EUROOPAN
KOMISSIO

Bryssel 16.12.2020
COM(2020) 823 final

2020/0359 (COD)

Ehdotus

EUROOPAN PARLAMENTIN JA NEUVOSTON DIREKTIIVI

toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi koko unionissa ja direktiivin (EU) 2016/1148 kumoamisesta

(ETA:n kannalta merkityksellinen teksti)

{SEC(2020) 430 final} - {SWD(2020) 344 final} - {SWD(2020) 345 final}

PERUSTELUT

1. EHDOTUKSEN TAUSTA

• Ehdotuksen perustelut ja tavoitteet

Tämä ehdotus on osa toimenpidepakettia, jolla parannetaan julkisten ja yksityisten toimijoiden, toimivaltaisten viranomaisten ja yleensäkin koko unionin kykyä selviytyä kyberturvallisuuteen ja kriittisen infrastruktuuriin suojaamisen liittyvistä turvallisuuspoikkeamista ja vastata tähän liittyviin uhkiin. Ehdotus auttaa osaltaan saavuttamaan komission päätavoitteita, eli tuomaan Euroopan digiaikakaudelle ja rakentaa tulevaisuussuuntautunutta taloutta, joka palvelee ihmisten tarpeita. Kyberturvallisuus on hyvin tärkeällä sijalla tavoissa, joilla komissio vastaa covid-19-kriisiin. Koko pakettiin kuuluu uusi kyberturvallisuusstrategia, jolla halutaan vahvistaa unionin strategista autonomiaa niin, että pystymme paremmin selviytymään uhkista ja vastaamaan niihin yhdessä sekä kehittämään avointa ja globaalia internetiä. Kokonaisuuteen kuuluu myös ehdotus direktiiviksi keskeisten palvelujen kriittisen tärkeiden tarjoajien kyvystä suojautua ulkoisilta uhkilta. Se keskittyy tällaisten toimijoiden kohtaamiin fyysisiin turvallisuusuhkiin.

Tämä ehdotus perustuu verkko- ja tietojärjestelmien turvallisuutta koskevaan NIS-direktiiviin (EU) 2016/1148, jonka se myös kumoaa. NIS on ollut ensimmäinen EU:n laajuinen kyberturvasäädös ja antanut oikeudellisia keinoja parantaa kyberturvallisuuden yleistä tasoa unionissa. NIS-direktiivi on 1) auttanut parantamaan kyberturvallisuusvalmiuksia kansallisella tasolla edellyttämällä kansallisia kyberstrategioita ja siitä vastaavien viranomaisten nimeämistä, 2) lisännyt EU-maiden yhteistyötä saamalla aikaan erilaisia foorumeja strategisen ja operatiivisen tiedon vaihtoa varten ja 3) parantanut julkisten ja yksityisten toimijoiden kyberturvallisuusvalmiuksia seitsemällä yleisellä toimialalla (energia, liikenne, pankkitoiminta, rahoitusmarkkinoiden infrastruktuurit, terveydenhuolto, juomaveden tuottaminen ja jakelu sekä digitaalinen infrastruktuuri) ja kolmella digipalvelualalla (verkkokaupat, hakukoneet ja pilvipalvelut), kun EU-maiden on pitänyt varmistaa, että välttämättömien palvelujen tarjoajat ja digipalveluntarjoajat noudattavat kyberturvallisuusvaatimuksia ja raportoivat turvallisuuspoikkeamista.

Ehdotuksella nykyaikaistetaan lainsäädäntöä ottaen huomioon sisämarkkinoiden viime vuosina edennyt digitalisaatio ja alati muuttuva kyberturvallisuusympäristö. Molempia kehityskulkuja on edelleen vahvistanut covid-19-kriisi. Ehdotuksella puututaan myös useisiin heikkouksiin, joiden johdosta NIS-direktiivistä ei saatu kaikkia hyötyjä irti.

NIS-direktiivi, josta toki oli paljon hyötyä, kun se johti merkittävään muutokseen suhtautumisessa institutionaaliseen ja sääntelyajatteluun kyberkysymyksissä monissa EU-maissa, oli myös monissa kohdin puutteellinen. Yhteiskuntien digitalisaatio (jota covid-19-kriisi edelleen on vahvistanut) on laajentanut tilannekuvaa uhkista ja luo uusia haasteita, jotka vaativat tarkemmin suunnattuja ja entistä innovatiivisempia puolustuskeinoja. Kyberhyökkäykset lisääntyvät. Ne ovat entistä sofistikoituneempia ja tulevat hyvin monista lähteistä sekä EU:n sisältä että sen ulkopuolelta.

Tämän direktiivin vaikutustenarviointia varten tehdyssä NIS-direktiivin toimivuuden selvityksessä todettiin seuraavat ongelmat: 1) EU:ssa toimivien yritysten heikko kyberuhkien sietokyky, 2) erot häiriönsietokyvyssä jäsenvaltioiden ja toimialojen välillä ja 3) heikko yhteinen tilannetietoisuus ja kyky yhteiseen reagointiin. Esimerkiksi jossain EU-maassa tietyt suuret sairaalat eivät kuulu NIS-direktiivin soveltamisalaan eikä niiltä siten edellytetä direktiivin mukaisia turvatoimia, kun taas toisessa EU-maassa joka ikinen terveydenhuollon toimija kuuluu direktiivin tietoturvavaatimusten piiriin.

Ehdotus sisältyy sääntelyn toimivuutta ja tuloksellisuutta koskevaan REFIT-ohjelmaan, joten sillä pyritään keventämään toimivaltaisten viranomaisten sääntelytaakkaa ja vähentämään julkisille ja yksityisille toimijoille sääntöjen noudattamisesta aiheutuvia kustannuksia. Tähän päästään erityisesti poistamalla toimivaltaisten viranomaisten velvollisuus yksilöidä keskeisten palvelujen tarjoajat ja edelleen yhdenmukaistamalla turva- ja raportointivaatimuksia, jotta rajat ylittäviä palveluja tarjoavien toimijoiden on helpompi noudattaa sääntöjä. Toimivaltaisille viranomaisille annetaan kuitenkin muutamia uusia tehtäviä, kuten sellaisten alojen toimijoiden valvonta, jotka eivät toistaiseksi ole kuuluneet NIS-direktiivin piiriin.

- **Yhdenmukaisuus muiden alaa koskevien politiikkojen säännösten kanssa**

Ehdotus on osa laajempaa jo olemassa olevan lainsäädännön ja tulossa olevien EU-tason aloitteiden kokonaisuutta, jolla pyritään parantamaan julkisten ja yksityisten toimijoiden suojautumista uhkilta.

Kyberturvallisuuden alalla kyseeseen tulevat erityisesti eurooppalaisesta sähköisen viestinnän säännöstöstä annettu direktiivi (EU) 2018/1972 (jonka kyberturvallisuussäännökset korvataan tämän ehdotuksen säännöksillä) ja ehdotus asetukseksi finanssialan digitaalisesta häiriönsietokyvystä (COM(2020) 595 final), joka katsotaan tämän ehdotuksen suhteen erityislainsäädännöksi (*lex specialis*) sen jälkeen kun molemmat säädökset ovat tulleet voimaan.

Fyysisen turvallisuuden suhteen ehdotus täydentää kriittisten toimijoiden häiriönsietokykyä koskevaa direktiiviehdotusta, jolla tarkistetaan Euroopan elintärkeän infrastruktuurin määrittämisestä ja nimeämisestä sekä arvioinnista, joka koskee tarvetta parantaa sen suojaamista annettua direktiiviä 2008/114/EY (ECI-direktiivi). Sillä luodaan unionitason prosessi Euroopan kriittisten infrastruktuurien tunnistamiseksi ja määrittämiseksi ja esitetään lähestymistapa niiden suojan parantamiseksi. Heinäkuussa 2020 komissio hyväksyi EU:n turvallisuusunionistrategian[1], jossa nostettiin esiin fyysisten ja digitaalisten infrastruktuurien lisääntynyt verkottuneisuus ja keskinäisriippuvuus. Siinä korostettiin tarvetta yhtenäisemmälle ja johdonmukaisemmalle lähestymistavalle ECI-direktiivin ja toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa annetun direktiivin (EU) 2016/1148 välillä.

Tämä ehdotus on siis tiiviisti linjassa suhteessa kriittisten toimijoiden häiriönsietokykyä koskevaan direktiiviehdotukseen, jolla pyritään parantamaan niiden suojautumista fyysisiltä uhkilta hyvin monilla toimialoilla. Tällä ehdotuksella pyritään varmistamaan, että molempien säädösten mukaiset toimivaltaiset viranomaiset toimivat toisiaan täydentävästi ja vaihtavat tarvittavassa määrin kyber- ja muita uhkia koskevaa tietoa ja että tämän ehdotuksen mukaisesti ’keskeisiksi’ katsottujen alojen kriittisiin toimijoihin sovelletaan myös yleisempiä suojaa parantavia velvoitteita, jotka painottuvat muihin kuin kyberuhkiin.

- **Yhdenmukaisuus unionin muiden politiikkojen kanssa**

Kuten tiedonannossa ”Euroopan digitaalista tulevaisuutta rakentamassa”[2] todetaan, on ratkaisevan tärkeää, että Eurooppa hyödyntää kaikki digiajan edut ja vahvistaa teollista ja innovointikapasiteettiaan turvallisten ja eettisten rajojen puitteissa. Euroopan datastrategiassa

[1] COM(2020) 605 final.
[2] COM(2020) 67 final.

esitetään neljä pilaria – tietosuoja, perusoikeudet, turvallisuus ja kyberturvallisuus – datavetoisen yhteiskunnan olennaisina edellytyksinä.

Euroopan parlamentti kehotti 12. maaliskuuta 2019 antamassaan päätöslauselmassa *”[...] komissiota arvioimaan, onko verkko- ja tietoturvadirektiivin soveltamisalaa tarpeen laajentaa edelleen koskemaan muita kriittisiä aloja ja palveluita, jotka eivät kuulu minkään alakohtaisen lainsäädännön soveltamisalaan”*.[3] Neuvosto pani 9. kesäkuuta 2020 antamissaan päätelmissä tyytyväisenä merkille *”[...] komission suunnitelmat varmistaa markkinaosapuolia koskevat johdonmukaiset säännöt ja helpottaa uhkia ja kyberhäiriötilanteita koskevien tietojen turvallista, luotettavaa ja asianmukaista jakamista, myös tarkastelemalla uudelleen verkko- ja tietoturvadirektiiviä, selvittää kyberuhkien sietokyvyn parantamista ja vaihtoehtoja vastata tehokkaammin erityisesti talouden ja yhteiskunnan välttämättömiin toimintoihin kohdistuviin kyberhyökkäyksiin kunnioittaen samalla jäsenvaltioiden toimivaltaa ja pitäen mielessä niiden vastuun kansallisesta turvallisuudestaan*.[4] Ehdotetulla säädöksellä ei rajoiteta Euroopan unionin toiminnasta tehdyssä sopimuksessa (SEUT-sopimus) vahvistettujen kilpailusääntöjen soveltamista.

Koska suurimmassa osassa kyberuhkia alkuperä on EU:n ulkopuolella, tarvitaan johdonmukaista lähestymistapaa myös kansainväliseen yhteistyöhön. Tästä direktiivistä muodostuu viitemalli, jota edistetään EU:n yhteistyössä EU:n ulkopuolisten maiden kanssa, erityisesti silloin, kun kyseessä on teknisen avun tarjoaminen.

2. OIKEUSPERUSTA, TOISSIJAISUUSPERIAATE JA SUHTEELLISUUSPERIAATE

• Oikeusperusta

NIS-direktiivin oikeusperusta on Euroopan unionin toiminnasta tehdyn sopimuksen 114 artikla, jonka tavoitteena on luoda sisämarkkinat ja edistää niiden toimintaa yhdenmukaistamalla kansallisia sääntöjä. Kuten EU-tuomioistuin asiassa C-58/08, Vodafone ja muut on vahvistanut, SEUT-sopimuksen 114 artiklaan turvautuminen on perusteltua, kun kansallisissa säännöissä on eroja, jotka suoraan vaikuttavat sisämarkkinoiden toimintaan. Samassa asiassa tuomioistuin toteaa, että kun SEUT-sopimuksen 114 artiklaan perustuvalla toimella on jo poistettu kaupan esteitä alalla, jota sillä yhdenmukaistetaan, unionin lainsäätäjältä ei voida viedä mahdollisuutta mukauttaa kyseistä toimea olosuhteiden muutoksiin tai tiedon kehitykseen, koska yhteisön lainsäätäjän tehtävänä on turvata perussopimuksessa tunnustettujen yleisten etujen suojelu. Lopuksi tuomioistuin toteaa, että SEUT-sopimuksen 114 artiklan kattamissa yhdenmukaistamistoimissa on tarkoitus sallia parhaiten toivotun tuloksen saavuttamiseen sopivan yhdenmukaistamistavan valinnan suhteen tietty liikkumavara riippuen yhdenmukaistamisen kohteen yleisestä asiayhteydestä ja erityisolosuhteista. Ehdotettu säädös poistaisi sisämarkkinoiden esteitä ja edistäisi sisämarkkinoiden syntyä ja toimintaa keskeisten ja tärkeiden toimijoiden osalta luomalla selkeät ja yleisesti sovellettava säännöt NIS-direktiivin soveltamisalan määrittelylle sekä yhdenmukaistamalla kyberriskinhallinnan poikkeamista raportoinnin sääntöjä. Nykyiset sekä lainsäädännön että valvonnan erot tällä alalla niin kansallisella kuin EU-tasollakin muodostavat sisämarkkinoiden esteitä, koska rajat ylittävät toimijat joutuvat noudattamaan erilaisia ja osin päällekkäisiä vaatimuksia ja/tai vaatimusten soveltamistapoja, mikä aiheuttaa

[3] https://www.europarl.europa.eu/doceo/document/TA-8-2019-0156_FI.html
[4] https://data.consilium.europa.eu/doc/document/ST-8711-2020-INIT/fi/pdf

haittaa niiden pyrkiessä hyödyntämään sijoittautumisvapautta ja palveluntarjonnan vapautta. Erot säännöissä vaikuttavat haitallisesti myös kilpailuolosuhteisiin sisämarkkinoilla, kun verrataan saman tyyppisiä toimijoita eri EU-maissa.

- **Toissijaisuusperiaate (jaetun toimivallan osalta)**

Kyberturvatoiminta unionissa ei voi olla tuloksellista, jos asiaa lähestytään hajanaisesti kansallisten tai alueellisten siilojen näkökulmasta. NIS-direktiivillä korjattiin osittain puutteita luomalla puitteet verkkojen ja tietojärjestelmien tietoturvalle kansallisella ja unionitasolla. Sen täytäntöönpano ja toteutus paljasti kuitenkin myös tiettyjen säännösten ja lähestymistapojen sisälähtöisiä heikkouksia ja rajoituksia. Tällainen on esimerkiksi direktiivin soveltamisalan epäselvä rajaus, mikä on johtanut huomattaviin eroihin EU-näkökulman käytännön laajuudessa ja määrässä EU-maissa. Lisäksi Euroopan taloudesta on covid-19-kriisin myötä tullut vieläkin riippuvaisempi verkoista ja tietojärjestelmistä, ja eri toimialat ja palvelut ovat enenevässä määrin sidoksissa toisiinsa. Nykyistä NIS-direktiiviä vahvempi EU-tason sääntely on perusteltavissa erityisesti seuraavilla seikoilla: i) verkkojen ja tietojärjestelmien suojaan liittyvät uhat ja haasteet ovat luonteeltaan yhä enemmän rajat ylittäviä, ii) EU-tason toimilla voidaan parantaa ja helpottaa kansallisen tason tuloksellista ja koordinoitua toimintaa ja iii) yhtenäisellä ja yhteistyöhön perustuvalla toiminnalla voidaan tuloksellisesti tukea tietosuojaa ja yksityisyyden suojaa.

- **Suhteellisuusperiaate**

Ehdotetun direktiivin säännöt eivät ylitä sitä, mikä on tarpeen sen erityistavoitteiden saavuttamiseksi tyydyttävällä tavalla. Kaavaillut turvatoimien ja raportointivelvoitteiden yhdenmukaistamis- ja sujuvoittamistoimet perustuvat EU-maiden ja yritysten pyyntöihin parantaa nykyjärjestelmää.

Ehdotuksessa otetaan huomioon EU-maissa jo vallitsevat käytänteet. Tällaisilla selkeämmillä ja koordinoiduilla vaatimuksilla saavutettava parempi suojataso on oikeassa suhteessa kohdattaviin yhä suurempiin riskeihin, myös niihin, joihin liittyy rajat ylittävä ulottuvuus. Vaatimukset ovat kohtuullisia ja vastaavat laajasti niiden toimijoiden etuja, jotka pyrkivät varmistamaan palvelujensa jatkuvuuden ja laadun. EU-maiden järjestelmällisen yhteistyön kustannukset olisivat pieniä verrattuna kyberturvapoikkeamien aiheuttamiin taloudellisiin ja yhteiskunnallisiin tappioihin ja haittoihin. Lisäksi NIS-direktiivin tarkistamiselle edellä kuvatulla tavalla saatiin tukea direktiivin uudelleentarkasteluun liittyneissä sidosryhmäkuulemisissa sekä avoimessa julkisessa kuulemisessa ja kohdennetuissa kyselyissä.

- **Toimintatavan valinta**

Ehdotuksella selkeytetään edelleen yrityksille asetettuja velvoitteita ja yhdenmukaistetaan niitä lisää. Toisaalta ehdotuksella pyritään sallimaan EU-maille riittävästi joustoa, jotta kansalliset erityisolosuhteet voidaan ottaa huomioon (esimerkiksi mahdollisuus nimetä keskeisiä tai tärkeitä toimijoita laajemminkin kuin säädöksessä). Tulevan oikeudellisen välineen olisi sen vuoksi oltava direktiivi, koska se mahdollistaa kohdennetun paremman yhdenmukaistamisen ja tietynasteisen jouston toimivaltaisille viranomaisille.

3. JÄLKIARVIOINTIEN, SIDOSRYHMIEN KUULEMISTEN JA VAIKUTUSTENARVIOINTIEN TULOKSET

- **Jälkiarvioinnit/toimivuustarkastukset**

Komissio on tehnyt arvioinnin[5] verkko- ja tietoturvadirektiivin toimivuudesta. Komissio on analysoinut sen relevanssia, EU:n tason lisäarvoa, johdonmukaisuutta, vaikuttavuutta ja tehokkuutta. Analyysin tärkeimmät tulokset ovat seuraavat:

- NIS-direktiivin soveltamisala on liian suppea sen kattamien alojen suhteen, mikä johtuu pääasiassa seuraavista syistä: i) viime vuosien lisääntynyt digitalisaatio ja kytkösten lisääntyminen ja ii) se, että NIS-direktiivin soveltamisala ei enää heijasta kaikkia digitalisoituneita aloja, jotka tarjoavat keskeisiä palveluja taloudelle ja koko yhteiskunnalle.
- NIS-direktiivi ei ole riittävän selkeä soveltamisalaan kuuluvien keskeisten palvelujen tarjoajien suhteen, eivätkä sen säännökset tarjoa riittävää selvyyttä digitaalisten palvelujen tarjoajia koskevasta kansallisesta toimivallasta. Tämä on johtanut tilanteeseen, jossa tietyntyyppisiä toimijoita ei ole otettu direktiivin piiriin kaikissa EU-maissa, minkä vuoksi niiden ei ole tarvinnut ottaa käyttöön turvatoimia eikä raportoida poikkeamista.
- NIS-direktiivissä annettiin EU-maille laaja harkintavalta, kun ne säätävät keskeisten palvelujen tarjoajille asetettavista turvallisuutta ja poikkeamia koskevista raportointivaatimuksista. Arviointi osoittaa, että joissakin tapauksissa EU-maat ovat panneet vaatimukset täytäntöön hyvin eri tavoin, mikä on aiheuttanut lisärasitetta useammassa kuin yhdessä EU-maassa toimiville yrityksille.
- NIS-direktiivin valvonta- ja täytäntöönpanojärjestelmä on tehoton. EU-maat ovat esimerkiksi olleet hyvin haluttomia soveltamaan seuraamuksia toimijoihin, jotka eivät ole noudattaneet turvavaatimuksia tai ilmoittaneet poikkeamista. Tällä voi olla kielteisiä vaikutuksia yksittäisten toimijoiden kykyyn sietää häiriöitä.
- Taloudelliset ja henkilöresurssit, jotka EU-maat ovat varanneet tehtäviensä (kuten keskeisten palvelujen tarjoajien selvittämisen tai valvonnan) hoitamista varten – ja näin ollen kyberturvariskien käsittelyn eri kehitystasot – vaihtelevat suuresti. Tämä kasvattaa entisestään EU-maiden välisiä eroja kyberuhkien sietokyvyssä.
- EU-maat eivät vaihda tietoja järjestelmällisesti keskenään, millä on kielteisiä vaikutuksia erityisesti kyberturvatoimenpiteiden tehokkuuteen ja yhteisen tilannetietoisuuden tasoon EU:n tasolla. Tämä koskee myös yksityisen sektorin toimijoiden välistä tiedonvaihtoa sekä EU:n tason yhteistyörakenteiden ja yksityisen sektorin toimijoiden välistä yhteistyötä.

- **Sidosryhmien kuuleminen**

Komissio on kuullut laajasti erilaisia sidosryhmiä. EU-maita ja sidosryhmiä pyydettiin osallistumaan avoimeen julkiseen kuulemiseen sekä Wavestonen, CEPS:n ja ICF:n (joilla komissio teetti selvityksen NIS-direktiivin uudelleentarkastelun tueksi) järjestämiin kyselyihin ja työpajoihin. Kuultuja sidosryhmiä olivat toimivaltaiset viranomaiset, kyberturvallisuutta käsittelevät unionin elimet, keskeisten palvelujen tarjoajat, digitaalisten palvelujen tarjoajat, nykyisen NIS-direktiivin soveltamisalaan kuulumattomia palveluja tarjoavat toimijat, toimialajärjestöt ja kuluttajajärjestöt sekä yksityishenkilöt.

[5] [Vaikutustenarvioinnin liite 5.]

Lisäksi komissio on ollut jatkuvasti yhteydessä NIS-direktiivin täytäntöönpanosta vastaaviin toimivaltaisiin viranomaisiin. Erityinen yhteistyöryhmä on käsitellyt laajasti useita monialaisia ja alakohtaisia täytäntöönpanoon liittyviä näkökohtia. Vuosina 2019 ja 2020 tehtyjen NIS-maavierailujensa aikana komissio haastatteli 154 julkista ja yksityistä tahoa sekä 117 toimivaltaista viranomaista.

- **Asiantuntijatiedon keruu ja käyttö**

Komissio on tehnyt sopimuksen Wavestonen, CEPS:n ja ICF:n konsortion kanssa komission tukemiseksi NIS-direktiivin uudelleentarkastelussa[6]. Sen lisäksi, että toimeksisaaja on tavoittanut kohdennettujen kyselyjen ja työpajojen avulla sidosryhmät, joihin NIS-direktiivi vaikuttaa suoraan, se on myös kuullut useita kyberturvallisuuden alan asiantuntijoita, kuten kyberturvautkijoita ja kyberturvatoimialan ammattilaisia.

- **Vaikutustenarviointi**

Tähän ehdotukseen liittyy vaikutustenarviointi[7], joka toimitettiin sääntelyntarkastelulautakunnalle 23. lokakuuta 2020 ja joka sai sääntelyntarkastelulautakunnalta myönteisen lausunnon kommentteineen 20. marraskuuta 2020. Sääntelyntarkastelulautakunta suositteli parannuksia joillakin aloilla, jotta voidaan 1) ottaa paremmin huomioon rajat ylittävien heijastusvaikutusten merkitys ongelma-analyysissä, 2) selittää paremmin, miten aloitteen onnistumista mitattaisiin, 3) esittää laajemmat perustelut tarkasteltaviksi valituille toimintavaihtoehdoille ja 4) tarkentaa ehdotettujen toimenpiteiden kustannusarvioita. Vaikutustenarviointia mukautettiin näiden seikkojen sekä sääntelyntarkastelulautakunnan yksityiskohtaisempien huomautusten perusteella. Se sisältää nyt yksityiskohtaisempia selvityksiä rajat ylittävien heijastusvaikutusten roolista kyberturvallisuuden alalla, selkeämmän yleiskuvan siitä, miten onnistumista voidaan mitata, yksityiskohtaisemman selvityksen tarkasteltaviksi valittujen eri toimintavaihtoehtojen ja toimien rakenteesta ja logiikasta, yksityiskohtaisemman selvityksen NIS-direktiivin toimialakattavuuteen liittyvistä analysoiduista näkökohdista sekä lisäselvityksiä kustannuksista.

Komissio tarkasteli useita toimintavaihtoehtoja oikeudellisen kehyksen parantamiseksi kyberuhkien sietokyvyn ja poikkeamiin reagoinnin alalla:

- ”Ei tehdä mitään”: NIS-direktiivi säilyisi muuttumattomana, eikä toteutettaisi myöskään ei-lainsäädännöllisiä toimenpiteitä direktiivin arvioinnissa havaittujen ongelmien ratkaisemiseksi.
- Vaihtoehto 1: Lainsäädäntötasolla ei tehtäisi muutoksia. Sen sijaan komissio antaisi suosituksia ja ohjeita (jotka koskevat esimerkiksi keskeisten palvelujen tarjoajien tunnistamista, turvallisuusvaatimuksia, poikkeamien ilmoittamismenettelyjä ja valvontaa) kuultuaan asiaa koskevaa yhteistyöryhmää, EU:n kyberturvallisuusvirastoa (ENISA) ja tarvittaessa tietoturvaloukkauksiin reagoivien CSIRT-yksiköiden verkostoa.
- Vaihtoehto 2: Tämä vaihtoehto edellyttäisi kohdennettuja muutoksia NIS-direktiiviin, mukaan lukien soveltamisalan laajentaminen, ja useita muita muutoksia,

[6] Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) – N° 2020-665. Wavestone, CEPS and ICF.

[7] **[linkit lopulliseen asiakirjaan ja tiivistelmään lisätään myöhemmin.]**

joilla pyritään takaamaan tietyt välittömät ratkaisut havaittuihin ongelmiin, selkeyttämään tilannetta ja lisäämään yhdenmukaisuutta (esimerkiksi säännökset tunnistamiskynnysten yhdenmukaistamiseksi). Muutetussa NIS-direktiivissä säilytettäisiin kuitenkin tärkeimmät rakenneosat, lähestymistapa ja perusteet.

- Vaihtoehto 3: Tässä skenaariossa NIS-direktiiviin tehtäisiin systeemisiä ja rakenteellisia muutoksia (uudella direktiivillä). Tarkoituksena olisi muuttaa lähestymistapaa perusteellisemmin niin, että se kattaisi laajemman osan talouksista kaikkialla unionissa. Valvonta olisi kuitenkin entistä kohdennetumpaa ja painottuisi suuriin avaintoimijoihin. Tässä vaihtoehdossa myös virtaviivaistettaisiin yrityksille asetettuja velvoitteita ja varmistettaisiin velvoitteiden laajempi yhdenmukaisuus, luotaisiin tehokkaammat puitteet operatiivisille näkökohdille sekä luotaisiin selkeä perusta eri sidosryhmien jaetulle vastuulle ja eri toimijoiden kulloisillekin vastuille kyberturvatoimien osalta.

Vaikutustenarvioinnissa todetaan, että parhaaksi arvioitu vaihtoehto on vaihtoehto 3 (eli NIS-kehykseen tehtävät systeemiset ja rakenteelliset muutokset). Vaikuttavuuden kannalta tämä vaihtoehto määrittäisi selkeästi NIS-direktiivin soveltamisalan, joka ulottuisi edustavampaan osaan EU:n talouksia ja yhteiskuntia. Se myös virtaviivaistaisi vaatimuksia sekä loisi tarkemmin määritellyt puitteet valvonnalle ja täytäntöönpanolle niin, että vaatimusten noudattamisen tasoa voitaisiin nostaa. Siihen sisältyy myös toimenpiteitä, joilla pyritään parantamaan toimintamalleja EU-maiden tasolla ja muuttamaan niiden yleistä ajattelutapaa, edistämään uusia puitteita alihankkijasuhteiden riskinhallinnalle ja koordinoimaan haavoittuvuuksien julkituomista. Samalla parhaaksi arvioitu toimintavaihtoehto luo selkeän perustan jaetulle vastuulle ja vastuuvelvollisuudelle, ja siihen sisältyy mekanismeja, joilla pyritään lisäämään luottamusta EU-maiden, sekä viranomaisten että toimialan, välillä, kannustamaan tietojen jakamiseen ja varmistamaan toimivampi lähestymistapa, joka hyödyntää esimerkiksi keskinäistä avunantoa ja vertaisarviointimekanismeja. Tässä vaihtoehdossa luotaisiin myös EU:n kriisinhallintakehys, joka perustuisi äskettäin käynnistettyyn EU:n operatiiviseen verkostoon, ja varmistettaisiin ENISAn nykyistä aktiivisempi osallistuminen nykyisten toimivaltuuksiensa puitteissa tarkan yleiskuvan luomiseen kyberturvallisuuden tilasta unionissa.

Tehokkuuden osalta voidaan todeta, että vaikka parhaaksi arvioitu vaihtoehto aiheuttaisi sääntöjen noudattamisesta ja täytäntöönpanon valvonnasta johtuvia lisäkustannuksia yrityksille ja EU-maille, se johtaisi myös tehokkaisiin kompromisseihin ja synergioihin ja tarjoaisi kaikista analysoiduista toimintavaihtoehdoista parhaat mahdollisuudet varmistaa, että keskeisten toimijoiden kyky sietää kyberuhkia paranisi ja olisi yhdenmukainen kaikkialla unionissa, mikä johtaisi lopulta kustannussäästöihin sekä yrityksille että yhteiskunnalle. Tämä vaihtoehto lisäisi jonkin verran EU-maiden viranomaisten hallinnollista taakkaa ja säännösten noudattamisesta aiheutuvia kustannuksia. Kaiken kaikkiaan se toisi kuitenkin keskipitkällä ja pitkällä aikavälillä huomattavia etuja lisäämällä EU-maiden yhteistyötä, myös operatiivisella tasolla, sekä kannustamalla keskinäisen avun, vertaisarviointimekanismien ja keskeisten yritysten paremman yleiskuvan ja vuorovaikutuksen avulla lisäämään yleisesti kyberturvavalmiuksia kansallisella ja alueellisella tasolla. Parhaaksi arvioitu toimintavaihtoehto varmistaisi myös suurelta osin johdonmukaisuuden muun lainsäädännön, muiden aloitteiden tai muiden politiikkatoimien, myös alakohtaisen erityislainsäädännön, kanssa.

Kyberturvavalmiuden jatkuvaan riittämättömyyteen puuttuminen EU-maiden tasolla sekä yritysten ja muiden organisaatioiden tasolla voisi johtaa tehokkuusetuihin ja kyberturvapoikkeamien aiheuttamien lisäkustannusten vähenemiseen.

- Keskeisten ja tärkeiden tahojen osalta kyberturvallisuusvalmiuksien tason nostaminen voisi johtaa häiriöistä – myös teollisuusvakoilusta – johtuvien mahdollisten tulonmenetysten vähenemiseen ja vähentää uhkia lieventävistä tapauskohtaisista toimista aiheutuvia suuria kustannuksia. Tällaiset hyödyt ovat todennäköisesti suuremmat kuin tarvittavat investointikustannukset. Sisämarkkinoiden hajanaisuuden vähentäminen tasapuolistasi myös toimijoiden toimintaedellytyksiä.
- EU-maiden näkökulmasta se voisi edelleen vähentää riskiä, että tapauskohtaisesta uhkien lieventämisestä aiheutuvat julkiset menot kasvaisivat, ja kyberturvapoikkeamiin liittyvät hätätilanteet aiheuttaisivat lisäkustannuksia.
- Kansalaisten kannalta kyberturvapoikkeamiin puuttumisen odotetaan vähentävän tulonmenetyksiä, jotka johtuvat talouden häiriötiloista.

Kyberturvallisuuden korkeampi taso kaikissa EU-maissa sekä yritysten ja viranomaisten kyky reagoida poikkeamiin nopeasti ja lieventää niiden vaikutuksia johtavat mitä todennäköisimmin siihen, että kansalaisten yleinen luottamus digitaalitalouteen lisääntyy, millä voi olla myönteinen vaikutus kasvuun ja investointeihin.

Kyberturvallisuuden yleisen tason nostaminen johtaa todennäköisesti yleisen turvallisuuden lisääntymiseen ja yhteiskunnan kannalta kriittisten keskeisten palvelujen sujuvaan keskeytymättömään toimintaan. Aloite voi myös myötävaikuttaa muihin yhteiskunnallisiin vaikutuksiin, kuten tietoverkkorikollisuuden ja terrorismin vähenemiseen ja kansalaisten yleisen suojan paranemiseen. Yritysten ja muiden organisaatioiden kybervalmiuksien parantaminen saattaa välttää mahdolliset taloudelliset menetykset, joita johtuisi kyberhyökkäyksistä, ja siten estää tarpeita irtisanoa työntekijöitä.

Kyberturvallisuuden yleisen tason nostaminen voisi myös johtaa ympäristöriskien ja -vahinkojen ehkäisemiseen, kun on kyse hyökkäyksistä keskeisiin palveluihin. Tämä voisi koskea erityisesti energia-, vesihuolto- ja jakelualaa tai liikennettä. Kyberturvavalmiuksia vahvistamalla aloite voisi johtaa myös ympäristön kannalta kestävämpiin uusimman sukupolven tieto- ja viestintätekniikan infrastruktuureihin ja palveluihin sekä tehottomien ja vähemmän turvallisten vanhojen infrastruktuurien korvaamiseen. Tämän odotetaan myös auttavan vähentämään kalliiden verkkoturvapoikkeamien määrää ja vapauttavan resursseja kestäviin investointeihin.

- **Sääntelyn toimivuus ja yksinkertaistaminen**

Ehdotuksessa esitetään mikro- ja pienten toimijoiden jättämistä yleisesti NIS-soveltamisalan ulkopuolelle ja kevyempää jälkikäteisvalvontaa , jota sovelletaan suureen määrään tarkistetun soveltamisalan piiriin kuuluvia uusia toimijoita (ns. tärkeät toimijat). Näillä toimenpiteillä pyritään minimoimaan ja tasapainottamaan yrityksille ja julkishallinnoille aiheutuva rasite. Lisäksi ehdotuksella korvataan keskeisten palvelujen tarjoajien monimutkainen tunnistusjärjestelmä yleisesti sovellettavalla velvoitteella ja yhdenmukaistetaan enemmän turvallisuus- ja raportointivelvoitteita, mikä vähentäisi säännösten noudattamisesta aiheutuvaa rasitetta erityisesti rajat ylittäviä palveluja tarjoaville toimijoille.

Ehdotuksella minimoidaan säännösten noudattamisesta pk-yrityksille aiheutuvat kustannukset, sillä yritysten edellytetään toteuttavan ainoastaan sellaisia toimenpiteitä, jotka ovat tarpeen sen varmistamiseksi, että verkko- ja tietojärjestelmien turvataso on oikeassa suhteessa aiheutuvaan riskiin.

- **Perusoikeudet**

EU on sitoutunut varmistamaan perusoikeuksien korkeatasoisen suojelun. Kaikki vapaaehtoiset tiedonjakojärjestelyt toimijoiden välillä, joita tällä direktiivillä edistetään, toteutettaisiin luotettavissa ympäristöissä noudattaen täysimääräisesti unionin tietosuojasääntöjä, erityisesti Euroopan parlamentin ja neuvoston asetusta (EU) N:o 2016/679[8].

4. TALOUSARVIOVAIKUTUKSET

Ks. rahoitusselvitys

5. LISÄTIEDOT

- **Toteuttamissuunnitelmat, seuranta, arviointi ja raportointijärjestelyt**

Ehdotukseen sisältyy erityistavoitteiden seurantaa ja arviointia koskeva yleissuunnitelma, jonka mukaan komission on tehtävä uudelleentarkastelu vähintään [54 kuukauden] kuluttua voimaantulosta ja raportoitava tärkeimmistä havainnoistaan Euroopan parlamentille ja neuvostolle.

Uudelleentarkastelu on suoritettava parempaa sääntelyä koskevien komission suuntaviivojen mukaisesti.

- **Ehdotukseen sisältyvien säännösten yksityiskohtaiset selitykset**

Ehdotus on jäsennelty useisiin kokonaisuuksiin, jotka liittyvät toisiinsa ja joiden tarkoituksena on parantaa kyberturvallisuuden tasoa unionissa.

Kohde ja soveltamisala (1 ja 2 artikla)

Direktiivissä säädetään erityisesti seuraavaa: a) jäsenvaltiot velvoitetaan laatimaan kansallinen kyberturvallisuusstrategia sekä nimeämään toimivaltaiset kansalliset viranomaiset, keskitetyt yhteyspisteet ja CSIRT-yksiköt, b) jäsenvaltioiden on vahvistettava kyberturvariskien hallintaa ja raportointia koskevat velvoitteet liitteessä I tarkoitetuille keskeisille toimijoille ja liitteessä II tarkoitetuille tärkeille toimijoille, c) jäsenvaltioiden on vahvistettava kyberturvatietojen jakamista koskevat velvoitteet.

Direktiiviä sovelletaan tiettyihin julkisiin tai yksityisiin keskeisiin toimijoihin, jotka toimivat liitteessä I luetelluilla toimialoilla (energia, liikenne, pankkitoiminta, rahoitusmarkkinoiden infrastruktuurit, terveys, juomavesi, jätevesi, digitaalinen infrastruktuuri, julkishallinto ja avaruus) ja tiettyihin tärkeisiin toimijoihin, jotka toimivat liitteessä II luetelluilla toimialoilla (posti- ja kuriiripalvelut, jätehuolto, kemikaalien valmistus, tuotanto ja jakelu, elintarvikkeiden tuotanto, jalostus ja jakelu, valmistusteollisuus ja digitaaliset palvelut). Direktiivin soveltamisalan ulkopuolelle jäävät 6 päivänä toukokuuta 2003 annetussa komission suosituksessa 2003/361/EY tarkoitetut mikro- ja pientoimijat, lukuun ottamatta sähköisten viestintäverkkojen tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajia, luottamuspalvelujen tarjoajia, aluetunnusrekistereitä (TLD-rekisterit) ja

[8] Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27. huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus) (EUVL L 119, 4.5.2016, s. 1).

julkishallintoa sekä tiettyjä muita toimijoita, kuten tietyn palvelun ainoaa tarjoajaa tietyssä jäsenvaltiossa.

Kansalliset kyberturvallisuuspuitteet (5–11 artikla)

Jäsenvaltioiden on laadittava kansallinen kyberturvallisuusstrategia, jossa määritellään strategiset tavoitteet sekä asianmukaiset politiikka- ja sääntelytoimenpiteet kyberturvallisuuden korkean tason saavuttamiseksi ja ylläpitämiseksi.

Direktiivissä vahvistetaan myös puitteet koordinoidulle haavoittuvuustietojen jakamiselle ja edellytetään, että jäsenvaltiot nimeävät CSIRT-yksiköt toimimaan luotettavina välittäjinä ja helpottamaan vuorovaikutusta raportoivien toimijoiden sekä tieto- ja viestintätekniikan tuotteiden ja palvelujen valmistajien tai tarjoajien välillä. ENISAn on kehitettävä eurooppalainen haavoittuvuusrekisteri havaittuja haavoittuvuuksia varten ja ylläpidettävä sitä.

Jäsenvaltioiden on otettava käyttöön kansalliset kyberturvallisuuden kriisinhallintakehykset muun muassa nimeämällä kansalliset toimivaltaiset viranomaiset, jotka vastaavat laajamittaisten kyberturvapoikkeamien ja -kriisien hallinnasta.

Jäsenvaltioiden on myös nimettävä yksi tai useampi kyberturvallisuuden alalla toimivaltainen kansallinen viranomainen tämän direktiivin mukaisia valvontatehtäviä varten ja kyberturvallisuuden kansallinen keskitetty yhteyspiste, joka hoitaa yhteyksiä jäsenvaltioiden rajat ylittävän viranomaisyhteistyön varmistamiseksi. Jäsenvaltioiden on myös nimettävä CSIRT-yksiköt.

Yhteistyö (12–16 artikla)

Direktiivillä perustetaan yhteistyöryhmä tukemaan ja helpottamaan strategista yhteistyötä ja tiedonvaihtoa jäsenvaltioiden välillä sekä vahvistamaan keskinäistä luottamusta. Lisäksi sillä perustetaan CSIRT-verkosto edistämään luottamuksen vahvistumista jäsenvaltioiden välillä sekä nopeaa ja tehokasta operatiivista yhteistyötä.

Direktiivillä perustetaan myös Euroopan kyberkriisien yhteysorganisaatioiden verkosto (EU-CyCLONe) tukemaan laajamittaisten kyberturvapoikkeamien ja -kriisien koordinoitua hallintaa ja varmistamaan säännöllinen tietojenvaihto jäsenvaltioiden ja EU:n toimielinten välillä.

ENISAn on annettava yhteistyössä komission kanssa joka toinen vuosi raportti kyberturvallisuuden tilasta unionissa.

Komission on perustettava vertaisarviointijärjestelmä, joka mahdollistaa säännölliset vertaisarvioinnit jäsenvaltioiden kyberturvapolitiikkojen toimivuudesta.

Kyberturvariskien hallintaa ja raportointia koskevat velvoitteet (17–23 artikla)

Direktiivin mukaan jäsenvaltioiden on säädettävä, että kaikkien soveltamisalaan kuuluvien toimijoiden hallintoelimet hyväksyvät kyseisten toimijoiden kyberturvariskien hallintatoimenpiteet ja osallistuvat kyberturvaan liittyvään erityiskoulutukseen.

Jäsenvaltioiden on varmistettava, että soveltamisalaan kuuluvat toimijat toteuttavat asianmukaiset ja oikeasuhteiset tekniset ja organisatoriset toimenpiteet verkko- ja tietojärjestelmien turvallisuuteen kohdistuvien kyberturvariskien hallitsemiseksi. Niiden on

myös varmistettava, että toimijat ilmoittavat kansallisille toimivaltaisille viranomaisille tai CSIRT-yksiköille kaikista kyberturvapoikkeamista, joilla on merkittävä vaikutus palveluntarjontaan.

Aluetunnusrekisterien ja aluetunnusten alaisten verkkotunnusten rekisteröintipalveluja tarjoavien toimijoiden on kerättävä ja ylläpidettävä tarkkoja ja täydellisiä verkkotunnusten rekisteröintitietoja. Lisäksi niiden on tarjottava sitä perustellusti pyytäville tosiasiallinen pääsy verkkotunnusten rekisteröintitietoihin.

Lainkäyttövalta ja rekisteröinti (24 ja 25 artikla)

Keskeisten ja tärkeiden toimijoiden katsotaan pääsääntöisesti kuuluvan sen jäsenvaltion lainkäyttövaltaan, jossa ne tarjoavat palvelujaan. Tietyntyyppisten toimijoiden (verkkotunnuspalvelujen tarjoajat, aluetunnusrekisterit, pilvipalvelujen tarjoajat, datakeskuspalvelujen tarjoajat ja sisällönjakeluverkkojen tarjoajat sekä tietyt digitaalisten palvelujen tarjoajat) katsotaan kuitenkin kuuluvan sen jäsenvaltion lainkäyttövaltaan, jossa niiden päätoimipaikka on unionissa. Näin varmistetaan, että tällaisiin toimijoihin ei kohdistu monia erilaisia oikeudellisia vaatimuksia, koska ne tarjoavat palveluja rajojen yli erityisen suuressa määrin. ENISAn on luotava rekisteri viimeksi mainitun tyyppisistä toimijoista ja ylläpidettävä sitä.

Tietojenvaihto (26 ja 27 artikla)

Jäsenvaltioiden on vahvistettava säännöt, jotka antavat toimijoille mahdollisuuden osallistua kyberturvallisuuteen liittyvien tietojen jakamiseen erityisten kyberturvatietojen jakamisjärjestelyjen puitteissa Euroopan unionin toiminnasta tehdyn sopimuksen 101 artiklan mukaisesti. Lisäksi jäsenvaltioiden on sallittava, että tämän direktiivin soveltamisalaan kuulumattomat toimijat raportoivat vapaaehtoisesti merkittävistä poikkeamista, kyberuhkista tai läheltä piti -tilanteista.

Valvonta ja täytäntöönpano (28–34 artikla)

Toimivaltaisten viranomaisten on valvottava direktiivin soveltamisalaan kuuluvia toimijoita ja erityisesti varmistettava, että ne noudattavat turvallisuutta ja poikkeamien ilmoittamista koskevia vaatimuksia. Direktiivissä erotetaan toisistaan ennakkovalvontajärjestelmä, joka koskee keskeisiä toimijoita, ja jälkikäteisvalvontajärjestelmä, joka koskee tärkeitä toimijoita. Jälkimmäisessä edellytetään, että toimivaltaiset viranomaiset ryhtyvät toimiin, jos ne saavat näyttöä tai viitteitä siitä, että tärkeä toimija ei täytä turvallisuutta ja poikkeamien ilmoittamista koskevia vaatimuksia.

Direktiivissä edellytetään myös, että jäsenvaltiot määräävät tarvittaessa hallinnollisia sakkoja keskeisille ja tärkeille toimijoille, ja määritellään tietyt enimmäissakot.

Jäsenvaltioiden on tehtävä yhteistyötä ja avustettava toisiaan tarpeen mukaan, kun toimijat tarjoavat palveluja useammassa kuin yhdessä jäsenvaltiossa tai kun toimijan päätoimipaikka tai sen edustaja sijaitsee tietyssä jäsenvaltiossa, mutta sen verkko- ja tietojärjestelmät sijaitsevat yhdessä tai useammassa muussa jäsenvaltiossa.

2020/0359 (COD)

Ehdotus

EUROOPAN PARLAMENTIN JA NEUVOSTON DIREKTIIVI

toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi koko unionissa ja direktiivin (EU) 2016/1148 kumoamisesta

(ETA:n kannalta merkityksellinen teksti)

EUROOPAN PARLAMENTTI JA EUROOPAN UNIONIN NEUVOSTO, jotka

ottavat huomioon Euroopan unionin toiminnasta tehdyn sopimuksen ja erityisesti sen 114 artiklan,

ottavat huomioon Euroopan komission ehdotuksen,

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

ottavat huomioon Euroopan talous- ja sosiaalikomitean lausunnon[9],

ottavat huomioon alueiden komitean lausunnon[10],

noudattavat tavallista lainsäätämisjärjestystä,

sekä katsovat seuraavaa:

(1) Euroopan parlamentin ja neuvoston direktiivin (EU) 2016/1148[11] tavoitteena oli kehittää kyberturvallisuusvalmiuksia kaikkialla unionissa, lieventää keskeisten palvelujen tarjoamiseen keskeisillä aloilla käytettäviin verkko- ja tietojärjestelmiin kohdistuvia uhkia ja varmistaa tällaisten palvelujen jatkuvuus kyberturvapoikkeamatilanteissa, ja tukea näin unionin talouden ja yhteiskunnan tehokasta toimintaa.

(2) Direktiivin (EU) 2016/1148 voimaantulon jälkeen on edistytty merkittävästi kyberturvavalmiuksien parantamisessa unionissa. Kyseisen direktiivin uudelleentarkastelu on osoittanut, että se on vauhdittanut institutionaalista ja sääntelyyn perustuvaa lähestymistapaa kyberturvallisuuteen unionissa ja tasoittanut tietä merkittävälle ajattelutavan muutokselle. Direktiivillä on varmistettu kansallisten kehysten luominen määrittelemällä kansalliset kyberturvallisuusstrategiat, luomalla kansallisia valmiuksia ja toteuttamalla sääntelytoimenpiteitä, jotka kattavat kunkin jäsenvaltion yksilöimät keskeiset infrastruktuurit ja toimijat. Se on myös edistänyt yhteistyötä unionin tasolla, kun on perustettu erityinen yhteistyöryhmä[12] ja tietoturvaloukkauksiin reagoivien kansallisten yksiköiden verkosto, jäljempänä

[9] EUVL C […], […], s. […].

[10] EUVL C […], […], s. […].

[11] Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/1148, annettu 6 päivänä heinäkuuta 2016, toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa (EUVL L 194, 19.7.2016, s. 1).

[12] Direktiivin (EU) 2016/1148 11 artikla.

’CSIRT-verkosto’[13]. Näistä saavutuksista huolimatta direktiivin (EU) 2016/1148 uudelleentarkastelussa on tullut esiin sisälähtöisiä puutteita, joiden vuoksi direktiivillä ei kyetä tuloksellisesti puuttumaan nykyisiin ja esiin nousemassa oleviin kyberturvallisuushaasteisiin.

(3) Verkko- ja tietojärjestelmät ovat kehittyneet arjen keskeiseksi osaksi yhteiskuntien nopean digitalisaation ja verkottumisen myötä, myös rajat ylittävässä yhteydenpidossa. Tämä kehitys on laajentanut kyberturvauhkia ja tuonut mukanaan uusia haasteita, jotka edellyttävät mukautettuja, koordinoituja ja innovatiivisia vastatoimia kaikissa jäsenvaltioissa. Kyberturvapoikkeamien määrä, laajuus, kehittyneisyys, esiintymistiheys ja vaikutukset lisääntyvät, ja ne muodostavat merkittävän uhan verkko- ja tietojärjestelmien toiminnalle. Tämän seurauksena kyberturvapoikkeamat voivat haitata taloudellisen toiminnan harjoittamista sisämarkkinoilla, aiheuttaa taloudellisia tappioita, heikentää käyttäjien luottamusta ja aiheuttaa huomattavaa vahinkoa unionin taloudelle ja yhteiskunnalle. Kyberturvavalmiudet ja kyberturvan toimivuus ovat siksi nyt tärkeämpiä kuin koskaan sisämarkkinoiden moitteettoman toiminnan kannalta.

(4) Direktiivin 1148/2016/EU oikeusperusta oli Euroopan unionin toiminnasta tehdyn sopimuksen (SEUT) 114 artikla, jonka tavoitteena on sisämarkkinoiden toteuttaminen ja toiminta tehostamalla toimenpiteitä kansallisten sääntöjen lähentämiseksi. Palveluja tai taloudellisesti merkityksellisiä toimintoja tarjoaville toimijoille asetetut kyberturvallisuusvaatimukset vaihtelevat huomattavasti jäsenvaltioittain vaatimusten tyypin, yksityiskohtaisuuden ja valvontamenetelmän osalta. Nämä erot aiheuttavat lisäkustannuksia ja vaikeuksia yrityksille, jotka tarjoavat tavaroita tai palveluja rajojen yli. Yhden jäsenvaltion asettamat vaatimukset, jotka ovat erilaisia tai jopa ristiriidassa toisen jäsenvaltion asettamien vaatimusten suhteen, voivat vaikuttaa merkittävästi rajat ylittävään toimintaan. Lisäksi kyberturvastandardien puutteellisella toteutuksella yhdessä jäsenvaltiossa on todennäköisesti vaikutuksia muiden jäsenvaltioiden kyberturvatasoon, erityisesti kun otetaan huomioon rajojen yli tapahtuvan toiminnan määrä. Direktiivin (EU) 2016/1148 uudelleentarkastelu on osoittanut, että jäsenvaltiot ovat panneet sen täytäntöön hyvin eri tavoin, myös sen soveltamisalan osalta, jonka rajaaminen on suurelta osin jätetty jäsenvaltioiden harkintavaltaan. Direktiivissä (EU) 2016/1148 säädetään myös, että jäsenvaltioilla on hyvin laaja harkintavalta siinä säädettyjen turvallisuutta ja vaaratilanteista ilmoittamista koskevien velvoitteiden täytäntöönpanossa. Nämä velvoitteet on näin ollen pantu täytäntöön huomattavasti eri tavoin kansallisella tasolla. Samankaltaisia eroja esiintyi valvontaa ja täytäntöönpanoa koskevien direktiivin säännösten osalta.

(5) Kaikki nämä erot aiheuttavat sisämarkkinoiden pirstoutumista ja voivat haitata niiden toimintaa, mikä vaikuttaa erityisesti rajat ylittävään palveluntarjontaan ja kyberturvatasoon, kun käytössä on toisistaan poikkeavia standardeja. Tällä direktiivillä pyritään poistamaan näitä suuria eroja jäsenvaltioiden välillä erityisesti vahvistamalla vähimmäissäännöt koordinoidun sääntelykehyksen toiminnalle, vahvistamalla mekanismit kunkin jäsenvaltion vastuuviranomaisten toimivaa yhteistyötä varten, päivittämällä luettelo aloista ja toiminnoista, joihin sovelletaan kyberturvavelvoitteita, ja säätämällä tehokkaista oikeussuojakeinoista ja seuraamuksista, jotka ovat olennaisen tärkeitä velvoitteiden tehokkaan täytäntöönpanon kannalta. Sen vuoksi direktiivi (EU) 2016/1148 olisi kumottava ja korvattava tällä direktiivillä.

[13] Direktiivin (EU) 2016/1148 12 artikla.

(6) Tällä direktiivillä ei rajoiteta jäsenvaltioiden mahdollisuutta toteuttaa tarvittavat toimenpiteet keskeisten turvallisuusetujensa suojaamiseksi, yleisen järjestyksen ja turvallisuuden takaamiseksi sekä rikosten tutkinnan, selvittämisen ja syytteeseenpanon mahdollistamiseksi unionin oikeuden mukaisesti. SEUT-sopimuksen 346 artiklan mukaan mikään jäsenvaltio ei ole velvollinen antamaan tietoja, joiden ilmaiseminen olisi vastoin sen keskeisiä yleiseen turvallisuuteen liittyviä etuja. Tässä yhteydessä merkityksellisiä ovat turvallisuusluokiteltujen tietojen suojaamista koskevat kansalliset ja unionin säännöt, salassapitosopimukset ja epäviralliset salassapitosopimukset , kuten Traffic Light Protocol -käsittelyluokitus[14].

(7) Kun direktiivi (EU) 2016/1148 kumotaan, toimialoittainen soveltamisala olisi laajennettava koskemaan suurempaa osaa taloudesta johdanto-osan kappaleissa 4–6 esitettyjen huomioiden perusteella. Direktiivin (EU) 2016/1148 soveltamisalaa olisi sen vuoksi laajennettava kattavasti niihin aloihin ja palveluihin, jotka ovat olennaisen tärkeitä yhteiskunnan ja talouden avaintoimintojen kannalta sisämarkkinoilla. Säännöt eivät saisi poiketa toisistaan sen mukaan, ovatko toimijat keskeisten palvelujen tarjoajia vai digitaalisten palvelujen tarjoajia. Tämä erottelu on osoittautunut tarpeettomaksi, koska se ei kuvasta toimialojen tai palvelujen todellista merkitystä yhteiskunnalliselle ja taloudelliselle toiminnalle sisämarkkinoilla.

(8) Direktiivin (EU) 2016/1148 mukaisesti jäsenvaltiot olivat vastuussa sen määrittämisestä, mitkä toimijat täyttävät kriteerit, joiden perusteella niitä voidaan pitää keskeisten palvelujen tarjoajina, jäljempänä ’tunnistamisprosessi’. Jotta voidaan poistaa jäsenvaltioiden väliset suuret erot tältä osin ja varmistaa kaikkien asianomaisten toimijoiden riskinhallintavaatimusten ja raportointivelvoitteiden oikeusvarmuus, olisi vahvistettava yhdenmukainen kriteeri, jolla määritetään tämän direktiivin soveltamisalaan kuuluvat toimijat. Tämän kriteerin olisi koostuttava kokokattosäännön soveltamisesta, jolloin kaikki komission suosituksessa 2003/361/EY[15] määritellyt keskisuuret ja suuret yritykset, jotka toimivat tämän direktiivin kattamilla aloilla tai tarjoavat tämän direktiivin kattamia palveluja, kuuluvat sen soveltamisalaan. Jäsenvaltioita ei pitäisi vaatia laatimaan luetteloa toimijoista, jotka täyttävät tämän yleisesti sovellettavan kokoon liittyvän kriteerin.

(9) Tämän direktiivin olisi kuitenkin katettava myös sellaiset pienet tai mikrotoimijat, jotka täyttävät tietyt kriteerit, jotka osoittavat niiden olevan avainasemassa jäsenvaltion taloudessa tai yhteiskunnassa tai tietyllä alalla tai tietyntyyppisissä palveluissa. Jäsenvaltioiden olisi vastattava tällaisten toimijoiden luettelon laatimisesta ja toimitettava se komissiolle.

(10) Komissio voi yhteistyössä yhteistyöryhmän kanssa antaa ohjeita mikro- ja pienyrityksiin sovellettavien kriteerien käytöstä.

(11) Tämän direktiivin soveltamisalaan kuuluvat toimijat olisi luokiteltava kahteen luokkaan sen mukaan, millä alalla ne toimivat tai millaisia palveluja ne tarjoavat: keskeisiin ja tärkeisiin. Luokittelussa olisi otettava huomioon alan tai palvelutyypin kriittisyys sekä muiden alojen tai palvelutyyppien riippuvuus siitä. Sekä keskeisiin että tärkeisiin toimijoihin olisi sovellettava samoja riskinhallintavaatimuksia ja

---

14 Liikennevalomalli (Traffic Light Protocol, TLP) on tapa, jolla tietoa antava taho voi tiedottaa tiedon vastaanottajille mahdollisista rajoituksista tietojen levittämisessä edelleen. Sitä käytetään lähes kaikissa CSIRT-yhteisöissä ja joissakin ISAC-keskuksissa (Information Analysis and Sharing Centres).

15 Komission suositus 2003/361/EY, annettu 6 päivänä toukokuuta 2003, mikroyritysten sekä pienten ja keskisuurten yritysten määritelmästä (EUVL L 124, 20.5.2003, s. 36).

raportointivelvoitteita. Näiden kahden toimijaluokan valvonta- ja seuraamusjärjestelmät olisi eriytettävä, jotta voidaan varmistaa oikeudenmukainen tasapaino toisaalta vaatimusten ja velvoitteiden ja toisaalta sääntöjen noudattamisen valvonnasta aiheutuvan hallinnollisen rasituksen välillä.

(12) Alakohtaisella lainsäädännöllä ja alakohtaisilla toimilla voidaan osaltaan varmistaa korkea kyberturvataso samalla kun otetaan kaikilta osin huomioon eri alojen erityispiirteet ja riippuvuussuhteet. Jos alakohtaisessa unionin säädöksessä edellytetään, että keskeiset tai tärkeät toimijat ottavat käyttöön kyberturvariskien hallintatoimenpiteitä tai ilmoittavat poikkeamista tai merkittävistä kyberuhista, ja tällä on vähintään vastaava vaikutus kuin tässä direktiivissä säädetyillä velvoitteilla, olisi sovellettava kyseisiä alakohtaisia säännöksiä, mukaan lukien valvontaa ja täytäntöönpanoa koskevat säännökset. Komissio voi laatia erityissäädösten (*lex specialis*) täytäntöönpanoa koskevia ohjeita. Tämä direktiivi ei estä hyväksymästä lisää alakohtaisia unionin säädöksiä, jotka koskevat kyberturvariskien hallintatoimenpiteitä ja poikkeamailmoituksia. Tämä direktiivi ei vaikuta nykyiseen täytäntöönpanovaltaan, joka on siirretty komissiolle useilla aloilla, mukaan lukien liikenne ja energia.

(13) Euroopan parlamentin ja neuvoston asetusta XXXX/XXXX[16] olisi pidettävä tähän direktiiviin liittyvänä alakohtaisena unionin säädöksenä finanssialan toimijoiden osalta. Asetuksen XXXX/XXXX säännöksiä, jotka liittyvät tieto- ja viestintätekniikan riskinhallintatoimenpiteisiin, tieto- ja viestintätekniikkaan liittyvien poikkeamien hallintaan ja erityisesti poikkeamista raportointiin sekä digitaalisen toiminnallisen häiriönsietokyvyn testaukseen, tiedonjakojärjestelyihin ja kolmannen osapuolen tieto- ja viestintätekniikan riskeihin, olisi sovellettava asiaan liittyvien tämän direktiivin säännösten asemesta. Sen vuoksi jäsenvaltioiden ei pitäisi soveltaa tämän direktiivin säännöksiä, jotka koskevat kyberturvariskien hallintaa ja raportointivelvoitteita, tietojen jakamista sekä valvontaa ja täytäntöönpanoa, asetuksen XXXX/XXXX soveltamisalaan kuuluviin finanssialan toimijoihin. Samalla on tärkeää säilyttää tämän direktiivin mukainen vahva yhteys ja tiedonvaihto finanssialan kanssa. Tätä varten asetuksessa XXXX/XXXX annetaan kaikille finanssivalvojille, finanssialan osalta Euroopan valvontaviranomaisille ja asetuksen XXXX/XXXX mukaisille kansallisille toimivaltaisille viranomaisille mahdollisuus osallistua yhteistyöryhmän strategisiin periaatekeskusteluihin ja tekniseen toimintaan sekä vaihtaa tietoja ja tehdä yhteistyötä tämän direktiivin nojalla nimettyjen keskitettyjen asiointipisteiden ja kansallisten CSIRT-yksiköiden kanssa. Asetuksen XXXX/XXXX mukaisten toimivaltaisten viranomaisten olisi toimitettava tiedot merkittävistä tieto- ja viestintätekniikkaan liittyvistä poikkeamista myös tämän direktiivin mukaisesti nimetyille yhteyspisteille. Lisäksi jäsenvaltioiden olisi edelleen sisällytettävä rahoitusala kyberturvallisuusstrategioihinsa, ja kansalliset CSIRT-yksiköt voivat kattaa finanssisektorin toiminnassaan.

(14) Kyberturvallisuuden ja toimijoiden fyysisen turvallisuuden välisten yhteyksien vuoksi olisi varmistettava johdonmukainen lähestymistapa Euroopan parlamentin ja neuvoston direktiivin (EU) XXX/XXX[17] ja tämän direktiivin välillä. Tämän saavuttamiseksi jäsenvaltioiden olisi varmistettava, että direktiivin (EU) XXX/XXX mukaisia kriittisiä toimijoita ja vastaavia toimijoita pidetään tämän direktiivin mukaisina keskeisinä toimijoina. Jäsenvaltioiden olisi myös varmistettava, että niiden

16 *[lisätään koko nimi ja EUVL:n julkaisuviite, kun ne ovat tiedossa]*

17 *[lisätään koko nimi ja EUVL:n julkaisuviite, kun ne ovat tiedossa]*

kyberturvallisuusstrategiat sisältävät puitteet tämän direktiivin ja direktiivin (EU) XXX/XXX mukaisen toimivaltaisen viranomaisen välisen koordinoinnin tehostamiselle poikkeamia ja kyberuhkia koskevan tietojenvaihdon ja valvontatehtävien hoitamisen yhteydessä. Molempien direktiivien nojalla nimettyjen viranomaisten olisi tehtävä yhteistyötä ja vaihdettava tietoja erityisesti kriittisten toimijoiden, kyberuhkien, kyberturvariskien ja kriittisiin toimijoihin vaikuttavien poikkeamien tunnistamisen sekä kriittisten toimijoiden kyberturvatoimenpiteiden suhteen. Direktiivin (EU) XXX/XXX mukaisten toimivaltaisten viranomaisten pyynnöstä tämän direktiivin mukaisten toimivaltaisten viranomaisten olisi voitava käyttää valvonta- ja täytäntöönpanovaltuuksiaan kriittiseksi määritellyn keskeisen toimijan osalta. Molempien viranomaisten olisi tehtävä yhteistyötä ja vaihdettava tietoja tätä tarkoitusta varten.

(15) Luotettavan, häiriönsietokykyisen ja turvallisen verkkotunnusjärjestelmän (DNS) ylläpitäminen ja säilyttäminen on keskeinen tekijä internetin eheyden kannalta, ja olennaisen tärkeää internetin jatkuvan ja vakaan toiminnan kannalta, mistä koko digitaalitalous ja -yhteiskunta ovat riippuvaisia. Sen vuoksi tätä direktiiviä olisi sovellettava kaikkiin DNS-palvelujen tarjoajiin DNS-selvitysketjussa, mukaan lukien juuripalvelinten ylläpitäjät, ylätason tunnusten nimipalvelimet (TLD), verkkotunnuksia vastaavia IP-osoitteita selvittävät auktoritatiiviset nimipalvelimet ja osoitteita ensin sisäisesti selvittävät rekursiiviset nimipalvelimet.

(16) Pilvipalvelujen olisi katettava palvelut, jotka mahdollistavat skaalattavien ja joustavien tietoteknisten resurssien jaettavan ja hajautetun reservin laajan tarveperusteisen etäkäytön. Näihin tietoteknisiin resursseihin kuuluu esimerkiksi verkkoja, palvelimia ja muuta infrastruktuuria, käyttöjärjestelmiä, ohjelmistoja, tallennustilaa, sovelluksia ja palveluja. Pilvipalvelujen toimintamalleina olisi otettava huomioon yksityiset, yhteisövetoiset, julkiset ja hybridipilvipalvelut. Edellä mainituilla palvelu- ja toimintamalleilla tarkoitetaan samaa kuin standardissa ISO/IEC 17788:2014 määritellyillä palvelu- ja toimintamalleilla. Pilvipalvelun käyttäjän kykyä käyttää yksipuolisesti ja oma-aloitteisesti tietojenkäsittelyvalmiuksia, kuten palvelinaikaa tai verkkotallennustilaa ilman pilvipalveluntarjoajan inhimillistä panosta voitaisiin kuvata ’tarvepohjaiseksi ohjaukseksi’. ’Laajalla etäkäytöllä’ tarkoitetaan sitä, että pilvipalveluresursseja tarjotaan verkossa ja niitä voidaan käyttää menetelmillä, jotka sallivat erilaisten prosessointivalmiuksiltaan kevyiden tai raskaiden päätelaitteiden käytön (esim. älypuhelimet, tablettitietokoneet, kannettavat tietokoneet, työasemat). Termi ’skaalautuva’ viittaa tietoteknisiin resursseihin, joita pilvipalvelujen tarjoaja jakaa muuntuvasti resurssien maantieteellisestä sijainnista riippumatta kysynnän vaihtelun mukaan. ’Joustavuudella’ viitataan tietoteknisiin resursseihin joita vapautetaan käyttöön ja tarjotaan kysynnän mukaan niin, että resursseja voidaan nopeasti kasvattaa ja vähentää kuormituksen mukaisesti. ’Jaettavalla’ viitataan tietoteknisiin resursseihin, joita tarjotaan yhteisen pääsyn resursseihin jakavalle käyttäjäkunnalle niin, että prosessointi tapahtuu käyttäjäkohtaisesti vaikka palvelua tarjotaan saman laitteiston kautta. Termiä ’hajautettu’ käytetään kuvaamaan tietoteknisiä resursseja, jotka sijaitsevat erillisissä verkotetuissa tietokoneissa tai laitteissa ja jotka viestivät ja koordinoivat toimintaansa keskenään rakenteisella viestinvaihdolla.

(17) Innovatiivisten teknologioiden ja uusien liiketoimintamallien myötä markkinoille odotetaan tulevan uusia pilvipalvelujen käyttö- ja palvelumalleja vastauksena asiakkaiden muuttuviin tarpeisiin. Pilvipalveluja voidaan tarjota hyvin hajautetussa

muodossa ja entistä lähempänä paikkaa, jossa dataa tuotetaan tai kerätään, jolloin siirrytään perinteisestä mallista pitkälle hajautettuun malliin (ns. reunalaskentamalli).

(18) Datakeskuspalveluja ei välttämättä aina tarjota pilvipalveluna. Näin ollen datakeskukset eivät välttämättä aina ole osa pilvipalveluinfrastruktuuria. Kaikkien verkko- ja tietojärjestelmien turvallisuuteen kohdistuvien riskien hallitsemiseksi tämän direktiivin olisi katettava myös sellaisten datakeskuspalvelujen tarjoajat, jotka eivät ole pilvipalveluja. Tässä direktiivissä ’datakeskuspalvelulla’ olisi tarkoitettava sellaisen palvelun tarjoamista, joka käsittää rakenteita tai rakenteiden ryhmiä, jotka on tarkoitettu datan tallennus-, käsittely- ja siirtopalveluja tarjoavien tietoteknisten ja verkkolaitteiden keskitettyyn ylläpitoon, yhteenliittämiseen ja ohjaukseen yhdessä kaikkien tarvittavien sähkönjakeluun ja toimintaolosuhteiden säätelyyn tarkoitettujen laitteiden ja infrastruktuurien kanssa. Termi ’datakeskuspalvelu’ ei kata tietyn toimijan itse omistamia ja omiin käyttötarkoituksiinsa käyttämiä sisäisiä datakeskuksia.

(19) Euroopan parlamentin ja neuvoston direktiivissä 97/67/EY[18] tarkoitettujen postipalvelujen tarjoajien sekä pikalähetys- ja kuriiripalvelujen tarjoajien olisi kuuluttava tämän direktiivin soveltamisalaan, jos ne tarjoavat vähintään yhden postiketjun vaiheista ja erityisesti osoitteenselvityksen, lajittelun tai jakelun, mukaan lukien noutopalvelut. Kuljetuspalvelut, jotka eivät koske jotain näistä vaiheista, olisi jätettävä postipalvelujen määritelmän ulkopuolelle.

(20) Nämä kasvavat keskinäiset riippuvuussuhteet ovat tulosta yhä useammin rajat ylittävästä ja keskinäisriippuvaisesta palveluntarjontaverkostosta, jossa käytetään keskeisiä infrastruktuureja eri puolilla unionia energian, liikenteen, digitaalisen infrastruktuurin, juoma- ja jäteveden, terveyden, julkishallinnon tiettyjen näkökohtien alalla sekä avaruustoiminnassa siltä osin kuin on kyse tiettyjen sellaisten palvelujen tarjoamisesta, jotka riippuvat joko jäsenvaltioiden tai yksityisten osapuolten omistamasta, hallinnoimasta ja käyttämästä maassa sijaitsevasta infrastruktuurista, eli lukuun ottamatta infrastruktuureja, jotka ovat unionin omistamia, hallinnoimia tai sen puolesta hallinnoituja osana sen avaruusohjelmia. Nämä keskinäiset riippuvuussuhteet merkitsevät sitä, että kaikilla häiriöillä, vaikka ne alun perin rajoittuisivatkin yhteen toimijaan tai yhteen toimialaan, voi olla ketjureaktiovaikutuksia, jotka voivat johtaa kauaskantoisiin ja pitkäaikaisiin kielteisiin vaikutuksiin palvelujen tarjontaan sisämarkkinoilla. Covid-19-pandemia on osoittanut yhä voimakkaammin keskinäisriippuvaisten yhteiskuntiemme haavoittuvuuden kohdatessamme alhaisen todennäköisyyden riskejä.

(21) Kansallisten hallintorakenteiden erojen vuoksi ja jo olemassa olevien alakohtaisten järjestelyjen tai unionin valvonta- ja sääntelyelinten turvaamiseksi jäsenvaltioiden olisi voitava nimetä useampi kuin yksi kansallinen toimivaltainen viranomainen, joka vastaa keskeisten ja tärkeiden toimijoiden verkko- ja tietojärjestelmien turvallisuuteen liittyvien tämän direktiivin mukaisten tehtävien suorittamisesta. Jäsenvaltioiden olisi voitava antaa tämä tehtävä jo olemassa olevalle viranomaiselle.

(22) Viranomaisten välisen rajat ylittävän yhteistyön ja viestinnän helpottamiseksi ja tämän direktiivin tehokkaan täytäntöönpanon mahdollistamiseksi on tarpeen, että kukin jäsenvaltio nimeää kansallisen keskitetyn yhteyspisteen, joka vastaa verkko- ja

[18] Euroopan parlamentin ja neuvoston direktiivi 97/67/EY, annettu 15 päivänä joulukuuta 1997, yhteisön postipalvelujen sisämarkkinoiden kehittämistä ja palvelun laadun parantamista koskevista yhteisistä säännöistä (EYVL L 15, 21.1.1998, s. 14).

tietojärjestelmien turvallisuuteen ja rajat ylittävään yhteistyöhön liittyvien kysymysten koordinoinnista unionin tasolla.

(23) Toimivaltaisten viranomaisten tai CSIRT-yksiköiden olisi saatava ilmoitukset poikkeamista toimijoilta toimivalla ja tehokkaalla tavalla. Keskitetyille yhteyspisteille olisi annettava tehtäväksi toimittaa poikkeamailmoitukset edelleen muiden asianomaisten jäsenvaltioiden keskitettyihin yhteyspisteisiin. Jäsenvaltioiden viranomaisten tasolla sen varmistamiseksi, että jokaisessa jäsenvaltiossa on yksi keskitetty asiointipiste, yhteyspisteiden olisi myös oltava toimivaltaisten viranomaisten asetuksen XXXX/XXXX mukaisesti toimittamien, finanssialan yhteisöjä koskevia turvapoikkeamia koskevien asiaankuuluvien tietojen vastaanottajia, jotta ne voisivat tarvittaessa toimittaa nämä tiedot eteenpäin tämän direktiivin mukaisille asiaankuuluville kansallisille toimivaltaisille viranomaisille tai CSIRT-yksiköille.

(24) Jäsenvaltioilla olisi oltava käytössään riittävät sekä tekniset että organisatoriset valmiudet, jotta voidaan ehkäistä ja havaita verkko- ja tietojärjestelmien poikkeamia ja riskejä, reagoida niihin ja lieventää niiden vaikutuksia. Jäsenvaltioiden olisi sen vuoksi varmistettava, että niillä on hyvin toimivat CSIRT-yksiköt, joita kutsutaan myös tietotekniikan CERT-kriisiryhmiksi ja jotka täyttävät keskeiset vaatimukset, jotta voidaan taata tehokkaat ja yhteensopivat valmiudet käsitellä poikkeamia ja riskejä ja varmistaa tehokas yhteistyö unionin tasolla. Toimijoiden ja CSIRT-yksiköiden välisen luottamussuhteen parantamiseksi tapauksissa, joissa CSIRT on osa toimivaltaista viranomaista, jäsenvaltioiden olisi harkittava CSIRT-yksiköiden operatiivisten tehtävien erottamista toiminnallisesti erityisesti tietojen jakamisen ja yhteisöille annettavan tuen osalta ja toimivaltaisten viranomaisten valvontatoimista.

(25) Henkilötietojen osalta CSIRT-yksiköiden olisi voitava Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679[19] mukaisesti tarjota tämän direktiivin nojalla tahon puolesta ja pyynnöstä ennakoiva skannaus verkko- ja tietojärjestelmistä, joita kyseinen taho käyttää palvelujensa tarjontaan. Jäsenvaltioiden olisi pyrittävä varmistamaan, että kaikilla toimialakohtaisilla CSIRT-yksiköillä on yhtäläiset tekniset valmiudet. Jäsenvaltiot voivat pyytää kansallisten CSIRT-yksiköiden kehittämisessä apua Euroopan unionin kyberturvallisuusvirastolta (ENISA).

(26) Kun otetaan huomioon kyberturvallisuutta koskevan kansainvälisen yhteistyön tärkeys, CSIRT-yksiköiden olisi voitava osallistua kansainvälisiin yhteistyöverkostoihin tällä direktiivillä perustetun CSIRT-verkoston lisäksi.

(27) Koordinoidusta reagoinnista laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin annetun komission suosituksen (EU) 2017/1548[20] liitteen mukaisesti laajamittaisella poikkeamalla olisi tarkoitettava poikkeamaa, jolla on merkittävä vaikutus vähintään kahteen jäsenvaltioon tai jonka aiheuttama häiriö ylittää yksittäisen jäsenvaltion valmiudet reagoida siihen. Laajamittaiset poikkeamat voivat niiden syistä ja vaikutuksista riippuen kärjistyä ja muuttua todellisiksi kriiseiksi, jotka estävät sisämarkkinoiden moitteettoman toiminnan. Kun otetaan huomioon tällaisten poikkeamien laaja vaikuttavuus ja useimmissa tapauksissa rajat ylittävä luonne,

[19] Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27. huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus) (EUVL L 119, 4.5.2016, s. 1).

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

jäsenvaltioiden ja asiaankuuluvien unionin toimielinten, elinten ja virastojen olisi tehtävä yhteistyötä teknisellä, operatiivisella ja poliittisella tasolla, jotta reagointia voidaan koordinoida asianmukaisesti kaikkialla unionissa.

(28) Koska verkko- ja tietojärjestelmien haavoittuvuuksien hyödyntäminen voi aiheuttaa merkittäviä häiriöitä ja haittoja, näiden haavoittuvuuksien nopea tunnistaminen ja korjaaminen on tärkeä tekijä kyberturvallisuusriskin vähentämisessä. Tällaisia järjestelmiä kehittävien tahojen olisi sen vuoksi otettava käyttöön asianmukaiset menettelyt haavoittuvuuksien käsittelemiseksi, kun niitä havaitaan. Koska haavoittuvuuksia havaitsevat ja ilmoittavat (julkistavat) usein kolmannet osapuolet (raportoivat tahot), tieto- ja viestintätekniikan tuotteiden tai palvelujen valmistajan tai tarjoajan olisi myös otettava käyttöön tarvittavat menettelyt haavoittuvuustietojen saamiseksi kolmansilta osapuolilta. Tältä osin kansainvälisissä standardeissa ISO/IEC 30111 ja ISO/IEC 29417 annetaan ohjeita haavoittuvuuksien käsittelystä ja haavoittuvuuksien havaitsemisesta. Haavoittuvuuksien julkistamisen osalta on erityisen tärkeää koordinoida toimia raportoivien tahojen ja tieto- ja viestintätekniikan tuotteiden tai palvelujen valmistajien tai tarjoajien välillä. Koordinoidussa haavoittuvuuksien ilmaisemisessa määritellään jäsennelty prosessi, jonka avulla haavoittuvuuksista ilmoitetaan organisaatiolle siten, että se voi diagnosoida haavoittuvuuden ja korjata sen ennen kuin yksityiskohtaiset haavoittuvuustiedot paljastetaan kolmansille osapuolille tai yleisölle. Koordinoituun haavoittuvuuksien ilmaisemiseen olisi kuuluttava myös raportoivan tahon ja organisaation välinen koordinointi korjaamisen ajoituksen ja haavoittuvuuksien julkistamisen osalta.

(29) Jäsenvaltioiden olisi sen vuoksi toteutettava toimenpiteitä haavoittuvuuksien koordinoidun ilmaisemisen helpottamiseksi laatimalla asiaa koskevat kansalliset periaatteet. Tätä varten jäsenvaltioiden olisi nimettävä CSIRT-yksikkö toimimaan koordinaattorina, joka toimii tarvittaessa välittäjänä raportoivien tahojen ja tieto- ja viestintätekniikan tuotevalmistajien tai palveluntarjoajien välillä. CSIRT-koordinaattorin tehtäviin olisi kuuluttava erityisesti asianomaisten tahojen tunnistaminen ja kontaktointi, ilmoittavien tahojen tukeminen, tietojen ilmaisemisen aikataulusta neuvotteleminen ja useisiin organisaatioihin vaikuttavien haavoittuvuuksien hallinta (monenvälinen haavoittuvuuden ilmaiseminen). Jos haavoittuvuudet vaikuttavat useisiin tieto- ja viestintätekniikan laitevalmistajiin tai palveluntarjoajiin, jotka ovat sijoittautuneet useampaan kuin yhteen jäsenvaltioon, kustakin asianomaisesta jäsenvaltiosta nimettyjen CSIRT-yksiköiden olisi tehtävä yhteistyötä CSIRT-verkostossa.

(30) Virheetön ja nopea tiedonsaanti tieto- ja viestintätekniikan tuotteisiin ja palveluihin vaikuttavista haavoittuvuuksista parantaa kyberturvallisuusriskien hallintaa. Tässä mielessä julkisesti saatavilla olevat haavoittuvuuksia koskevat tietolähteet ovat tärkeä apuväline organisaatioille ja niiden käyttäjille mutta myös kansallisille toimivaltaisille viranomaisille ja CSIRT-yksiköille. Tästä syystä ENISAn olisi perustettava haavoittuvuusrekisteri, jossa keskeisen ja tärkeät toimijat ja niiden alihankkijat sekä tahot, jotka eivät kuulu tämän direktiivin soveltamisalaan, voivat vapaaehtoisesti ilmoittaa haavoittuvuuksista ja antaa haavoittuvuustietoja, joiden avulla käyttäjät voivat toteuttaa asianmukaisia lieventäviä toimenpiteitä.

(31) Vaikka vastaavia haavoittuvuusrekistereitä tai tietokantoja on olemassa, niitä isännöivät ja ylläpitävät tahot, jotka eivät ole sijoittautuneet unioniin. ENISAn ylläpitämä Euroopan haavoittuvuusrekisteri lisäisi julkistamisprosessin läpinäkyvyyttä ennen kuin haavoittuvuus virallisesti paljastetaan ja selviytymiskykyä tilanteissa, joissa samankaltaisten palvelujen tarjonta heikentyy tai keskeytyy. Päällekkäisyyksien

välttämiseksi ja täydentävyyden saavuttamiseksi mahdollisimman pitkälle ENISAn olisi tutkittava mahdollisuutta tehdä järjestelmällisiä yhteistyösopimuksia kolmansien maiden lainkäyttöalueilla sijaitsevien vastaavien rekisterien kanssa.

(32) Yhteistyöryhmän olisi laadittava joka toinen vuosi työohjelma, joka sisältää toimet, jotka ryhmän on määrä saada aikaan tavoitteidensa ja tehtäviensä toteuttamiseksi. Tämän direktiivin mukaisesti hyväksytyn ensimmäisen ohjelman aikataulu olisi mukautettava direktiivin (EU) 2016/1148 mukaisesti hyväksytyn viimeisen ohjelman aikatauluun, jotta vältetään mahdolliset häiriöt ryhmän työskentelyssä.

(33) Laatiessaan ohjeasiakirjoja yhteistyöryhmän olisi säännönmukaisesti kartoitettava kansallisia ratkaisuja ja kokemuksia, arvioitava yhteistyöryhmän tulosten vaikutusta kansallisiin lähestymistapoihin, keskusteltava täytäntöönpanon haasteista ja laadittava erityisiä suosituksia olemassa olevien sääntöjen täytäntöönpanon parantamiseksi.

(34) Yhteistyöryhmän olisi pysyttävä joustavana foorumina, ja sen olisi voitava reagoida muuttuviin ja uusiin poliittisiin painopisteisiin ja haasteisiin ottaen samalla huomioon käytettävissä olevat resurssit. Sen olisi järjestettävä säännöllisiä yhteisiä kokouksia asiaankuuluvien yksityisten sidosryhmien kanssa eri puolilta unionia keskustellakseen ryhmän toteuttamista toimista ja kerätäkseen näkemyksiä esiin nousevista politiikkaan vaikuttavista haasteista. Unionin tason yhteistyön tehostamiseksi ryhmän olisi harkittava kyberturvallisuuspolitiikkaan osallistuvien unionin elinten ja virastojen, kuten Euroopan verkkorikostorjuntakeskuksen (EC3), Euroopan unionin lentoturvallisuusviraston (EASA) ja Euroopan unionin avaruusohjelman (EUSPA), kutsumista osallistumaan sen työhön.

(35) Toimivaltaisille viranomaisille ja CSIRT-yksiköille olisi annettava valtuudet osallistua muiden jäsenvaltioiden virkamiesten vaihtojärjestelmiin yhteistyön parantamiseksi. Toimivaltaisten viranomaisten olisi toteutettava tarvittavat toimenpiteet, jotta muiden jäsenvaltioiden virkamiehet voivat tuloksellisesti osallistua vastaanottavan toimivaltaisen viranomaisen toimintaan.

(36) Unionin olisi tarvittaessa tehtävä Euroopan unionin toiminnasta tehdyn sopimuksen 218 artiklan mukaisesti kolmansien maiden tai kansainvälisten järjestöjen kanssa kansainvälisiä sopimuksia, joissa sallitaan ja järjestetään niiden osallistuminen joihinkin yhteistyöryhmän ja CSIRT-verkoston toimiin. Tällaisilla sopimuksilla olisi varmistettava riittävä tietosuoja.

(37) Jäsenvaltioiden olisi osallistuttava suosituksessa (EU) 2017/1584 esitetyn EU:n kyberturvallisuuden kriisinhallintakehyksen perustamiseen olemassa olevien yhteistyöverkostojen, erityisesti kyberkriisien yhteysorganisaatioiden verkoston (EU-CyCLONe), CSIRT-verkoston ja yhteistyöryhmän kautta. EU-CyCLONen ja CSIRT-verkoston olisi tehtävä yhteistyötä sellaisten menettelyllisten järjestelyjen pohjalta, joissa määritellään kyseisen yhteistyön yksityiskohtaiset säännöt. EU-CyCLONen työjärjestyksessä olisi täsmennettävä tarkemmin verkoston toimintatavat, mukaan lukien muun muassa roolit, yhteistyömuodot, vuorovaikutus muiden asiaankuuluvien toimijoiden kanssa ja tiedonvaihdon mallit sekä tiedonvaihdon tekninen toteutustapa. Unionin tason kriisinhallinnassa asianomaisten osapuolten olisi tukeuduttava poliittisen kriisitoiminnan integroituihin järjestelyihin (IPCR). Komission olisi käytettävä tähän tarkoitukseen ARGUS-ohjelman korkean tason monialaista kriisinkoordinointiprosessia. Jos kriisiin liittyy merkittävä ulkoinen tai yhteisen turvallisuus- ja puolustuspolitiikan (YTPP) ulottuvuus, olisi aktivoitava Euroopan ulkosuhdehallinnon (EUH) kriisinhallintamekanismi (CRM).

(38) Tässä direktiivissä termillä ’riski’ olisi viitattava kyberturvallisuuspoikkeaman aiheuttamaan mahdolliseen menetykseen tai häiriöön, ja se olisi ilmaistava tällaisen menetyksen tai häiriön suuruuden ja kyseisen poikkeaman toteutumisen todennäköisyyden yhdistelmänä.

(39) Tässä direktiivissä termillä ’läheltä piti -tilanne’ olisi viitattava tapahtumaan, joka olisi voinut aiheuttaa vahinkoa, mutta jonka täysi toteutuminen kyettiin estämään.

(40) Riskinhallintatoimenpiteisiin olisi sisällyttävä toimenpiteitä, joilla tunnistetaan poikkeamariskit, ehkäistään, havaitaan ja käsitellään niitä ja lievennetään niiden vaikutuksia. Verkko- ja tietojärjestelmien turvallisuuden olisi katettava tallennettavan, siirrettävän ja käsiteltävän datan turvallisuus.

(41) Jotta keskeisille ja tärkeille toimijoille ei aiheutuisi kohtuutonta taloudellista ja hallinnollista rasitetta, kyberturvallisuusriskien hallintaa koskevien vaatimusten olisi oltava oikeassa suhteessa asianomaisen verkko- ja tietojärjestelmän aiheuttamaan riskiin, ottaen huomioon suojatoimenpiteiden viimeisin kehitys.

(42) Keskeisten ja tärkeiden toimijoiden olisi varmistettava toiminnassaan käyttämiensä verkko- ja tietojärjestelmien turvallisuus. Nämä ovat pääasiassa yksityisiä verkko- ja tietojärjestelmiä, joita hallinnoi organisaation sisäinen tietotekniikkahenkilöstö tai joiden turvallisuudesta vastaa alihankkija. Tämän direktiivin mukaisia kyberturvallisuusriskien hallintaa ja raportointia koskevia vaatimuksia olisi sovellettava asiaankuuluviin keskeisiin ja tärkeisiin toimijoihin riippumatta siitä, hoitavatko ne verkko- ja tietojärjestelmiensä ylläpidon sisäisesti vai on se ulkoistettu.

(43) Toimijan toimitusketjusta ja toimijan suhteesta alihankkijoihin johtuviin kyberturvallisuusriskeihin puuttuminen on erityisen tärkeää, kun otetaan huomioon sellaisten poikkeamien yleisyys, joissa toimijat ovat joutuneet kyberhyökkäysten uhreiksi ja joissa vihamieliset toimijat ovat voineet vaarantaa toimijan verkko- ja tietojärjestelmien turvallisuuden hyödyntämällä kolmansien osapuolten tuotteisiin ja palveluihin vaikuttavia haavoittuvuuksia. Toimijoiden olisi sen vuoksi arvioitava ja otettava huomioon käyttämiensä alihankkijoiden ja palveluntarjoajien tuotteiden ja kyberturvallisuuskäytäntöjen kokonaislaatu, mukaan lukien tuotekehityksen suojausmenettelyt.

(44) Palveluntarjoajista erityisen tärkeällä sijalla ovat turvapoikkeamavalvontaa, tunkeutumisenestotestausta, turva-auditointeja ja konsultointia tarjoavat tietoturvapalveluntarjoajat (MSSP), joiden tehtävänä on avustaa toimijoita niiden pyrkiessä havaitsemaan turvapoikkeamat ja reagoimaan niihin. Nämä MSSP-yritykset ovat kuitenkin itsekin olleet kyberhyökkäysten kohteina, ja niiden tiivis integroituminen toimijoiden toimintarakenteisiin aiheuttaa erityisen kyberturvallisuusriskin. Toimijoiden olisi sen vuoksi noudatettava entistä suurempaa huolellisuutta MSSP-palveluntarjoajaa valitessaan.

(45) Toimijoiden olisi puututtava myös sellaisiin kyberturvallisuusriskeihin, jotka johtuvat niiden vuorovaikutussuhteista ja muista kytköksistä sidosryhmiin laajemmassa ekosysteemissä. Toimijoiden olisi erityisesti varmistettava, että niiden yhteistyö akateemisten laitosten ja tutkimuslaitosten kanssa tapahtuu niiden kyberturvallisuusperiaatteiden mukaisesti ja että yhteistyössä noudatetaan hyviä käytäntöjä yleisesti tiedon suojatun saatavuuden ja levittämisen ja erityisesti teollis- ja tekijänoikeuksien suojan suhteen. Kun otetaan huomioon datan merkitys ja arvo toimijoille, niiden olisi vastaavasti toteutettava kaikki asianmukaiset

kyberturvallisuustoimenpiteet tukeutuessaan kolmansilta osapuolilta hankittaviin tietojen muuntamis- ja analysointipalveluihin.

(46) Jotta voidaan edelleen paremmin puuttua keskeisiin toimitusketjun riskeihin ja auttaa tämän direktiivin soveltamisalaan kuuluvien alojen toimijoita hallitsemaan asianmukaisesti toimitusketjuun ja alihankkijoihin liittyviä kyberturvallisuusriskejä, yhteistyöryhmän, johon osallistuvat asiaankuuluvat kansalliset viranomaiset, olisi yhteistyössä komission ja ENISAn kanssa toteutettava koordinoituja alakohtaisia toimitusketjun riskinarviointeja, kuten tehtiin jo 5G-verkkojen osalta 5G-verkkojen kyberturvallisuudesta annetun suosituksen (EU) 2019/534[21] mukaisesti , jotta voidaan määrittää alakohtaiset kriittiset tieto- ja viestintätekniikan palvelut, järjestelmät tai tuotteet sekä kyseeseen tulevat uhat ja haavoittuvuudet.

(47) Toimitusketjun riskinarvioinneissa olisi kyseisen alan erityispiirteiden mukaisesti otettava huomioon sekä tekniset että tarvittaessa muut tekijät, mukaan lukien suosituksessa (EU) 2019/534, 5G-verkkojen turvallisuutta koskevassa EU:n laajuisessa koordinoidussa riskinarvioinnissa ja yhteistyöryhmän hyväksymässä 5G-kyberturvallisuutta koskevassa EU:n välineistössä määritellyt yhteistyöryhmän hyväksymät tekijät. Koordinoitua riskinarviointia edellyttävien toimitusketjujen määrittämisessä olisi otettava huomioon seuraavat kriteerit: i) se, missä määrin keskeiset ja tärkeät toimijat käyttävät tiettyjä kriittisiä tieto- ja viestintätekniikan palveluja, järjestelmiä tai tuotteita ja tukeutuvat niihin; ii) tiettyjen kriittisten tieto- ja viestintätekniikan palvelujen, järjestelmien tai tuotteiden merkitys kriittisten tai arkaluonteisten toimintojen suorittamisessa, mukaan lukien henkilötietojen käsittely; iii) vaihtoehtoisten tieto- ja viestintäteknisten palvelujen, järjestelmien tai tuotteiden saatavuus; iv) tieto- ja viestintätekniikan palvelujen, järjestelmien tai tuotteiden koko toimitusketjun kyky sietää häiriötilanteita ja v) käyttöön tulevien uusien tieto- ja viestintätekniikan palvelujen, järjestelmien tai tuotteiden osalta niiden mahdollinen tuleva merkitys toimijoille.

(48) Jotta voidaan virtaviivaistaa yleisten sähköisten viestintäverkkojen tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajille ja luottamuspalvelujen tarjoajille asetettuja oikeudellisia velvoitteita, jotka liittyvät niiden verkko- ja tietojärjestelmien turvallisuuteen, sekä antaa näille toimijoille ja niitä sääntöleville toimivaltaisille viranomaisille mahdollisuus hyötyä tällä direktiivillä perustetusta oikeudellisesta kehyksestä (mukaan lukien riskien ja poikkeamien käsittelystä vastaavan CSIRT-yksikön nimeäminen sekä toimivaltaisten viranomaisten ja elinten osallistuminen yhteistyöryhmän ja CSIRT-verkoston työhön), ne olisi sisällytettävä tämän direktiivin soveltamisalaan. Euroopan parlamentin ja neuvoston asetuksessa (EU) N:o 910/2014[22] ja Euroopan parlamentin ja neuvoston direktiivissä (EU) 2018/1972[23] vahvistetut vastaavat säännökset, jotka koskevat tällaisten toimijoiden turvallisuus- ja ilmoitusvaatimuksia, olisi sen vuoksi kumottava.

---

21 Komission suositus (EU) 2019/534, annettu 26 päivänä maaliskuuta 2019, 5G-verkkojen kyberturvallisuudesta (EUVL L 88, 29.3.2019, s. 42).

22 Euroopan parlamentin ja neuvoston asetus (EU) N:o 910/2014, annettu 23 päivänä heinäkuuta 2014, sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta (EUVL L 257, 28.8.2014, s. 73).

23 Euroopan parlamentin ja neuvoston direktiivi (EU) 2018/1972, annettu 11 päivänä joulukuuta 2018, eurooppalaisesta sähköisen viestinnän säännöstöstä (EUVL L 321, 17.12.2018, s. 36).

Raportointivelvoitteita koskevat säännöt eivät saisi rajoittaa asetuksen (EU) 2016/679 ja Euroopan parlamentin ja neuvoston direktiivin 2002/58/EY[24] soveltamista.

(49) Tähän direktiiviin perustuvasta valvonnasta ja täytäntöönpanosta vastaavien toimivaltaisten viranomaisten olisi tarkoituksenmukaisissa tapauksissa ja tarpeettomien katkosten välttämiseksi edelleen käytettävä olemassa olevaa kansallista ohjeistusta ja lainsäädäntöä, joka koskee direktiivin (EU) 2018/1972 40 artiklan 1 kohdassa säädettyjen turvatoimiin liittyvien sääntöjen ja kyseisen direktiivin 40 artiklan 2 kohdassa säädettyjen, poikkeaman merkittävyyteen liittyvien parametrien kansallista täytäntöönpanoa.

(50) Kun otetaan huomioon numeroista riippumattomien henkilöviestintäpalvelujen kasvava merkitys, on tarpeen varmistaa, että myös tällaisiin palveluihin sovelletaan asianmukaisia turvallisuusvaatimuksia niiden erityisluonteen ja taloudellisen merkityksen mukaisesti. Myös tällaisten palvelujen tarjoajien olisi näin ollen varmistettava, että verkko- ja tietojärjestelmien turvallisuustaso on oikeassa suhteessa aiheutuvaan riskiin. Koska numeroista riippumattomien henkilöiden välisten viestintäpalvelujen tarjoajat eivät yleensä tosiasiallisesti valvo signaalien siirtoa verkoissa, tällaisten palvelujen osalta riskiä voidaan joiltakin osin pitää perinteisiä sähköisiä viestintäpalveluja alhaisempana. Sama koskee sellaisia henkilöviestintäpalveluja, joissa käytetään yhteysnumeroita, mutta joissa palveluntarjoaja ei tosiasiallisesti valvo signaalinsiirtoa.

(51) Sisämarkkinat ovat entistä riippuvaisempia internetin toiminnasta. Käytännöllisesti katsoen kaikkien keskeisten ja tärkeiden toimijoiden palvelut ovat riippuvaisia internetin kautta tarjottavista palveluista. Keskeisten ja tärkeiden palvelujen sujuvan tarjonnan varmistamiseksi on tärkeää, että yleisten sähköisten viestintäverkkojen osien, kuten internetin runkoverkon tai merenalaisten tietoliikennekaapelien, suhteen on käytössä asianmukaiset kyberturvatoimet ja että niihin liittyvistä turvapoikkeamista raportoidaan.

(52) Toimijoiden olisi tarvittaessa tiedotettava palvelujensa käyttäjille yksittäisistä ja merkittävistä uhkista sekä toimenpiteistä, joita käyttäjät voivat toteuttaa pienentääkseen niistä itselleen aiheutuvaa riskiä. Vaatimus ilmoittaa palvelun käyttäjille uhkista ei saisi vapauttaa toimijoita velvollisuudesta toteuttaa omalla kustannuksellaan asianmukaisia ja välittömiä toimenpiteitä uhkien ehkäisemiseksi tai korjaamiseksi ja palvelun normaalin turvallisuustason palauttamiseksi. Turvallisuusuhkia koskevien tietojen toimittamisen käyttäjille olisi oltava käyttäjille maksutonta.

(53) Yleisten sähköisten viestintäverkkojen tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajien olisi tiedotettava palvelujensa käyttäjille yksittäisistä merkittävistä kyberuhkista sekä toimenpiteistä, joita käyttäjät voivat toteuttaa viestintänsä turvallisuuden suojelemiseksi esimerkiksi käyttämällä tietyntyyppisiä ohjelmistoja tai salaustekniikoita.

(54) Sähköisten viestintäverkkojen ja -palvelujen turvallisuuden takaamiseksi olisi edistettävä salauksen ja erityisesti yhteyden päästä päähän ulottuvan läpisalauksen käyttöä, ja sen olisi tarvittaessa oltava pakollista tällaisten palvelujen ja verkkojen

[24] Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY, annettu 12 päivänä heinäkuuta 2002, henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla (sähköisen viestinnän tietosuojadirektiivi) (EYVL L 201, 31.7.2002, s. 37).

tarjoajille oletusarvoisen ja sisäänrakennetun turvallisuuden ja yksityisyydensuojan periaatteiden mukaisesti 18 artiklaa sovellettaessa. Läpisalauksen käytön olisi kuvastettava jäsenvaltioiden toimivaltaa varmistaa niiden keskeisten turvallisuusintressien ja yleisen turvallisuuden suojelu ja mahdollistaa rikosten tutkinta, selvittäminen ja syytteeseenpano unionin oikeuden mukaisesti. Ratkaisujen, joilla mahdollistetaan laillinen pääsy tietoihin läpisalatussa viestinnässä, olisi säilytettävä salauksen kyky suojata viestinnän yksityisyyttä ja tietoturvaa samalla kun rikollisuuteen voidaan puuttua tuloksellisesti.

(55) Tässä direktiivissä säädetään poikkeamien ilmoittamista koskevasta kaksivaiheisesta lähestymistavasta, jotta löydetään oikea tasapaino toisaalta nopean raportoinnin, joka auttaa lieventämään poikkeamien mahdollista leviämistä ja antaa toimijoille mahdollisuuden hakea tukea, ja toisaalta sellaisen syvällisemmän raportoinnin välillä, jossa otetaan tärkeää oppia yksittäisistä poikkeamista ja parannetaan ajan mittaan yksittäisten yritysten ja kokonaisten toimialojen kykyä sietää kyberuhkia. Kun toimija saa tietoonsa poikkeaman, sitä olisi vaadittava toimittamaan ensimmäinen ilmoitus 24 tunnin kuluessa ja sen jälkeen loppuraportti viimeistään kuukauden kuluttua. Ensimmäisen ilmoituksen olisi sisällettävä ainoastaan ne tiedot, jotka ovat ehdottoman välttämättömiä, jotta toimivaltaiset viranomaiset tulevat tietoisiksi poikkeamasta ja kyseinen toimija voi tarvittaessa pyytää apua. Ensimmäisessä ilmoituksessa olisi soveltuvin osin ilmoitettava, johtuuko tapahtuma oletettavasti laittomasta tai vihamielisestä toiminnasta. Jäsenvaltioiden olisi varmistettava, että vaatimus tämän ensimmäisen ilmoituksen toimittamisesta ei vie raportoivan toimijan resursseja pois poikkeamien käsittelyyn liittyvistä toimista, jotka olisi asetettava etusijalle. Jotta voidaan edelleen estää se, että poikkeamista ilmoittamista koskevat velvoitteet joko ohjaavat resursseja pois poikkeamiin reagoimisesta tai voivat muulla tavoin vaarantaa toimijan tähän liittyvät toimet, jäsenvaltioiden olisi myös säädettävä, että asianmukaisesti perustelluissa tapauksissa ja yhteisymmärryksessä toimivaltaisten viranomaisten tai CSIRT-yksikön kanssa kyseinen toimija voi poiketa 24 tunnin määräajasta ensimmäisen ilmoituksen osalta ja yhden kuukauden määräajasta loppuraportin osalta.

(56) Keskeiset ja tärkeät toimijat ovat usein tilanteessa, jossa tietystä poikkeamasta on sen ominaisuuksien vuoksi ilmoitettava eri viranomaisille eri säädöksiin sisältyvien ilmoitusvelvoitteiden vuoksi. Tällaiset tapaukset aiheuttavat lisärasitteita ja voivat myös johtaa epävarmuuteen tällaisten ilmoitusten muodon ja menettelyjen suhteen. Tätä varten ja turvapoikkeamien raportoinnin yksinkertaistamiseksi jäsenvaltioiden olisi perustettava *keskitetty asiointipiste* kaikille tässä direktiivissä ja myös muussa unionin lainsäädännössä, kuten asetuksessa (EU) 2016/679 ja direktiivissä 2002/58/EY, edellytetyille ilmoituksille. ENISAn olisi yhteistyössä yhteistyöryhmän kanssa kehitettävä yhteiset ilmoitusmallit ohjeilla, joilla yksinkertaistettaisiin ja virtaviivaistettaisiin unionin lainsäädännössä edellytettyjä raportointitietoja ja vähennettäisiin yrityksille aiheutuvaa rasitetta.

(57) Jos epäillään, että poikkeama liittyy unionin tai kansallisen lainsäädännön nojalla vakavaan rikolliseen toimintaan, jäsenvaltioiden olisi kannustettava keskeisiä ja tärkeitä toimijoita raportoimaan epäillyistä vakavista rikosoikeudellisista poikkeamista asiaankuuluville lainvalvontaviranomaisille sovellettavien rikosoikeudellisia menettelyjä koskevien sääntöjen perusteella ja unionin lainsäädännön mukaisesti. Tarvittaessa ja rajoittamatta Europoliin sovellettavien henkilötietojen suojaa koskevien sääntöjen soveltamista on suotavaa, että eri jäsenvaltioiden toimivaltaisten

viranomaisten ja lainvalvontaviranomaisten välinen koordinointi tapahtuu Euroopan verkkorikostorjuntakeskuksen (EC3) ja ENISAn myötävaikutuksella.

(58) Turvapoikkeamat vaarantavat monissa tapauksissa henkilötietojen suojan. Tässä yhteydessä toimivaltaisten viranomaisten olisi tehtävä yhteistyötä ja vaihdettava tietoja kaikista asiaankuuluvista asioista tietosuojaviranomaisten ja valvontaviranomaisten kanssa direktiivin 2002/58/EY mukaisesti.

(59) Verkkotunnusten ja rekisteröintitietojen (ns. WHOIS-tiedot) tarkkojen ja kattavien tietokantojen ylläpitäminen ja laillisen pääsyn tarjoaminen tällaisiin tietoihin on olennaisen tärkeää, jotta voidaan varmistaa internetin DNS-nimipalvelinjärjestelmän turvallisuus, vakaus ja häiriönsietokyky, mikä puolestaan edistää yhteistä korkeatasoista kyberturvallisuutta unionissa. Jos käsittelyyn sisältyy henkilötietoja, käsittelyssä on noudatettava unionin tietosuojalainsäädäntöä.

(60) Näiden tietojen saatavuus ja nopea pääsy niihin viranomaisille, kuten unionin tai kansallisen lainsäädännön mukaisesti toimivaltaisille viranomaisille rikosten ehkäisemistä, tutkimista tai syytteeseenpanoa varten, CERT-yksiköille, CSIRT-yksiköille ja asiakkaitaan koskevien tietojen osalta kyseisten asiakkaiden puolesta toimiville sähköisten viestintäverkkojen ja -palvelujen tarjoajille ja kyberturvallisuusteknologioiden ja -palvelujen tarjoajille on olennaisen tärkeää DNS-verkkotunnusjärjestelmän väärinkäytön ehkäisemiseksi ja torjumiseksi, erityisesti kyberturvallisuuspoikkeamien ehkäisemiseksi, havaitsemiseksi ja niihin reagoimiseksi. Tällaisen pääsyn olisi oltava unionin tietosuojalainsäädännön mukaista siltä osin kuin se liittyy henkilötietoihin.

(61) Tarkkojen ja täydellisten verkkotunnusten rekisteröintitietojen saatavuuden varmistamiseksi aluetunnusrekisterien (TLD-rekisterien) ja niiden alaisten verkkotunnusten rekisteröintipalveluja tarjoavien toimijoiden (niin kutsuttujen rekisterinpitäjien) olisi kerättävä verkkotunnusten rekisteröintitiedot ja taattava niiden eheys ja saatavuus. TLD-rekisterien ja niiden alaisten verkkotunnusten rekisteröintipalveluja tarjoavien tahojen olisi erityisesti vahvistettava toimintatavat ja menettelyt, joilla kerätään ja ylläpidetään tarkkoja ja täydellisiä rekisteröintitietoja sekä ehkäistään ja korjataan virheellisiä rekisteröintitietoja unionin tietosuojasääntöjen mukaisesti.

(62) TLD-rekisterien ja niiden alaisten verkkotunnusten rekisteröintipalveluja tarjoavien tahojen olisi asetettava julkisesti saataville verkkotunnusten rekisteröintitiedot, jotka eivät kuulu unionin tietosuojasääntöjen soveltamisalaan, kuten oikeushenkilöitä koskevat tiedot[25]. TLD-rekisterien ja niiden alaisten verkkotunnusten rekisteröintipalveluja tarjoavien tahojen olisi myös unionin tietosuojalainsäädännön mukaisesti annettava perustelluissa tapauksissa tietoja pyytäville laillinen pääsy yksittäisiin luonnollisia henkilöitä koskeviin verkkotunnusten rekisteröintitietoihin. Jäsenvaltioiden olisi varmistettava, että TLD-rekisterit ja niiden alaisten verkkotunnusten rekisteröintipalveluja tarjoavat toimijat vastaavat ilman aiheetonta viivytystä perustelluissa tapauksissa esitettyihin pyyntöihin verkkotunnusten rekisteröintitietojen luovuttamisesta. TLD-rekisterien ja niiden alaisten verkkotunnusten rekisteröintipalveluja tarjoavien tahojen olisi vahvistettava periaatteet ja menettelyt rekisteröintitietojen julkaisemista ja luovuttamista varten, mukaan lukien

[25] Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679 johdanto-osan kappale 14, jonka mukaan ”Tämä asetus ei koske oikeushenkilöiden ja erityisesti oikeushenkilön muodossa perustettujen yritysten henkilötietojen käsittelyä, kuten oikeushenkilön nimeä, oikeudellista muotoa ja yhteystietoja.”.

palvelutasosopimukset laillisten tietopyyntöjen käsittelemiseksi. Tietojenluovutusmenettelyyn voi kuulua myös rajapinnan, portaalin tai muun teknisen menetelmän käyttö tehokkaan järjestelyn tarjoamiseksi rekisteröintitietojen pyytämistä ja niihin pääsyä varten. Yhdenmukaisten käytäntöjen edistämiseksi sisämarkkinoilla komissio voi antaa tällaisia menettelyjä koskevia ohjeita, sanotun kuitenkaan rajoittamatta Euroopan tietosuojaneuvoston toimivaltaa.

(63) Kaikkien tämän direktiivin soveltamisalaan kuuluvien keskeisten ja tärkeiden toimijoiden olisi kuuluttava sen jäsenvaltion lainkäyttövaltaan, jossa ne tarjoavat palvelujaan. Jos toimija tarjoaa palveluja useammassa kuin yhdessä jäsenvaltiossa, sen olisi kuuluttava kunkin jäsenvaltion erillisen ja rinnakkaisen lainkäyttövallan piiriin. Näiden jäsenvaltioiden toimivaltaisten viranomaisten olisi tehtävä yhteistyötä, annettava toisilleen keskinäistä apua ja tarvittaessa toteutettava yhteisiä valvontatoimia.

(64) Jotta voidaan ottaa huomioon internetin nimipalvelinjärjestelmän DNS-palveluntarjoajien, aluetunnusrekisterien (TLD-rekisterien), sisällönjakeluverkon tarjoajien, pilvipalvelujen tarjoajien, datakeskuspalvelujen tarjoajien ja digitaalisten palvelujen tarjoajien palvelujen ja toimintojen rajat ylittävä luonne, vain yhdellä jäsenvaltiolla olisi oltava lainkäyttövalta näihin toimijoihin nähden. Lainkäyttövalta olisi oltava sillä jäsenvaltiolla, jossa kyseisen toimijan päätoimipaikka sijaitsee unionissa. Tätä direktiiviä sovellettaessa sijoittautumiskriteerillä tarkoitetaan toiminnan tosiasiallista harjoittamista kiinteiden toimipaikkojen kautta. Sijoittautumisen oikeudellisella muodolla eli sillä, onko kyseessä sivuliike vai tytäryhtiö, jolla on oikeushenkilöys, ei ole tässä suhteessa ratkaisevaa merkitystä. Tämän kriteerin täyttyminen ei saisi riippua siitä, sijaitsevatko verkko- ja tietojärjestelmät fyysisesti kyseisessä paikassa; tällaisten järjestelmien sijainti ja käyttöpaikka eivät itsessään muodosta tällaista päätoimipaikkaa, eivätkä ne näin ollen ole ratkaisevia perusteita päätoimipaikan määrittämisessä. Päätoimipaikan olisi oltava paikka, jossa kyberturvallisuusriskien hallintatoimenpiteisiin liittyvät päätökset tehdään unionissa. Tämä vastaa tyypillisesti yritysten keskushallinnon paikkaa unionissa. Jos tällaisia päätöksiä ei tehdä unionissa, päätoimipaikan olisi katsottava sijaitsevan niissä jäsenvaltioissa, joissa toimijalla on eniten työntekijöitä unionissa. Jos palvelut suorittaa yritysryhmä, sen päätoimipaikaksi olisi katsottava määräysvaltaa käyttävän yrityksen päätoimipaikka.

(65) Kun internetin nimipalvelinjärjestelmän DNS-palveluntarjoaja, aluetunnusrekisteri (TLD-rekisterien), sisällönjakeluverkon tarjoaja, pilvipalvelujen tarjoaja, datakeskuspalvelujen tarjoaja tai digitaalisten palvelujen tarjoaja, joka ei ole sijoittautunut unioniin, tarjoaa palveluja unionissa, sen olisi nimettävä edustaja. Jotta voidaan määrittää, tarjoaako tällainen toimija palveluja unionissa, olisi varmistettava, onko ilmeistä, että toimija aikoo tarjota palveluja henkilöille yhdessä tai useammassa jäsenvaltiossa. Pelkkä toimijan tai välittäjän verkkosivuston tai sähköpostiosoitteen ja muiden yhteystietojen saatavuus unionissa taikka se, että käytetään siinä kolmannessa maassa, johon toimija on sijoittautunut, yleisesti käytettävää kieltä, ei sellaisenaan riitä tällaisen aikomuksen varmistamiseksi. Sellaiset seikat, kuten yhdessä tai useammassa jäsenvaltiossa yleisesti käytettävän kielen tai rahayksikön käyttö ja mahdollisuus tilata palveluja kyseisellä muulla kielellä tai maininta unionissa olevista asiakkaista tai käyttäjistä, voivat kuitenkin osoittaa olevan ilmeistä, että toimija aikoo tarjota palveluja unionissa. Edustajan olisi toimittava toimijan puolesta, ja toimivaltaisten viranomaisten tai CSIRT-yksiköiden olisi voitava ottaa yhteyttä edustajaan. Edustaja olisi nimenomaisesti nimettävä toimijan antamalla kirjallisella valtuutuksella

hoitamaan tämän puolesta tämän direktiivin mukaiset velvollisuudet, mukaan lukien poikkeamista raportointi.

(66) Jos kansallisen tai unionin lainsäädännön mukaisesti turvallisuusluokiteltuina pidettyjä tietoja vaihdetaan, ilmoitetaan tai muutoin jaetaan tämän direktiivin säännösten mukaisesti, olisi sovellettava turvallisuusluokiteltujen tietojen käsittelyä koskevia vastaavia erityissääntöjä.

(67) Koska kyberuhat muuttuvat monimutkaisemmiksi ja kehittyneemmiksi, hyvät havaitsemis- ja ennaltaehkäisytoimenpiteet edellyttävät suurelta osin uhkiin ja haavoittuvuuteen liittyvän tiedon säännöllistä jakamista toimijoiden välillä. Tietojenvaihto lisää tietoisuutta kyberuhkista, mikä puolestaan parantaa toimijoiden valmiuksia estää uhkia kehittymästä todellisiksi poikkeamiksi ja auttaa niitä hallitsemaan paremmin poikkeamien vaikutuksia ja palautumaan niistä tehokkaammin. Koska unionin tasolla ei ole annettu ohjeita, vaikuttaa siltä, että useat tekijät, erityisesti epävarmuus yhteensopivuudesta kilpailu- ja vastuusääntöjen kanssa, ovat estäneet tällaisen tietojen jakamisen.

(68) Toimijoita olisi kannustettava hyödyntämään kollektiivisesti omaa tietämystään ja käytännön kokemustaan strategisella, taktisella ja operatiivisella tasolla, jotta voidaan parantaa niiden valmiuksia arvioida ja seurata kyberuhkia, puolustautua niitä vastaan ja reagoida niihin. Sen vuoksi on tarpeen mahdollistaa vapaaehtoisten tietojenvaihtojärjestelyjen synty unionin tasolla. Tätä varten jäsenvaltioiden olisi aktiivisesti tuettava ja kannustettava myös sellaisia asiaankuuluvia toimijoita, jotka eivät kuulu tämän direktiivin soveltamisalaan, osallistumaan tällaisiin tietojenvaihtojärjestelyihin. Järjestelyt olisi toteutettava noudattaen kaikilta osin unionin kilpailusääntöjä ja unionin tietosuojalainsäädännön sääntöjä.

(69) Siinä määrin kuin on ehdottoman välttämätöntä ja oikeasuhteista verkko- ja tietoturvan varmistamiseksi, toimijoiden, viranomaisten, CERT-ryhmien, CSIRT-yksiköiden sekä turvallisuusteknologioiden ja -palvelujen tarjoajien suorittaman henkilötietojen käsittelyn olisi katsottava muodostavan asianomaisen rekisterinpitäjän osalta asetuksessa (EU) 2016/679 tarkoitetun oikeutetun intressin. Tämän olisi katettava toimenpiteet, jotka liittyvät poikkeamien ehkäisemiseen, havaitsemiseen, analysointiin ja niihin reagoimiseen, toimenpiteet yksittäisistä kyberuhkista tiedottamiseksi, tietojenvaihto haavoittuvuuden korjaamisen ja koordinoidun paljastamisen yhteydessä sekä näitä poikkeamia koskeva vapaaehtoinen tietojenvaihto sekä toimenpiteet, jotka liittyvät kyberuhkiin ja haavoittuvuuksiin, riskien ilmenemisen indikaattoreihin, taktiikkaan, tekniikoihin ja menettelyihin, kyberturvallisuushälytyksiin ja konfigurointivälineisiin. Tällaiset toimenpiteet voivat edellyttää seuraavan tyyppisten henkilötietojen käsittelyä: IP-osoitteet, URL-osoitteet, verkkotunnukset ja sähköpostiosoitteet.

(70) Jotta voidaan vahvistaa valvontavaltuuksia ja -toimia, jotka auttavat varmistamaan sääntöjen tosiasiallisen noudattamisen, tässä direktiivissä olisi vahvistettava vähimmäisluettelo valvontatoimista ja -keinoista, joiden avulla toimivaltaiset viranomaiset voivat valvoa keskeisiä ja tärkeitä toimijoita. Lisäksi tässä direktiivissä olisi säädettävä valvontajärjestelmän eriyttämisestä keskeisten ja tärkeiden toimijoiden välillä, jotta voidaan varmistaa sekä toimijoiden että toimivaltaisten viranomaisten velvoitteiden oikeudenmukainen tasapaino. Näin ollen keskeisiin toimijoihin olisi sovellettava täysimittaista valvontajärjestelmää (etukäteisvalvonta ja jälkikäteisvalvonta), kun taas tärkeisiin toimijoihin olisi sovellettava kevyttä valvontajärjestelmää eli vain jälkikäteisvalvontaa. Viimeksi mainittujen osalta tämä

tarkoittaa sitä, että tärkeiden toimijoiden ei pitäisi dokumentoida järjestelmällisesti kyberturvallisuusriskien hallintaa koskevien vaatimusten noudattamista, ja toimivaltaisten viranomaisten olisi harjoitettava reaktiivista jälkikäteisvalvontaa eikä niillä näin ollen olisi yleistä velvoitetta valvoa kyseisiä toimijoita.

(71) Jotta valvonta olisi tuloksellista, olisi vahvistettava vähimmäisluettelo hallinnollisista seuraamuksista, joita määrätään tässä direktiivissä säädettyjen kyberturvallisuusriskien hallintaa ja raportointia koskevien velvoitteiden laiminlyömisestä, ja vahvistettava selkeä ja johdonmukainen kehys tällaisille seuraamuksille koko unionissa. Olisi otettava asianmukaisesti huomioon rikkomisen luonne, vakavuus ja kesto, aiheutetut todelliset vahingot tai menetykset tai mahdolliset vahingot tai menetykset, jotka olisi voitu aiheuttaa, rikkomisen tahallisuus tai tuottamuksellisuus, vahingon ja/tai menetysten ehkäisemiseksi tai lieventämiseksi toteutetut toimet, vastuun aste tai asiaan liittyvät aiemmat laiminlyönnit, toimivaltaisen viranomaisen kanssa tehdyn yhteistyön aste ja mahdolliset muut raskauttavat tai lieventävät tekijät. Seuraamusten, myös hallinnollisten sakkojen, määräämiseen olisi sovellettava asianmukaisia menettelyllisiä suojatoimenpiteitä unionin oikeuden ja Euroopan unionin perusoikeuskirjan yleisten periaatteiden mukaisesti, mukaan lukien tosiasiallinen oikeussuoja ja asianmukainen käsittelyprosessi.

(72) Tässä direktiivissä säädettyjen velvoitteiden tuloksellisen täytäntöönpanon varmistamiseksi kullakin toimivaltaisella viranomaisella olisi oltava valtuudet määrätä hallinnollisia sakkoja tai pyytää niiden määräämistä.

(73) Silloin kun sakkoja määrätään yritykselle, yritys olisi ymmärrettävä Euroopan unionin toiminnasta tehdyn sopimuksen (SEUT) 101 ja 102 artiklan mukaiseksi yritykseksi. Jos hallinnollisia sakkoja määrätään henkilöille, jotka eivät ole yrityksiä, valvontaviranomaisen olisi sakon sopivan määrän harkinnassa otettava huomioon jäsenvaltion yleinen tulotaso ja henkilön taloudellinen tilanne. Jäsenvaltioilla olisi oltava vastuu määritellä onko viranomaisille määrättävä hallinnollisia sakkoja ja missä määrin. Hallinnollisen sakon määrääminen ei vaikuta toimivaltaisten viranomaisten muihin valtuuksiin tai muihin seuraamuksiin, joista säädetään tämän direktiivin kansalliseen lainsäädäntöön sisällyttävissä kansallisissa säännöissä.

(74) Jäsenvaltioiden olisi voitava säätää rikosoikeudellisia seuraamuksia koskevista säännöistä, joita sovelletaan tämän direktiivin kansalliseen lainsäädäntöön sisällyttävien kansallisten sääntöjen rikkomiseen. Tällaisten kansallisten sääntöjen rikkomisesta määrättävien rikosoikeudellisten seuraamusten ja niihin liittyvien hallinnollisten seuraamusten ei kuitenkaan pitäisi johtaa *ne bis in idem* -periaatteen rikkomiseen, sellaisena kuin unionin tuomioistuin on sitä tulkinnut.

(75) Sikäli kuin tässä direktiivissä ei yhdenmukaisteta hallinnollisia seuraamuksia tai tarvittaessa muissa tapauksissa, esimerkiksi silloin, kun kyseessä on tämän direktiivin velvoitteiden vakava laiminlyönti, jäsenvaltioiden olisi pantava täytäntöön järjestelmä, jossa määrätään tehokkaista, oikeasuhteisista ja varoittavista seuraamuksista. Tällaisten rikosoikeudellisten tai hallinnollisten seuraamusten luonne olisi määriteltävä jäsenvaltion lainsäädännössä.

(76) Jotta voidaan edelleen vahvistaa tämän direktiivin nojalla säädettyjen velvoitteiden rikkomiseen sovellettavien seuraamusten vaikuttavuutta ja varoittavuutta, toimivaltaisilla viranomaisilla olisi oltava valtuudet asettaa seuraamuksia, jotka koostuvat keskeisen toimijan tarjoamiin palveluihin tai osaan niistä liittyvän todistuksen tai luvan voimassaolon keskeyttämisestä ja luonnollisen henkilön määräämisestä väliaikaiseen kieltoon harjoittaa johtotehtäviä. Kun otetaan huomioon

tällaisten seuraamusten vakavuus ja vaikutus toimijoiden palveluihin ja viime kädessä niiden kuluttajiin, niitä olisi sovellettava ainoastaan suhteessa rikkomisen vakavuuteen ja ottaen huomioon kunkin tapauksen erityisolosuhteet, mukaan lukien rikkomisen tahallisuus tai tuottamuksellisuus sekä toimet, joita on toteutettu aiheutuneen vahingon ja/tai menetyksen estämiseksi tai lieventämiseksi. Tällaisia seuraamuksia olisi sovellettava ainoastaan *ultima ratio* -periaatteen mukaisesti eli vasta viimeisenä keinona sen jälkeen, kun muut tässä direktiivissä säädetyt asiaankuuluvat täytäntöönpanotoimet on käytetty, ja ainoastaan siihen asti, kunnes toimijat, joihin niitä sovelletaan, toteuttavat tarvittavat toimet puutteiden korjaamiseksi tai niiden toimivaltaisen viranomaisen vaatimusten noudattamiseksi, joiden johdosta seuraamuksia on sovellettu. Tällaisten seuraamusten määräämiseen olisi sovellettava asianmukaisia menettelyllisiä suojatoimia unionin oikeuden ja Euroopan unionin perusoikeuskirjan yleisten periaatteiden mukaisesti, mukaan lukien tehokas oikeussuoja, asianmukainen käsittelyprosessi, syyttömyysolettama ja oikeus puolustukseen.

(77) Tässä direktiivissä olisi vahvistettava toimivaltaisten viranomaisten ja valvontaviranomaisten välistä yhteistyötä koskevat säännöt asetuksen (EU) 2016/679 mukaisesti henkilötietoihin liittyvien rikkomusten käsittelemiseksi.

(78) Tällä direktiivillä olisi pyrittävä varmistamaan organisaatiotasolla korkeatasoinen vastuu kyberturvallisuusriskien hallintatoimenpiteistä ja raportointivelvoitteista. Näistä syistä tämän direktiivin soveltamisalaan kuuluvien toimijoiden hallintoelinten olisi hyväksyttävä kyberturvallisuusriskitoimenpiteet ja valvottava niiden täytäntöönpanoa.

(79) Olisi otettava käyttöön vertaisarviointimekanismi, jonka avulla jäsenvaltioiden nimeämät asiantuntijat voivat arvioida kyberturvallisuuspolitiikkojen täytäntöönpanoa, myös jäsenvaltioiden valmiuksien ja käytettävissä olevien resurssien tasoa.

(80) Uusien kyberuhkien, teknologian kehityksen tai alakohtaisten erityispiirteiden huomioon ottamiseksi komissiolle olisi siirrettävä valta hyväksyä Euroopan unionin toiminnasta tehdyn sopimuksen 290 artiklan mukaisesti säädösvallan siirron nojalla annettavia delegoituja säädöksiä, jotka koskevat tässä direktiivissä edellytettyihin riskinhallintatoimenpiteisiin liittyviä seikkoja. Komissiolle olisi myös siirrettävä valta antaa delegoituja säädöksiä, joissa vahvistetaan, miltä keskeisten toimijoiden luokilta edellytetään sertifiointia ja minkä eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän mukaisesti. On erityisen tärkeää, että komissio asiaa valmistellessaan toteuttaa asianmukaiset kuulemiset, myös asiantuntijatasolla, ja että nämä kuulemiset toteutetaan paremmasta lainsäädännöstä 13 päivänä huhtikuuta 2016 tehdyssä toimielinten välisessä sopimuksessa[26] vahvistettujen periaatteiden mukaisesti. Jotta voitaisiin erityisesti varmistaa tasavertainen osallistuminen delegoitujen säädösten valmisteluun, Euroopan parlamentille ja neuvostolle toimitetaan kaikki asiakirjat samaan aikaan kuin jäsenvaltioiden asiantuntijoille, ja Euroopan parlamentin ja neuvoston asiantuntijoilla on järjestelmällisesti oikeus osallistua komission asiantuntijaryhmien kokouksiin, joissa valmistellaan delegoituja säädöksiä.

(81) Jotta voidaan varmistaa tämän direktiivin asiaankuuluvien säännösten yhdenmukainen täytäntöönpano yhteistyöryhmän toiminnan edellyttämien menettelyllisten järjestelyjen, riskinhallintatoimenpiteisiin liittyvien teknisten seikkojen tai poikkeamailmoitusten tietotyyppien, muodon ja menettelyn osalta, komissiolle olisi

[26] EUVL L 123, 12.5.2016, s. 1.

siirrettävä täytäntöönpanovaltaa. Tätä valtaa olisi käytettävä Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 182/2011[27] mukaisesti.

(82) Komission olisi tarkasteltava tätä direktiiviä säännöllisin väliajoin uudelleen asianomaisia osapuolia kuullen, erityisesti yhteiskunnan, politiikan, tekniikan ja markkinaolojen kehitykseen perustuvien muutostarpeiden selvittämiseksi.

(83) Jäsenvaltiot eivät voi riittävällä tavalla saavuttaa tämän direktiivin tavoitetta, joka on yhteinen korkea kyberturvallisuuden taso unionissa, vaan se voidaan toiminnan vaikutusten vuoksi saavuttaa paremmin unionin tasolla. Sen vuoksi unioni voi toteuttaa toimenpiteitä Euroopan unionista tehdyn sopimuksen 5 artiklassa vahvistetun toissijaisuusperiaatteen mukaisesti. Mainitussa artiklassa vahvistetun suhteellisuusperiaatteen mukaisesti tässä direktiivissä ei ylitetä sitä, mikä on tarpeen tämän tavoitteen saavuttamiseksi.

(84) Tässä direktiivissä kunnioitetaan Euroopan unionin perusoikeuskirjassa tunnustettuja perusoikeuksia ja noudatetaan siinä tunnustettuja periaatteita, erityisesti oikeutta yksityiselämän ja viestien kunnioittamiseen, henkilötietojen suojaa, elinkeinovapautta, omistusoikeutta, oikeutta tehokkaisiin oikeussuojakeinoihin tuomioistuimessa ja oikeutta tulla kuulluksi. Tämä direktiivi olisi pantava täytäntöön näiden oikeuksien ja periaatteiden mukaisesti,

OVAT HYVÄKSYNEET TÄMÄN DIREKTIIVIN:

I LUKU

Yleiset säännökset

1 artikla

Kohde

1. Tässä direktiivissä säädetään toimenpiteistä, joilla varmistetaan yhteinen korkea kyberturvallisuuden taso unionissa.

2. Tätä varten tässä direktiivissä

a) vahvistetaan jäsenvaltioiden velvoitteet hyväksyä kansalliset kyberturvallisuusstrategiat sekä nimetä toimivaltaiset kansalliset viranomaiset, keskitetyt yhteyspisteet ja tietoturvaloukkauksiin reagoivat ja niitä tutkivat yksiköt (CSIRT-yksiköt);

b) vahvistetaan kyberturvallisuusriskien hallintaa ja raportointia koskevat velvoitteet liitteessä I tarkoitetuille keskeisille toimijoille ja liitteessä II tarkoitetuille tärkeille toimijoille;

c) vahvistetaan kyberturvallisuustietojen jakamista koskevat velvoitteet.

[27] Euroopan parlamentin ja neuvoston asetus (EU) N:o 182/2011, annettu 16 päivänä helmikuuta 2011, yleisistä säännöistä ja periaatteista, joiden mukaisesti jäsenvaltiot valvovat komission täytäntöönpanovallan käyttöä (EUVL L 55, 28.2.2011, s. 13).

2 artikla

Soveltamisala

1. Tätä direktiiviä sovelletaan julkisiin ja yksityisiin liitteessä I tarkoitettuihin keskeisiin toimijoihin ja julkisiin ja yksityisiin liitteessä II tarkoitettuihin tärkeisiin toimijoihin. Tätä direktiiviä ei sovelleta toimijoihin, jotka katsotaan komission suosituksessa 2003/361/EY[28] tarkoitetuiksi mikro- ja pienyrityksiksi.

2. Tätä direktiiviä sovelletaan kuitenkin myös toimijan koosta riippumatta liitteissä I ja II tarkoitettuihin toimijoihin, kun

   a) palveluntarjoaja on jokin seuraavista toimijoista:

      i) liitteessä I olevassa 8 kohdassa tarkoitettu yleinen sähköinen viestintäverkko tai yleisesti saatavilla oleva sähköinen viestintäpalvelu;

      ii) liitteessä I olevassa 8 kohdassa tarkoitettu luottamuspalvelun tarjoaja;

      iii) liitteessä I olevassa 8 kohdassa tarkoitettu aluetunnusrekisteri (TLD-rekisteri) tai verkkotunnusjärjestelmän (DNS) palveluntarjoaja;

   b) toimija on 4 artiklan 23 kohdassa määritelty julkishallinnon yksikkö;

   c) toimija on tietyn palvelun ainoa tarjoaja jäsenvaltiossa;

   d) häiriö toimijan tarjoamassa palvelussa voisi vaikuttaa yleiseen järjestykseen, yleiseen turvallisuuteen tai kansanterveyteen;

   e) häiriö toimijan tarjoamassa palvelussa voisi aiheuttaa järjestelmäriskejä erityisesti aloilla, joilla häiriöllä voisi olla valtioiden rajat ylittäviä vaikutuksia;

   f) toimija on kriittisessä asemassa, koska se on alueellisella tai kansallisella tasolla tietyn toimialan tai palvelutyypin tai jäsenvaltion muiden keskinäisriippuvaisten toimialojen kannalta erityisen tärkeä toimija;

   g) toimija on määritelty kriittiseksi toimijaksi Euroopan parlamentin ja neuvoston direktiivin (EU) XXXX/XXXX[29] [kriittisten toimijoiden häiriönsietokykyä koskeva direktiivi] mukaisesti tai kriittistä toimijaa vastaavaksi toimijaksi kyseisen direktiivin 7 artiklan mukaisesti.

   Jäsenvaltioiden on laadittava luettelo b–f alakohdan mukaisista toimijoista ja toimitettava se komissiolle viimeistään [6 kuukauden kuluttua määräajasta, johon mennessä direktiivi on saatettava osaksi kansallista lainsäädäntöä]. Jäsenvaltioiden on sen jälkeen tarkasteltava luetteloa uudelleen säännöllisesti ja vähintään joka toinen vuosi ja saatettava se tarvittaessa ajan tasalle.

3. Tämä direktiivi ei vaikuta jäsenvaltioiden toimivaltaan, joka koskee yleisen turvallisuuden, puolustuksen ja kansallisen turvallisuuden ylläpitämistä unionin oikeuden mukaisesti.

---

[28] Komission suositus 2003/361/EY, annettu 6 päivänä toukokuuta 2003, mikroyritysten sekä pienten ja keskisuurten yritysten määritelmästä (EUVL L 124, 20.5.2003, s. 36).

[29] *[lisätään koko nimi ja EUVL:n julkaisuviite, kun ne ovat tiedossa]*

4. Tämän direktiivin soveltaminen ei rajoita neuvoston direktiivin 2008/114/EY[30] eikä Euroopan parlamentin ja neuvoston direktiivien 2011/93/EU[31] ja 2013/40/EU[32] soveltamista.

5. Tietoja, jotka katsotaan luottamuksellisiksi unionin ja kansallisten sääntöjen, kuten liikesalaisuuksia koskevien sääntöjen mukaisesti, saa vaihtaa komission ja muiden asianomaisten viranomaisten kanssa vain silloin kun tällainen vaihtaminen on välttämätöntä tämän direktiivin soveltamiseksi, sanotun kuitenkaan rajoittamatta Euroopan unionin toiminnasta tehdyn sopimuksen 346 artiklan soveltamista. Tällöin on vaihdettava ainoastaan sellaisia tietoja, jotka ovat merkityksellisiä ja oikeasuhteisia tällaisen vaihdon tarkoituksen kannalta. Tällaisessa tiedonvaihdossa on säilytettävä kyseisten tietojen luottamuksellisuus sekä suojeltava keskeisten tai tärkeiden toimijoiden turvallisuusetuja ja kaupallisia etuja.

6. Jos unionin alakohtaisten säädösten säännöksissä edellytetään, että keskeiset tai tärkeät toimijat joko hyväksyvät kyberturvallisuusriskien hallintatoimenpiteitä tai ilmoittavat poikkeamista tai merkittävistä kyberuhista, ja jos kyseiset vaatimukset vastaavat vaikutukseltaan vähintään tässä direktiivissä säädettyjä velvoitteita, tämän direktiivin asiaankuuluvia säännöksiä, mukaan lukien VI luvussa säädetty valvontaa ja täytäntöönpanoa koskeva säännös, ei sovelleta.

3 artikla

Vähimmäistason yhdenmukaistaminen

Jäsenvaltiot voivat tämän direktiivin mukaisesti antaa tai pitää voimassa säännöksiä, joilla varmistetaan kyberturvallisuuden korkeampi taso, sanotun kuitenkaan rajoittamatta niiden muita unionin oikeuden mukaisia velvoitteita.

4 artikla

Määritelmät

Tässä direktiivissä tarkoitetaan:

1) ’verkko- ja tietojärjestelmällä’

   a) direktiivin (EU) 2018/1972 2 artiklan 1 kohdassa tarkoitettua sähköistä viestintäverkkoa;

   b) laitetta taikka yhteen kytkettyjen tai toisiinsa yhteydessä olevien laitteiden ryhmää, joista yksi tai useampi suorittaa ohjelman avulla digitaalisten tietojen automaattista käsittelyä;

---

30 Neuvoston direktiivi 2008/114/EY, annettu 8 päivänä joulukuuta 2008, Euroopan elintärkeän infrastruktuurin määrittämisestä ja nimeämisestä sekä arvioinnista, joka koskee tarvetta parantaa sen suojaamista (EUVL L 345, 23.12.2008, s. 75).

31 Euroopan parlamentin ja neuvoston direktiivi 2011/93/EU, annettu 13 päivänä joulukuuta 2011, lasten seksuaalisen hyväksikäytön ja seksuaalisen riiston sekä lapsipornografian torjumisesta ja neuvoston puitepäätöksen 2004/68/YOS korvaamisesta (EUVL L 335, 17.12.2011, s. 1).

32 Euroopan parlamentin ja neuvoston direktiivi 2013/40/EU, annettu 12 päivänä elokuuta 2013, tietojärjestelmiin kohdistuvista hyökkäyksistä ja neuvoston puitepäätöksen 2005/222/YOS korvaamisesta (EUVL L 218, 14.8.2013, s. 8).

c) digitaalisia tietoja, joita a ja b alakohdassa tarkoitetuissa järjestelmissä säilytetään, käsitellään, haetaan tai siirretään niiden toimintaa, käyttöä, suojausta tai ylläpitoa varten;

2) ’verkko- ja tietojärjestelmien turvallisuudella’ verkko- ja tietojärjestelmien kykyä suojautua tietyllä varmuudella toimilta, jotka vaarantavat kyseisissä verkko- ja tietojärjestelmissä tarjottujen tai niiden välityksellä saatavilla olevien tallennettujen, siirrettyjen tai käsiteltyjen tietojen tai niihin liittyvien palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden;

3) ’kyberturvallisuudella’ ja ’kyberturvalla’ Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/881[33] 2 artiklan 1 kohdassa tarkoitettua kyberturvallisuutta;

4) ’kansallisella kyberturvallisuusstrategialla ’ jäsenvaltion yhtenäistä kehystä, jossa esitetään verkko- ja tietojärjestelmien turvallisuutta koskevat strategiset tavoitteet ja painopisteet kyseisessä jäsenvaltiossa;

5) ’poikkeamalla’ tapahtumaa, joka vaarantaa verkko- ja tietojärjestelmissä tarjottujen tai niiden välityksellä saatavilla olevien tallennettujen, siirrettyjen tai käsiteltyjen tietojen tai niihin liittyvien palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden;

6) ’poikkeaman käsittelyllä’ kaikkia toimia ja menettelyjä, joilla pyritään havaitsemaan, analysoimaan ja estämään poikkeama ja reagoimaan siihen;

7) ’kyberuhalla’ asetuksen (EU) 2019/881 2 artiklan 8 kohdassa tarkoitettua kyberuhkaa;

8) ’haavoittuvuudella’ omaisuuserän, järjestelmän, prosessin tai valvonnan heikkoutta, herkkyyttä tai vikaa, jota kyberuhkan lähde voi hyödyntää;

9) ’edustajalla’ unioniin sijoittautunutta luonnollista henkilöä tai oikeushenkilöä, joka on nimenomaisesti nimetty toimimaan i) liitteessä I olevassa 8 kohdassa tarkoitetun DNS-palveluntarjoajan, aluetunnusrekisterin (TLD-rekisteri), pilvipalveluntarjoajan, datakeskuspalvelun tarjoajan tai sisällönjakeluverkon tarjoajan tai ii) liitteessä II olevassa 6 kohdassa tarkoitetun unioniin sijoittautumattoman toimijan puolesta ja johon kansallinen toimivaltainen viranomainen tai CSIRT-yksikkö voi olla yhteydessä toimijan sijaan kyseisen toimijan tämän direktiivin mukaisten velvoitteiden osalta;

10) ’standardilla’ Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 1025/2012[34] 2 artiklan 1 kohdassa tarkoitettua standardia;

11) ’teknisellä eritelmällä’ asetuksen (EU) N:o 1025/2012 2 artiklan 4 kohdassa tarkoitettua teknistä eritelmää;

---

[33] 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).

[34] Euroopan parlamentin ja neuvoston asetus (EU) N:o 1025/2012, annettu 25 päivänä lokakuuta 2012, eurooppalaisesta standardoinnista, neuvoston direktiivien 89/686/ETY ja 93/15/ETY sekä Euroopan parlamentin ja neuvoston direktiivien 94/9/EY, 94/25/EY, 95/16/EY, 97/23/EY, 2004/22/EY, 2007/23/EY, 2009/23/EY ja 2009/105/EY muuttamisesta ja neuvoston päätöksen 87/95/ETY ja Euroopan parlamentin ja neuvoston päätöksen N:o 1673/2006/EY kumoamisesta (EUVL L 316, 14.11.2012, s. 12).

12) ’internetin yhdysliikennepisteellä (IXP)’ verkkoinfrastruktuurin osaa, joka mahdollistaa useamman kuin kahden riippumattoman verkon (autonomisen järjestelmän) yhdistämisen pääasiassa internet-liikenteen välittämisen helpottamiseksi; IXP tarjoaa autonomisille järjestelmille ainoastaan yhteenliitäntää; IXP ei edellytä minkään yhteenliittämänsä kahden autonomisen järjestelmän väliseltä internet-liikenteeltä kulkemista minkään kolmannen autonomisen järjestelmän kautta, eikä se muokkaa tällaista liikennettä tai muutoin puutu siihen;

13) ’verkkotunnusjärjestelmällä (DNS)’ hierarkkista hajautettua nimeämisjärjestelmää, jonka avulla loppukäyttäjät voivat tunnistaa palveluja ja resursseja internetissä;

14) ’DNS-palvelutarjoajalla’ toimijaa, joka tarjoaa rekursiivisia tai autoritatiivisia verkkotunnusten selvityspalveluja internetin loppukäyttäjille ja muille DNS-palveluntarjoajille;

15) ’aluetunnusrekisterillä (TLD-rekisterillä)’ toimijaa, jolle on myönnetty oikeus hallinnoida tiettyä aluetunnusta (TLD) ja joka vastaa muun muassa verkkotunnusten rekisteröinnistä kyseisen aluetunnuksen alle sekä kyseisen aluetunnuksen teknisestä toiminnasta, siihen liittyvien nimipalvelinten toiminnasta, sen tietokantojen ylläpidosta ja aluetunnuksen vyöhyketiedostojen jakelusta nimipalvelimille;

16) ’digitaalisella palvelulla’ Euroopan parlamentin ja neuvoston direktiivin (EU) 2015/1535[35] 1 artiklan 1 kohdan b alakohdassa tarkoitettua palvelua;

17) ’verkon kauppapaikalla’ Euroopan parlamentin ja neuvoston direktiivin 2005/29/EY[36] 2 artiklan n alakohdassa tarkoitettua digitaalista palvelua;

18) ’verkon hakukoneella’ Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/1150[37] 2 artiklan 5 kohdassa tarkoitettua digitaalista palvelua;

19) ’pilvipalvelulla’ digitaalista palvelua, joka mahdollistaa skaalattavien ja joustavien tietoteknisten resurssien jaettavan ja hajautetun laajan tarveperusteisen etäkäytön;

20) ’datakeskuspalvelulla’ palvelua, joka käsittää rakenteita tai rakenteiden ryhmiä, jotka on tarkoitettu datan tallennus-, käsittely- ja siirtopalveluja tarjoavien tietoteknisten ja verkkolaitteiden keskitettyyn ylläpitoon, yhteenliittämiseen ja ohjaukseen yhdessä kaikkien tarvittavien sähkönjakeluun ja toimintaolosuhteiden säätelyyn tarkoitettujen laitteiden ja infrastruktuurien kanssa;

21) ’sisällönjakeluverkolla’ maantieteellisesti hajautettujen palvelimien verkostoa, jonka tarkoituksena on varmistaa digitaalisen sisällön ja digitaalisten palvelujen korkea saatavuus, käytettävyys ja nopea jakelu internetin käyttäjille sisällön ja palvelujen tarjoajien puolesta;

---

35 Euroopan parlamentin ja neuvoston direktiivi (EU) 2015/1535, annettu 9 päivänä syyskuuta 2015, teknisiä määräyksiä ja tietoyhteiskunnan palveluja koskevia määräyksiä koskevien tietojen toimittamisessa noudatettavasta menettelystä (EUVL L 241, 17.9.2015, s. 1).

36 Euroopan parlamentin ja neuvoston direktiivi 2005/29/EY, annettu 11 päivänä toukokuuta 2005, sopimattomista elinkeinonharjoittajien ja kuluttajien välisistä kaupallisista menettelyistä sisämarkkinoilla ja neuvoston direktiivin 84/450/ETY, Euroopan parlamentin ja neuvoston direktiivien 97/7/EY, 98/27/EY ja 2002/65/EY sekä Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 2006/2004 muuttamisesta (sopimattomia kaupallisia menettelyjä koskeva direktiivi) (EUVL L 149, 11.6.2005, s. 22).

37 Euroopan parlamentin ja neuvoston asetus (EU) 2019/1150, annettu 20 päivänä kesäkuuta 2019, oikeudenmukaisuuden ja avoimuuden edistämisestä verkossa toimivien välityspalvelujen yrityskäyttäjiä varten (EUVL L 186, 11.7.2019, s. 57).

22) ’verkkoyhteisöalustalla’ alustaa, jonka avulla loppukäyttäjät voivat olla yhteydessä toisiinsa, jakaa sisältöä, hakea tietoa ja viestiä monenlaisilla päätelaitteilla erityisesti pikaviestikeskustelujen, julkaisujen, videoiden ja suositusten muodossa;

23) ’julkishallinnon toimijalla’ jäsenvaltiossa sijaitsevaa toimijaa, joka täyttää seuraavat kriteerit:

a) se on perustettu tyydyttämään yleisen edun mukaisia tarpeita, eikä sillä ole teollista tai kaupallista luonnetta;

b) se on oikeushenkilö;

c) sen rahoituksesta suurin osa on peräisin valtiolta, alueelliselta viranomaiselta tai muilta julkisoikeudellisilta laitoksilta; tai sen johto on näiden viranomaisten tai laitosten valvonnan alainen; tai valtio, alueviranomaiset tai muut julkisoikeudelliset laitokset nimittävät yli puolet sen hallinto-, johto- tai valvontaelimen jäsenistä;

d) sillä on valtuudet osoittaa luonnollisille henkilöille tai oikeushenkilöille hallinnollisia tai sääntelyyn liittyviä päätöksiä, jotka vaikuttavat näiden oikeuksiin liittyen henkilöiden, tavaroiden, palvelujen tai pääoman liikkuvuuteen rajojen yli.

Mukaan ei lueta julkishallinnon toimijoita, jotka toimivat yleisen turvallisuuden, lainvalvonnan, puolustuksen tai kansallisen turvallisuuden alalla;

24) ’toimijalla’ luonnollista henkilöä tai sijoittautumispaikkansa kansallisen oikeuden perusteella muodostettua ja tunnustettua oikeushenkilöä, joka voi omissa nimissään käyttää oikeuksia ja jolle voidaan asettaa velvoitteita;

25) ’keskeisellä toimijalla’ liitteessä I tarkoitettua keskeistä toimijaa;

26) ’tärkeällä toimijalla’ liitteessä II tarkoitettua tärkeää toimijaa.

II LUKU

Koordinoidut kyberturvallisuuden sääntelykehykset

5 artikla

Kansallinen kyberturvallisuusstrategia

1. Kunkin jäsenvaltion on hyväksyttävä kansallinen kyberturvallisuusstrategia, jossa määritellään strategiset tavoitteet sekä asianmukaiset politiikka- ja sääntelytoimenpiteet kyberturvallisuuden korkean tason saavuttamiseksi ja ylläpitämiseksi. Kansalliseen kyberturvallisuusstrategiaan on sisällyttävä erityisesti seuraavat:

a) jäsenvaltion kyberturvallisuusstrategian tavoitteiden ja painopisteiden määrittely;

b) hallintokehys näiden tavoitteiden ja painopisteiden saavuttamiseksi, mukaan lukien 2 kohdassa tarkoitetut toimintaperiaatteet sekä julkisten elinten ja toimijoiden sekä muiden asiaankuuluvien tahojen roolit ja vastuut;

c) arvio asiaankuuluvista toiminnoista ja kyberturvallisuusriskeistä kyseisessä jäsenvaltiossa;

d) toimenpiteet, joilla varmistetaan poikkeamiin varautuminen, reagointi ja niistä toipuminen, mukaan lukien julkisen ja yksityisen sektorin yhteistyö;

e) luettelo kansallisen kyberturvallisuusstrategian täytäntöönpanoon osallistuvista eri viranomaisista ja tahoista;

f) toimintakehys toimivaltaisten viranomaisten välisen koordinoinnin tehostamiseksi tämän direktiivin ja Euroopan parlamentin ja neuvoston direktiivin (EU) XXXX/XXXX[38] [kriittisten yksiköiden häiriönsietokykyä koskeva direktiivi] mukaisesti poikkeamia ja kyberuhkia koskevien tietojen jakamiseksi ja valvontatehtävien hoitamiseksi.

2. Osana kansallista kyberturvallisuusstrategiaa jäsenvaltioiden on erityisesti vahvistettava seuraavat toimintaperiaatteet:

a) toimintaperiaatteet, jotka koskevat kyberturvallisuutta sellaisten tieto- ja viestintätekniikan tuotteiden ja palvelujen toimitusketjussa, joita keskeiset ja tärkeät toimijat käyttävät palvelujensa tarjoamiseen;

b) toimintaperiaatteet tieto- ja viestintäteknisten tuotteiden ja palvelujen kyberturvallisuusvaatimusten huomioimiseksi ja määrittelemiseksi julkisissa hankinnoissa;

c) toimintaperiaatteet 6 artiklassa tarkoitetun koordinoidun haavoittuvuuksien ilmaisemisen edistämiseksi ja sujuvoittamiseksi;

d) toimintaperiaatteet avoimen internetin yleisen ydinverkon yleisen saatavuuden ja eheyden ylläpitämiseksi;

e) toimintaperiaatteet kyberturvaosaamisen edistämiseksi ja kehittämiseksi, kyberturvatietoisuuden lisäämiseksi sekä alan tutkimuksen ja kehityksen edistämiseksi;

f) toimintaperiaatteet akateemisten ja tutkimuslaitosten tukemiseksi niiden kehittäessä kyberturvamenetelmiä ja turvallista verkkoinfrastruktuuria;

g) toimintaperiaatteet, asiaankuuluvat menettelyt ja asianmukaiset tiedonjakovälineet, joilla tuetaan vapaaehtoista kyberturvallisuustietojen jakamista yritysten välillä unionin oikeuden mukaisesti;

h) toimintaperiaatteet, joilla vastataan pk-yritysten, erityisesti tämän direktiivin soveltamisalan ulkopuolelle jäävien pk-yritysten, erityistarpeisiin, jotka liittyvät ohjeistukseen ja tukeen niiden kyberturvauhkien sietokyvyn parantamiseksi.

3. Jäsenvaltioiden on toimitettava kansalliset kyberturvallisuusstrategiansa komissiolle kolmen kuukauden kuluessa niiden hyväksymisestä. Jäsenvaltiot voivat tässä yhteydessä jättää pois tiettyjä tietoja jos ja siinä määrin kuin se on ehdottoman välttämätöntä kansallisen turvallisuuden säilyttämiseksi.

4. Jäsenvaltioiden on arvioitava kansalliset kyberturvallisuusstrategiansa vähintään neljän vuoden välein keskeisten suorituskykyindikaattoreiden perusteella ja tarvittaessa muutettava strategioita. Euroopan unionin kyberturvallisuusvirasto (ENISA) avustaa pyynnöstä jäsenvaltioita kansallisen strategian ja keskeisten suorituskykyindikaattoreiden laatimisessa strategian arviointia varten.

[38] *[lisätään koko nimi ja EUVL:n julkaisuviite, kun ne ovat tiedossa]*

6 artikla

Koordinoitu haavoittuvuuden ilmaiseminen ja Euroopan haavoittuvuusrekisteri

1. Kunkin jäsenvaltion on nimettävä yksi 9 artiklassa tarkoitetuista CSIRT-yksiköistään koordinaattoriksi koordinoitua haavoittuvuuksien ilmaisemista varten. Nimetty CSIRT-yksikkö toimii luotettuna välittäjänä ja edesauttaa tarvittaessa raportoivan toimijan ja tieto- ja viestintätekniikan tuotteiden tai palvelujen valmistajan tai tarjoajan välistä vuorovaikutusta. Jos raportoitu haavoittuvuus koskee useita tieto- ja viestintätekniikan tuotteiden tai palvelujen valmistajia tai tarjoajia eri puolilla unionia, kunkin asianomaisen jäsenvaltion nimetyn CSIRT-yksikön on tehtävä yhteistyötä CSIRT-verkoston kanssa.

2. ENISA perustaa Euroopan haavoittuvuusrekisterin ja ylläpitää sitä. Tätä varten ENISA luo asianmukaiset tietojärjestelmät, toimintatavat ja menettelyt ja pitää niitä yllä, jotta tärkeät ja keskeiset toimijat ja niiden verkko- ja tietojärjestelmien toimittajat voivat ilmaista ja rekisteröidä tieto- ja viestintäteknisissä tuotteissa tai palveluissa esiintyviä haavoittuvuuksia ja jotta rekisterin sisältämät haavoittuvuustiedot ovat kaikkien asianomaisten osapuolten saatavilla. Rekisterin on sisällettävä erityisesti tiedot haavoittuvuudesta, siitä, mihin tieto- ja viestintätekniikan tuotteeseen tai palveluun se vaikuttaa, sekä haavoittuvuuden vakavuudesta niiden olosuhteiden perusteella, joissa sitä voidaan hyödyntää, asiaan liittyvien ohjelmistokorjausten saatavuudesta ja tällaisten puuttuessa haavoittuvien tuotteiden ja palvelujen käyttäjille suunnatusta ohjeistuksesta siitä, miten haavoittuvuudesta johtuvia riskejä voidaan vähentää.

7 artikla

Kansalliset kyberturvallisuuden kriisinhallintapuitteet

1. Kunkin jäsenvaltion on nimettävä yksi tai useampi toimivaltainen viranomainen, joka vastaa laajamittaisten poikkeamien ja kriisien hallinnasta. Jäsenvaltioiden on varmistettava, että toimivaltaisilla viranomaisilla on niille annettujen tehtävien tuloksellisen ja tehokkaan hoitamisen edellyttämät resurssit.

2. Kunkin jäsenvaltion on yksilöitävä valmiudet, voimavarat ja menettelyt, joita voidaan käyttää kriisitilanteissa tämän direktiivin soveltamiseksi.

3. Kunkin jäsenvaltion on laadittava kansallinen kyberturvapoikkeama- ja -kriisinhallintasuunnitelma, jossa vahvistetaan laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien hallinnan tavoitteet ja menettelysäännöt. Suunnitelmassa on vahvistettava erityisesti seuraavat seikat:

   a) kansallisten varautumiskeinojen ja -toimien tavoitteet;

   b) kansallisten toimivaltaisten viranomaisten tehtävät ja vastuut;

   c) kriisinhallintamenettelyt ja tiedonvaihtokanavat;

   d) varautumiskeinot, mukaan lukien harjoitukset ja koulutus;

   e) asianomaiset julkiset ja yksityiset sidosryhmät ja asiaan liittyvä infrastruktuuri;

f) asiaankuuluvien kansallisten viranomaisten ja elinten väliset kansalliset menettelyt ja järjestelyt sen varmistamiseksi, että jäsenvaltio osallistuu tuloksellisesti laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien koordinoituun hallinnointiin unionin tasolla ja tukee sitä.

4. Jäsenvaltioiden on ilmoitettava komissiolle 1 kohdassa tarkoitettujen toimivaltaisten viranomaistensa nimeämisestä ja toimitettava 3 kohdassa tarkoitetut kansalliset kyberturvapoikkeama- ja -kriisisuunnitelmansa kolmen kuukauden kuluessa nimeämisestä ja kyseisten suunnitelmien hyväksymisestä. Jäsenvaltiot voivat tässä yhteydessä jättää suunnitelmasta pois tiettyjä tietoja jos ja siinä määrin kuin se on kansallisen turvallisuuden kannalta ehdottoman välttämätöntä.

8 artikla

Kansalliset toimivaltaiset viranomaiset ja keskitetyt yhteyspisteet

1. Kunkin jäsenvaltion on nimettävä yksi tai useampi toimivaltainen viranomainen, joka vastaa kyberturvallisuudesta ja tämän direktiivin VI luvussa tarkoitetuista valvontatehtävistä. Jäsenvaltiot voivat nimetä tätä tarkoitusta varten yhden tai useamman jo olemassa olevan viranomaisen.

2. Edellä 1 kohdassa tarkoitettujen toimivaltaisten viranomaisten on valvottava tämän direktiivin soveltamista kansallisella tasolla.

3. Kunkin jäsenvaltion on nimettävä yksittäinen kansallinen kyberturvallisuusasioiden yhteyspiste, jäljempänä ’keskitetty yhteyspiste’. Jos jäsenvaltio nimeää vain yhden toimivaltaisen viranomaisen, kyseinen toimivaltainen viranomainen on myös kyseisen jäsenvaltion keskitetty yhteyspiste.

4. Kunkin keskitetyn yhteyspisteen on toimittava välittäjänä ja varmistettava oman jäsenvaltionsa viranomaisten yhteistyö muiden jäsenvaltioiden asiaankuuluvien viranomaisten kanssa sekä varmistettava hallinnonalojen rajat ylittävä yhteistyö maansa muiden kansallisten toimivaltaisten viranomaisten kanssa.

5. Jäsenvaltioiden on varmistettava, että 1 kohdassa tarkoitetuilla toimivaltaisilla viranomaisilla ja keskitetyillä yhteyspisteillä on riittävät resurssit suorittaa niille osoitetut tehtävät tuloksellisesti ja tehokkaasti ja siten saavuttaa tämän direktiivin tavoitteet. Jäsenvaltioiden on varmistettava, että nimetyt edustajat kykenevät tulokselliseen, toimivaan ja tietoturvattuun yhteistyöhön 12 artiklassa tarkoitetussa yhteistyöryhmässä.

6. Kunkin jäsenvaltion on ilmoitettava komissiolle ilman aiheetonta viivytystä 1 kohdassa tarkoitetun toimivaltaisen viranomaisen ja 3 kohdassa tarkoitetun keskitetyn yhteyspisteen nimeämisestä, niiden tehtävistä ja näihin myöhemmin mahdollisesti tehtävistä muutoksista. Kunkin jäsenvaltion on julkistettava nimitykset. Komissio julkaisee luettelon nimetyistä keskitetyistä yhteyspisteistä.

9 artikla

Tietoturvaloukkauksiin reagoivat ja niitä tutkivat yksiköt (CSIRT)

1. Kunkin jäsenvaltion on nimettävä yksi tai useampi CSIRT-yksikkö, jonka on täytettävä 10 artiklan 1 kohdassa säädetyt vaatimukset ja joka kattaa ainakin liitteissä I ja II tarkoitetut toimialat, alasektorit tai toimijat ja joka on vastuussa poikkeamien

käsittelystä tarkasti määritellyn prosessin mukaisesti. CSIRT voidaan perustaa 8 artiklassa tarkoitetun toimivaltaisen viranomaisen alaisuuteen.

2. Jäsenvaltioiden on varmistettava, että kullakin CSIRT-yksiköllä on 10 artiklan 2 kohdassa säädettyjen tehtäviensä tuloksellisen hoitamisen edellyttämät resurssit.

3. Jäsenvaltioiden on varmistettava, että kullakin CSIRT-yksiköllä on käytössään asianmukainen, suojattu ja häiriönsietokykyinen viestintä- ja tietoinfrastruktuuri tietojen vaihtamiseksi keskeisten ja tärkeiden toimijoiden ja muiden asianomaisten osapuolten kanssa. Tätä varten jäsenvaltioiden on varmistettava, että CSIRT-yksiköt ovat mukana turvallisten tiedonjakovälineiden käyttöönotossa.

4. CSIRT-toimijoiden on tehtävä yhteistyötä ja tarvittaessa vaihdettava asiaankuuluvia tietoja 26 artiklan mukaisesti keskeisten ja tärkeiden toimijoiden luotettujen alakohtaisten tai monialaisten yhteisöjen kanssa.

5. CSIRT-yksiköiden on osallistuttava 16 artiklan mukaisesti järjestettäviin vertaisarviointeihin.

6. Jäsenvaltioiden on varmistettava, että niiden CSIRT-yksiköt tekevät tuloksellista, tehokasta ja tietoturvattua yhteistyötä 13 artiklassa tarkoitetussa CSIRT-verkostossa.

7. Jäsenvaltioiden on ilmoitettava komissiolle ilman aiheetonta viivytystä 1 kohdan mukaisesti nimetyt CSIRT-yksiköt, 6 artiklan 1 kohdan mukaisesti nimetty CSIRT-koordinaattori ja niiden liitteissä I ja II tarkoitettuihin toimijoihin liittyvät tehtävät.

8. Jäsenvaltiot voivat pyytää ENISAn apua kansallisten CSIRT-yksiköiden toiminnan kehittämiseen.

10 artikla

CSIRT-yksiköiden vaatimukset ja tehtävät

1. CSIRT-yksiköiden on täytettävä seuraavat vaatimukset:

   a) CSIRT-yksiköiden on varmistettava viestintäpalvelujensa kattava saatavuus välttämällä yksittäisiä pisteitä, joiden toimintahäiriö keskeyttäisi koko palvelun, ja niiden on pidettävä käytössä useita kanavia, joiden kautta niihin voidaan ottaa yhteyttä ja joiden kautta ne itse voivat ottaa yhteyttä muualle milloin tahansa. CSIRT-yksiköiden on määriteltävä selkeästi viestintäkanavat ja tiedotettava niistä kohderyhmilleen ja yhteistyökumppaneille;

   b) CSIRT-yksiköiden toimitilat ja tietojärjestelmät on sijoitettava suojattuihin paikkoihin;

   c) CSIRT-yksiköillä on oltava tarkoituksenmukainen järjestelmä pyyntöjen hallintaa ja reititystä varten erityisesti tapausten tuloksellisen ja tehokkaan edelleenohjauksen helpottamiseksi;

   d) CSIRT-yksiköillä on oltava riittävä henkilöstö, jotta ne voivat olla käytettävissä jatkuvasti;

   e) CSIRT-yksiköillä on oltava varajärjestelmät ja -työtilat niiden palvelujen jatkuvuuden varmistamiseksi;

   f) CSIRT-yksiköillä on oltava mahdollisuus osallistua kansainvälisiin yhteistyöverkostoihin.

2. CSIRT-yksiköiden tehtävänä on

a) seurata kyberuhkia, haavoittuvuuksia ja poikkeamia kansallisella tasolla;

b) antaa kyberuhkia, haavoittuvuuksia ja poikkeamia koskevia varhaisvaroituksia, hälytyksiä, ilmoituksia ja tietoja keskeisille ja tärkeille toimijoille sekä muille asianomaisille osapuolille;

c) reagoida poikkeamiin;

d) laatia dynaamisesti tilanteen mukaan kyberturvallisuuteen liittyviä riski- ja poikkeama-analyysejä ja ylläpitää kyberturvallisuuden tilannekuvaa;

e) toteuttaa toimijoiden pyynnöstä niiden palveluntarjonnassa käyttämien verkko- ja tietojärjestelmien ennakoivia kartoituksia;

f) osallistua CSIRT-verkostoon ja antaa pyynnöstä apua verkoston muille jäsenille.

3. CSIRT-yksiköiden on luotava yhteistyösuhteet asiaan liittyvien yksityisen sektorin tahojen kanssa, jotta direktiivin tavoitteet voidaan saavuttaa paremmin.

4. Yhteistyön helpottamiseksi CSIRT-yksiköiden on edistettävä yhteisten tai standardoitujen käytäntöjen, luokitusjärjestelmien ja taksonomioiden määrittämistä ja käyttöä seuraavien osalta:

a) poikkeamien käsittelymenettelyt;

b) kyberturvallisuuskriisien hallinta;

c) koordinoitu haavoittuvuuksien ilmaisu:

11 artikla

Kansallisen tason yhteistyö

1. Jos ne ovat erillisiä, saman jäsenvaltion 8 artiklassa tarkoitettujen toimivaltaisten viranomaisten, keskitetyn yhteyspisteen ja CSIRT-yksiköiden on tehtävä yhteistyötä tässä direktiivissä säädettyjen velvoitteiden täyttämiseksi.

2. Jäsenvaltioiden on varmistettava, että joko niiden toimivaltaiset viranomaiset tai CSIRT-yksiköt saavat tämän direktiivin nojalla toimitetut ilmoitukset poikkeamista ja merkittävistä kyberuhista ja läheltä piti -tilanteista. Jos jäsenvaltio päättää, että sen CSIRT-yksiköt eivät saa kyseisiä ilmoituksia, CSIRT-yksiköille on annettava pääsy keskeisten tai tärkeiden toimijoiden 20 artiklan nojalla ilmoittamien poikkeamien tietoihin siinä määrin kuin se on tarpeen niiden tehtävien hoitamiseksi.

3. Kunkin jäsenvaltion on varmistettava, että sen toimivaltaiset viranomaiset tai CSIRT-yksiköt ilmoittavat keskitetylle yhteyspisteelleen tämän direktiivin nojalla saaduista poikkeamia, merkittäviä kyberuhkia ja läheltä piti -tilanteita koskevista ilmoituksista.

4. Siinä määrin kuin se on tarpeen tässä direktiivissä säädettyjen tehtävien ja velvollisuuksien tehokkaan suorittamisen kannalta, jäsenvaltioiden on varmistettava asianmukainen yhteistyö toimivaltaisten viranomaisten ja keskitettyjen asiointipisteiden ja lainvalvontaviranomaisten, tietosuojaviranomaisten sekä kriittisestä infrastruktuurista direktiivin (EU) XXXX/XXXX [kriittisten toimijoiden häiriönsietokykyä koskeva direktiivi] nojalla vastaavien viranomaisten ja Euroopan

parlamentin ja neuvoston asetuksen (EU) XXXX/XXXX[39] [DORA-asetus] mukaisesti nimettyjen kansallisten finanssialan viranomaisten välillä kyseisessä jäsenvaltiossa.

5. Jäsenvaltioiden on varmistettava, että niiden toimivaltaiset viranomaiset toimittavat direktiivin (EU) XXXX/XXXX [kriittisten toimijoiden häiriönsietokykyä koskeva direktiivi] nojalla nimetyille toimivaltaisille viranomaisille säännöllisesti tiedot kyberturvallisuusriskeistä, kyberuhkista ja poikkeamista, jotka vaikuttavat direktiivin (EU) XXXX/XXXX [kriittisten toimijoiden häiriönsietokykyä koskeva direktiivi] mukaisesti kriittisiksi tai niitä vastaaviksi yksilöityihin toimijoihin, sekä toimenpiteistä, joita toimivaltaiset viranomaiset ovat toteuttaneet näiden riskien ja poikkeamien johdosta.

LUKU III

Yhteistyö

12 artikla
Yhteistyöryhmä

1. Perustetaan yhteistyöryhmä tukemaan ja helpottamaan jäsenvaltioiden välistä strategista yhteistyötä ja tietojenvaihtoa tämän direktiivin soveltamisalalla.

2. Yhteistyöryhmä suorittaa tehtävänsä 6 kohdassa tarkoitettujen kaksivuotisten työohjelmien pohjalta.

3. Yhteistyöryhmä koostuu jäsenvaltioiden, komission ja ENISAn edustajista. Euroopan ulkosuhdehallinto osallistuu yhteistyöryhmän toimintaan tarkkailijana. Euroopan valvontaviranomaiset voivat osallistua yhteistyöryhmän toimintaan asetuksen (EU) XXXX/XXXX [DORA-asetus] 17 artiklan 5 kohdan c alakohdan mukaisesti.

   Yhteistyöryhmä voi tarvittaessa kutsua asiaankuuluvien sidosryhmien edustajia osallistumaan työskentelyynsä.

   Komissio huolehtii sihteeristötehtävistä.

4. Yhteistyöryhmän tehtävänä on

   a) ohjeistaa toimivaltaisia viranomaisia tämän direktiivin saattamisessa osaksi kansallista lainsäädäntöä ja sen täytäntöönpanossa;

   b) vaihtaa tietoa tämän direktiivin täytäntöönpanon parhaista käytännöistä ja käydä vuoropuhelua liittyen muun muassa kyberuhkiin, poikkeamiin, haavoittuvuuksiin, läheltä piti -tilanteisiin, tiedotushankkeisiin, koulutukseen, harjoituksiin ja osaamiseen, valmiuksien kehittämiseen sekä standardeihin ja teknisiin eritelmiin;

   c) antaa neuvoja ja tehdä yhteistyötä komission kanssa tulevissa kyberturvallisuuspoliittisissa aloitteissa;

[39] *[lisätään koko nimi ja EUVL:n julkaisuviite, kun ne ovat tiedossa]*

d) antaa neuvoja ja tehdä yhteistyötä komission kanssa liittyen ehdotuksiin tämän direktiivin nojalla annettaviksi komission täytäntöönpanosäädöksiksi tai delegoiduiksi säädöksiksi;

e) vaihtaa tietoa parhaista käytännöistä ja käydä vuoropuhelua asiaankuuluvien unionin toimielinten, virastojen, elinten ja laitosten kanssa;

f) keskustella 16 artiklan 7 kohdassa tarkoitetuista vertaisarviointiraporteista;

g) keskustella 34 artiklassa tarkoitettujen rajat ylittävien yhteisvalvontatoimien tuloksista;

h) antaa CSIRT-verkostolle strategista ohjausta esiin nousevissa kysymyksissä;

i) edesauttaa kyberturvallisuusvalmiuksien kehittymistä unionissa helpottamalla kansallisten virkamiesten vaihtoa kehitysohjelmalla, johon osallistuu jäsenvaltioiden toimivaltaisten viranomaisten tai CSIRT-yksiköiden henkilöstöä;

j) järjestää säännöllisesti eri puolilta unionia tulevien asiaankuuluvien yksityisten sidosryhmien kanssa yhteiskokouksia, joissa keskustellaan ryhmän toteuttamista toimista ja kerätään näkemyksiä esiin nousevista toimintapoliittisista haasteista;

k) keskustella kyberturvallisuusharjoituksiin liittyvästä työstä, mukaan lukien ENISAn tekemä työ.

5. Yhteistyöryhmä voi pyytää CSIRT-verkostolta teknisiä raportteja haluamistaan aiheista.

6. Viimeistään [24 kuukautta tämän direktiivin voimaantulosta] ja sen jälkeen joka toinen vuosi yhteistyöryhmä laatii työohjelman tavoitteidensa saavuttamiseksi ja tehtäviensä hoitamiseksi. Tämän direktiivin mukaisesti hyväksytyn ensimmäisen ohjelman aikataulu on mukautettava direktiivin (EU) 2016/1148 mukaisesti hyväksytyn viimeisen ohjelman aikatauluun.

7. Komissio voi hyväksyä täytäntöönpanosäädöksiä, joissa vahvistetaan yhteistyöryhmän toimintaa varten tarvittavia menettelytapajärjestelyjä. Nämä täytäntöönpanosäädökset hyväksytään 37 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

8. Yhteistyöryhmä kokoontuu säännöllisesti ja vähintään kerran vuodessa direktiivillä (EU) XXXX/XXXX [kriittisten toimijoiden häiriönsietokykyä koskeva direktiivi] perustetun kriittisten toimijoiden häiriönsietokykyä käsittelevän ryhmän kanssa edistääkseen strategista yhteistyötä ja tietojenvaihtoa.

13 artikla
CSIRT-verkosto

1. Jotta voidaan edistää luottamusta sekä ripeää ja tuloksellista operatiivista yhteistyötä jäsenvaltioiden välillä, perustetaan kansallisten CSIRT-yksiköiden verkosto.

2. CSIRT-verkosto koostuu jäsenvaltioiden CSIRT-yksiköiden ja tietotekniikan kriisiryhmän (CERT-EU) edustajista. Komissio osallistuu CSIRT-verkostoon tarkkailijana. ENISA huolehtii sihteeristötehtävistä ja tukee aktiivisesti CSIRT-yksiköiden välistä yhteistyötä.

3. CSIRT-verkoston tehtävänä on

a) vaihtaa tietoa CSIRT-yksiköiden valmiuksista;

b) vaihtaa asiaankuuluvaa tietoa poikkeamista, läheltä piti -tilanteista, kyberuhista, riskeistä ja haavoittuvuuksista;

~~c)~~ poikkeaman vaikutuspiiriin mahdollisesti kuuluvan CSIRT-verkoston jäsenen pyynnöstä vaihtaa tietoa ja keskustella kyseisestä poikkeamasta ja siihen liittyvistä kyberuhista, riskeistä ja haavoittuvuuksista;

d) CSIRT-verkoston jäsenen pyynnöstä keskustella kyseisen jäsenvaltion lainkäyttöalueella todettua poikkeamaa koskevasta koordinoidusta vasteesta ja mahdollisuuksien mukaan sen toteuttamisesta;

e) tukea jäsenvaltioita rajat ylittävien poikkeamien käsittelyssä tämän direktiivin mukaisesti;

f) tehdä yhteistyötä ja avustaa 6 artiklassa tarkoitettuja nimettyjä CSIRT-yksiköitä, kun ilmaistaan hallitusti ja monen osapuolen välillä koordinoidusti haavoittuvuuksia, jotka vaikuttavat useisiin, eri jäsenvaltioihin sijoittautuneisiin tieto- ja viestintäteknisten tuotteiden, tieto- ja viestintäteknisten palvelujen ja tieto- ja viestintäteknisten prosessien valmistajiin tai tarjoajiin;

g) keskustella uusista operatiivisen yhteistyön muodoista liittyen esimerkiksi seuraaviin:

i) kyberuhkien ja poikkeamien luokittelu;

ii) ennakkovaroitukset;

iii) keskinäinen avunanto;

iv) koordinoinnin periaatteet ja toimintatavat vastattaessa rajat ylittäviin riskeihin ja poikkeamiin;

v) rooli 7 artiklan 3 kohdassa tarkoitetun kansallisen kyberturvapoikkeama- ja -kriisinhallintasuunnitelman laadinnassa;

h) tiedottaa yhteistyöryhmälle verkoston toiminnasta ja muista g alakohdan mukaisista käsitellyistä operatiivisen yhteistyön muodoista ja pyytää tarvittaessa ohjeistusta tältä osin;

i) koota yhteen oppeja kyberturvallisuusharjoituksista, myös ENISAn järjestämistä harjoituksista;

j) yksittäisen CSIRT-yksikön pyynnöstä keskustella kyseisen CSIRT-yksikön valmiuksista ja varautumisesta;

k) tehdä yhteistyötä ja vaihtaa tietoja alueellisten ja unionin tason turvaoperaatiokeskusten kanssa, jotta voidaan parantaa yhteistä tilannekuvaa poikkeamista ja uhista unionissa;

l) keskustella 16 artiklan 7 kohdassa tarkoitetuista vertaisarviointiraporteista;

m) antaa ohjeistusta operatiivisten käytäntöjen lähentämisen helpottamiseksi siltä osin kuin kyse on operatiivista yhteistyötä koskevien tämän artiklan säännösten soveltamisesta.

4. CSIRT-verkoston on 35 artiklassa tarkoitettua uudelleentarkastelua varten ja viimeistään [24 kuukauden kuluttua tämän direktiivin voimaantulosta] ja sen jälkeen joka toinen vuosi arvioitava operatiivisen yhteistyön edistymistä ja laadittava siitä raportti. Raportissa on erityisesti esitettävä päätelmät 16 artiklassa tarkoitettujen, kansallisia CSIRT-yksiköitä koskevien vertaisarviointien tuloksista, mukaan lukien johtopäätökset ja suositukset, joihin on päädytty tämän artiklan nojalla. Kyseinen raportti toimitetaan myös yhteistyöryhmälle.

5. CSIRT-verkosto vahvistaa työjärjestyksensä.

14 artikla

Euroopan kyberkriisien yhteysorganisaatioiden verkosto (EU-CyCLONe)

1. Perustetaan Euroopan kyberkriisien yhteysorganisaatioiden verkosto (EU-CyCLONe) tukemaan laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien koordinoitua hallintaa operatiivisella tasolla ja varmistamaan säännöllinen tiedonvaihto jäsenvaltioiden ja unionin toimielinten, elinten ja virastojen välillä.

2. EU-CyCLONe koostuu 7 artiklan mukaisesti nimettyjen jäsenvaltioiden kriisinhallintaviranomaisten, komission ja ENISAn edustajista. ENISA huolehtii verkoston sihteeristön tehtävistä ja tukee tiedonvaihdon suojaamista.

3. EU-CyCLONen tehtävänä on

a) parantaa valmistautumista laajamittaisten poikkeamien ja kriisien hallintaan;

b) luoda yhteinen tilannekuva merkityksellisistä kyberturvallisuustapahtumista;

c) koordinoida laajamittaisten poikkeamien ja kriisien hallintaa ja tukea tällaisiin poikkeamiin ja kriiseihin liittyvää poliittisen tason päätöksentekoa;

d) keskustella 7 artiklan 2 kohdassa tarkoitetuista kansallisista kyberturvapoikkeama- ja -kriisinhallintasuunnitelmista.

4. EU-CyCLONe vahvistaa työjärjestyksensä.

5. EU-CyCLONe raportoi säännöllisesti yhteistyöryhmälle kyberuhkista, poikkeamista ja alan suuntauksista keskittyen erityisesti niiden vaikutuksiin keskeisiin ja tärkeisiin toimijoihin.

6. EU-CyCLONe tekee yhteistyötä CSIRT-verkoston kanssa sovittujen menettelyjen pohjalta.

15 artikla

Raportti kyberturvallisuuden tilasta unionissa

1. ENISA laatii yhteistyössä komission kanssa joka toinen vuosi raportin kyberturvallisuuden tilasta unionissa. Raportissa on esitettävä arvio erityisesti seuraavista:

a) kyberturvallisuusvalmiuksien kehittyminen unionissa;

b) toimivaltaisten viranomaisten ja kyberturvallisuushallinnan tarkoituksiin käytettävissä olevat tekniset, taloudelliset ja henkilöresurssit sekä valvontatoimenpiteiden ja täytäntöönpanotoimien toteutus 16 artiklassa tarkoitettujen vertaisarviointien tulosten johdosta;

c) kyberturvallisuusindeksi, joka muodostaa kokonaisarvion kyberturvallisuusvalmiuksien kehitystasosta.

2. Raportin on sisällettävä toimintapoliittisia suosituksia kyberturvallisuuden tason nostamiseksi koko unionissa sekä yhteenveto kyseistä kautta koskevista havainnoista, jotka sisältyvät ENISAn asetuksen (EU) 2019/881 7 artiklan 6 kohdan mukaisesti antamiin unionin kyberturvallisuuden teknisiin tilanneraportteihin.

16 artikla

Vertaisarvioinnit

1. Komissio vahvistaa yhteistyöryhmää ja ENISAa kuultuaan ja viimeistään 18 kuukauden kuluttua tämän direktiivin voimaantulosta toimintatavat ja -mallin vertaisarviointijärjestelmälle, jolla arvioidaan kunkin jäsenvaltion kyberturvallisuuspolitiikan toimivuutta. Vertaisarvioinnit suorittavat muista kuin arvioitavasta jäsenvaltiosta tulevat kyberturvallisuuden tekniset asiantuntijat ja arviointien on katettava vähintään seuraavat seikat:

   i) toiminnan tuloksellisuus suhteessa 18 ja 20 artiklassa tarkoitettuihin kyberturvallisuusriskien hallintaa koskeviin vaatimuksiin ja raportointivelvoitteisiin;

   ii) valmiuksien taso, mukaan lukien käytettävissä olevat taloudelliset, tekniset ja henkilöresurssit, sekä kansallisten toimivaltaisten viranomaisten tuloksellisuus tehtäviensä hoidossa;

   iii) CSIRT-yksiköiden operatiiviset valmiudet ja toimivuus;

   iv) 34 artiklassa tarkoitetun keskinäisen avunannon toimivuus;

   v) tämän direktiivin 26 artiklassa tarkoitetun tiedonvaihtojärjestelyn toimivuus.

2. Vertailumenetelmässä käytetään objektiivisia, syrjimättömiä, oikeudenmukaisia ja läpinäkyviä kriteerejä, joiden perusteella jäsenvaltioiden on nimettävä vertaisarviointien suorittamiseen kykenevät asiantuntijat. ENISA ja komissio nimeävät omat asiantuntijansa osallistumaan vertaisarviointeihin tarkkailijoina. Komissio luo ENISAn tuella 1 kohdassa tarkoitettujen toimintatapojen osaksi objektiivisen, syrjimättömän, oikeudenmukaisen ja läpinäkyvän järjestelmän asiantuntijoiden valitsemiseksi ja osoittamiseksi satunnaisesti kuhunkin vertaisarviointiin.

3. Vertaisarviointien organisatorisista näkökohdista päättää komissio ENISAn tuella, ja ne perustuvat yhteistyöryhmää kuullen 1 kohdassa tarkoitetuissa toimintatavoissa määriteltyihin kriteereihin. Vertaisarvioinneissa arvioidaan 1 kohdassa tarkoitettuja näkökohtia kaikkien jäsenvaltioiden ja toimialojen osalta, myös yhdelle tai useammalle jäsenvaltiolle tai yhdelle tai useammalle toimialalle ominaisia näkökohtia.

4. Vertaisarviointeihin sisältyy fyysisiä tai virtuaalisia kohdeselvityksiä sekä yleistä tiedonvaihtoa. Arvioinnin kohteena olevien jäsenvaltioiden on hyvän yhteistyön hengessä annettava nimetyille asiantuntijoille heidän pyytämänsä, arvioitavien näkökohtien edellyttämät tiedot. Vertaisarviointiprosessissa saatuja tietoja saa käyttää ainoastaan tähän tarkoitukseen. Vertaisarviointiin osallistuvat asiantuntijat eivät saa paljastaa arvioinnin aikana saatuja arkaluonteisia tai luottamuksellisia tietoja ulkopuolisille.

5. Kun tietyt näkökohdat on arvioitu tietyssä jäsenvaltiossa, niitä ei arvioida uudelleen samassa jäsenvaltiossa kahden vertaisarvioinnin päättymistä seuraavan vuoden aikana, ellei komissio ENISAa ja yhteistyöryhmää kuultuaan toisin päätä.

6. Jäsenvaltioiden on varmistettava, että nimettyjä asiantuntijoita koskevat eturistiriitariskit ilmoitetaan muille jäsenvaltioille, komissiolle ja ENISAlle ilman aiheetonta viivytystä.

7. Vertaisarviointeihin osallistuvien asiantuntijoiden on laadittava raportit arviointien tuloksista ja päätelmistä. Raportit on toimitettava komissiolle, yhteistyöryhmälle, CSIRT-verkostolle ja ENISAlle. Raporteista keskustellaan yhteistyöryhmässä ja CSIRT-verkostossa. Raportit voidaan julkaista yhteistyöryhmän verkkosivustolla.

IV LUKU

Kyberturvallisuusriskien hallinta- ja raportointivelvoitteet

I JAKSO

Kyberturvallisuusriskien hallinta ja raportointi

17 artikla

Hallinnointi

1. Jäsenvaltioiden on varmistettava, että keskeisten ja tärkeiden toimijoiden hallintoelimet hyväksyvät näiden toimijoiden 18 artiklan noudattamiseksi toteuttamat kyberturvallisuusriskien hallintatoimenpiteet, valvovat niiden täytäntöönpanoa ja ovat vastuuvelvollisia, jos toimijat eivät noudata tämän artiklan mukaisia velvoitteita.

2. Jäsenvaltioiden on varmistettava, että näiden hallintoelinten jäsenet osallistuvat säännöllisesti erityiskoulutukseen riittävien tietojen ja taitojen hankkimiseksi, jotta he voivat ymmärtää ja arvioida kyberturvallisuusriskejä ja -hallintakäytäntöjä sekä niiden vaikutusta toimijaan.

18 artikla

Kyberturvallisuusriskien hallintatoimenpiteet

1. Jäsenvaltioiden on varmistettava, että keskeiset ja tärkeät toimijat toteuttavat asianmukaiset ja oikeasuhteiset tekniset ja organisatoriset toimenpiteet hallitakseen

riskejä, joita kohdistuu niiden palveluntarjonnassaan käyttämien verkko- ja tietojärjestelmien turvallisuuteen. Näillä toimenpiteillä on varmistettava riskiin suhteutettu verkko- ja tietojärjestelmien turvallisuuden taso uusin tekniikka huomioon ottaen.

2. Edellä 1 kohdassa tarkoitettuihin toimenpiteisiin on sisällyttävä ainakin seuraavat:

   a) riskianalyysejä ja tietojärjestelmien turvallisuutta koskevat toimintaperiaatteet;

   b) poikkeamien käsittely (poikkeamien ehkäisy, havaitseminen ja niihin reagointi);

   c) toiminnan jatkuvuuden ja kriisitilanteiden hallinta;

   d) toimitusketjun turvallisuus, mukaan lukien turvallisuuteen liittyvät näkökohdat, jotka koskevat kunkin toimijan ja sen alihankkijoiden tai palveluntarjoajien, kuten datatallennus- ja -käsittelypalvelujen tai tietoturvapalveluntarjoajien (MSSP), välisiä suhteita;

   e) verkko- ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuus, mukaan lukien haavoittuvuuksien käsittely ja ilmaiseminen;

   f) toimintatavat ja menettelyt (testaus ja auditointi), joilla arvioidaan kyberturvallisuuteen liittyvien riskinhallintatoimenpiteiden toimivuutta;

   g) salaustekniikoiden käyttö.

3. Jäsenvaltioiden on varmistettava, että harkitessaan 2 kohdan d alakohdassa tarkoitettuja asianmukaisia toimenpiteitä toimijoiden on otettava huomioon kullekin alihankkijalle ja palveluntarjoajalle ominaiset haavoittuvuudet, tuotteiden yleinen laatu sekä alihankkijoidensa ja palveluntarjoajiensa kyberturvallisuuskäytännöt, mukaan lukien niiden tuotekehityksen suojausmenettelyt.

4. Jäsenvaltioiden on varmistettava, että jos toimija toteaa, että sen palvelut tai tehtävät eivät ole 2 kohdassa säädettyjen vaatimusten mukaisia, sen on ilman aiheetonta viivytystä toteutettava kaikki tarvittavat korjaavat toimenpiteet kyseisen palvelun saattamiseksi vaatimusten mukaiseksi.

5. Komissio voi hyväksyä täytäntöönpanosäädöksiä, joissa vahvistetaan 2 kohdassa tarkoitettujen osatekijöiden teknisiä ja metodologisia eritelmiä. Valmistellessaan näitä säädöksiä komissio noudattaa 37 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä ja noudattaa mahdollisimman pitkälle kansainvälisiä ja eurooppalaisia standardeja sekä asiaankuuluvia teknisiä eritelmiä.

6. Siirretään komissiolle valta antaa 36 artiklan mukaisesti delegoituja säädöksiä, joilla täydennetään 2 kohdassa säädettyjä osatekijöitä uusien kyberuhkien, teknologian kehityksen tai alakohtaisten erityispiirteiden huomioon ottamiseksi.

19 artikla

Kriittisiä toimitusketjuja koskevat EU:n koordinoidut riskinarvioinnit

1. Yhteistyöryhmä voi yhteistyössä komission ja ENISAn kanssa tehdä koordinoituja turvallisuusriskinarviointeja yksittäisistä kriittisistä tieto- ja viestintätekniikan palvelujen, järjestelmien tai tuotteiden toimitusketjuista ottaen huomioon tekniset ja tarvittaessa muut kuin tekniset riskitekijät.

2. Komissio määrittää yhteistyöryhmää ja ENISAa kuultuaan kriittiset tieto- ja viestintätekniset palvelut, järjestelmät tai tuotteet, joille voidaan tehdä 1 kohdassa tarkoitettu koordinoitu riskinarviointi.

20 artikla

Raportointivelvoitteet

1. Jäsenvaltioiden on varmistettava, että keskeiset ja tärkeät toimijat ilmoittavat ilman aiheetonta viivytystä toimivaltaisille viranomaisille tai CSIRT-yksikölle 3 ja 4 kohdan mukaisesti kaikista poikkeamista, joilla on merkittävä vaikutus niiden palvelujen tarjoamiseen. Näiden toimijoiden on tarvittaessa ilmoitettava ilman aiheetonta viivytystä palvelujensa käyttäjille poikkeamista, jotka todennäköisesti vaikuttavat haitallisesti kyseisen palvelun tarjoamiseen. Jäsenvaltioiden on varmistettava, että kyseiset toimijat ilmoittavat muun muassa kaikki tiedot, joiden avulla toimivaltaiset viranomaiset tai CSIRT-yksikkö voivat määrittää poikkeaman mahdolliset maiden rajat ylittävät vaikutukset.

2. Jäsenvaltioiden on varmistettava, että keskeiset ja tärkeät toimijat ilmoittavat ilman aiheetonta viivytystä toimivaltaisille viranomaisille tai CSIRT-yksikölle kaikista havaitsemistaan merkittävistä kyberuhkista, jotka olisivat voineet johtaa merkittävään poikkeamaan.

   Näiden toimijoiden on tarvittaessa ilmoitettava ilman aiheetonta viivytystä palvelujensa käyttäjille, joihin merkittävä kyberuhka saattaa vaikuttaa, kaikista toimenpiteistä tai suojakeinoista, joita käyttäjät voivat toteuttaa uhan torjumiseksi. Asianmukaisissa tapauksissa toimijoiden on ilmoitettava käyttäjille myös itse uhasta. Ilmoittaminen ei lisää ilmoituksen tekevän toimijan vastuuta.

3. Poikkeama katsotaan merkittäväksi, jos

   a) poikkeama on aiheuttanut tai voi aiheuttaa kyseiselle toimijalle merkittävän toimintahäiriön tai merkittäviä taloudellisia tappioita;

   b) poikkeama on vaikuttanut tai voi vaikuttaa muihin luonnollisiin henkilöihin tai oikeushenkilöihin aiheuttamalla huomattavia aineellisia tai aineettomia tappioita.

4. Jäsenvaltioiden on varmistettava, että 1 kohdan mukaista ilmoitusta varten asianomaiset toimijat toimittavat toimivaltaisille viranomaisille tai CSIRT-yksikölle

   a) ilman aiheetonta viivytystä ja joka tapauksessa 24 tunnin kuluessa siitä, kun poikkeama on tullut tietoon, alustavan ilmoituksen, jossa on tarvittaessa ilmoitettava, johtuuko poikkeama oletettavasti laittomasta tai vihamielisestä toiminnasta;

   b) toimivaltaisen viranomaisen tai CSIRT-yksikön pyynnöstä väliraportin asiaan liittyvistä tilapäivityksistä;

   c) viimeistään kuukauden kuluttua a alakohdan mukaisesta ilmoituksesta loppuraportin, joka sisältää vähintään seuraavat tiedot:

      i) yksityiskohtainen kuvaus poikkeamasta, sen vakavuudesta ja vaikutuksista;

ii) poikkeaman todennäköisesti aiheuttaneen uhan tai juurisyyn tyyppi;

iii) toteutetut ja meneillään olevat toimenpiteet vaikutusten lieventämiseksi.

Jäsenvaltioiden on säädettävä, että asianomainen toimija voi asianmukaisesti perustelluissa tapauksissa ja toimivaltaisten viranomaisten tai CSIRT-yksikön suostumuksella poiketa a ja c alakohdassa säädetyistä määräajoista.

5. Toimivaltaisten kansallisten viranomaisten tai CSIRT-yksikön on annettava 24 tunnin kuluessa 4 kohdan a alakohdassa tarkoitetun alustavan ilmoituksen vastaanottamisesta ilmoituksen tehneelle toimijalle vastaus, mukaan lukien alustava palaute poikkeamasta ja kyseisen toimijan pyynnöstä ohjeet mahdollisista toimenpiteistä vaikutusten lieventämiseksi. Jos CSIRT-yksikkö ei ole saanut 1 kohdassa tarkoitettua ilmoitusta, toimivaltaisen viranomaisen on annettava ohjeet yhteistyössä CSIRT-yksikön kanssa. CSIRT-yksikkö antaa teknistä lisätukea, jos asianomainen toimija sitä pyytää. Jos poikkeaman epäillään olevan luonteeltaan rikollinen, toimivaltaisten kansallisten viranomaisten tai CSIRT-yksikön on annettava ohjeita myös poikkeaman ilmoittamisesta lainvalvontaviranomaisille.

6. Toimivaltaisen viranomaisen tai CSIRT-yksikön on tarvittaessa ja erityisesti silloin, kun 1 kohdassa tarkoitettu poikkeama koskee kahta tai useampaa jäsenvaltiota, tiedotettava asiasta muille asiaan liittyville jäsenvaltioille ja ENISAlle. Näin tehdessään toimivaltaisten viranomaisten, CSIRT-yksiköiden ja keskitettyjen yhteyspisteiden on unionin oikeuden tai unionin oikeuden mukaisen kansallisen lainsäädännön mukaisesti säilytettävä toimijan turvallisuusedut ja kaupalliset edut sekä annettujen tietojen luottamuksellisuus.

7. Jos yleinen tiedotus on tarpeen poikkeaman estämiseksi tai meneillään olevan poikkeaman käsittelemiseksi tai jos poikkeaman ilmaiseminen on muutoin yleisen edun mukaista, toimivaltainen viranomainen tai CSIRT-yksikkö ja tarvittaessa muiden asianomaisten jäsenvaltioiden viranomaiset tai CSIRT-yksiköt voivat asianomaista toimijaa kuultuaan tiedottaa poikkeamasta yleisölle tai vaatia toimijaa tekemään niin.

8. Keskitetyn yhteyspisteen on toimivaltaisen viranomaisen tai CSIRT-yksikön pyynnöstä toimitettava 1 ja 2 kohdan mukaisesti vastaanotetut ilmoitukset muiden asianomaisten jäsenvaltioiden keskitetyille yhteyspisteille.

9. Keskitetyn yhteyspisteen on toimitettava ENISAlle kuukausittain tiivistelmä, joka sisältää anonymisoidut koontitiedot poikkeamista, merkittävistä kyberuhista ja läheltä piti -tilanteista, joista on ilmoitettu 1 ja 2 kohdan ja 27 artiklan mukaisesti. Parantaakseen tietojen vertailukelpoisuutta ENISA voi antaa teknisiä ohjeita tiivistelmään sisältyvien tietojen rakenteesta.

10. Toimivaltaisten viranomaisten on toimitettava direktiivin (EU) XXXX/XXXX [kriittisten toimijoiden häiriönsietokykyä koskeva direktiivi] mukaisesti nimetyille toimivaltaisille viranomaisille tiedot poikkeamista ja kyberuhista, jotka direktiivin (EU) XXXX/XXXX [kriittisten toimijoiden häiriönsietokykyä koskeva direktiivi] mukaisesti kriittisiksi toimijoiksi tai niitä vastaaviksi toimijoiksi määritellyt keskeiset toimijat ovat ilmoittaneet 1 ja 2 kohdan mukaisesti.

11. Komissio voi hyväksyä täytäntöönpanosäädöksiä, joissa määritellään tarkemmin 1 ja 2 kohdan nojalla toimitettavan ilmoituksen tietorakenne, muoto ja toimitustapa. Komissio voi myös hyväksyä täytäntöönpanosäädöksiä, joissa määritellään

tarkemmin tapaukset, joissa poikkeama katsotaan 3 kohdassa tarkoitetuksi merkittäväksi tapahtumaksi. Nämä täytäntöönpanosäädökset hyväksytään 37 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

21 artikla

Eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien käyttö

1. Tiettyjen 18 artiklan vaatimusten noudattamisen osoittamiseksi jäsenvaltiot voivat edellyttää, että keskeiset ja tärkeät toimijat sertifioivat tietyt tieto- ja viestintätekniset tuotteet, palvelut ja prosessit asetuksen (EU) 2019/881 49 artiklan nojalla hyväksyttyjen erityisten eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien mukaisesti. Sertifioitavat tuotteet, palvelut ja prosessit voivat olla keskeisen tai tärkeän toimijan itse kehittämiä tai ulkopuoliselta taholta hankittuja.
2. Siirretään komissiolle valta antaa delegoituja säädöksiä, joissa vahvistetaan, miltä keskeisten toimijoiden luokilta edellytetään 1 kohdan nojalla sertifiointia ja minkä eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän mukaisesti. Delegoidut säädökset hyväksytään 36 artiklan mukaisesti.
3. Komissio voi pyytää ENISAa valmistelemaan asetuksen (EU) 2019/881 48 artiklan 2 kohdan mukaisen ehdokasjärjestelmän tapauksissa, joissa asianmukaista eurooppalaista kyberturvallisuuden sertifiointijärjestelmää 2 kohdan soveltamiseksi ei ole käytettävissä.

22 artikla
Standardointi

1. Jäsenvaltioiden on 18 artiklan 1 ja 2 kohdan johdonmukaisen täytäntöönpanon edistämiseksi kannustettava käyttämään verkko- ja tietojärjestelmien turvallisuuden kannalta merkityksellisiä eurooppalaisia tai kansainvälisesti hyväksyttyjä standardeja ja eritelmiä ilman, että ne määräävät käyttämään jotain tiettyä teknologiaa tai harjoittavat syrjintää jonkin tietyn teknologian käytön suosimiseksi.
2. ENISA antaa yhteistyössä jäsenvaltioiden kanssa neuvoja ja suuntaviivoja teknisistä aloista, joita on tarkasteltava 1 kohdan soveltamiseksi, sekä jo olemassa olevista standardeista, mukaan lukien jäsenvaltioiden kansalliset standardit, millä varmistetaan se, että nämä alat kuuluvat tarkastelun piiriin.

23 artikla

Verkkotunnusten ja rekisteröintitietojen tietokannat

1. DNS-nimipalvelinjärjestelmän turvallisuuden, vakauden ja häiriönsietokyvyn edistämiseksi jäsenvaltioiden on varmistettava, että TLD-rekisterit ja niiden alaisten verkkotunnusten rekisteröintipalveluja tarjoavat toimijat keräävät ja ylläpitävät tarkkoja ja täydellisiä verkkotunnusten rekisteröintitietoja erityisessä tietokantajärjestelmässä noudattaen asianmukaista huolellisuutta, johon sovelletaan henkilötietoja koskevaa unionin tietosuojalainsäädäntöä.

2. Jäsenvaltioiden on varmistettava, että 1 kohdassa tarkoitetut verkkotunnusten rekisteröintitietojen tietokannat sisältävät asiaankuuluvat tiedot verkkotunnusten haltijoiden ja TLD-aluetunnusten alaisia verkkotunnuksia hallinnoivien yhteyspisteiden tunnistamiseksi ja niihin yhteyden saamiseksi.

3. Jäsenvaltioiden on varmistettava, että TLD-rekistereillä ja niiden alaisten verkkotunnusten rekisteröintipalveluja tarjoavilla toimijoilla on käytössä toimintaperiaatteet ja menettelyt, joilla varmistetaan, että tietokannat sisältävät tarkat ja täydelliset tiedot. Jäsenvaltioiden on varmistettava, että tiedot näistä toimintaperiaatteista ja menettelyistä asetetaan julkisesti saataville.

4. Jäsenvaltioiden on varmistettava, että TLD-rekisterit ja niiden alaisten verkkotunnusten rekisteröintipalveluja tarjoavat toimijat julkaisevat ilman aiheetonta viivytystä verkkotunnuksen rekisteröinnin jälkeen verkkotunnuksen rekisteröintitiedot henkilötietoja lukuun ottamatta.

5. Jäsenvaltioiden on varmistettava, että TLD-rekisterit ja niiden alaisten verkkotunnusten rekisteröintipalveluja tarjoavat toimijat antavat pääsyn tiettyihin verkkotunnusten rekisteröintitietoihin laillisten ja asianmukaisesti perusteltujen pyyntöjen perusteella unionin tietosuojalainsäädännön mukaisesti. Jäsenvaltioiden on varmistettava, että TLD-rekisterit ja niiden alaisten verkkotunnusten rekisteröintipalveluja tarjoavat toimijat vastaavat ilman aiheetonta viivytystä kaikkiin pyyntöihin, jotka koskevat tietoihin pääsyä. Jäsenvaltioiden on varmistettava, että tiedot tällaisten tietojen antamista koskevista toimintaperiaatteista ja menettelyistä asetetaan julkisesti saataville.

II jakso

Lainkäyttövalta ja rekisteröinti

24 artikla

Lainkäyttövalta ja alueperiaate

1. Liitteessä I olevassa 8 kohdassa tarkoitettujen DNS-palveluntarjoajien, TLD-rekisterien, pilvipalvelujen tarjoajien, datakeskuspalvelujen tarjoajien ja sisällönjakeluverkkojen tarjoajien sekä liitteessä II olevassa 6 kohdassa tarkoitettujen digitaalisen palvelun tarjoajien katsotaan kuuluvan sen jäsenvaltion lainkäyttövaltaan, jossa niiden päätoimipaikka on unionissa.

2. Tätä direktiiviä sovellettaessa 1 kohdassa tarkoitettujen toimijoiden päätoimipaikan katsotaan olevan unionissa siinä jäsenvaltiossa, jossa kyberturvallisuusriskien hallintatoimenpiteisiin liittyvät päätökset tehdään. Jos tällaisia päätöksiä ei tehdä missään unionissa sijaitsevassa toimipaikassa, päätoimipaikan katsotaan olevan siinä jäsenvaltiossa, jossa toimijalla on eniten työntekijöitä unionissa.

3. Jos 1 kohdassa tarkoitettu toimija ei ole sijoittautunut unioniin mutta tarjoaa palveluja unionissa, sen on nimettävä edustaja unioniin. Edustajan on oltava sijoittautunut johonkin niistä jäsenvaltioista, joissa palveluja tarjotaan. Tällaisen toimijan katsotaan kuuluvan sen jäsenvaltion lainkäyttövallan piiriin, johon edustaja on sijoittautunut. Jos toimijalla ei ole unionissa tämän artiklan mukaista nimettyä edustajaa, mikä tahansa jäsenvaltio, jossa toimija tarjoaa palveluja, voi ryhtyä oikeustoimiin toimijaa vastaan tämän direktiivin mukaisten velvoitteiden noudattamatta jättämisen vuoksi.

4. Se, että 1 kohdassa tarkoitettu toimija on nimennyt edustajan, ei rajoita oikeustoimia, joita voidaan panna vireille toimijaa itseään vastaan.

25 artikla

Keskeisten ja tärkeiden toimijoiden rekisteri

1. ENISA perustaa 24 artiklan 1 kohdassa tarkoitettujen keskeisten ja tärkeiden toimijoiden rekisterin ja ylläpitää sitä. Toimijoiden on toimitettava ENISAlle seuraavat tiedot viimeistään [12 kuukauden kuluttua direktiivin voimaantulosta]:

   a) toimijan nimi;

   b) päätoimipaikan ja muiden unionissa sijaitsevien laillisten toimipaikkojen osoite tai, jos toimija ei ole sijoittautunut unioniin, sen 24 artiklan 3 kohdan mukaisen nimetyn edustajan osoite;

   c) ajantasaiset yhteystiedot, mukaan lukien sähköpostiosoitteet ja puhelinnumerot.

2. Edellä 1 kohdassa tarkoitettujen toimijoiden on ilmoitettava ENISAlle kaikista muutoksista 1 kohdan mukaisesti toimittamiinsa tietoihin viipymättä ja joka tapauksessa kolmen kuukauden kuluessa päivästä, jona muutos tuli voimaan.

3. Saatuaan 1 kohdassa tarkoitetut tiedot ENISA toimittaa ne keskitetyille yhteyspisteille riippuen kunkin toimijan päätoimipaikan tai, jos se ei ole sijoittautunut unioniin, nimetyn edustajan ilmoitetusta sijainnista. Jos 1 kohdassa tarkoitetulla toimijalla on päätoimipaikkansa lisäksi unionissa muita toimipaikkoja muissa jäsenvaltioissa, ENISA ilmoittaa asiasta myös näiden jäsenvaltioiden yhteyspisteille.

4. Jos toimija ei rekisteröi toimintaansa tai toimita asiaankuuluvia tietoja 1 kohdassa säädetyssä määräajassa, millä tahansa jäsenvaltiolla, jossa toimija tarjoaa palveluja, on toimivalta varmistaa, että toimija ryhtyy noudattamaan tässä direktiivissä säädettyjä velvoitteita.

V LUKU

Tietojenvaihto

26 artikla

Kyberturvallisuustietojen jakamista koskevat järjestelyt

1. Jäljempänä sanotun rajoittamatta asetuksen (EU) 2016/679 soveltamista jäsenvaltioiden on varmistettava, että keskeiset ja tärkeät toimijat voivat vaihtaa keskenään asiaankuuluvia kyberturvallisuustietoja, mukaan lukien tietoja kyberuhkista, haavoittuvuuksista, vaarantumista kuvaavista IoC-indikaattoreista, taktiikasta, tekniikoista ja menettelyistä, kyberturvallisuushälytyksistä ja konfigurointivälineistä, jos tällainen tiedonvaihto

   a) tähtää poikkeamien ehkäisyyn tai havaitsemiseen, niihin vastaamiseen tai niiden vaikutusten lieventämiseen;

b) parantaa kyberturvallisuuden tasoa erityisesti lisäämällä tietoisuutta kyberuhkista, rajoittamalla tai estämällä tällaisten uhkien leviämiskykyä tai tukemalla erilaisia puolustusvalmiuksia, haavoittuvuuden korjaamista ja ilmaisemista, uhkien havaitsemistekniikoita, lieventämisstrategioita tai reagointi- ja palautumisvaiheita.

2. Jäsenvaltioiden on varmistettava, että tietojenvaihto tapahtuu keskeisten ja tärkeiden toimijoiden luotetuissa yhteisöissä. Tällainen tietojenvaihto on toteutettava tietojenvaihtojärjestelyillä, joissa otetaan huomioon jaettujen tietojen mahdollinen arkaluonteisuus, ja 1 kohdassa tarkoitettuja unionin oikeuden sääntöjä noudattaen.

3. Jäsenvaltioiden on vahvistettava säännöt, joissa täsmennetään 2 kohdassa tarkoitettujen tietojenvaihtojärjestelyjen menettelytavat, operatiiviset osat (mukaan lukien tiettyjen tieto- ja viestintäteknisten alustojen käyttö), sisältö ja edellytykset. Säännöissä on myös vahvistettava yksityiskohtaiset tiedot viranomaisten osallistumisesta tällaisiin järjestelyihin sekä operatiiviset osat, mukaan lukien erityisten tietoteknisten alustojen käyttö. Jäsenvaltioiden on tarjottava tukea tällaisten järjestelyjen käyttöön 5 artiklan 2 kohdan g alakohdassa tarkoitettujen toimintaperiaatteidensa mukaisesti.

4. Keskeisten ja tärkeiden toimijoiden on ilmoitettava toimivaltaisille viranomaisille osallistumisestaan 2 kohdassa tarkoitettuihin tietojenvaihtojärjestelyihin, kun ne liittyvät tällaisiin järjestelyihin, tai tapauksen mukaan vetäytymisestään tällaisista järjestelyistä, kun vetäytyminen tulee voimaan.

5. ENISA tukee unionin oikeuden mukaisesti kyberturvallisuustietojen jakamista koskevien 2 kohdassa tarkoitettujen järjestelyjen toteuttamista tarjoamalla tietoa parhaista käytännöistä sekä ohjeistusta.

27 artikla

Asiaankuuluvien tietojen vapaaehtoinen ilmoittaminen

Jäsenvaltioiden on varmistettava, että tämän direktiivin soveltamisalan ulkopuolelle jäävät toimijat voivat vapaaehtoisesti ilmoittaa merkittävistä poikkeamista, kyberuhista tai läheltä piti -tilanteista, sanotun kuitenkaan rajoittamatta 3 artiklan soveltamista. Kun jäsenvaltiot käsittelevät ilmoituksia, niiden on noudatettava 20 artiklassa säädettyä menettelyä. Jäsenvaltiot voivat antaa etusijan pakollisten ilmoitusten käsittelylle vapaaehtoisten ilmoitusten käsittelyyn nähden. Vapaaehtoinen raportointi ei saa johtaa sellaisten velvollisuuksien asettamiseen raportoivalle toimijalle, joita siihen ei olisi sovellettu, jos se ei olisi antanut kyseistä ilmoitusta.

VI LUKU

Valvonta ja täytäntöönpano

28 artikla

Valvontaa ja täytäntöönpanoa koskevat yleiset näkökohdat

1. Jäsenvaltioiden on varmistettava, että toimivaltaiset viranomaiset valvovat tosiasiallisesti tämän direktiivin ja erityisesti sen 18 ja 20 artiklassa säädettyjen

velvoitteiden noudattamista ja toteuttavat tarvittavat toimenpiteet sen varmistamiseksi.

2. Toimivaltaisten viranomaisten on toimittava tiiviisti yhteistyössä tietosuojaviranomaisten kanssa käsitellessään henkilötietojen tietoturvaloukkauksiin johtaneita poikkeamia.

29 artikla

Valvonta ja täytäntöönpano keskeisten toimijoiden osalta

1. Jäsenvaltioiden on varmistettava, että tässä direktiivissä säädettyjen velvoitteiden noudattamisen valvontaa tai täytäntöönpanoa koskevat toimenpiteet, jotka koskevat keskeisiä toimijoita, ovat vaikuttavia, oikeasuhteisia ja varoittavia ottaen huomioon kunkin yksittäisen tapauksen olosuhteet.

2. Jäsenvaltioiden on varmistettava, että hoitaessaan keskeisiä toimijoita koskevia valvontatehtäviään toimivaltaisilla viranomaisilla on valtuudet seuraaviin:

   a) paikan päällä tehtävät tarkastukset ja toimipaikkojen ulkopuolinen valvonta, mukaan lukien satunnaistarkastukset;

   b) säännölliset auditoinnit;

   c) riskinarviointeihin tai käytettävissä oleviin riskitietoihin perustuvat kohdennetut turvallisuusauditoinnit;

   d) objektiivisiin, syrjimättömiin, oikeudenmukaisiin ja läpinäkyviin riskinarviointikriteereihin perustuvat turvallisuuskartoitukset;

   e) tietopyynnöt, jotka ovat tarpeen toimijan hyväksymien kyberturvallisuustoimenpiteiden arvioimiseksi, mukaan lukien dokumentoidut kyberturvaperiaatteet, sekä 25 artiklan 1 ja 2 kohdan mukaisen ENISAlle ilmoittamista koskevan velvoitteen noudattamisen arvioimiseksi;

   f) pyynnöt saada tutustua kaikkeen dataan ja kaikkiin asiakirjoihin tai muihin tietoihin, joita ne tarvitsevat valvontatehtäviensä suorittamiseksi;

   g) pyynnöt saada näyttöä kyberturvallisuusperiaatteiden täytäntöönpanosta, kuten pätevän tarkastajan tekemien turvallisuusauditointien tulokset ja niiden perustana oleva näyttö.

3. Käyttäessään 2 kohdan e–g alakohdan mukaisia valtuuksiaan toimivaltaisten viranomaisten on ilmoitettava pyynnön tarkoitus ja täsmennettävä pyydetyt tiedot.

4. Jäsenvaltioiden on varmistettava, että käyttäessään täytäntöönpanovaltuuksiaan keskeisten toimijoiden osalta toimivaltaisilla viranomaisilla on valtuudet

   a) varoittaa toimijoita siitä, että ne eivät ole noudattaneet tässä direktiivissä säädettyjä velvoitteita;

   b) antaa sitovia määräyksiä, joissa kyseisiä toimijoita vaaditaan korjaamaan havaitut puutteet tai saattamaan toimintansa tässä direktiivissä säädettyjen velvoitteiden mukaiseksi;

   c) määrätä kyseiset toimijat lopettamaan toiminta, joka ei ole tässä direktiivissä säädettyjen velvoitteiden mukaista, ja pidättäytymään toistamasta tätä toimintaa;

d) määrätä kyseiset toimijat saattamaan riskinhallintatoimenpiteensä ja/tai raportointivelvoitteensa 18 ja 20 artiklassa säädettyjen velvoitteiden mukaisiksi määrätyllä tavalla ja määrätyn ajan kuluessa;

e) määrätä kyseiset toimijat ilmoittamaan niiden palveluja tai toimintoja hyödyntäville luonnollisille tai oikeushenkilöille, joihin merkittävä kyberuhka saattaa vaikuttaa, mahdollisista suoja- tai korjaavista toimenpiteistä, joita kyseiset luonnolliset tai oikeushenkilöt voivat toteuttaa uhan johdosta;

f) määrätä kyseiset toimijat panemaan täytäntöön turvallisuusauditoinnin tuloksena annetut suositukset kohtuullisessa määräajassa;

g) nimetä valvova virkamies, joka tarkoin määriteltyjen tehtävien puitteissa määrätyn ajan valvoo, että kyseiset toimijat noudattavat 18 ja 20 artiklassa säädettyjä velvollisuuksiaan;

h) määrätä kyseiset toimijat julkistamaan tietyllä tavalla seikkoja, jotka liittyvät tässä direktiivissä säädettyjen velvoitteiden noudattamatta jättämiseen;

i) antaa julkisia lausuntoja, joissa yksilöidään yksi tai useampi oikeushenkilö ja luonnollinen henkilö, joka on vastuussa tässä direktiivissä säädetyn velvoitteen rikkomisesta, sekä rikkomisen luonne;

j) määrätä tai pyytää asiaankuuluvia elimiä tai tuomioistuimia määräämään kansallisen lainsäädännön mukaisesti hallinnollisia sakkoja 31 artiklan nojalla tämän kohdan a–i alakohdassa tarkoitettujen toimenpiteiden lisäksi tai niiden sijasta kunkin yksittäisen tapauksen olosuhteista riippuen.

5. Jos 4 kohdan a–d ja f alakohdan mukaiset täytäntöönpanotoimet eivät tuota tulosta, jäsenvaltioiden on varmistettava, että toimivaltaisilla viranomaisilla on valtuudet asettaa määräaika, jonka kuluessa keskeistä toimijaa kehotetaan toteuttamaan tarvittavat toimet puutteiden korjaamiseksi tai kyseisten viranomaisten vaatimusten noudattamiseksi. Jos pyydettyjä toimia ei toteuteta asetetussa määräajassa, jäsenvaltioiden on varmistettava, että toimivaltaisilla viranomaisilla on valtuudet

a) keskeyttää tai pyytää sertifiointi- tai lupaelintä keskeyttämään kokonaan tai osittain keskeisen toimijan tarjoamia palveluja tai toimintoja koskevan sertifioinnin tai luvan;

b) määrätä tai pyytää asiaankuuluvia elimiä tai tuomioistuimia määräämään kansallisen lainsäädännön mukaisesti väliaikainen kielto, jolla kielletään ketä tahansa toimitusjohtajan tai laillisen edustajan tasolla kyseisen keskeisen toimijan johtotehtävissä toimivaa henkilöä ja ketä tahansa muuta rikkomisesta vastuussa olevana pidettyä luonnollista henkilöä hoitamasta kyseisen toimijan johtotehtäviä.

Näitä seuraamuksia on sovellettava ainoastaan siihen asti, kunnes toimija toteuttaa tarvittavat toimet seuraamusten syynä olleiden puutteiden korjaamiseksi tai toimivaltaisen viranomaisen vaatimusten noudattamiseksi.

6. Jäsenvaltioiden on varmistettava, että jokaisella luonnollisella henkilöllä, joka on vastuussa keskeisestä toimijasta tai toimii sen edustajana sillä perusteella, että hänellä on valtuudet edustaa sitä, valtuudet tehdä päätöksiä sen puolesta tai valtuudet valvoa sitä, on valta varmistaa, että toimija noudattaa tässä direktiivissä säädettyjä velvoitteita. Jäsenvaltioiden on varmistettava, että nämä luonnolliset henkilöt voidaan saattaa vastuuseen, jos he ovat laiminlyöneet velvollisuutensa varmistaa, että toimija noudattaa tässä direktiivissä säädettyjä velvoitteita.

7. Toteuttaessaan täytäntöönpanotoimia tai soveltaessaan seuraamuksia 4 ja 5 kohdan nojalla toimivaltaisten viranomaisten on kunnioitettava puolustautumisoikeuksia ja otettava huomioon kunkin yksittäisen tapauksen olosuhteet sekä vähintään seuraavat seikat:

   a) rikkomisen vakavuus ja rikottujen säännösten merkitys. Vakavina pidettäviä rikkomisia ovat muun muassa seuraavat: toistuvat väärinkäytökset, sellaisten poikkeamien ilmoittamatta tai korjaamatta jättäminen, joilla on merkittävä haitallinen vaikutus, toimivaltaisten viranomaisten sitovien ohjeiden mukaisten korjaavien toimenpiteiden laiminlyönti ja toimivaltaisen viranomaisen rikkomisen johdosta määräämien auditointien tai seurantatoimien estäminen sekä 18 ja 20 artiklassa säädettyihin riskinhallintavaatimuksiin tai raportointivelvoitteisiin liittyvien väärien tai erittäin virheellisten tietojen antaminen.

   b) rikkomisen kesto, mukaan lukien toistuvuus;

   c) tosiasiallisesti aiheutuneet vahingot tai menetykset tai mahdolliset vahingot tai menetykset, jotka olisi voitu aiheuttaa, jos ne ovat määritettävissä. Tätä näkökohtaa arvioitaessa on otettava huomioon muun muassa todelliset tai mahdolliset rahoitukseen liittyvät ja taloudelliset tappiot, vaikutukset muihin palveluihin sekä niiden käyttäjien määrä, joihin vaikutukset kohdistuvat tai voivat kohdistua;

   d) rikkomisen tahallisuus tai tuottamuksellisuus;

   e) toimenpiteet, jotka toimija on toteuttanut vahingon ja/tai menetysten ehkäisemiseksi tai lieventämiseksi;

   f) hyväksyttyjen käytännesääntöjen tai hyväksyttyjen sertifiointimekanismien noudattaminen;

   g) vastuussa olevana pidetyn yhden tai useamman luonnollisen henkilön tai oikeushenkilön yhteistyön taso toimivaltaisten viranomaisten kanssa.

8. Toimivaltaisten viranomaisten on esitettävä täytäntöönpanopäätöstensä yksityiskohtaiset perustelut. Ennen tällaisten päätösten tekemistä toimivaltaisten viranomaisten on ilmoitettava asianomaisille toimijoille alustavista havainnoistaan ja annettava toimijoille kohtuullinen aika huomautusten esittämiseen.

9. Jäsenvaltioiden on varmistettava, että niiden toimivaltaiset viranomaiset ilmoittavat direktiivin (EU) XXXX/XXXX [kriittisten toimijoiden häiriönsietokykyä koskeva direktiivi] mukaisesti nimetyille kyseisen jäsenvaltion toimivaltaisille viranomaisille, kun ne käyttävät valvonta- ja täytäntöönpanovaltuuksiaan, joiden tarkoituksena on varmistaa, että direktiivin (EU) XXXX/XXXX [kriittisten toimijoiden häiriönsietokykyä koskeva direktiivi] mukaisesti kriittiseksi tai kriittistä toimijaa vastaavaksi todettu keskeinen toimija täyttää tämän direktiivin mukaiset velvoitteet. Toimivaltaiset viranomaiset voivat direktiivin (EU) XXXX/XXXX [kriittisten toimijoiden häiriönsietokykyä koskeva direktiivi] mukaisten toimivaltaisten viranomaisten pyynnöstä käyttää valvonta- ja täytäntöönpanovaltuuksiaan suhteessa kriittiseksi tai vastaavaksi todettuun keskeiseen toimijaan.

30 artikla

Valvonta ja täytäntöönpano tärkeiden toimijoiden osalta

1. Jos jäsenvaltiot saavat näyttöä tai viitteitä siitä, että tärkeä toimija ei noudata tässä direktiivissä ja erityisesti sen 18 ja 20 artiklassa säädettyjä velvoitteita, niiden on varmistettava, että toimivaltaiset viranomaiset puuttuvat tilanteeseen tarpeen mukaan jälkikäteisvalvonnallisin toimin.

2. Jäsenvaltioiden on varmistettava, että hoitaessaan tärkeitä toimijoita koskevia valvontatehtäviään toimivaltaisilla viranomaisilla on valtuudet seuraaviin:

   a) paikan päällä tehtävät tarkastukset ja toimipaikkojen ulkopuolinen jälkikäteisvalvonta;

   b) riskinarviointeihin tai käytettävissä oleviin riskitietoihin perustuvat kohdennetut turvallisuusauditoinnit;

   c) objektiivisiin, oikeudenmukaisiin ja läpinäkyviin riskinarviointikriteereihin perustuvat turvallisuuskartoitukset;

   d) tietopyynnöt, jotka ovat tarpeen kyberturvallisuustoimenpiteiden, mukaan lukien dokumentoidut kyberturvaperiaatteet, jälkikäteiseksi arvioimiseksi sekä 25 artiklan 1 ja 2 kohdan mukaisen ENISAlle ilmoittamista koskevan velvoitteen noudattamisen arvioimiseksi;

   e) pyynnöt saada tutustua kaikkeen dataan ja kaikkiin asiakirjoihin ja/tai muihin tietoihin, joita ne tarvitsevat valvontatehtävien suorittamiseksi.

3. Käyttäessään 2 kohdan d tai e alakohdan mukaisia valtuuksiaan toimivaltaisten viranomaisten on ilmoitettava pyynnön tarkoitus ja täsmennettävä pyydetyt tiedot.

4. Jäsenvaltioiden on varmistettava, että käyttäessään täytäntöönpanovaltuuksiaan tärkeiden toimijoiden osalta toimivaltaisilla viranomaisilla on valtuudet

   a) varoittaa toimijoita siitä, että ne eivät ole noudattaneet tässä direktiivissä säädettyjä velvoitteita;

   b) antaa sitovia määräyksiä, joissa kyseisiä toimijoita vaaditaan korjaamaan havaitut puutteet tai saattamaan toimintansa tässä direktiivissä säädettyjen velvoitteiden mukaiseksi;

   c) määrätä kyseiset toimijat lopettamaan toiminta, joka ei ole tässä direktiivissä säädettyjen velvoitteiden mukaista, ja pidättäytymään toistamasta tätä toimintaa;

   d) määrätä kyseiset toimijat saattamaan riskinhallintatoimenpiteensä ja/tai raportointivelvoitteensa 18 ja 20 artiklassa säädettyjen velvoitteiden mukaisiksi määrätyllä tavalla ja määrätyn ajan kuluessa;

   e) määrätä kyseiset toimijat ilmoittamaan niiden palveluja tai toimintoja hyödyntäville luonnollisille tai oikeushenkilöille, joihin merkittävä kyberuhka saattaa vaikuttaa, mahdollisista suoja- tai korjaavista toimenpiteistä, joita kyseiset luonnolliset tai oikeushenkilöt voivat toteuttaa uhan johdosta;

   f) määrätä kyseiset toimijat panemaan täytäntöön turvallisuusauditoinnin tuloksena annetut suositukset kohtuullisessa määräajassa;

   g) määrätä kyseiset toimijat julkistamaan tietyllä tavalla seikkoja, jotka liittyvät tässä direktiivissä säädettyjen velvoitteiden noudattamatta jättämiseen;

h) antaa julkisia lausuntoja, joissa yksilöidään yksi tai useampi oikeushenkilö ja luonnollinen henkilö, joka on vastuussa tässä direktiivissä säädetyn velvoitteen rikkomisesta, sekä rikkomisen luonne;

i) määrätä tai pyytää asiaankuuluvia elimiä tai tuomioistuimia määräämään kansallisen lainsäädännön mukaisesti hallinnollisia sakkoja 31 artiklan nojalla tämän kohdan a–h alakohdassa tarkoitettujen toimenpiteiden lisäksi tai niiden sijasta kunkin yksittäisen tapauksen olosuhteista riippuen.

5. Tämän asetuksen 29 artiklan 6–8 kohtaa sovelletaan myös tässä artiklassa liitteessä II lueteltujen tärkeiden toimijoiden osalta säädettyihin valvonta- ja täytäntöönpanotoimenpiteisiin.

31 artikla

Yleiset edellytykset hallinnollisten sakkojen määräämiselle keskeisille ja tärkeille toimijoille

1. Jäsenvaltioiden on varmistettava, että tämän artiklan nojalla keskeisille ja tärkeille toimijoille tässä direktiivissä säädettyjen velvoitteiden rikkomisesta määrätyt hallinnolliset sakot ovat kussakin yksittäistapauksessa vaikuttavia, oikeasuhteisia ja varoittavia.

2. Hallinnolliset sakot määrätään kunkin yksittäisen tapauksen olosuhteiden mukaisesti 29 artiklan 4 kohdan a–i alakohdassa, 29 artiklan 5 kohdassa ja 30 artiklan 4 kohdan a–h alakohdassa tarkoitettujen toimenpiteiden lisäksi tai niiden sijasta.

3. Päätettäessä hallinnollisen sakon määräämisestä ja sen suuruudesta kussakin yksittäistapauksessa on otettava asianmukaisesti huomioon vähintään 29 artiklan 7 kohdassa säädetyt seikat.

4. Jäsenvaltioiden on varmistettava, että 18 artiklassa tai 20 artiklassa säädettyjen velvoitteiden rikkomisesta määrätään tämän artiklan 2 ja 3 kohdan mukaisesti hallinnollinen sakko, joka voi olla enimmillään vähintään 10 000 000 euroa tai enimmillään 2 % yrityksen, johon keskeinen tai tärkeä toimija kuuluu, edellisen tilikauden maailmanlaajuisesta vuotuisesta kokonaisliikevaihdosta sen mukaan, kumpi näistä määristä on suurempi.

5. Jäsenvaltiot voivat säätää valtuudesta määrätä uhkasakkoja saadakseen keskeisen tai tärkeän toimijan lopettamaan rikkomisen toimivaltaisen viranomaisen etukäteen tekemän päätöksen mukaisesti.

6. Kukin jäsenvaltio voi vahvistaa säännöt siitä, voidaanko 4 artiklan 23 kohdassa tarkoitetuille julkishallinnon toimijoille, joihin sovelletaan tässä direktiivissä säädettyjä velvoitteita, määrätä hallinnollisia sakkoja ja missä määrin, sanotun kuitenkaan rajoittamatta toimivaltaisten viranomaisten 29 ja 30 artiklan mukaisia valtuuksia.

32 artikla

Henkilötietojen tietoturvaloukkaukseen johtavat rikkomiset

1. Jos toimivaltaisilla viranomaisilla on viitteitä siitä, että keskeisen tai tärkeän toimijan 18 ja 20 artiklassa säädettyjen velvollisuuksien laiminlyönti aiheuttaa asetuksen (EU)

2016/679 4 artiklan 12 kohdassa määritellyn henkilötietojen tietoturvaloukkauksen, josta on ilmoitettava mainitun asetuksen 33 artiklan mukaisesti, niiden on ilmoitettava asiasta kyseisen asetuksen 55 ja 56 artiklan nojalla toimivaltaisille valvontaviranomaisille kohtuullisen ajan kuluessa.

2. Jos asetuksen (EU) 2016/679 55 ja 56 artiklan mukaisesti toimivaltaiset valvontaviranomaiset päättävät käyttää kyseisen asetuksen 58 artiklan i kohdan mukaisia valtuuksiaan ja määrätä hallinnollisen sakon, toimivaltaiset viranomaiset eivät saa määrätä hallinnollista sakkoa samasta rikkomisesta tämän direktiivin 31 artiklan nojalla. Toimivaltaiset viranomaiset voivat kuitenkin soveltaa täytäntöönpanotoimia tai käyttää seuraamusvaltuuksiaan tämän direktiivin 29 artiklan 4 kohdan a–i alakohdan, 29 artiklan 5 kohdan ja 30 artiklan 4 kohdan a–h alakohdan mukaisesti.

3. Jos asetuksen (EU) 2016/679 nojalla toimivaltainen valvontaviranomainen on sijoittautunut toiseen jäsenvaltioon kuin toimivaltainen viranomainen, toimivaltainen viranomainen voi ilmoittaa asiasta samaan jäsenvaltioon sijoittautuneelle valvontaviranomaiselle.

33 artikla

Seuraamukset

1. Jäsenvaltioiden on säädettävä tämän direktiivin nojalla annettujen kansallisten säännösten rikkomiseen sovellettavista seuraamuksista ja toteutettava kaikki tarvittavat toimenpiteet sen varmistamiseksi, että ne pannaan täytäntöön. Seuraamusten on oltava tehokkaita, oikeasuhteisia ja varoittavia.

2. Jäsenvaltioiden on annettava komissiolle tiedoksi nämä säännökset ja toimenpiteet viimeistään [kahden] vuoden kuluttua tämän direktiivin voimaantulosta ja ilmoitettava sille ilman aiheetonta viivytystä niihin vaikuttavista myöhemmistä muutoksista.

34 artikla

Keskinäinen avunanto

1. Jos keskeinen tai tärkeä toimija tarjoaa palveluja useammassa kuin yhdessä jäsenvaltiossa tai sen pääasiallinen toimipaikka tai edustaja sijaitsee tietyssä jäsenvaltiossa mutta sen verkko- ja tietojärjestelmät sijaitsevat yhdessä tai useammassa muussa jäsenvaltiossa, pääasiallisen toimipaikan, muun toimipaikan tai edustajan jäsenvaltion toimivaltaisen viranomaisen ja näiden muiden jäsenvaltioiden toimivaltaisten viranomaisten on tehtävä yhteistyötä ja avustettava toisiaan tarpeen mukaan. Tähän yhteistyöhön kuuluu vähintään, että

   a) valvonta- tai täytäntöönpanotoimenpiteitä jäsenvaltiossa soveltavat toimivaltaiset viranomaiset informoivat ja kuulevat toteutetuista 29 ja 30 artiklan mukaisista valvonta- ja täytäntöönpanotoimenpiteistä keskitetyn yhteyspisteen kautta muiden asianomaisten jäsenvaltioiden toimivaltaisia viranomaisia;

b) toimivaltainen viranomainen voi pyytää toista toimivaltaista viranomaista toteuttamaan 29 ja 30 artiklassa tarkoitettuja valvonta- tai täytäntöönpanotoimenpiteitä;

c) toimivaltaisen viranomaisen on toisen toimivaltaisen viranomaisen perustellun pyynnön saatuaan annettava toiselle toimivaltaiselle viranomaiselle apua, jotta 29 ja 30 artiklassa tarkoitetut valvonta- tai täytäntöönpanotoimet voidaan toteuttaa tuloksellisesti, tehokkaasti ja johdonmukaisesti. Tällainen keskinäinen avunanto voi sisältää tietopyyntöjä ja valvontatoimenpiteitä, mukaan lukien pyynnöt, jotka koskevat paikan päällä suoritettavia tarkastuksia tai muualla suoritettavaa valvontaa tai kohdennettuja turvallisuusauditointeja. Toimivaltainen viranomainen, jolle avunantopyyntö on osoitettu, ei voi evätä kyseistä pyyntöä, paitsi jos muiden asianomaisten viranomaisten, ENISAn ja komission kanssa käydyn näkemystenvaihdon jälkeen todetaan, että joko viranomaisella ei ole toimivaltaa antaa pyydettyä apua tai että pyydetty apu ei ole oikeassa suhteessa toimivaltaisen viranomaisen 29 tai 30 artiklan mukaisesti suorittamiin valvontatehtäviin nähden.

2. Eri jäsenvaltioiden toimivaltaiset viranomaiset voivat tarvittaessa ja yhteisestä sopimuksesta toteuttaa 29 ja 30 artiklassa tarkoitettuja yhteisiä valvontatoimia.

VII LUKU

Siirtymä- ja loppusäännökset

35 artikla

Uudelleentarkastelu

Komissio tarkastelee määräajoin uudelleen tämän direktiivin toimivuutta ja laatii raportin Euroopan parlamentille ja neuvostolle. Raportissa arvioidaan erityisesti liitteissä I ja II tarkoitettujen toimijoiden toimialojen, alasektoreiden, koon ja tyypin merkitystä talouden ja yhteiskunnan toiminnalle kyberturvallisuuden näkökulmasta. Tätä tarkoitusta varten sekä strategisen ja operatiivisen yhteistyön edistämiseksi edelleen komissio ottaa huomioon yhteistyöryhmän ja CSIRT-verkoston raportit strategisella ja operatiivisella tasolla saaduista kokemuksista. Ensimmäinen raportti annetaan viimeistään... päivänä... kuuta... [54 kuukautta tämän direktiivin voimaantulosta].

36 artikla

Siirretyn säädösvallan käyttäminen

1. Komissiolle siirrettyä valtaa antaa delegoituja säädöksiä koskevat tässä artiklassa säädetyt edellytykset.

2. Siirretään komissiolle [...] lähtien viideksi vuodeksi valta antaa 18 artiklan 6 kohdassa ja 21 artiklan 2 kohdassa tarkoitettuja delegoituja säädöksiä.

3. Euroopan parlamentti tai neuvosto voi milloin tahansa peruuttaa 18 artiklan 6 kohdassa ja 21 artiklan 2 kohdassa tarkoitetun säädösvallan siirron. Peruuttamispäätöksellä lopetetaan tuossa päätöksessä mainittu säädösvallan siirto.

Peruuttaminen tulee voimaan sitä päivää seuraavana päivänä, jona sitä koskeva päätös julkaistaan *Euroopan unionin virallisessa lehdessä*, tai jonakin myöhempänä, kyseisessä päätöksessä mainittuna päivänä. Peruuttamispäätös ei vaikuta jo voimassa olevien delegoitujen säädösten pätevyyteen.

4. Ennen kuin komissio hyväksyy delegoidun säädöksen, se kuulee kunkin jäsenvaltion nimeämiä asiantuntijoita paremmasta lainsäädännöstä 13 päivänä huhtikuuta 2016 tehdyssä toimielinten välisessä sopimuksessa vahvistettujen periaatteiden mukaisesti.

5. Heti kun komissio on antanut delegoidun säädöksen, komissio antaa sen tiedoksi yhtäaikaisesti Euroopan parlamentille ja neuvostolle.

6. Edellä olevien 18 artiklan 6 kohdan tai 21 artiklan 2 kohdan nojalla annettu delegoitu säädös tulee voimaan ainoastaan, jos Euroopan parlamentti tai neuvosto ei ole kahden kuukauden kuluessa siitä, kun asianomainen säädös on annettu tiedoksi Euroopan parlamentille ja neuvostolle, ilmaissut vastustavansa sitä tai jos sekä Euroopan parlamentti että neuvosto ovat ennen mainitun määräajan päättymistä ilmoittaneet komissiolle, että ne eivät vastusta säädöstä. Euroopan parlamentin tai neuvoston aloitteesta tätä määräaikaa jatketaan kahdella kuukaudella.

37 artikla

Komiteamenettely

1. Komissiota avustaa komitea. Tämä komitea on asetuksessa (EU) N:o 182/2011 tarkoitettu komitea.

2. Kun viitataan tähän kohtaan, sovelletaan asetuksen (EU) N:o 182/2011 5 artiklaa.

3. Kun komitean lausunto on määrä hankkia kirjallista menettelyä noudattaen, tämä menettely päätetään tuloksettomana, jos komitean puheenjohtaja lausunnon antamiselle asetetussa määräajassa niin päättää tai komitean jäsen sitä pyytää.

38 artikla

Saattaminen osaksi kansallista lainsäädäntöä

1. Jäsenvaltioiden on hyväksyttävä ja julkaistava tämän direktiivin noudattamisen edellyttämät lait, asetukset ja hallinnolliset määräykset viimeistään [18 kuukauden kuluttua tämän direktiivin voimaantulopäivästä]. Niiden on viipymättä ilmoitettava tästä komissiolle. Niiden on sovellettava näitä säädöksiä … päivästä …kuuta … [ensimmäisessä alakohdassa tarkoitettua päivää seuraavasta päivästä].

2. Näissä jäsenvaltioiden antamissa säädöksissä on viitattava tähän direktiiviin tai niihin on liitettävä tällainen viittaus, kun ne julkaistaan virallisesti. Jäsenvaltioiden on säädettävä siitä, miten viittaukset tehdään.

39 artikla

Asetuksen (EU) N:o 910/2014 muuttaminen

Poistetaan asetuksen (EU) N:o 910/2014 19 artikla.

40 artikla

Direktiivin (EU) 2018/1972 muuttaminen

Poistetaan direktiivin (EU) 2018/1972 40 ja 41 artikla.

41 artikla

Kumoaminen

Kumotaan direktiivi (EU) 2016/1148 [siitä päivästä, johon mennessä tämä direktiivi on saatettava osaksi kansallista lainsäädäntöä].

Viittauksia direktiiviin (EU) 2016/1148 pidetään viittauksina tähän direktiiviin liitteessä III olevan vastaavuustaulukon mukaisesti.

42 artikla

Voimaantulo

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

43 artikla

Osoitus

Tämä direktiivi on osoitettu kaikille jäsenvaltioille.

Tehty Brysselissä

Euroopan parlamentin puolesta	*Neuvoston puolesta*
Puhemies	*Puheenjohtaja*

SÄÄDÖSEHDOTUKSEEN LIITTYVÄ RAHOITUSSELVITYS

Sisällysluettelo

1. PERUSTIEDOT EHDOTUKSESTA/ALOITTEESTA

1.1. Ehdotuksen/aloitteen nimi

Ehdotus direktiiviksi toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi koko unionissa ja direktiivin (EU) 2016/1148 kumoamisesta

1.2. Toimintalohko(t) *(ohjelmaklusteri)*

Viestintäverkot, sisällöt ja teknologia

1.3. Ehdotus/aloite liittyy

☐ **uuteen toimeen**

☐ **uuteen toimeen, joka perustuu pilottihankkeeseen tai valmistelutoimeen**[40]

☒ **käynnissä olevan toimen jatkamiseen**

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

1.4. Ehdotuksen/aloitteen perustelut

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

Tarkistuksen tavoitteena on lisätä Euroopan unionissa toimivien yritysten laajan joukon kykyä torjua kyberuhkia kaikilla asiaankuuluvilla aloilla, vähentää häiriönsietokyvyn epäjohdonmukaisuuksia sisämarkkinoilla direktiivin jo kattamilla aloilla sekä parantaa yhteistä tilannetietoisuutta ja yhteisiä valmiuksia valmistautua ja reagoida kyberuhkiin.

1.4.2. 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.

Kyberturvallisuustoiminta unionissa ei voi olla tuloksellista, jos asiaa lähestytään hajanaisesti kansallisten tai alueellisten siilojen näkökulmasta. Verkko- ja tietoturvadirektiivillä (NIS-direktiivillä) haluttiin korjata tätä puutetta luomalla puitteet verkkojen ja tietojärjestelmien tietoturvalle kansallisella ja unionitasolla. NIS-direktiivin ensimmäisessä määräaikaistarkastelussa tuotiin kuitenkin esiin useita sisälähtöisiä puutteita, jotka ovat lopulta johtaneet huomattaviin eroihin jäsenvaltioiden välillä valmiuksien, suunnittelun ja suojelun tason osalta, mikä vaikuttaa samalla samankaltaisten yritysten tasapuolisiin toimintaedellytyksiin sisämarkkinoilla. Nykyistä NIS-direktiiviä vahvempi EU-tason sääntely on perusteltavissa erityisesti seuraavilla seikoilla: i) ongelma on luonteeltaan maiden rajat ylittävä ii) EU-tason toimilla voidaan parantaa ja helpottaa tuloksellista toimintaa kansallisella tasolla ja iii) yhtenäisellä ja yhteistyöhön perustuvalla verkko- ja tietoturvatoiminnalla voidaan tuloksellisesti tukea tietosuojaa ja yksityisyyden suojaa.

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

Ehdotuksen tavoitteet voidaan näin ollen saavuttaa paremmin EU:n tasolla kuin jäsenvaltioiden omin toimin.

1.4.3. Vastaavista toimista saadut kokemukset

NIS-direktiivi on ensimmäinen horisontaalinen sisämarkkinasäädös, jolla pyritään parantamaan unionin verkkojen ja järjestelmien kykyä sietää kyberturvariskejä. Se on jo merkittävästi nostanut kyberturvallisuuden yhteistä tasoa jäsenvaltioiden keskuudessa. Direktiivin toiminnan ja täytäntöönpanon uudelleentarkastelu on kuitenkin tuonut esiin useita puutteita. Kun lisäksi digitalisaatio on edennyt ja tarvitaan ajanmukaisempia tapoja reagoida uhkiin, puutteet olisi korjattava tarkistetulla säädöksellä.

1.4.4. Yhteensopivuus muiden kyseeseen tulevien välineiden kanssa ja mahdolliset synergiaedut

Uusi ehdotus on täysin linjassa ja johdonmukainen muiden asiaan liittyvien aloitteiden kanssa, joita ovat muun muassa ehdotus asetukseksi finanssialan digitaalisesta häiriönsietokyvystä (DORA) ja ehdotus direktiiviksi keskeisten palvelujen kriittisen tärkeiden tarjoajien kyvystä suojautua ulkoisilta uhkilta. Se on johdonmukainen myös suhteessa eurooppalaiseen sähköisen viestinnän säännöstöön, yleiseen tietosuoja-asetukseen ja eIDAS-asetukseen.

Ehdotus on olennainen osa EU:n turvallisuusunionia koskevaa strategiaa.

1.5. Kesto ja rahoitusvaikutukset

☐ **kesto on rajattu**

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

– ☐ Maksusitoumusmäärärahoihin kohdistuvat rahoitusvaikutukset koskevat vuosia VVVV–VVVV ja maksumäärärahoihin kohdistuvat rahoitusvaikutukset vuosia VVVV–VVVV.

☒ **kestoa ei ole rajattu**

– Käynnistysvaihe alkaa vuonna 2022 ja päättyy vuonna 2025,

– minkä jälkeen toteutus täydessä laajuudessa.

1.6. Hallinnointitapa (Hallinnointitavat)[41]

Suora hallinnointi, jonka komissio toteuttaa käyttämällä

– ☒ yksiköitään, myös unionin ulkopuolisissa 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

– X☐ 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, huomautuksille varatussa kohdassa olisi annettava lisätietoja.*

Huomautukset

Euroopan unionin kyberturvallisuusvirasto ENISA, jolle on kyberturvallisuussäädöksellä myönnetty uusi pysyvä toimeksianto, auttaisi jäsenvaltioita ja komissiota tarkistetun NIS-direktiivin täytäntöönpanossa.

Tarkistetun NIS-direktiivin seurauksena ENISAlla on 2022–2023 alkaen uusia toiminta-aloja. Vaikka nämä toiminta-alat kuuluisivat myös ENISAn yleisiin tehtäviin sen toimeksiannon

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

mukaisesti, ne lisäävät viraston työtaakkaa. Tarkemmin sanottuna NIS-direktiivin tarkistamista koskevan komission ehdotuksen mukaan ENISAn on nykyisten toiminta-alojensa lisäksi sisällytettävä työohjelmaansa muun muassa seuraavat toimet: i) kehittää ja ylläpitää Euroopan haavoittuvuusrekisteriä (ehdotuksen 6 artiklan 2 kohta), ii) huolehtia Euroopan kyberkriisien yhteysorganisaatioiden verkoston (CyCLONe) sihteeristöstä (ehdotuksen 14 artikla) ja laatia vuosiraportti kyberturvallisuuden tilasta EU:ssa (ehdotuksen 15 artikla), iii) tukea vertaisarviointien järjestämistä jäsenvaltioiden välillä (ehdotuksen 16 artikla), iv) kerätä poikkeamia koskevia koontitietoja jäsenvaltioilta ja antaa teknisiä ohjeita (ehdotuksen 20 artiklan 9 kohta) ja luoda rekisteri rajat ylittäviä palveluja tarjoavista toimijoista ja ylläpitää sitä (ehdotuksen 25 artikla).

Näin ollen vuodesta 2022 alkaen pyydetään viittä kokoaikaista lisätyöntekijää, joiden määrärahat ovat noin 0,61 miljoonaa euroa vuodessa näiden uusien toimien kattamiseksi (ks. virastoja koskeva erillinen rahoitusselvitys).

2. HALLINNOINTI

2.1. Seuranta- ja raportointisäännöt

Ilmoitetaan sovellettavat aikavälit ja edellytykset.

Komissio tarkastelee säännöllisesti direktiivin toimivuutta ja antaa siitä raportin Euroopan parlamentille ja neuvostolle ensimmäisen kerran kolmen vuoden kuluttua direktiivin voimaantulosta. Komissio arvioi myös direktiivin täytäntöönpanotoimet jäsenvaltioissa.

2.2. Hallinnointi- ja valvontajärjestelmä(t)

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

Kyseisestä politiikan alasta vastaava viestintäverkkojen, sisältöjen ja teknologian pääosaston yksikkö hallinnoi direktiivin täytäntöönpanoa.

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

Riski on hyvin pieni, koska NIS-direktiivin ekosysteemi on jo olemassa.

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

Ei sovelleta. Käytetään ainoastaan hallintomäärärahoja (kokonaismäärärahat).

2.3. Toimenpiteet petosten ja sääntöjenvastaisuuksien ehkäisemiseksi

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

Ei sovelleta. Käytetään ainoastaan hallintomäärärahoja (kokonaismäärärahat).

3. EHDOTUKSEN/ALOITTEEN ARVIOIDUT RAHOITUSVAIKUTUKSET

3.1. Kyseeseen tuleva monivuotisen rahoituskehyksen otsake ja menopuolelle ehdotettu uusi budjettikohta (ehdotetut uudet budjettikohdat)

Monivuotisen rahoituskehyksen otsake	Budjettikohta	Menolaji	Rahoitusosuudet			
	Numero [Nimi... 7.....]	JM/EI-JM[42]	EFTA-mailta[43]	ehdokasmailta[44]	kolmansilta mailta	varainhoitoasetuksen [21 artiklan 2 kohdan b alakohdassa] tarkoitetut rahoitusosuudet
	20 02 06 hallintomenot 20 02 06	EI-JM	EI	EI	EI	EI

[42] JM = jaksotetut määrärahat / EI-JM = jaksottamattomat määrärahat.
[43] EFTA: Euroopan vapaakauppaliitto.
[44] Ehdokasmaat ja soveltuvin osin Länsi-Balkanin mahdolliset ehdokasmaat.

3.2. Arvioidut vaikutukset menoihin

3.2.1. Yhteenveto arvioiduista vaikutuksista menoihin

milj. euroa (kolmen desimaalin tarkkuudella)

Monivuotisen rahoituskehyksen otsake	**<…>**	[Otsake.....]

			2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	***Vuoden 2027 jälkeen***	**YHTEENSÄ**
Toimintamäärärahat (jaoteltuina kohdassa 3.1 lueteltujen budjettikohtien mukaan)	Sitoumukset	1)									
	Maksut	2)									
Ohjelman määrärahoista katettavat hallintomäärärahat[45]	Sitoumukset = Maksut	3)									
Ohjelman määrärahat YHTEENSÄ	Sitoumukset	=1+3									
	Maksut	=2+3									

Monivuotisen rahoituskehyksen otsake	7	”Hallintomenot” Kokoukset: NIS-yhteistyöryhmän täysistunnot pidetään yleensä 4 kertaa vuodessa. Komissio kattaa 27 jäsenvaltion edustajien ateria- ja matkakulut (yksi edustaja kustakin jäsenvaltiosta). Yhden kokouksen kustannukset voivat olla enimmillään 15 000 euroa. Virkamatkat: Virkamatkat liittyvät NIS-direktiivin täytäntöönpanon seurantaan. Esimerkki: Yhden vuoden aikana (toukokuu 2019 – heinäkuu 2020) on tarkoitus järjestää niin kutsuttuja NIS-maavierailuja kaikkiin 27 jäsenvaltioon tavoitteena

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

		keskustella NIS-direktiivin täytäntöönpanosta koko EU:ssa.

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

milj. euroa (kolmen desimaalin tarkkuudella)

		2021	2022	2023	2024	2025	2026	2027	*Vuoden 2027 jälkeen*	YHTEENSÄ
Henkilöresurssit:		1,14	1,14	1,14	1,14	1,14	1,14	**1,14**		**7,98**
Muut hallintomenot		**0,09**	**0,09**	**0,09**	**0,09**	**0,09**	**0,09**	**0,09**		**0,63**
Monivuotisen rahoituskehyksen OTSAKKEESEEN 7 kuuluvat määrärahat YHTEENSÄ	(Sitoumukset yhteensä = maksut yhteensä)	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**		**8,61**

milj. euroa (kolmen desimaalin tarkkuudella)

		2021	2022	2023	2024	2025	2026	2027	*Vuoden 2027 jälkeen*	YHTEENSÄ
Monivuotisen rahoituskehyksen **OTSAKKEISIIN kuuluvat määrärahat YHTEENSÄ**	Sitoumukset									
	Maksut									

3.2.2. Yhteenveto arvioiduista vaikutuksista hallintomäärärahoihin

– ☐ Ehdotus/aloite ei edellytä hallintomäärärahoja.

– ☐X Ehdotus/aloite edellyttää hallintomäärärahoja seuraavasti:

milj. euroa (kolmen desimaalin tarkkuudella)

Vuodet	2021	2022	2023	2024	2025	2026	2027	YHTEENSÄ
OTSAKE 7 monivuotisessa rahoituskehyksessä								
Henkilöresurssit:	1,14	1,14	1,14	1,14	1,14	1,14	**1,14**	**7,98**
Muut hallintomenot	0,09	0,09	0,09	0,09	0,09	0,09	**0,09**	**0,63**
Välisumma, OTSAKE 7 monivuotisessa rahoituskehyksessä	1,23	1,23	1,23	1,23	1,23	1,23	**1,23**	**8,61**
OTSAKKEESEEN 7 sisältymättömät[46] monivuotisessa rahoituskehyksessä								
Henkilöresurssit:								
Muut hallintomenot								
Välisumma, OTSAKEESEEN 7 sisältymättömät monivuotisessa rahoituskehyksessä								
YHTEENSÄ	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**8,61**

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.

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

3.2.2.1. Henkilöresurssien arvioitu tarve

– ☐ Ehdotus/aloite ei edellytä henkilöresursseja.

– X☐ Ehdotus/aloite edellyttää henkilöresursseja seuraavasti:

Arvio kokoaikaiseksi henkilöstöksi muutettuna

Vuodet		**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**
• Henkilöstötaulukkoon sisältyvät virat/toimet (virkamiehet ja väliaikaiset toimihenkilöt)								
Päätoimipaikka ja komission edustustot EU:ssa		6	6	6	6	6	6	6
Edustustot EU:n ulkopuolella								
Tutkimustoiminta								
• Ulkopuolinen henkilöstö (kokoaikaiseksi muutettuna): AC, AL, END, INT ja JPD [47] Otsake 7								
Monivuotisen rahoituskehyksen OTSAKKEESTA 7 rahoitettavat	- päätoimipaikassa	3	3	3	3	3	3	3
	- EU:n ulkop. edustustoissa							
Ohjelman määrärahoista rahoitettavat [48]	- päätoimipaikassa							
	- EU:n ulkop. edustustoissa							
Tutkimustoiminta								
Muu (täsmennä)								
YHTEENSÄ		**9**	**9**	**9**	**9**	**9**	**9**	**9**

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	• Delegoitujen säädösten valmistelu 18 artiklan 6 kohdan, 21 artiklan 2 kohdan ja 36 artiklan mukaisesti • Täytäntöönpanosäädösten valmistelu 12 artiklan 8 kohdan, 18 artiklan 5 kohdan ja 20 artiklan 11 kohdan mukaisesti • NIS-yhteistyöryhmän sihteeristöpalvelut • NIS-yhteistyöryhmän täysistuntojen ja työryhmäkokousten järjestäminen • Eri asiakirjoja (ohjeet, toimintamallit jne.) koskevan jäsenvaltioiden työn koordinointi • Yhteydet muihin komission yksiköihin, ENISAan ja kansallisiin viranomaisiin NIS-direktiivin täytäntöönpanemiseksi • NIS-direktiivin täytäntöönpanoon liittyvien kansallisten menetelmien ja parhaiden käytäntöjen analysointi
Ulkopuolinen henkilöstö	Tuki kaikille edellä mainituille toimille tarpeen mukaan

[47] AC = sopimussuhteiset toimihenkilöt, AL = paikalliset toimihenkilöt, END = kansalliset asiantuntijat, INT = vuokrahenkilöstö ja JPD = nuoremmat asiantuntijat EU:n ulkopuolisissa edustustoissa.

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

3.2.3. Ulkopuolisten tahojen rahoitusosuudet

Ehdotuksen/aloitteen

– X☐ rahoittamiseen ei osallistu ulkopuolisia tahoja

– ☐ rahoittamiseen osallistuu ulkopuolisia tahoja seuraavasti (arvio):

määrärahat, milj. euroa (kolmen desimaalin tarkkuudella)

Vuodet	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**YHTEENSÄ**
Rahoitukseen osallistuva taho								
Yhteisrahoituksella katettavat määrärahat YHTEENSÄ								

3.3. Arvioidut vaikutukset tuloihin

– ☐X 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:	Ehdotuksen/aloitteen vaikutus[49]						
	2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**
Momentti ….							

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

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

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

SÄÄDÖKSEEN LIITTYVÄN RAHOITUSSELVITYKSEN LIITE

Ehdotuksen/aloitteen nimi:

Ehdotus direktiiviksi toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa 6 päivänä heinäkuuta 2016 annetun Euroopan parlamentin ja neuvoston direktiivin (EU) 2016/1148 tarkistamisesta

……
……

1. TARVITTAVIEN HENKILÖRESURSSIEN MÄÄRÄ JA KUSTANNUKSET

2. MUIDEN HALLINTOMENOJEN KUSTANNUKSET

3. LASKENTAMENETELMÄT KUSTANNUSTEN ARVIOIMISEKSI

3.1 Henkilöresurssit:

3.2 Muut hallintomenot

*Tämä liite, jonka **kukin ehdotukseen/aloitteeseen osallistuva pääosasto/yksikkö täyttää**, on liitettävä säädökseen liittyvään rahoitusselvitykseen komission yksiköiden lausuntokierroksen alkaessa.*

Tietotaulukoita käytetään säädökseen liittyvän rahoitusselvityksen taulukoiden lähteinä. Ne on tarkoitettu vain komission sisäiseen käyttöön.

1. Tarvittavien henkilöresurssien kustannukset

☐ Ehdotus/aloite ei edellytä henkilöresursseja.

X☐ Ehdotus/aloite edellyttää henkilöresursseja seuraavasti:

milj. euroa (kolmen desimaalin tarkkuudella)

SAKE 7 vuotisessa skehyksessä		2021		2022		2023		2024		2025		2026		2027		YH
		Kokoaikaiseksi muutettuna	Määrärahat	Kokoaikaiseksi muutettuna	Määrärahat	Kokoaikaiseksi muutettuna	Määrärahat	Kokoaikaiseksi muutettuna	Määrärahat	Kokoaikaiseksi muutettuna	Määrärahat	Kokoaikaiseksi muutettuna	Määrärahat	Kokoaikaiseksi muutettuna	Määrärahat	Kokoaikaiseksi muutettu
tötaulukkoon sisältyvät virat/toimet (virkamiehet ja väliaikaiset toimihenkilöt)																
kka ja edustustot	AD	6	0,9	6	0,9	6	0,9	6	0,9	6	0,9	6	0,9	6	0,9	42
	AST															
sa EU:n	AD															
	AST															
linen henkilöstö[50] 0,24																
	AC	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	21
ärärahat	END															
	INT															
sa EU:n	AC															
	AL															

[50] AC = sopimussuhteiset toimihenkilöt, AL = paikalliset toimihenkilöt, END = kansalliset asiantuntijat, INT = vuokrahenkilöstö ja JPD = nuoremmat asiantuntijat EU:n ulkopuolisissa edustustoissa.

	END															
	INT															
	JPD															
djettikohta *ävä*)																
nma – KE 7 tisessa nyksessä		9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	63

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.

N 7 sisältymättömät rahoituskehyksessä		2021		2022		2023		2024		2025		2025		2025	
		Kokoaikaiseksi muutettuna	Määrärahat	Kokoaikaiseksi muutettuna	Määrärahat	Kokoaikaiseksi muutettuna	Määrärahat	Kokoaikaiseksi muutettuna	Määrärahat	Kokoaikaiseksi muutettuna	Määrärahat	Kokoaikaiseksi muutettuna	Määrärahat	Kokoaikaiseksi muutettuna	Määrärahat
koon sisältyvät virat/toimet (virkamiehet ja väliaikaiset toimihenkilöt)															
	AD														
	AST														
kilöstö [51]															
- päätoimipaikassa	AC														
	END														
	INT														
- edustustoissa EU:n ulkopuolella	AC														
	AL														
	END														
	INT														
	JPD														
	AC														
	END														
	INT														

[51] AC = sopimussuhteiset toimihenkilöt, AL = paikalliset toimihenkilöt, END = kansalliset asiantuntijat, INT = vuokrahenkilöstö ja JPD = nuoremmat asiantuntijat EU:n ulkopuolisissa edustustoissa.

mennettävä)															
SAkKEESEEN 7 ättömät noituskehyksessä															

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.

Arvioidut vaikutukset ENISAn henkilöresursseihin

Euroopan unionin kyberturvallisuusvirasto ENISA, jolle on kyberturvallisuussäädöksellä myönnetty uusi pysyvä toimeksianto, auttaisi jäsenvaltioita ja komissiota tarkistetun NIS-direktiivin täytäntöönpanossa.

Tarkistetun NIS-direktiivin seurauksena ENISAlla on 2022–2023 alkaen uusia toiminta-aloja. Vaikka nämä toiminta-alat kuuluisivat myös ENISAn yleisiin tehtäviin sen toimeksiannon mukaisesti, ne lisäävät viraston työtaakkaa. Tarkemmin sanottuna NIS-direktiivin tarkistamista koskevan komission ehdotuksen mukaan ENISAn on nykyisten toiminta-alojensa lisäksi sisällytettävä työohjelmaansa muun muassa seuraavat toimet: i) kehittää ja ylläpitää Euroopan haavoittuvuusrekisteriä (ehdotuksen 6 artiklan 2 kohta), ii) huolehtia Euroopan kyberkriisien yhteysorganisaatioiden verkoston (CyCLONe) sihteeristöstä (ehdotuksen 14 artikla) ja laatia vuosiraportti kyberturvallisuuden tilasta EU:ssa (ehdotuksen 15 artikla), iii) tukea vertaisarviointien järjestämistä jäsenvaltioiden välillä (ehdotuksen 16 artikla), iv) kerätä poikkeamia koskevia koontitietoja jäsenvaltioilta ja antaa teknisiä ohjeita (ehdotuksen 20 artiklan 9 kohta) ja v) luoda rekisteri rajat ylittäviä palveluja tarjoavista toimijoista ja ylläpitää sitä (ehdotuksen 25 artikla).

Näin ollen vuodesta 2022 alkaen pyydetään viittä kokoaikaista lisätyöntekijää, joiden määrärahat ovat noin 0,61 miljoonaa euroa vuodessa näiden uusien toimien kattamiseksi (ks. virastoja koskeva erillinen rahoitusselvitys).

Näin ollen vuodesta 2022 alkaen pyydetään viittä kokoaikaista lisätyöntekijää ja tämän edellyttämiä lisämäärärahoja.

☐ Ehdotus/aloite ei edellytä hallintomäärärahoja.

☐X Ehdotus/aloite edellyttää hallintomäärärahoja seuraavasti:

milj. euroa (kolmen desimaalin tarkkuudella)

	Vuosi **N** [52] **2022**	Vuosi **N+1** **2023**	Vuosi **N+2** **2024**	Vuosi **N+3** **2025**	Ilmoitetaan kaikki vuodet, joille ehdotuksen vaikutukset ulottuvat (ks. kohta 1.6)			**YHTEENSÄ**
Väliaikaiset toimihenkilöt (AD-palkkaluokat)	0,450	0,450	0,450	0,450	0,450	0,450		**2,7**

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

Väliaikaiset toimihenkilöt (AST-palkkaluokat)								
Sopimussuhteiset toimihenkilöt	0,160	0,160	0,160	0,160	0,160	0,160		
Kansalliset asiantuntijat								**0,96**
YHTEENSÄ	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**		**3,66**

Henkilöstötarpeet (kokoaikaiseksi muutettuna)

	Vuosi **N** [53] **2022**	Vuosi **N+1** **2023**	Vuosi **N+2** **2024**	Vuosi **N+3** **2025**	Ilmoitetaan kaikki vuodet, joille ehdotuksen vaikutukset ulottuvat (ks. kohta 1.6)			**YHTEENSÄ**
Väliaikaiset toimihenkilöt (AD-palkkaluokat)	3	3	3	3	3	3		**18**
Väliaikaiset toimihenkilöt (AST-palkkaluokat)								
Sopimussuhteiset toimihenkilöt	2	2	2	2	2	2		**12**

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

Kansalliset asiantuntijat								
YHTEENSÄ	**5**	**5**	**5**	**5**	**5**	**5**		**30**

2. Muista hallintomenoista aiheutuvat kustannukset

☐ Ehdotus/aloite ei edellytä hallintomäärärahoja.

X☐ Ehdotus/aloite edellyttää hallintomäärärahoja seuraavasti:

milj. euroa (kolmen desimaalin tarkkuudella)

OTSAKE 7 monivuotisessa rahoituskehyksessä	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Yhteensä**
Päätoimipaikassa								
Virkamatka- ja edustuskulut	0,03	0,03	0,03	0,03	0,03	0,03	0,03	**0,21**
Konferenssi- ja kokouskulut	0,06	0,06	0,06	0,06	0,06	0,06	0,06	**0,42**
Komiteat[54]								
Selvitykset ja kuulemiset								
Tieto- ja hallintajärjestelmät								

[54] Ilmoitetaan, millaisesta komiteasta on kysymys ja mihin ryhmään se kuuluu.

TVT-laitteet ja -palvelut[55]								
Muut budjettikohdat (*ilmoitetaan tarvittaessa*)								
Edustustoissa EU:n ulkopuolella								
Virkamatkat, konferenssit ja edustuskulut								
Henkilöstön täydennyskoulutus								
Hankinta, vuokraus ja niihin liittyvät kulut								
Laitteisto, kalusto, tarvikkeet ja palvelut								
Välisumma, OTSAKE 7 monivuotisessa rahoituskehyksessä	0,09	0,09	0,09	0,09	0,09	0,09	0,09	**0,63**

[55] TVT: Tieto- ja viestintätekniikka: konsultoitava DIGIT-pääosastoa.

milj. euroa (kolmen desimaalin tarkkuudella)

OTSAKKEESEEN 7 sisältymättömät monivuotisessa rahoituskehyksessä	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Yhteensä**
Teknisen ja hallinnollisen tuen menot (ulkopuolista henkilöstöä lukuun ottamatta) toimintamäärärahoista (entiset BA-budjettikohdat)								
- päätoimipaikassa								
- edustustoissa EU:n ulkopuolella								
Muut hallintomenot tutkimuksen toimintalohkossa								
Muut budjettikohdat (*ilmoitetaan tarvittaessa*)								
Välisumma – OTSAKKEESEEN 7 sisältymättömät monivuotisessa rahoituskehyksessä								

YHTEENSÄ monivuotisen rahoituskehyksen **OTSAKE 7 ja OTSAKKEESEEN 7 sisältymättömät**	1,23	1,23	1,23	1,23	1,23	1,23	1,23	**8,61**

Hallintomäärärahojen tarve katetaan toimen hallinnointiin jo osoitetuilla määrärahoilla ja/tai siirroilla sekä tarvittaessa sellaisilla lisäresursseilla, jotka toimea hallinnoiva pääosasto voi saada käyttöönsä vuotuisessa määrärahojen jakomenettelyssä talousarvion puitteissa.

3. Laskentamenetelmät kustannusten arvioimiseksi

3.1 Henkilöresurssit:

Tässä osassa esitetään laskentamenetelmä tarpeelliseksi arvioitujen henkilöresurssien laskemiseksi (arvioitu työkuormitus, mukaan lukien erityistehtävät (Sysper 2 -tehtäväalueet), henkilöstöryhmät ja vastaavat keskimääräiset kustannukset)

Monivuotisen rahoituskehyksen **OTSAKE 7**
HUOM. Tiedot kunkin henkilöstöryhmän keskimääräisistä kustannuksista ovat saatavilla budjettipääosaston verkkosivustolla osoitteessa https://myintracomm.ec.europa.eu/budgweb/EN/pre/legalbasis/Pages/pre-040-020_preparation.aspx
• Virkamiehet ja väliaikaiset toimihenkilöt 6 kokoaikaista virkamiestä (keskikustannus 0,150) = 0,9 vuodessa - Delegoitujen säädösten valmistelu 18 artiklan 6 kohdan, 21 artiklan 2 kohdan ja 36 artiklan mukaisesti - Täytäntöönpanosäädösten valmistelu 12 artiklan 8 kohdan, 18 artiklan 5 kohdan ja 20 artiklan 11 kohdan mukaisesti - NIS-yhteistyöryhmän sihteeristöpalvelut - NIS-yhteistyöryhmän täysistuntojen ja työryhmäkokousten järjestäminen - Eri asiakirjoja (ohjeet, toimintamallit jne.) koskevan jäsenvaltioiden työn koordinointi - Yhteydet muihin komission yksiköihin, ENISAan ja kansallisiin viranomaisiin NIS-direktiivin täytäntöönpanemiseksi - NIS-direktiivin täytäntöönpanoon liittyvien kansallisten menetelmien ja parhaiden käytäntöjen analysointi
• Ulkopuolinen henkilöstö 3 AC (keskikustannus 0,08) = 0,24 vuodessa - Tuki kaikille edellä mainituille toimille tarpeen mukaan

Monivuotisen rahoituskehyksen **OTSAKKEESEEN 7 sisältymättömät**
• Vain tutkimusmenoista rahoitettavat toimet
• Ulkopuolinen henkilöstö

3.2 Muut hallintomenot

Yksityiskohtaiset tiedot laskentamenetelmästä jokaisen budjettikohdan osalta

ja etenkin taustaoletukset (kokousten määrä vuodessa, keskimääräiset kustannukset jne.)

Monivuotisen rahoituskehyksen **OTSAKE 7**
Kokoukset: NIS-yhteistyöryhmän täysistunnot pidetään yleensä 4 kertaa vuodessa. Komissio kattaa 27 jäsenvaltion edustajien ateria- ja matkakulut (yksi edustaja kustakin jäsenvaltiosta). Yhden kokouksen kustannukset ovat enimmillään 15 000 euroa, eli kulut yhteensä 60 000 euroa vuodessa. Virkamatkat: Virkamatkat liittyvät NIS-direktiivin täytäntöönpanon seurantaan. Esimerkki: Yhden vuoden aikana (toukokuu 2019 – heinäkuu 2020) on tarkoitus järjestää niin kutsuttuja NIS-maavierailuja kaikkiin 27 jäsenvaltioon tavoitteena keskustella NIS-direktiivin täytäntöönpanosta koko EU:ssa.

Monivuotisen rahoituskehyksen **OTSAKKEESEEN 7 sisältymättömät**

LIITE 7

KOMISSION PÄÄTÖKSEEN

Euroopan unionin yleisen talousarvion toteuttamista koskevista sisäisistä säännöistä (Euroopan komissiota koskeva pääluokka) tiedoksi komission yksiköille

SÄÄDÖSEHDOTUKSEEN LIITTYVÄ RAHOITUSSELVITYS – ’VIRASTOT’

Tämä rahoitusselvitys kattaa pyynnön lisätä ENISAn henkilöstöä viidellä kokoaikaisella työntekijällä vuodesta 2022 NIS-direktiivin täytäntöönpanoon liittyviä lisätehtäviä varten. Nämä toimintamuodot sisältyvät jo ENISAn toimeksiantoon.

Sisällysluettelo

1. PERUSTIEDOT EHDOTUKSESTA/ALOITTEESTA

1.1. Ehdotuksen/aloitteen nimi

Ehdotus direktiiviksi toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi koko unionissa ja direktiivin (EU) 2016/1148 kumoamisesta

1.2. Toimintalohko(t)

Viestintäverkot, sisällöt ja teknologia

1.3. Ehdotus liittyy

☐ **uuteen toimeen**

☐ **uuteen toimeen, joka perustuu pilottihankkeeseen tai valmistelutoimeen**[56]

☒ **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)

Tarkistuksen tavoitteena on lisätä Euroopan unionissa toimivien yritysten laajan joukon kykyä torjua kyberuhkia kaikilla asiaankuuluvilla aloilla, vähentää häiriönsietokyvyn epäjohdonmukaisuuksia sisämarkkinoilla direktiivin jo kattamilla aloilla sekä parantaa yhteistä tilannetietoisuutta ja yhteisiä valmiuksia valmistautua ja reagoida.

1.4.2. Erityistavoite (Erityistavoitteet)

Euroopan unionissa toimivien yritysten heikkoon kyberriskien sietokykyyn liittyvän ongelman ratkaisemiseksi erityistavoitteena on varmistaa, että kaikilla verkko- ja tietojärjestelmistä riippuvaisilla aloilla toimivien toimijoiden, jotka tarjoavat avainasemassa olevia palveluja taloudelle ja koko yhteiskunnalle, on toteutettava kyberturvatoimenpiteitä ja raportoitava poikkeamista kybervalmiuksien yleisen tason nostamiseksi kaikkialla sisämarkkinoilla.

Jäsenvaltioiden ja toimialojen välisen epäjohdonmukaisen häiriönsietokyvyn ongelman ratkaisemiseksi erityistavoitteena on varmistaa, että kaikkiin toimijoihin, jotka toimivat NIS-kehyksen kattamilla aloilla ja jotka ovat kooltaan toisiinsa verrattavissa ja joilla on toisiaan vastaava rooli, sovelletaan samaa sääntelyjärjestelmää (eli ne joko kuuluvat soveltamisalaan tai eivät kuulu) riippumatta siitä, mihin lainkäyttöalueeseen ne kuuluvat EU:ssa.

Sen varmistamiseksi, että kaikkien NIS-kehyksen kattamilla aloilla toimivien toimijoiden on noudatettava samoja velvoitteita, jotka perustuvat turvatoimenpiteiden osalta riskinhallintamalliin, ja raportoitava kaikista poikkeamista yhdenmukaisten kriteerien perusteella, erityistavoitteina on varmistaa, että toimivaltaiset viranomaiset panevat säädöksessä vahvistetut säännöt tehokkaammin täytäntöön yhdenmukaisten valvonta- ja täytäntöönpanotoimenpiteiden avulla, ja varmistaa, että toimivaltaisille viranomaisille

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

osoitetaan kaikissa jäsenvaltioissa samantasoiset resurssit, joiden avulla ne voivat hoitaa NIS-kehyksessä vahvistetut ydintehtävät.

Yhteisen tilannetietoisuuden ja yhteisten kriisitoimien puuttumisen ongelman ratkaisemiseksi erityistavoitteena on varmistaa, että jäsenvaltiot vaihtavat keskenään olennaisia tietoja, asettamalla toimivaltaisille viranomaisille selkeät velvoitteet jakaa tietoja ja tehdä yhteistyötä kyberuhkien ja -poikkeamien osalta ja kehittämällä unionin yhteiset operatiiviset kriisinhallintavalmiudet.

1.4.3. Odotettavissa olevat tulokset ja vaikutukset

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

Ehdotuksen odotetaan tuottavan merkittäviä etuja. Arvioiden mukaan se voi johtaa kyberturvapoikkeamien kustannusten alenemiseen 11,3 miljardilla eurolla. NIS-kehyksen kattamia toimialoja tulisi huomattavasti lisää, mutta edellä mainittujen hyötyjen lisäksi NIS-vaatimuksista erityisesti valvontanäkökulmasta mahdollisesti aiheutuva rasite myös tasapainottuisi sekä soveltamisalan piiriin tulevien uusien toimijoiden että toimivaltaisten viranomaisten osalta. Tämä perustuisi siihen, että uudessa NIS-kehyksessä noudatettaisiin kaksitasoista lähestymistapaa, jossa keskityttäisiin suuriin avaintoimijoihin, sekä eriytettyä valvontajärjestelmää, jossa sallittaisiin ainoastaan jälkikäteisvalvonta hyvin monien toimijoiden osalta ja varsinkin ’tärkeiksi’ mutta ei ’keskeisiksi’ katsottujen toimijoiden osalta.

Kokonaisuudessaan voidaan todeta, että ehdotus johtaisi tehokkaisiin kompromisseihin ja synergioihin ja tarjoaisi kaikista analysoiduista toimintavaihtoehdoista parhaat mahdollisuudet varmistaa, että keskeisten toimijoiden kyky sietää kyberturvallisuusuhkia paranisi ja olisi yhdenmukainen kaikkialla unionissa, mikä johtaisi lopulta kustannussäästöihin sekä yrityksille että yhteiskunnalle.

Ehdotus aiheuttaisi myös jäsenvaltioiden viranomaisille tiettyjä vaatimustenmukaisuuden varmistamiseen ja valvontaan liittyviä kustannuksia (resurssitarpeen kokonaiskasvuksi arvioitiin 20–30 %). Toisaalta uusi kehys toisi myös huomattavia hyötyjä, kun kokonaiskuva avainyrityksistä ja yhteydenpito niiden kanssa paranisi, EU-maiden välinen operatiivinen yhteistyö tehostuisi ja käyttöön saataisiin keskinäisen avunannon ja vertaisarvioinnin mekanismeja. Tämä parantaisi kyberturvan kokonaisvalmiuksia jäsenvaltioissa.

Uuden NIS-kehyksen soveltamisalaan tulevien yritysten osalta arvioidaan, että niiden olisi kasvatettava nykyisiä tieto- ja viestintätekniikan turvallisuuteen liittyviä menojaan enintään 22 % NIS-kehyksen ensimmäisinä vuosina (jo nykyisen NIS-direktiivin soveltamisalaan kuuluvien yritysten osalta luku olisi 12 %). Tämä keskimääräinen kulujen kasvu tuottaisi myös kohtuullisen tuoton näille investoinneille, varsinkin kun kyberturvapoikkeamien kustannukset laskisivat merkittävästi (arviolta 118 miljardia euroa kymmenen vuoden aikana).

NIS-kehystä ei sovellettaisi pien- ja mikroyrityksiin. Keskisuurten yritysten osalta voidaan olettaa, että tieto- ja viestintätekniikan turvallisuuteen liittyvät kulut kasvaisivat uuden NIS-kehyksen ensimmäisinä vuosina. Samalla tietoturvavaatimusten tiukentaminen tällaisten toimijoiden osalta loisi niille kannustimia parantaa kyberturvavalmiuksiaan ja auttaisi parantamaan niiden tieto- ja viestintäteknisten riskien hallintaa.

Jäsenvaltioiden budjettiin ja julkishallintoon kohdistuisi vaikutuksia: lyhyellä ja keskipitkällä aikavälillä lisäresurssitarpeeksi arvioidaan 20–30 %.

Muita merkittäviä negatiivisia vaikutuksia ei odoteta olevan. Ehdotuksen oletetaan johtavan parempiin kyberturvavalmiuksiin, joten tätä kautta se vähentäisi merkittävämmin poikkeamien, myös tietoturvaloukkausten, määrää ja vakavuutta. Se auttaa myös todennäköisesti tasaamaan jäsenvaltioiden välisiä eroja NIS-kehyksen piiriin kuuluvien toimijoiden toimintaedellytyksissä ja vähentämään epäsuhtia kyberturvatiedon saatavuudessa.

1.4.4. Tuloksellisuusindikaattorit

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

Komissio arvioi kehitystä indikaattorien perusteella ENISAn ja yhteistyöryhmän tuella ensimmäisen kerran kolmen vuoden kuluttua uuden NIS-säädöksen voimaantulosta. Kehitystä arvioitaisiin muun muassa seuraavien indikaattorien avulla:

- Poikkeamien parempi käsittely: Kyberturvatoimenpiteiden avulla yritykset eivät ainoastaan paranna valmiuksiaan välttää tietyt poikkeamat kokonaan vaan myös valmiuksiaan reagoida poikkeamiin. Onnistumismittareita ovat näin ollen i) poikkeaman havaitsemiseen kuluvan keskimääräisen ajan lyheneminen, ii) se, kuinka kauan organisaatioiden keskimääräinen toipuminen poikkeamasta kestää, ja iii) poikkeaman aiheuttaman vahingon keskimääräiset kustannukset.

- Yritysten ylimmän johdon parempi tietoisuus kyberturvariskeistä: Kun yrityksiltä vaaditaan asiassa toimenpiteitä, tarkistettu NIS-direktiivi lisäisi ylimmän johdon tietoisuutta kyberturvariskeistä. Tätä voidaan mitata tutkimalla, missä määrin NIS-kehyksen piiriin kuuluvat yritykset asettavat kyberturvallisuuden etusijalle yrityksen sisäisissä toimintaperiaatteissa ja prosesseissa, mikä käy ilmi sisäisestä dokumentaatiosta, asiaan liittyvistä koulutusohjelmista ja työntekijöille suunnatuista tiedotustoimista sekä siitä, priorisoidaanko tietoturvaa tieto- ja viestintäteknisissä investoinneissa. Kaikkien keskeisten ja tärkeiden toimijoiden johdon olisi myös oltava tietoinen NIS-direktiivin säännöistä.

- Menojen tasaaminen toimialojen välillä: Tieto- ja viestintätekniikan tietoturvaan liittyvät menot vaihtelevat huomattavasti toimialoittain EU:ssa. Kun useampien alojen yrityksiä vaaditaan toteuttamaan turvatoimenpiteitä, toimialojen ja jäsenvaltioiden väliset prosentuaaliset erot tieto- ja viestintätekniikan keskimääräisissä alakohtaisissa turvallisuusmenoissa suhteessa tieto- ja viestintätekniikan kokonaismenoihin oletettavasti pienenevät.

- Toimivaltaisten viranomaisten vahvistaminen ja yhteistyön lisääminen: Tarkistetussa NIS-direktiivissä annettaisiin mahdollisesti lisätehtäviä toimivaltaisille viranomaisille. Tällä olisi mitattavissa oleva rahoitus- ja resurssivaikutus kansallisen tason kyberturvayksiköille, ja sen pitäisi myös vaikuttaa myönteisesti toimivaltaisten viranomaisten valmiuksiin tehdä ennakoivaa yhteistyötä ja siten lisätä niiden tapausten määrää, joissa toimivaltaiset viranomaiset toimivat keskenään rajat ylittävien poikkeamien käsittelemiseksi tai yhteisten valvontatoimien toteuttamiseksi.

- Lisääntynyt tiedonvaihto: Tarkistettu NIS-direktiivi parantaisi myös tietojenvaihtoa yritysten kesken ja toimivaltaisten viranomaisten kanssa. Yksi tavoitteista voisi olla eri tiedonvaihtomuotoihin osallistuvien toimijoiden määrän lisääminen.

1.5. Ehdotuksen/aloitteen perustelut

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

Ehdotuksen tavoitteena on lisätä Euroopan unionissa toimivien yritysten laajan joukon kykyä torjua kyberuhkia kaikilla asiaankuuluvilla aloilla, vähentää häiriönsietokyvyn epäjohdonmukaisuuksia sisämarkkinoilla direktiivin jo kattamilla aloilla sekä parantaa yhteistä tilannetietoisuutta ja yhteisiä valmiuksia valmistautua ja reagoida. Se perustuu direktiivillä (EU) 2016/1148 viimeksi kuluneiden 4 vuoden aikana saavutettuun kehitykseen.

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.

Kyberturvallisuustoiminta unionissa ei voi olla tuloksellista, jos asiaa lähestytään hajanaisesti kansallisten tai alueellisten siilojen näkökulmasta. NIS-direktiivillä haluttiin korjata tätä puutetta luomalla puitteet verkkojen ja tietojärjestelmien tietoturvalle kansallisella ja unionitasolla. NIS-direktiivin ensimmäisessä määräaikaistarkastelussa tuotiin kuitenkin esiin useita sisälähtöisiä puutteita, jotka ovat lopulta johtaneet huomattaviin eroihin jäsenvaltioiden välillä valmiuksien, suunnittelun ja suojelun tason osalta, mikä vaikuttaa samalla samankaltaisten yritysten tasapuolisiin toimintaedellytyksiin sisämarkkinoilla.

Nykyistä NIS-direktiiviä vahvempi EU-tason sääntely on perusteltavissa erityisesti seuraavilla seikoilla: i) ongelma on luonteeltaan maiden rajat ylittävä, ii) EU-tason toimilla voidaan parantaa ja helpottaa tuloksellista toimintaa kansallisella tasolla ja iii) yhtenäisellä ja yhteistyöhön perustuvalla verkko- ja tietoturvatoiminnalla voidaan tuloksellisesti tukea tietosuojaa ja yksityisyyden suojaa.

Ehdotuksen tavoitteet voidaan näin ollen saavuttaa paremmin EU:n tasolla kuin jäsenvaltioiden omin toimin.

1.5.3. Vastaavista toimista saadut kokemukset

NIS-direktiivi on ensimmäinen horisontaalinen sisämarkkinasäädös, jolla pyritään parantamaan unionin verkkojen ja järjestelmien kykyä sietää kyberturvariskejä. Se on vuonna 2016 tapahtuneen voimaantulonsa jälkeen jo merkittävästi nostanut kyberturvallisuuden yhteistä tasoa jäsenvaltioiden keskuudessa. Direktiivin toiminnan ja täytäntöönpanon uudelleentarkastelu on kuitenkin tuonut esiin useita puutteita. Kun lisäksi digitalisaatio on edennyt ja tarvitaan ajanmukaisempia tapoja reagoida uhkiin, puutteet olisi korjattava tarkistetulla säädöksellä.

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

Uusi ehdotus on täysin linjassa ja johdonmukainen muiden asiaan liittyvien aloitteiden kanssa, joita ovat muun muassa ehdotus asetukseksi finanssialan digitaalisesta häiriönsietokyvystä (DORA) ja ehdotus direktiiviksi keskeisten palvelujen kriittisen tärkeiden tarjoajien kyvystä suojautua ulkoisilta uhkilta. Se on johdonmukainen myös suhteessa eurooppalaiseen sähköisen viestinnän säännöstöön, yleiseen tietosuoja-asetukseen ja eIDAS-asetukseen.

Ehdotus on olennainen osa EU:n turvallisuusunionia koskevaa strategiaa.

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

Näiden tehtävien hoitaminen ENISAssa edellyttää erityisiä osaamisprofiileja ja lisäpanostuksia, jotka edellyttävät henkilöresurssien lisäämistä.

1.6. Ehdotetun toimen/aloitteen kesto ja rahoitusvaikutukset

☐ **kesto on rajattu**

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

– ☐ Rahoitusvaikutukset koskevat vuosia YYYY–YYYY.

☒ **kestoa ei ole rajattu**

– Käynnistysvaihe alkaa vuonna 2022 ja päättyy vuonna 2025,

– minkä jälkeen toteutus täydessä laajuudessa.

1.7. Hallinnointitapa (Hallinnointitavat)[57]

☒ **Suora hallinnointi**, jonka komissio toteuttaa käyttämällä

:

– ☐ toimeenpanovirastoja

☐ **Hallinnointi yhteistyössä** jäsenvaltioiden kanssa

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

☐ kansainvälisille järjestöille ja niiden erityisjärjestöille (tarkennettava)

☐ Euroopan investointipankille tai Euroopan investointirahastolle

☒ 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.

Huomautukset

Euroopan unionin kyberturvallisuusvirasto ENISA, jolle on kyberturvallisuussäädöksellä myönnetty uusi pysyvä toimeksianto, auttaisi jäsenvaltioita ja komissiota tarkistetun NIS-direktiivin täytäntöönpanossa. Tarkistetun NIS-direktiivin seurauksena ENISAlla on 2022–2023 alkaen uusia toiminta-aloja. Vaikka nämä toiminta-alat kuuluisivat myös ENISAn yleisiin tehtäviin sen toimeksiannon mukaisesti, ne lisäävät viraston työtaakkaa. Tarkemmin sanottuna NIS-direktiivin tarkistamista koskevan komission ehdotuksen mukaan ENISAn on nykyisten toiminta-alojensa lisäksi sisällytettävä työohjelmaansa

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

muun muassa seuraavat toimet: i) kehittää ja ylläpitää Euroopan haavoittuvuusrekisteriä (ehdotuksen 6 artiklan 2 kohta), ii) huolehtia Euroopan kyberkriisien yhteysorganisaatioiden verkoston (CyCLONe) sihteeristöstä (ehdotuksen 14 artikla) ja laatia vuosiraportti kyberturvallisuuden tilasta EU:ssa (ehdotuksen 15 artikla), iii) tukea vertaisarviointien järjestämistä jäsenvaltioiden välillä (ehdotuksen 16 artikla), iv) kerätä poikkeamia koskevia koontitietoja jäsenvaltioilta ja antaa teknisiä ohjeita (ehdotuksen 20 artiklan 9 kohta) ja v) luoda rekisteri rajat ylittäviä palveluja tarjoavista toimijoista ja ylläpitää sitä (ehdotuksen 25 artikla).

Näin ollen vuodesta 2022 alkaen pyydetään viittä kokoaikaista lisätyöntekijää ja tämän edellyttämiä lisämäärärahoja eli n. 0,61 miljoonaa euroa vuodessa.

2. HALLINNOINTI

2.1. Seuranta- ja raportointisäännöt

Ilmoitetaan sovellettavat aikavälit ja edellytykset.

Komissio tarkastelee säännöllisesti direktiivin toimivuutta ja antaa siitä raportin Euroopan parlamentille ja neuvostolle ensimmäisen kerran kolmen vuoden kuluttua direktiivin voimaantulosta.

Komissio arvioi myös direktiivin täytäntöönpanotoimet jäsenvaltioissa.

Ehdotuksen seurannassa ja raportoinnissa noudatetaan periaatteita, jotka on esitetty asetuksen (EU) 2019/881 (kyberturvallisuusasetus) mukaisessa ENISAn pysyvässä toimeksiannossa.

Suunnitellussa seurannassa käytetään lähinnä ENISAn, yhteistyöryhmän, CSIRT-verkoston ja jäsenvaltioiden viranomaisten tietolähteitä. ENISAn raporteista (ml. vuotuiset toimintakertomukset), yhteistyöryhmältä ja CSIRT-verkostolta saatavien tietojen ohella voitaisiin käyttää tarpeen mukaan erityisiä tiedonkeruuvälineitä (esim. kansallisille viranomaisille tehtyjä kyselyjä, Eurobarometri-tutkimuksia sekä kyberturvallisuuskuukauden tiedotuskampanjasta ja yleiseurooppalaisista harjoituksista laadittuja raportteja).

2.2. Hallinnointi- ja valvontajärjestelmä(t)

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

Kyseisestä politiikan alasta vastaava viestintäverkkojen, sisältöjen ja teknologian pääosaston yksikkö hallinnoi direktiivin täytäntöönpanoa.

ENISAn hallinnon osalta kyberturvallisuusasetuksen 15 artiklassa on yksityiskohtainen luettelo ENISAn hallintoneuvoston valvontatehtävistä.

Kyberturvallisuusasetuksen 31 artiklan mukaan ENISAn pääjohtaja vastaa ENISAn talousarvion toteuttamisesta ja komission sisäisellä tarkastajalla on ENISAn suhteen samat valtuudet kuin komission yksiköiden osalta. ENISAn johtokunta antaa lausunnon ENISAn lopullisesta tilinpäätöksestä.

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

Riski on hyvin pieni, koska NIS-direktiivin ekosysteemi on jo olemassa ja kattaa jo ENISAn, jolla on pysyvä toimeksianto sen jälkeen, kun kyberturvallisuusasetus tuli voimaan vuonna 2019.

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

Pyydetty määrärahojen lisäys koskee osastoa 1, ja sillä on tarkoitus rahoittaa palkat. Tämä tarkoittaa hyvin pientä virheriskiä maksujen tasolla.

2.3. Toimenpiteet petosten ja sääntöjenvastaisuuksien ehkäisemiseksi

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

ENISAn torjunta- ja suojatoimenpiteisiin kuuluvat erityisesti seuraavat:

- Viraston henkilöstö tarkastaa kaikista palveluista tai pyydetyistä tutkimuksista suoritettavat maksut ennen niiden maksamista ottaen huomioon mahdolliset sopimusvelvoitteet, taloudenpidon periaatteet sekä moitteettoman varainhoidon tai hallinnon periaatteet. Kaikkiin viraston ja maksujen vastaanottajien välisiin sopimuksiin sisällytetään petosten torjuntaa koskevia määräyksiä (valvonta, selontekovaatimukset jne.).

- Petosten, lahjonnan ja muiden säännönvastaisuuksien torjumiseksi sovelletaan rajoituksetta Euroopan petostentorjuntaviraston (OLAF) tutkimuksista 25 päivänä toukokuuta 1999 annetun Euroopan parlamentin ja neuvoston asetuksen (EU, Euratom) N:o 883/2013 säännöksiä.

- Kyberturvallisuusasetuksen 33 artiklan nojalla ENISA liittyi ennen 28. joulukuuta 2019 Euroopan parlamentin, Euroopan unionin neuvoston ja Euroopan yhteisöjen komission Euroopan petostentorjuntaviraston (OLAF) sisäisistä tutkimuksista 25 päivänä toukokuuta 1999 tekemään toimielinten väliseen sopimukseen. ENISAlla on velvollisuus antaa viipymättä asianmukaiset säännökset, joita sovelletaan viraston kaikkiin työntekijöihin.

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[58]	EFTA-mailta[59]	ehdokasmailta[60]	kolmansilta mailta	varainhoitoasetuksen 21 artiklan 2 kohdan b alakohdassa tarkoitetut rahoitusosuudet
2	02 10 04	./EI-JM	KYLLÄ	EI	EI	/EI

- Uudet perustettaviksi esitetyt budjettikohdat

Monivuotisen rahoituskehyksen otsakkeiden ja budjettikohtien mukaisessa järjestyksessä

Monivuotisen	Budjettikohta	Menolaji	Rahoitusosuudet

[58] JM = jaksotetut määrärahat / EI-JM = jaksottamattomat määrärahat.
[59] EFTA: Euroopan vapaakauppaliitto.
[60] Ehdokasmaat ja soveltuvin osin Länsi-Balkanin mahdolliset ehdokasmaat.

rahoituskehyksen otsake	Numero	JM/EI-JM	EFTA-mailta	ehdokasmailta	kolmansilta mailta	varainhoitoasetuksen 21 artiklan 2 kohdan b alakohdassa tarkoitetut rahoitusosuudet
	[PP.KK.VVVV]		KYLLÄ/EI	KYLLÄ/EI	KYLLÄ/EI	KYLLÄ/EI

3.2. Arvioidut vaikutukset menoihin

3.2.1. Yhteenveto arvioiduista vaikutuksista menoihin

milj. euroa (kolmen desimaalin tarkkuudella)

Monivuotisen rahoituskehyksen otsake	Numero	[Otsake... 2 Sisämarkkinat, innovointi ja digitaalitalous.....]

[Elin]: <…ENISA….>			Vuosi **N**[61] **2022**	Vuosi **N+1** **2023**	Vuosi **N+2** **2024**	Vuosi **N+3** **2025**	Ilmoitetaan kaikki vuodet, joille ehdotuksen vaikutukset ulottuvat (ks. kohta 1.6) **2026**	**2027**		**YHTEENSÄ**
Osasto 1:	Sitoumukset	1)	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**
	Maksut	2)	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**
Osasto 2:	Sitoumukset	(1 a)								
	Maksut	(2 a)								
Osasto 3:	Sitoumukset	(3 a)								
	Maksut	(3 b)								
[Elimen] määrärahat YHTEENSÄ<ENISA…….>	Sitoumukset	= 1 + 1 a + 3 a	0,61	0,61	0.61	0,61	0,61	0,61		**3,66**
	Maksut	= 2 + 2 a + 3 b	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**

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

Monivuotisen rahoituskehyksen otsake	**5**	”Hallintomenot”

milj. euroa (kolmen desimaalin tarkkuudella)

		Vuosi **N**	Vuosi **N+1**	Vuosi **N+2**	Vuosi **N+3**	Ilmoitetaan kaikki vuodet, joille ehdotuksen vaikutukset ulottuvat (ks. kohta 1.6)			**YHTEENSÄ**
Pääosasto: <…….>									
• Henkilöresurssit									
• Muut hallintomenot									
<….> **Pääosasto YHTEENSÄ**	Määrärahat								

OTSAKKEEN 5 määrärahat YHTEENSÄ monivuotisessa rahoituskehyksessä	(Sitoumukset yhteensä = maksut yhteensä)								

milj. euroa (kolmen desimaalin tarkkuudella)

		Vuosi **N**[62] **2022**	Vuosi **N+1** **2023**	Vuosi **N+2** **2024**	Vuosi **N+3** **2025**	Ilmoitetaan kaikki vuodet, joille ehdotuksen vaikutukset ulottuvat (ks. kohta 1.6) **2026**	**2027**		**YHTEENSÄ**
OTSAKKEIDEN 1–5 määrärahat YHTEENSÄ monivuotisessa rahoituskehyksessä	Sitoumukset	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**
	Maksut	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**

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

3.2.2. Arvioidut vaikutukset [elimen] määrärahoihin

– ☐x Ehdotus/aloite ei edellytä toimintamäärärahoja.

– ☐ Ehdotus/aloite edellyttää toimintamäärärahoja seuraavasti:

Maksusitoumusmäärärahat, milj. euroa (kolmen desimaalin tarkkuudella)

Tavoitteet ja tuotokset			Vuosi **N**		Vuosi **N+1**		Vuosi **N+2**		Vuosi **N+3**		Ilmoitetaan kaikki vuodet, joille ehdotuksen vaikutukset ulottuvat (ks. kohta 1.6)						**YHTEENSÄ**	
	TUOTOKSET																	
⇩	Tyyppi[63]	Keskim. kustannukset	Ei	Kustannus	Ei	Kustannus	Ei	Kustannus	Ei	Kustannus	Ei	Kustannus	Ei	Kustannus	Ei	Kustannus	Lukumäärä yhteensä	Kustannukset yhteensä
ERITYISTAVOITE 1[64]...																		
- Tuotos																		
- Tuotos																		
- Tuotos																		
Välisumma, erityistavoite 1																		
ERITYISTAVOITE 2 ...																		
- Tuotos																		
Välisumma, erityistavoite 2																		
KOKONAISKUSTANNUKSET																		

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

64 Kuten kuvattu kohdassa 1.4.2. ”Erityistavoite (erityistavoitteet)...”.

3.2.3. Arvioidut vaikutukset ENISAn henkilöresursseihin

3.2.3.1. Yhteenveto

Tarkistetun NIS-direktiivin seurauksena ENISAlla on 2022–2023 alkaen uusia tehtäviä. Vaikka nämä tehtävät kuuluisivat myös ENISAn toimeksiantoon, ne lisäävät viraston työtaakkaa. Tarkemmin sanottuna NIS-direktiivin tarkistamista koskevan komission ehdotuksen mukaan ENISAlle tulisi nykytehtävien lisäksi seuraavat uudet tehtävät: i) kehittää ja ylläpitää Euroopan haavoittuvuusrekisteriä (6 artiklan 2 kohta), ii) huolehtia Euroopan kyberkriisien yhteysorganisaatioiden verkoston (CyCLONe) sihteeristöstä (14 artikla) ja laatia vuosiraportti kyberturvallisuuden tilasta EU:ssa (15 artikla), iii) tukea vertaisarviointien järjestämistä jäsenvaltioiden välillä (16 artikla), iv) kerätä poikkeamia koskevia koontitietoja jäsenvaltioilta ja antaa teknisiä ohjeita (20 artiklan 9 kohta) ja v) luoda rekisteri rajat ylittäviä palveluja tarjoavista toimijoista ja ylläpitää sitä (25 artikla).

Näin ollen vuodesta 2022 alkaen pyydetään viittä kokoaikaista lisätyöntekijää ja tämän edellyttämiä lisämäärärahoja.

– ☐ Ehdotus/aloite ei edellytä hallintomäärärahoja.

– ☐X Ehdotus/aloite edellyttää hallintomäärärahoja seuraavasti:

milj. euroa (kolmen desimaalin tarkkuudella)

	Vuosi **N** [65] **2022**	Vuosi **N+1** **2023**	Vuosi **N+2** **2024**	Vuosi **N+3** **2025**	Ilmoitetaan kaikki vuodet, joille ehdotuksen vaikutukset ulottuvat (ks. kohta 1.6) **2026**	**2027**		**YHTEENSÄ**
Väliaikaiset toimihenkilöt (AD-palkkaluokat)	0,450	0,450	0,450	0,450	0,450	0,450		**2,7**
Väliaikaiset toimihenkilöt (AST-palkkaluokat)								
Sopimussuhteiset toimihenkilöt	0,160	0,160	0,160	0,160	0,160	0,160		**0,96**
Kansalliset asiantuntijat								
YHTEENSÄ	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**		**3,66**

Henkilöstötarpeet (kokoaikaiseksi muutettuna)

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

	Vuosi **N** [66] **2022**	Vuosi **N+1** **2023**	Vuosi **N+2** **2024**	Vuosi **N+3** **2025**	Ilmoitetaan kaikki vuodet, joille ehdotuksen vaikutukset ulottuvat (ks. kohta 1.6) **2026** **2027**			**YHTEENSÄ**
Väliaikaiset toimihenkilöt (AD-palkkaluokat)	3	3	3	3	3	3		**18**
Väliaikaiset toimihenkilöt (AST-palkkaluokat)								
Sopimussuhteiset toimihenkilöt	2	2	2	2	2	2		**12**
Kansalliset asiantuntijat								
YHTEENSÄ	**5**	**5**	**5**	**5**	**5**	**5**		**30**

3.2.3.2. Henkilöresurssien arvioitu tarve vastuupääosastossa

– ☐ Ehdotus/aloite ei edellytä henkilöresursseja.

– ☐ Ehdotus/aloite edellyttää henkilöresursseja seuraavasti:

arvio kokonaislukuina (tai enintään yhden desimaalin tarkkuudella)

	Vuosi **N**	Vuosi **N+1**	Vuosi **N+2**	Vuosi **N+3**	Ilmoitetaan kaikki vuodet, joille ehdotuksen vaikutukset ulottuvat (ks. kohta 1.6)		
• **Henkilöstötaulukkoon sisältyvät virat/toimet (virkamiehet ja väliaikaiset toimihenkilöt)**							
XX 01 01 01 (päätoimipaikka ja komission edustustot EU:ssa)							
XX 01 01 02 (EU:n ulkopuoliset edustustot)							
XX 01 05 01 (epäsuora tutkimustoiminta)							
10 01 05 01 (suora tutkimustoiminta)							

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

• **Ulkopuolinen henkilöstö (kokoaikaiseksi muutettuna)**[67]								
XX 01 02 01 (kokonaismäärärahoista katettavat AC, END, INT)								
XX 01 02 02 (AC, AL, END, INT ja JPD EU:n ulkopuolisissa edustustoissa)								
XX 01 04 ***yy***[68]	- päätoimipaikassa[69]							
	- EU:n ulkop. edustustoissa							
XX 01 05 02 (epäsuora tutkimustoiminta: AC, END, INT)								
10 01 05 02 (suora tutkimustoiminta: AC, END, INT)								
Muu budjettikohta (täsmennettävä)								
YHTEENSÄ								

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	
Ulkopuolinen henkilöstö	

Kokoaikaiseksi muunnetun henkilöstön kustannusten laskentamenetelmä olisi kuvattava liitteessä V olevassa 3 kohdassa.

67 AC = sopimussuhteiset toimihenkilöt, AL = paikalliset toimihenkilöt, END = kansalliset asiantuntijat, INT = vuokrahenkilöstö ja JPD = nuoremmat asiantuntijat EU:n ulkopuolisissa edustustoissa.

68 Toimintamäärärahoista katettavan ulkopuolisen henkilöstön enimmäismäärä (entiset BA-budjettikohdat).

69 Etenkin rakennerahastot, Euroopan maaseudun kehittämisen maatalousrahasto (maaseuturahasto) ja Euroopan kalatalousrahasto.

3.2.4. Yhteensopivuus nykyisen monivuotisen rahoituskehyksen kanssa

– ☐X Ehdotus/aloite on nykyisen monivuotisen rahoituskehyksen mukainen.

– ☐ Ehdotus/aloite edellyttää monivuotisen rahoituskehyksen asianomaisen otsakkeen rahoitussuunnitelman muuttamista.

Selvitys rahoitussuunnitelmaan tarvittavista muutoksista, mainittava myös kyseeseen tulevat budjettikohdat ja määrät Ehdotus on vuosien 2021–2027 monivuotisen rahoituskehyksen mukainen. Määrärahat, jotka on pyydetty kattamaan ENISAn henkilöstöresurssien lisäys, kompensoidaan vähentämällä samalla määrällä Digitaalinen Eurooppa -ohjelman määrärahoja samassa otsakkeessa.

– ☐ Ehdotus/aloite edellyttää joustovälineen varojen käyttöön ottamista tai monivuotisen rahoituskehyksen tarkistamista[70].

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

3.2.5. Ulkopuolisten tahojen rahoitusosuudet

– Ehdotuksen/aloitteen rahoittamiseen ei osallistu ulkopuolisia tahoja.

– Ehdotuksen/aloitteen rahoittamiseen osallistuu ulkopuolisia tahoja seuraavasti (arvio):

milj. euroa (kolmen desimaalin tarkkuudella)

	Vuosi **N**	Vuosi **N+1**	Vuosi **N+2**	Vuosi **N+3**	Ilmoitetaan kaikki vuodet, joille ehdotuksen vaikutukset ulottuvat (ks. kohta 1.6)			Yhteensä
Rahoitukseen osallistuva taho								
Yhteisrahoituksella katettavat määrärahat YHTEENSÄ								

[70] Ks. vuosia 2014–2020 koskevan monivuotisen rahoituskehyksen vahvistamisesta annetun neuvoston asetuksen (EU, Euratom) N: o 1311/2013 artikla 11 ja 17.

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[71]						
		Vuosi **N**	Vuosi **N+1**	Vuosi **N+2**	Vuosi **N+3**	Ilmoitetaan kaikki vuodet, joille ehdotuksen vaikutukset ulottuvat (ks. kohta 1.6)		
Momentti ….								

Vastaava(t) menopuolen budjettikohta (budjettikohdat) käyttötarkoitukseensa sidottujen sekalaisten tulojen tapauksessa.

Selvitys tuloihin kohdistuvan vaikutuksen laskentamenetelmästä.

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