoitetun CSIRT-verkoston kautta.

2. CERT-EU voi vaihtaa poikkeamakohtaisia tietoja jäsenvaltioissa vastaavaa tehtävää hoitavien kansallisten elinten kanssa, jotta voidaan helpottaa samankaltaisten kyberuhkien tai -poikkeamien havaitsemista, ilman vaikutuksen kohteena olevan unionin toimielimen, elimen tai viraston suostumusta. CERT-EU voi vaihtaa sellaisia poikkeamakohtaisia tietoja, joista käy ilmi kyberturvallisuuspoikkeaman kohteen identiteetti, ainoastaan poikkeaman kohteena olleen tahon suostumuksella.

[8] 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).

17 artikla

CERT-EU:n yhteistyö muiden kuin jäsenvaltioiden vastaavien elinten kanssa

1. CERT-EU voi tehdä yhteistyötä muiden kuin jäsenvaltioiden vastaavien 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:n on pyydettävä ennakolta IICB:ltä hyväksyntä kaikkien tällaisten vastaavien elinten kanssa tehtävälle yhteistyölle, myös puitteissa, joissa EU:n ulkopuoliset vastaavat elimet tekevät yhteistyötä jäsenvaltioiden kansallisten vastaavien elinten 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 etukäteen hyväksynnän tällaisten kumppanien kanssa tehtävälle laajemmalle yhteistyölle.

3. CERT-EU voi vaikutuksen kohteena olevan unionin toimielimen, elimen tai viraston suostumuksella antaa poikkeamaan liittyviä tietoja kumppaneille, jotka voivat auttaa poikkeaman analysoinnissa.

V luku
YHTEISTYÖ- JA RAPORTOINTIVELVOITTEET

18 artikla

Tietojen käsittely

1. CERT-EU sekä unionin toimielimet, elimet ja virastot 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[9] säännöksiä, myös kyseisen asetuksen mukaista velvoitetta kuulla muita unionin toimielimiä, elimiä ja virastoja, kun pyyntö koskee niiden asiakirjoja.

3. Tämän asetuksen mukaisesti suoritettavaan henkilötietojen käsittelyyn sovelletaan Euroopan parlamentin ja neuvoston asetusta (EU) 2018/1725.

4. CERT-EU sekä siihen osallistuvat unionin toimielimet, elimet ja virastot noudattavat tietojen käsittelyssä asetuksessa [ehdotus asetukseksi tietoturvallisuudesta] vahvistettuja sääntöjä.

5. Kaikki yhteydenotot, joita kansalliset turvallisuus- tai tiedustelupalvelut toteuttavat tai pyrkivät toteuttamaan CERT-EU:n kanssa, on ilman aiheetonta viivytystä annettava tiedoksi komission turvallisuusosastolle ja IICB:n puheenjohtajalle.

[9] 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).

19 artikla

Tiedonjakovelvoitteet

1. Jotta CERT-EU kykenee koordinoimaan haavoittuvuuksien hallintaa ja poikkeamiin reagoimista, se voi pyytää unionin toimielimiä, elimiä ja virastoja toimittamaan sille tietoa niiden tietoteknisiin järjestelmiin liittyvistä selvityksistä, jotka ovat merkityksellisiä CERT-EU:n tuen kannalta. Pyynnön kohteena olevan toimielimen, elimen tai viraston on toimitettava pyydetyt tiedot ja niihin myöhemmin tehtävät muutokset ilman aiheetonta viivytystä.

2. Unionin toimielimet, elimet ja virastot 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 sellaisia poikkeamakohtaisia tietoja, joista käy ilmi poikkeaman vaikutuksen kohteena olevan unionin toimielimen, elimen tai viraston identiteetti, ainoastaan kyseisen toimielimen, elimen tai viraston suostumuksella. CERT-EU voi vaihtaa sellaisia poikkeamakohtaisia tietoja, joista käy ilmi kyberturvallisuuspoikkeaman kohteen identiteetti, ainoastaan vaikutuksen kohteena olevan yksikön suostumuksella.

4. Tiedonjakovelvoitteet eivät koske EU:n turvallisuusluokiteltuja tietoja eivätkä tietoja, jotka unionin toimielin, elin tai virasto on saanut jäsenvaltion turvallisuus- tai tiedustelupalvelulta tai lainvalvontaviranomaiselta nimenomaisesti sillä ehdolla, ettei tietoja jaeta CERT-EU:n kanssa.

20 artikla

Ilmoitusvelvoitteet

1. Kaikki unionin toimielimet, elimet ja virastot antavat CERT-EU:lle ensimmäisen ilmoituksen merkittävistä kyberuhkista, haavoittuvuuksista ja poikkeamista ilman aiheetonta viivytystä ja joka tapauksessa viimeistään 24 tunnin kuluessa siitä, kun tällainen uhka, haavoittuvuus tai poikkeama on tullut niiden tietoon.

   Unionin asianomainen toimielin, elin tai virasto voi asianmukaisesti perustelluissa tapauksissa ja CERT-EU:n suostumuksella poiketa edellisessä kohdassa säädetystä määräajasta.

2. Unionin toimielimet, elimet ja virastot ilmoittavat lisäksi CERT-EU:lle ilman aiheetonta viivytystä kyberuhkien, haavoittuvuuksien ja poikkeamien asianmukaiset tekniset tiedot, jotka mahdollistavat ongelmien havaitsemisen ennakolta, poikkeamiin reagoimisen tai lieventävien toimenpiteiden toteuttamisen. Ilmoituksen on sisällettävä seuraavat tiedot, jos ne ovat saatavilla:

   a) asiaan liittyvät vaarantumista kuvaavat indikaattorit;

   b) asiaan liittyvät havaitsemismekanismit;

   c) oletettu vaikutus;

   d) asiaan liittyvät lieventävät toimenpiteet.

3. CERT-EU toimittaa Euroopan unionin kyberturvallisuusvirastolle kuukausittain tiivistelmän, joka sisältää anonymisoidut koontitiedot merkittävistä kyberuhkista, haavoittuvuuksista ja poikkeamista, joista on ilmoitettu 1 kohdan mukaisesti.

4. IICB voi antaa ohjeasiakirjoja tai suosituksia ilmoitusta koskevista säännöistä ja sen sisällöstä. CERT-EU levittää asianmukaiset tekniset tiedot, jotta unionin toimielimet, elimet ja virastot voivat havaita ongelmat ennakolta, reagoida poikkeamiin tai toteuttaa lieventäviä toimenpiteitä.

5. Ilmoitusvelvoitteet eivät koske EU:n turvallisuusluokiteltuja tietoja eivätkä tietoja, jotka unionin toimielin, elin tai virasto on saanut jäsenvaltion turvallisuus- tai tiedustelupalvelulta tai lainvalvontaviranomaiselta nimenomaisesti sillä ehdolla, ettei tietoja jaeta CERT-EU:n kanssa.

21 artikla

Poikkeamiin reagoimisen koordinointi ja merkittäviä poikkeamia koskeva yhteistyö

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

   a) unionin toimielimet, elimet ja virastot;

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

2. CERT-EU edistää unionin toimielinten, elinten ja virastojen keskinäistä koordinointia poikkeamiin reagoimisen alalla muun muassa seuraavilla osa-alueilla:

   a) osallistuminen johdonmukaiseen ulkoiseen viestintään;

   b) keskinäinen avunanto;

   c) operatiivisten resurssien optimaalinen käyttö;

   d) koordinointi muiden unionin tason kriisinhallintamekanismien kanssa.

3. CERT-EU tukee unionin toimielimiä, elimiä ja virastoja kyberuhkia, haavoittuvuuksia ja poikkeamia koskevan tilannekuvan muodostamisessa.

4. IICB antaa ohjeita 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

Laajat hyökkäykset

1. CERT-EU koordinoi unionin toimielinten, elinten ja virastojen kanssa reagoimista laajoihin hyökkäyksiin. Se ylläpitää luetteloa teknisestä asiantuntemuksesta, jota tarvitaan poikkeamiin reagoimiseksi tällaisten hyökkäysten yhteydessä.

2. Unionin toimielimet, elimet ja virastot osallistuvat teknisen asiantuntemuksen luettelon kokoamiseen toimittamalla vuosittain päivitetyn luettelon organisaationsa käytettävissä olevista asiantuntijoista ja heidän teknisestä erityisosaamisestaan.

3. CERT-EU voi myös unionin asianomaisten toimielinten, elinten ja virastojen suostumuksella pyytää 2 kohdassa tarkoitettuihin luetteloihin sisältyviä asiantuntijoita osallistumaan laajaan hyökkäykseen reagoimiseen jossakin jäsenvaltiossa yhteisen kyberturvallisuusyksikön menettelyohjeiden mukaisesti.

VI luku
LOPPUSÄÄNNÖKSET

23 artikla
Ensimmäinen talousarvion uudelleen kohdentaminen

Komissio antaa ehdotuksen henkilöstöresurssien ja taloudellisten resurssien uudelleen kohdentamisesta asiaankuuluvista unionin toimielimistä, elimistä ja virastoista 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 ehdottaakseen muutoksia tähän asetukseen.
2. Komissio antaa Euroopan parlamentille ja neuvostolle kertomuksen tämän asetuksen täytäntöönpanosta viimeistään 48 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 aikaisintaan viiden vuoden kuluttua asetuksen voimaantulopäivästä.

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*

SÄÄDÖSEHDOTUKSEEN LIITTYVÄ RAHOITUSSELVITYS

1. PERUSTIEDOT EHDOTUKSESTA/ALOITTEESTA

1.1. Ehdotuksen/aloitteen nimi

1.2. Toimintalohko(t)

1.3. Ehdotus/aloite liittyy

1.4. Tavoite (Tavoitteet)

1.4.1. Yleistavoite (Yleistavoitteet)

1.4.2. Erityistavoite (Erityistavoitteet)

1.4.3. Odotettavissa olevat tulokset ja vaikutukset

1.4.4. Tulosindikaattorit

1.5. Ehdotuksen/aloitteen perustelut

1.5.1. Tarpeet, joihin ehdotuksella/aloitteella vastataan lyhyellä tai pitkällä aikavälillä sekä aloitteen yksityiskohtainen toteutusaikataulu

1.5.2. EU:n osallistumisesta saatava lisäarvo (joka voi olla seurausta eri tekijöistä, kuten koordinoinnin paranemisesta, oikeusvarmuudesta tai toiminnan vaikuttavuuden tai täydentävyyden paranemisesta). EU:n osallistumisesta saatavalla lisäarvolla tarkoitetaan tässä kohdassa arvoa, jonka EU:n osallistuminen tuottaa sen arvon lisäksi, joka olisi saatu aikaan pelkillä jäsenvaltioiden toimilla.

1.5.3. Vastaavista toimista saadut kokemukset

1.5.4. Yhteensopivuus monivuotisen rahoituskehyksen kanssa ja mahdolliset synergiaedut suhteessa muihin kyseeseen tuleviin välineisiin

1.5.5. Arvio käytettävissä olevista rahoitusvaihtoehdoista, mukaan lukien mahdollisuudet määrärahojen uudelleenkohdentamiseen

1.6. Ehdotetun toimen/aloitteen kesto ja rahoitusvaikutukset

1.7. Hallinnointitapa (Hallinnointitavat)

2. HALLINNOINTI

2.1. Seuranta- ja raportointisäännöt

2.2. Hallinnointi- ja valvontajärjestelmä(t)

2.2.1. Perustelut ehdotetu(i)lle hallinnointitavalle(/-tavoille), rahoituksen toteutusmekanismille(/-mekanismeille), maksujärjestelyille sekä valvontastrategialle

2.2.2. Tiedot todetuista riskeistä ja niiden vähentämiseksi käyttöön otetuista sisäisistä valvontajärjestelmistä

2.2.3. Valvonnan kustannustehokkuutta (valvontakustannusten suhde hallinnoitujen varojen arvoon) koskevat arviot ja perustelut sekä arviot maksujen suoritusajankohdan ja toimen päättämisajankohdan odotetuista virheriskitasoista

2.3. Toimenpiteet petosten ja sääntöjenvastaisuuksien ehkäisemiseksi

3. EHDOTUKSEN/ALOITTEEN ARVIOIDUT RAHOITUSVAIKUTUKSET

3.1. Kyseeseen tulevat monivuotisen rahoituskehyksen otsakkeet ja menopuolen budjettikohdat

3.2. Arvioidut vaikutukset määrärahoihin

3.2.1. Yhteenveto arvioiduista vaikutuksista toimintamäärärahoihin

3.2.2. Arvioidut toimintamäärärahoista rahoitetut tuotokset

3.2.3. Yhteenveto arvioiduista vaikutuksista hallintomäärärahoihin

3.2.4. Yhteensopivuus nykyisen monivuotisen rahoituskehyksen kanssa

3.2.5. Ulkopuolisten tahojen rahoitusosuudet

3.3. Arvioidut vaikutukset tuloihin

SÄÄDÖSEHDOTUKSEEN LIITTYVÄ RAHOITUSSELVITYS

1. PERUSTIEDOT EHDOTUKSESTA/ALOITTEESTA

1.1. Ehdotuksen/aloitteen nimi

Ehdotus Euroopan parlamentin ja neuvoston asetukseksi toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi unionin toimielimissä, elimissä ja laitoksissa

1.2. Toimintalohko(t)

EU:n yleinen hallinto

Ehdotus koskee toimenpiteitä, joilla varmistetaan yhteinen korkea kyberturvataso unionin toimielimissä, elimissä ja virastoissa

1.3. Ehdotus/aloite liittyy

☑uuteen toimeen

☐ uuteen toimeen, joka perustuu pilottihankkeeseen tai valmistelutoimeen[10]

☐ käynnissä olevan toimen jatkamiseen

☑ yhden tai useamman toimen sulauttamiseen tai uudelleen suuntaamiseen johonkin toiseen/uuteen toimeen

1.4. Tavoite (Tavoitteet)

1.4.1. Yleistavoite (Yleistavoitteet)

– Luoda puitteet, joilla varmistetaan yhteinen korkea kyberturvataso unionin toimielimissä, elimissä ja virastoissa

– Uusi oikeusperusta CERT-EU:n toimeksiannon ja rahoituksen vahvistamiseksi

1.4.2. Erityistavoite (Erityistavoitteet)

(1) Asettaa unionin toimielimille, elimille ja virastoille velvoitteet perustaa sisäisen kyberturvallisuusriskien hallinta- ja valvontakehys

(2) Asettaa unionin toimielimille, elimille ja virastoille velvoitteet raportoida sisäisen kyberturvallisuusriskien hallinta- ja valvontakehyksestään sekä kyberturvallisuuspoikkeamista

(3) Asettaa unionin toimielinten, elinten ja virastojen kyberturvallisuuskeskuksen (CERT-EU) organisaatioon ja toimintaan sekä toimielinten välisen kyberturvallisuuslautakunnan (IICB) organisaatioon ja toimintaan sovellettavat säännöt

(4) Osallistua yhteisen kyberturvallisuusyksikön toimintaan

1.4.3. Odotettavissa olevat tulokset ja vaikutukset

Selvitys siitä, miten ehdotuksella/aloitteella on tarkoitus vaikuttaa edunsaajien/kohderyhmän tilanteeseen

[10] Sellaisina kuin nämä on määritelty varainhoitoasetuksen 58 artiklan 2 kohdan a ja b alakohdassa.

– Sisäiset kyberturvallisuusriskien hallinta- ja valvontakehykset, kyberturvallisuuden perustasot, säännölliset kehitystason arvioinnit ja kyberturvallisuussuunnitelmat unionin toimielimissä, elimissä ja virastoissa – Kyberuhkien sietokyvyn ja kyvyn reagoida poikkeamiin parantaminen unionin toimielimissä, elimissä ja virastoissa – CERT-EU:n nykyaikaistaminen – Osallistuminen yhteisen kyberturvallisuusyksikön toimintaan

1.4.4. Tulosindikaattorit

Selvitys siitä, millaisin indikaattorein ehdotuksen/aloitteen etenemistä ja tuloksia seurataan.

– Käytössä olevat kehykset ja perustasot, säännölliset kehitystason arvioinnit ja kyberturvallisuussuunnitelmat unionin toimielimissä, elimissä ja virastoissa – Parantunut poikkeamien käsittely – Lisääntynyt kyberturvallisuusriskejä koskeva tietoisuus unionin toimielinten, elinten ja virastojen ylemmällä johtotasolla – Tasaisesti jakautuneet tieto- ja viestintätekniikan turvallisuusmenot prosenttiosuutena tieto- ja viestintätekniikan kokonaismenoista – Vahva johtajuus IICB:ssä ja CERT-EU:ssa – Lisääntynyt tiedonvaihto unionin toimielinten, elinten ja virastojen välillä sekä asiaankuuluvien EU:ssa olevien elinten ja sidosryhmien kanssa – Lisääntynyt kyberturvallisuusyhteistyö asiaankuuluvien EU:ssa olevien elinten ja sidosryhmien kanssa CERT-EU:n ja ENISAn kautta

1.5. Ehdotuksen/aloitteen perustelut

1.5.1. Tarpeet, joihin ehdotuksella/aloitteella vastataan lyhyellä tai pitkällä aikavälillä sekä aloitteen yksityiskohtainen toteutusaikataulu

Ehdotuksen tavoitteena on parantaa unionin toimielinten, elinten ja virastojen kyberuhkien sietokykyä, vähentää häiriönsietokyvyssä esiintyvää epätasapainoa näiden yksiköiden välillä ja parantaa yhteisen tilannetietoisuuden tasoa ja yhteisiä valmiuksia valmistautua ja reagoida poikkeamiin. Ehdotus on täysin johdonmukainen ja sopusoinnussa muiden asiaan liittyvien aloitteiden ja erityisesti ehdotuksen direktiiviksi toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi koko unionissa ja direktiivin (EU) 2016/1148 kumoamisesta [ehdotus tarkistetuksi verkko- ja tietoturvadirektiiviksi] kanssa. Ehdotus on olennainen osa EU:n turvallisuusunionistrategiaa ja EU:n kyberturvallisuusstrategiaa digitaaliselle vuosikymmenelle. Euroopan komission on määrä antaa asetusehdotus lokakuussa 2021, Euroopan parlamentin ja neuvoston odotetaan hyväksyvän asetuksen vuonna 2022, ja säännöksiä sovelletaan asetuksen voimaantulosta alkaen. Tässä rahoitusselvityksessä esitettyjen rahoitus- ja henkilöstövaikutusten on määrä alkaa vuonna 2023. Valmisteluvaihe on jo alkanut vuonna 2021, mutta valmistelutoimet vuosina 2021 ja 2022 eivät sisälly ehdotuksen rahoitusvaikutuksiin.

1.5.2. EU:n osallistumisesta saatava lisäarvo (joka voi olla seurausta eri tekijöistä, kuten koordinoinnin paranemisesta, oikeusvarmuudesta tai toiminnan vaikuttavuuden tai

täydentävyyden paranemisesta). EU:n osallistumisesta saatavalla lisäarvolla tarkoitetaan tässä kohdassa arvoa, jonka EU:n osallistuminen tuottaa sen arvon lisäksi, joka olisi saatu aikaan pelkillä jäsenvaltioiden toimilla.

Syyt siihen, miksi toimi toteutetaan EU:n tasolla (ennen toteutusta)
Kohdistettuja hyökkäyksiä suorittavien toimijoiden toteuttamien, unionin toimielimiin, elimiin ja virastoihin vaikuttaneiden merkittävien poikkeamien määrä kasvoi merkittävästi vuodesta 2019 vuoteen 2021. Vuoden 2021 ensimmäisellä puoliskolla havaittiin yhtä paljon merkittäviä poikkeamia kuin koko vuoden 2020 aikana. Tämä näkyi myös CERT-EU:n vuonna 2020 analysoimien forensisten peilikuvatiedostojen (kopiot hyökkäysten kohteena olevien järjestelmien tai laitteiden sisällöstä) määrässä, joka kolminkertaistui vuodesta 2019. Samalla merkittävien poikkeamien määrä yli kymmenkertaistui vuodesta 2018.
Kyberturvallisuuden kehitystasot vaihtelevat huomattavasti eri yksiköiden välillä.[11] Tällä asetuksella varmistetaan, että kaikki unionin toimielimet, elimet ja virastot toteuttavat turvatoimenpiteiden perustason ja tekevät yhteistyötä, jonka tavoitteena on unionin hallinnon avoin ja tehokas toiminta.
Säilytettävät järjestelmät kuuluvat unionin toimielinten, elinten ja virastojen itsemääräämisoikeuden piiriin ja kyseiset yksiköt hallinnoivat niitä; jäsenvaltiot eivät voineet luoda ehdotettuja toimia.

1.5.3. Vastaavista toimista saadut kokemukset

Verkko- ja tietoturvadirektiivi on ollut ensimmäinen horisontaalinen sisämarkkinoiden väline, jonka tarkoituksena on ollut parantaa unionin verkkojen ja järjestelmien häiriönsietokykyä kyberturvallisuusriskejä vastaan. Sen jälkeen, kun se tuli voimaan vuonna 2016, se on osaltaan parantanut merkittävästi yhteistä kyberturvatasoa jäsenvaltioissa. Ehdotuksella tarkistetuksi verkko- ja tietoturvadirektiiviksi pyritään parantamaan näitä toimenpiteitä.
Asetuksen avulla pyritään toteuttamaan vastaavia toimenpiteitä unionin toimielimissä, elimissä ja virastoissa.

1.5.4. Yhteensopivuus monivuotisen rahoituskehyksen kanssa ja mahdolliset synergiaedut suhteessa muihin kyseeseen tuleviin välineisiin

Ehdotus on monivuotisen rahoituskehyksen mukainen ja olennainen osa EU:n turvallisuusunionistrategiaa sekä EU:n kyberturvallisuusstrategiaa digitaaliselle vuosikymmenelle.
Ehdotuksen tarkoituksena on ottaa käyttöön toimenpiteitä, joilla varmistetaan yhteinen korkea kyberturvataso unionin toimielimissä, elimissä ja virastoissa. Ehdotus on ehdotuksen direktiiviksi toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi koko unionissa ja direktiivin (EU) 2016/1148 kumoamisesta [ehdotus tarkistetuksi verkko- ja tietoturvadirektiiviksi] mukainen.

[11] Viite: [Euroopan tilintarkastustuomioistuimen erityiskertomus kyberturvallisuudesta unionin toimielimissä, elimissä ja virastoissa].

1.5.5. Arvio käytettävissä olevista rahoitusvaihtoehdoista, mukaan lukien mahdollisuudet määrärahojen uudelleenkohdentamiseen

CERT-EU:n suorittama tehtävien hallinnointi edellyttää erityisiä profiileja ja ylimääräistä työtaakkaa, jota ei voida hoitaa ilman henkilöstö- ja rahoitusresurssien lisäämistä.

1.6. Ehdotetun toimen/aloitteen kesto ja rahoitusvaikutukset

☐ **kesto on rajattu**

– ☐ toiminta alkaa [PP/KK]VVVV ja päättyy [PP/KK]VVVV.

– ☐ maksusitoumusmäärärahoihin kohdistuvat rahoitusvaikutukset koskevat vuosia YYYY–YYYY ja maksumäärärahoihin kohdistuvat rahoitusvaikutukset vuosia YYYY–YYYY.

☑ **kestoa ei ole rajattu**

– Rahoitusvaikutusten odotetaan alkavan asetuksen voimaantulon jälkeen hyväksytystä ensimmäisestä talousarviosta. Resursseja unionin toimielimiltä ja tärkeimmistä elimistä kohdennettaisiin uudelleen komissiolle ensimmäisenä vuonna, joka katsotaan siirtymävuodeksi; tämä ja muut (uudelleen)kohdentamiset toteutetaan vuotuisten talousarvioiden puitteissa. Jos asetus hyväksytään vuonna 2022, siirtymäkausi on varainhoitovuosi 2023, ja vuonna 2024 toiminta käynnistyy täydessä mittakaavassa.

1.7. Hallinnointitapa (Hallinnointitavat)[12]

☑ **Suora hallinnointi**, jonka komissio ja kukin unionin toimielin, elin ja virasto toteuttaa käyttämällä

– ☑ yksiköitään, myös unionin edustustoissa olevaa henkilöstöään

– ☐ toimeenpanovirastoja

☐ **Hallinnointi yhteistyössä** jäsenvaltioiden kanssa

☐ **Välillinen hallinnointi**, jossa täytäntöönpanotehtäviä on siirretty

– ☐ kolmansille maille tai niiden nimeämille elimille

– ☐ kansainvälisille järjestöille ja niiden erityisjärjestöille (tarkennettava)

– ☐ Euroopan investointipankille tai Euroopan investointirahastolle

– ☐ varainhoitoasetuksen 70 ja 71 artiklassa tarkoitetuille elimille

– ☐ julkisoikeudellisille yhteisöille

– ☐ sellaisille julkisen palvelun tehtäviä hoitaville yksityisoikeudellisille elimille, jotka antavat riittävät rahoitustakuut

– ☐ sellaisille jäsenvaltion yksityisoikeuden mukaisille elimille, joille on annettu tehtäväksi julkisen ja yksityisen sektorin kumppanuuden täytäntöönpano ja jotka antavat riittävät rahoitustakuut

– ☐ henkilöille, joille on annettu tehtäväksi toteuttaa SEU-sopimuksen V osaston mukaisia yhteisen ulko- ja turvallisuuspolitiikan erityistoimia ja jotka nimetään asiaa koskevassa perussäädöksessä.

– *Jos käytetään useampaa kuin yhtä hallinnointitapaa, olisi annettava lisätietoja kohdassa ”Huomautukset”.*

Huomautukset:

Hallinto- ja rahoitusmenettelyjä soveltaessaan CERT-EU toimii komission valvonnassa.

[12] Kuvaukset eri hallinnointitavoista ja viittaukset varainhoitoasetukseen ovat saatavilla budjettipääosaston verkkosivuilla osoitteessa: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx

Asetusehdotuksesta johtuvat lisäresurssit:

Asetusehdotuksen 12 ja 13 artiklan täytäntöönpano johtaa laajennettuun palveluvalikoimaan, johon sisältyy uusia peruspalveluja. Kun toiminta saavuttaa täyden mittakaavansa, tarvitaan seuraavia lisäresursseja (monivuotisen rahoituskehyksen loppuun saakka vuoden 2027 loppuun): 21 kokoaikavastaavaa ja 14,05 miljoonaa euroa.

Talousarvion lisäresurssit jakautuvat eri tehtävien kesken seuraavasti:

(a) 12 artiklan 2 kohdan a, b, c ja e alakohdassa tarkoitettujen unionin toimielinten, elinten ja virastojen tehtävien hoitamiseen: 13,75 kokoaikavastaavaa ja 11,275 miljoonaa euroa;

(b) 12 artiklan 3 kohdassa määriteltyjen tehtävien hoitamiseen (osallistuminen yhteiseen kyberturvallisuusyksikköön): 2 kokoaikavastaavaa ja 381 000 euroa;

(c) 12 artiklan 4 kohdassa määriteltyjen tehtävien hoitamiseen (jäsennelty yhteistyö ENISAn kanssa): 0,25 kokoaikavastaavaa ja 236 000 euroa;

(d) 12 artiklan 6 kohdassa määriteltyjen tehtävien hoitamiseen (kyberturvallisuusharjoitukset): 0,25 kokoaikavastaavaa ja 79 000 euroa;

(e) 12 artiklan 2 kohdan d alakohdassa ja 13 artiklassa määriteltyjen tehtävien hoitamiseen (asetuksen täytäntöönpanoa koskeva analyysi ja raportointi, ohjeasiakirjojen, suositusten ja toimintapyyntöjen laatiminen): 3,75 kokoaikavastaavaa ja 2,079 miljoonaa euroa.

(f) Toimielinten välisen kyberturvallisuuslautakunnan (IICB) sihteeristön tukemiseen liittyvien tehtävien hoitamiseen: 1 kokoaikavastaava.

Yleiskatsaus tämänhetkisistä resursseista ja siirtymisestä täyteen mittakaavaan:

Syyskuussa 2021 CERT-EU toimi seuraavin resurssein:

– vakinaiset virat ja tilapäiset siirrot: 14 kokoaikavastaavaa,

– palvelutasosopimuksilla rahoitettavat sopimussuhteiset toimihenkilöt: 24 kokoaikavastaavaa,

– yhteensä 38 kokoaikavastaavaa.

CERT-EU:n talousarvio vuonna 2020 oli 250 000 euroa komission talousarviosta, 3,5 miljoonaa euroa käyttötarkoitukseensa sidottuja tuloja palvelutasosopimuksista. Yhteensä: 3,75 miljoonaa euroa. Tämä muodosti kokonaisuudessaan CERT-EU:n talousarvion kattaen koulutuksen, laitteistot, ohjelmistot, virkamatkat, tuen, sopimussuhteiset toimihenkilöt ja konferenssit.

Asetus tultua voimaan CERT-EU:n tulevien resurssien odotetaan olevan seuraavat:

– vakinaiset virat: 34 kokoaikavastaavaa,

– sopimussuhteiset toimihenkilöt: 15 kokoaikavastaavaa,

– yhteensä 49 kokoaikavastaavaa eli 11 kokoaikavastaavan nettolisäys.

Vakinaisten ja sopimussuhteisten toimihenkilöiden välisen jakauman muutoksella pyritään varautumaan siihen, että kyberturvallisuuden alan johtavien ammattilaisten palkkaaminen ja säilyttäminen on vaikeaa, koska heitä työmarkkinoilla vähän.

Lisäksi toimielinten välisen kyberturvallisuuslautakunnan tukemiseksi komission tietotekniikan pääosastossa tarvitaan yksi kokoaikainen sopimussuhteinen toimihenkilö.

Asetuksen täytäntöönpano edellyttää näin ollen yhteensä 21 kokoaikavastaavaa (20 kokoaikavastaavaa CERT-EU:lle ja yksi kokoaikavastaava komission tietotekniikan pääosastolle). Tämä kompensoidaan vähentämällä samanaikaisesti CERT-EU:n palveluksessa olevaa 9 kokoaikaista sopimussuhteista toimihenkilöä, jotka rahoitettiin aiemmin palvelutasosopimuksista saaduilla käyttötarkoitukseensa sidotuilla tuloilla.

CERT-EU:n muut kuin henkilöstöresurssit vuonna 2024 siirtymäkauden jälkeen kattavat edellä a–e alakohdassa luetellut tehtävät, ja ne on tarkoitus rahoittaa seuraavasti:

– 8,921 miljoonaa euroa vuodessa unionin toimielimiltä, jotka rahoitetaan unionin talousarvion otsakkeesta 7,

– 2,459 miljoonaa euroa unionin toimielimiltä, elimiltä ja virastoilta, jotka rahoitetaan unionin talousarvion otsakkeista 1–6,

– 2,670 miljoonaa euroa omarahoitteisilta unionin toimielimiltä, elimiltä ja virastoilta.

– CERT-EU:n talousarvio yhteensä: 14,05 miljoonaa euroa.

12 artiklan 5 kohdassa lueteltuja tehtäviä ei kuvata palvelujen luettelossa, vaan ne ovat maksullisia palveluja. Nämä ovat suhteellisen pieniä oheissummia, enimmäkseen tilapäisiä, ja niiden kustannukset peritään palvelujen edunsaajilta palvelutasosopimusten tai kirjallisten sopimusten kautta.

CERT-EU:n henkilöstön rahoitusosuuksien osalta: unionin toimielimet ja tärkeimmät elimet maksavat kohtuullisen osuuden, joka on suhteessa organisaation vakinaisten AD-virkojen osuuteen. Olisi selvitettävä, voivatko EKP ja EIP myös tarjota kohtuullisen osuuden lähettämällä vakinaista henkilöstöä.

2. HALLINNOINTI

2.1. Seuranta- ja raportointisäännöt

Ilmoitetaan sovellettavat aikavälit ja edellytykset.

Komissio tarkastelee IICB:n ja CERT-EU:n avustuksella säännöllisesti asetuksen toimintaa ja raportoi siitä Euroopan parlamentille ja neuvostolle ensimmäisen kerran viimeistään 48 kuukauden kuluttua tämän asetuksen voimaantulosta ja sen jälkeen joka kolmas vuosi.

Tarkasteluissa käytettävät tietolähteet olisivat pääasiassa IICB:n ja CERT-EU:n tietolähteitä. Lisäksi tarvittaessa voitaisiin käyttää erityisiä tiedonkeruuvälineitä, kuten unionin toimielimissä, elimissä ja virastoissa, ENISAssa tai CSIRT-verkostossa tehtäviä kyselytutkimuksia.

2.2. Hallinnointi- ja valvontajärjestelmä(t)

2.2.1. Perustelut ehdotetu(i)lle hallinnointitavalle(/-tavoille), rahoituksen toteutusmekanismille(/-mekanismeille), maksujärjestelyille sekä valvontastrategialle

Asetuksesta johtuvia toimia hallinnoidaan kussakin unionin toimielimessä, elimessä ja virastossa niissä sovellettavien sääntöjen ja määräysten mukaisesti.

CERT-EU:n toimien yleis- ja taloushallinto sisältyy komission hallintoon, ja siinä noudatetaan komissiossa sovellettavia hallinnointi- ja täytäntöönpanomekanismeja, maksutapoja ja valvontaa.

Komission sisäisellä tarkastajalla on CERT-EU:hun nähden samat valtuudet kuin komission yksiköihin nähden.

2.2.2. Tiedot todetuista riskeistä ja niiden vähentämiseksi käyttöön otetuista sisäisistä valvontajärjestelmistä

Hyvin pieni riski, sillä CERT-EU on jo hallinnollisesti yhteydessä tietotekniikan pääosaston pääjohtajaan komission työryhmänä ja IICB:n mallina on toiminut CERT-EU:n nykyinen johtoryhmä. Näin ollen varainhoidon ja sisäisen valvonnan ekosysteemi on jo käytössä.

2.2.3. Valvonnan kustannustehokkuutta (valvontakustannusten suhde hallinnoitujen varojen arvoon) koskevat arviot ja perustelut sekä arviot maksujen suoritusajankohdan ja toimen päättämisajankohdan odotetuista virheriskitasoista

Hankintoja, varainhoitoa ja valvontaa koskevat menettelyt ovat jo käytössä ja hyvin testattuja. Valvonnan kustannustehokkuus ja virheriskitasot vastaavat kunkin unionin toimielimen, elimen tai viraston tasoa ja CERT-EU:n toimien osalta komission tasoa.

2.3. Toimenpiteet petosten ja sääntöjenvastaisuuksien ehkäisemiseksi

Ilmoitetaan käytössä olevat ja suunnitellut ehkäisy- ja suojatoimenpiteet, esimerkiksi petostentorjuntastrategian pohjalta

CERT-EU:n toimiin sovelletaan komission varainhoidon ja sisäisen valvonnan järjestelmiä.

Petosten, lahjonnan ja muiden säännönvastaisuuksien torjumiseksi sovelletaan rajoituksetta Euroopan petostentorjuntaviraston (OLAF) tutkimuksista 11 päivänä syyskuuta 2013 annetun Euroopan parlamentin ja neuvoston asetuksen (EU, Euratom) N:o 883/2013 säännöksiä.

3. EHDOTUKSEN/ALOITTEEN ARVIOIDUT RAHOITUSVAIKUTUKSET

3.1. Kyseeseen tulevat monivuotisen rahoituskehyksen otsakkeet ja menopuolen budjettikohdat

- Talousarviossa jo olevat budjettikohdat

Monivuotisen rahoituskehyksen otsakkeiden ja budjettikohtien mukaisessa järjestyksessä.

Monivuotisen rahoituskehyksen otsake	Budjettikohta	Menolaji	Rahoitusosuudet			
	Numero	JM/EI-JM[13]	EFTA-mailta[14]	ehdokasmailta[15]	kolmansilta mailta	varainhoitoasetuksen 21 artiklan 2 kohdan b alakohdassa tarkoitetut
1–6	Unionin rahoitusosuudet erillisvirastoille ja -elimille kattavat budjettikohdat	JM	EI	EI	EI	EI
7	Henkilöstön palkkoja, tietotekniikkamenoja ja muita hallintomenoja koskevat budjettikohdat EU:n talousarvion eri pääluokissa	EI-JM	EI	EI	EI	EI

- Uudet perustettaviksi esitetyt budjettikohdat

Monivuotisen rahoituskehyksen otsakkeiden ja budjettikohtien mukaisessa järjestyksessä.

Monivuotisen rahoituskehyksen otsake	Budjettikohta	Menolaji	Rahoitusosuudet			
	Numero	JM/EI-JM	EFTA-mailta	ehdokasmailta	kolmansilta mailta	varainhoitoasetuksen 21 artiklan 2 kohdan b alakohdassa tarkoitetut
	–		KYLLÄ/EI	KYLLÄ/EI	KYLLÄ/EI	KYLLÄ/EI

[13] JM = jaksotetut määrärahat; EI-JM = jaksottamattomat määrärahat.
[14] EFTA: Euroopan vapaakauppaliitto.
[15] Ehdokasmaat ja soveltuvin osin Länsi-Balkanin mahdolliset ehdokasmaat.

3.2. Arvioidut vaikutukset määrärahoihin

3.2.1. Yhteenveto arvioiduista vaikutuksista toimintamäärärahoihin

– ☐ Ehdotus/aloite ei edellytä toimintamäärärahoja.

– ☑ Ehdotus/aloite edellyttää toimintamäärärahoja seuraavasti:

milj. euroa (kolmen desimaalin tarkkuudella)

Monivuotisen rahoituskehyksen otsake	1–6	Erillisvirastoille ja -elimille maksettavia rahoitusosuuksia koskevat otsakkeet

Pääosasto: useita			Vuosi **2023**	Vuosi **2024**	Vuosi **2025**	Vuosi **2026**	Vuosi **2027**	**YHTEENSÄ**
○ Toimintamäärärahat								
Unionin rahoitusosuudet erillisvirastoille ja -elimille kattavat budjettikohdat (xx 10 xx xx)[16]	Sitoumukset	(1a)	2,459	2,459	2,459	2,459	2,459	12,293
	Maksut	(2 a)	2,459	2,459	2,459	2,459	2,459	12,293
Tiettyjen ohjelmien määrärahoista katettavat hallintomäärärahat[17]								
Budjettikohta		(3)						
Pääosastojen määrärahat YHTEENSÄ	Sitoumukset	=1a+1b +3	2,459	2,459	2,459	2,459	2,459	12,293
	Maksut	=2a+2b +3	2,459	2,459	2,459	2,459	2,459	12,293

○ Toimintamäärärahat YHTEENSÄ	Sitoumukset	(4)	2,459	2,459	2,459	2,459	2,459	12,293

[16] Virallisen budjettinimikkeistön mukaisesti.

[17] Tekninen ja/tai hallinnollinen apu sekä EU:n ohjelmien ja/tai toimien toteuttamiseen liittyvät tukimenot (entiset BA-budjettikohdat), epäsuora ja suora tutkimustoiminta.

	Maksut	(5)	2,459	2,459	2,459	2,459	2,459	12,293
○ Tiettyjen ohjelmien määrärahoista katettavat hallintomäärärahat YHTEENSÄ		(6)						
Monivuotisen rahoituskehyksen **OTSAKKEISIIN 1–6 kuuluvat määrärahat YHTEENSÄ**	Sitoumukset	=4+ 6	2,459	2,459	2,459	2,459	2,459	12,293
	Maksut	=5+ 6	2,459	2,459	2,459	2,459	2,459	12,293

Jos ehdotuksella/aloitteella on vaikutuksia useampaan otsakkeeseen, toistetaan edellä oleva osa:

○ Toimintamäärärahat (kaikki otsakkeet) YHTEENSÄ	Sitoumukset	(4)	2,459	2,459	2,459	2,459	2,459	12,293
	Maksut	(5)	2,459	2,459	2,459	2,459	2,459	12,293
Tiettyjen ohjelmien määrärahoista katettavat hallintomäärärahat (kaikki otsakkeet) YHTEENSÄ		(6)						
Monivuotisen rahoituskehyksen **OTSAKKEISIIN 1–6 kuuluvat määrärahat YHTEENSÄ** (Viitemäärä)	Sitoumukset	=4+ 6	2,459	2,459	2,459	2,459	2,459	12,293
	Maksut	=5+ 6	2,459	2,459	2,459	2,459	2,459	12,293

Monivuotisen rahoituskehyksen otsake	7	”Hallintomenot”

Tämän osan täyttämisessä on käytettävä rahoitusselvityksen liitteessä (sisäisten sääntöjen liite V) olevaa hallintomäärärahoja koskevaa selvitystä, joka on laadittava ennen rahoitusselvityksen laatimista. Liite ladataan DECIDE-tietokantaan komission sisäistä lausuntokierrosta varten.

milj. euroa (kolmen desimaalin tarkkuudella)

		Vuosi **2023**	Vuosi **2024**	Vuosi **2025**	Vuosi **2026**	**Vuosi 2027**	**YHTEENSÄ**
Pääosasto: DIGIT (CERT-EU)							
○ Henkilöresurssit		1,184	2,126	2,754	3,225	3,225	12,514
○ Muut hallintomenot		7,938	8,921	8,921	8,921	8,921	43,622
PO DIGIT (CERT-EU) YHTEENSÄ	Määrärahat	9,122	11,047	11,675	12,146	12,146	56,136

Monivuotisen rahoituskehyksen **OTSAKKEESEEN 7 kuuluvat määrärahat YHTEENSÄ**	(Sitoumukset yhteensä = maksut yhteensä)	9,122	11,047	11,675	12,146	12,146	**56,136**

milj. euroa (kolmen desimaalin tarkkuudella)

		Vuosi 2023	Vuosi 2024	Vuosi 2025	Vuosi 2026	Vuosi 2027	**YHTEENSÄ**
Monivuotisen rahoituskehyksen **OTSAKKEISIIN 1–7 kuuluvat määrärahat YHTEENSÄ** (*)	Sitoumukset	11,581	13,506	14,134	14,605	14,605	68,429
	Maksut	11,581	13,506	14,134	14,605	14,605	68,429

(*) Unionin omarahoitteisten toimielinten, elinten ja virastojen rahoitusosuuksien määräksi arvioidaan 2,670 miljoonaa euroa vuodessa (viiden vuoden kokonaisrahoitus 13,350 miljoonaa euroa). Rahoitusosuudet ovat CERT-EU:n käyttötarkoitukseensa sidottuja tuloja. Edellä olevissa taulukoissa esitetään ainoastaan arvioitu kokonaisvaikutus unionin talousarvioon, mutta ne eivät sisällä kyseisiä rahoitusosuuksia.

3.2.2. Arvioidut toimintamäärärahoista rahoitetut tuotokset

maksusitoumusmäärärahat, milj. euroa (kolmen desimaalin tarkkuudella)

Tavoitteet ja tuotokset ⇩			Vuosi **N**		Vuosi **N+1**		Vuosi **N+2**		Vuosi **N+3**		ja näitä seuraavat vuodet (ilmoitetaan kaikki vuodet, joille ehdotuksen/aloitteen vaikutukset ulottuvat, ks. kohta 1.6)						**YHTEENSÄ**	
	TUOTOKSET																	
	Tyyppi[18]	Keski määr. kustannukset	Lkm	Kustannus	Lkm	Kustannus	Lkm	Kustannus	Lkm	Kustannus	Lkm	Kustannus	Lkm	Kustannus	Lkm	Kustannus	Lukumäärä yhteensä	Kustannukset yhteensä
ERITYISTAVOITE 1…[19]																		
– Tuotos																		
– Tuotos																		
– Tuotos																		
Välisumma, erityistavoite 1																		
ERITYISTAVOITE 2																		
– Tuotos																		
Välisumma, erityistavoite 2																		
KAIKKI YHTEENSÄ																		

[18] Tuotokset ovat tuloksena olevia tuotteita ja palveluita (esim. rahoitettujen opiskelijavaihtojen määrä tai rakennetut tiekilometrit).

[19] Kuten kuvattu kohdassa 1.4.2 ”Erityistavoitteet”.

3.2.3. Yhteenveto arvioiduista vaikutuksista hallintomäärärahoihin

– ☐ Ehdotus/aloite ei edellytä hallintomäärärahoja.

– ☑ Ehdotus/aloite edellyttää hallintomäärärahoja seuraavasti:

milj. euroa (kolmen desimaalin tarkkuudella)

	Vuosi 2023	Vuosi 2024	Vuosi 2025	Vuosi 2026	Vuosi 2027	**YHTEENSÄ**
Monivuotisen rahoituskehyksen OTSAKE 7						
Henkilöresurssit						
Vakinaiset toimihenkilöt (AD-palkkaluokat)	1,099	2,041	2,669	3,14	3,14	12,089
Sopimussuhteiset toimihenkilöt	0,085	0,085	0,085	0,085	0,085	0,425
Muut hallintomenot	7,938	8,921	8,921	8,921	8,921	43,622
Monivuotisen rahoituskehyksen OTSAKE 7, välisumma	9,122	11,047	11,675	12,146	12,146	56,136

Monivuotisen rahoituskehyksen OTSAKKEESEEN 7 sisältymättömät[20]						
Henkilöresurssit						
Muut hallintomenot						
Monivuotisen rahoituskehyksen OTSAKKEESEEN 7 sisältymättömät, välisumma						

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

Henkilöresursseja ja muita hallintomenoja koskeva määrärahatarve katetaan toimen hallinnointiin jo osoitetuilla pääosaston määrärahoilla ja/tai pääosastossa toteutettujen uudelleenjärjestelyjen tuloksena saaduilla määrärahoilla sekä tarvittaessa sellaisilla lisäresursseilla, jotka toimea hallinnoiva pääosasto voi saada käyttöönsä vuotuisessa määrärahojen jakomenettelyssä talousarvion puitteissa.

[20] Tekninen ja/tai hallinnollinen apu sekä EU:n ohjelmien ja/tai toimien toteuttamiseen liittyvät tukimenot (entiset BA-budjettikohdat), epäsuora ja suora tutkimustoiminta.

3.2.3.1. Henkilöresurssien arvioitu tarve

– ☐ Ehdotus/aloite ei edellytä henkilöresursseja.

– ☑ Ehdotus/aloite edellyttää henkilöresursseja seuraavasti:

Arvio kokoaikaiseksi henkilöstöksi muutettuna

		Vuosi 2023	Vuosi 2024	Vuosi 2025	Vuosi 2026	Vuosi 2027		
O Henkilöstötaulukkoon sisältyvät virat/toimet (virkamiehet ja väliaikaiset toimihenkilöt)								
20 01 02 01 (päätoimipaikka ja komission edustustot EU:ssa)		7	13	17	20	20		
20 01 02 03 (EU:n ulkopuoliset edustustot)								
01 01 01 01 (epäsuora tutkimustoiminta)								
01 01 01 11 (suora tutkimustoiminta)								
Muu budjettikohta (mikä?)								
O Ulkopuolinen henkilöstö (kokoaikaiseksi muutettuna)[21]								
20 02 01 (kokonaismäärärahoista katettavat sopimussuhteiset toimihenkilöt, kansalliset asiantuntijat ja vuokrahenkilöstö)		1	1	1	1	1		
20 02 03 (sopimussuhteiset ja paikalliset toimihenkilöt, kansalliset asiantuntijat, vuokrahenkilöstö ja nuoremmat asiantuntijat EU:n ulkopuolisissa edustustoissa)								
XX 01 xx **yy zz** [22]	– päätoimipaikassa							
	– EU:n ulkopuolisissa edustustoissa							
01 01 01 02 (sopimussuhteiset toimihenkilöt, kansalliset asiantuntijat ja vuokrahenkilöstö - epäsuora tutkimustoiminta)								
01 01 01 12 (sopimussuhteiset toimihenkilöt, kansalliset asiantuntijat ja vuokrahenkilöstö - suora tutkimustoiminta)								
Muu budjettikohta (mikä?)								
YHTEENSÄ		**8**	**14**	**18**	**21**	**21**		

XX viittaa kyseessä olevaan toimintalohkoon eli talousarvion osastoon.

Henkilöresurssien tarve katetaan toimen hallinnointiin jo osoitetulla pääosaston henkilöstöllä ja/tai pääosastossa toteutettujen henkilöstön uudelleenjärjestelyjen tuloksena saadulla henkilöstöllä sekä tarvittaessa sellaisilla lisäresursseilla, jotka toimea hallinnoiva pääosasto voi saada käyttöönsä vuotuisessa määrärahojen jakomenettelyssä talousarvion puitteissa.

Kuvaus henkilöstön tehtävistä:

Virkamiehet ja väliaikaiset toimihenkilöt	Virkamiehet toteuttavat CERT-EU:n tehtävät ja toimet asetuksen ja erityisesti sen IV ja V luvun mukaisesti.
Ulkopuolinen henkilöstö	Sopimussuhteinen toimihenkilö avustaa toimielinten välisen kyberturvallisuuslautakunnan sihteeritehtävissä.

[21] Sopimussuhteiset toimihenkilöt, paikalliset toimihenkilöt, kansalliset asiantuntijat, vuokrahenkilöstö ja nuoremmat asiantuntijat EU:n ulkopuolisissa edustustoissa.

[22] Toimintamäärärahoista katettavan ulkopuolisen henkilöstön enimmäismäärä (entiset BA-budjettikohdat).

3.2.4. Yhteensopivuus nykyisen monivuotisen rahoituskehyksen kanssa

Ehdotus/aloite

– ☑ voidaan rahoittaa kokonaan kohdentamalla menoja uudelleen monivuotisen rahoituskehyksen kyseisen otsakkeen sisällä.

Selvitys rahoitussuunnitelmaan tarvittavista muutoksista, mainittava myös kyseeseen tulevat budjettikohdat ja määrät. Merkittävät rahoitussuunnitelman muutokset on esitettävä Excel-taulukkona.

– ☐ edellyttää monivuotisen rahoituskehyksen kyseiseen otsakkeeseen sisältyvän kohdentamattoman liikkumavaran ja/tai monivuotista rahoituskehystä koskevassa asetuksessa määriteltyjen erityisvälineiden käyttöä.

Selvitys tarvittavista toimenpiteistä, mainittava myös kyseeseen tulevat rahoituskehyksen otsakkeet, budjettikohdat ja määrät sekä ehdotetut välineet.

– ☐ edellyttää monivuotisen rahoituskehyksen tarkistamista.

Selvitys tarvittavista toimenpiteistä, mainittava myös kyseeseen tulevat rahoituskehyksen otsakkeet, budjettikohdat ja määrät

3.2.5. Ulkopuolisten tahojen rahoitusosuudet

Ehdotus/aloite

– ☑ rahoittamiseen ei osallistu ulkopuolisia tahoja[23]

– ☐ rahoittamiseen osallistuu ulkopuolisia tahoja seuraavasti (arvio):

Määrärahat, milj. euroa (kolmen desimaalin tarkkuudella)

	Vuosi **N**[24]	Vuosi **N+1**	Vuosi **N+2**	Vuosi **N+3**	ja näitä seuraavat vuodet (ilmoitetaan kaikki vuodet, joille ehdotuksen/aloitteen vaikutukset ulottuvat, ks. kohta 1.6)			Yhteensä
Rahoitukseen osallistuva taho								
Yhteisrahoituksella katettavat määrärahat YHTEENSÄ								

[23] Käyttötarkoitukseensa sidottuja tuloja, jotka kertyvät 12 artiklan 5 kohdan c alakohdassa tarkoitetusta satunnaisesta palvelujen tarjoamisesta muille kuin tuottajaorganisaatioille, ei ole arvioitu, koska niiden pitäisi olla marginaalisia.

[24] Vuosi N on ehdotuksen/aloitteen toteutuksen aloitusvuosi. ”N” korvataan oletetulla ensimmäisellä toteutusvuodella (esimerkiksi: 2021). Seuraavat vuodet täydennetään vastaavasti.

3.3. Arvioidut vaikutukset tuloihin

– ☑ Ehdotuksella/aloitteella ei ole vaikutuksia tuloihin.

– ☐ Ehdotuksella/aloitteella on vaikutuksia tuloihin seuraavasti:

  – ☐ vaikutukset omiin varoihin

  – ☐ vaikutukset muihin tuloihin

  – tulot on kohdennettu menopuolen budjettikohtiin☐

milj. euroa (kolmen desimaalin tarkkuudella)

Tulopuolen budjettikohta:	Käytettävissä olevat määrärahat kuluvana varainhoitovuonna	Ehdotuksen/aloitteen vaikutus[25]						
		Vuosi **N**	Vuosi **N+1**	Vuosi **N+2**	Vuosi **N+3**	ja näitä seuraavat vuodet (ilmoitetaan kaikki vuodet, joille ehdotuksen/aloitteen vaikutukset ulottuvat, ks. kohta 1.6)		
Momentti ….								

Vastaava(t) menopuolen budjettikohta (budjettikohdat) käyttötarkoitukseensa sidottujen tulojen tapauksessa:

Muita huomautuksia (esim. tuloihin kohdistuvan vaikutuksen laskentamenetelmä/-kaava tai muita lisätietoja).

[25] Perinteiset omat varat (tulli- ja sokerimaksut) on ilmoitettava nettomääräisinä eli bruttomäärästä on vähennettävä kantokuluja vastaava 20 prosentin osuus.