EUROOPAN
KOMISSIO

Bryssel 4.10.2017
COM(2017) 477 final

2017/0225 (COD)

NOTE
This language version reflects the corrections done to the original EN version transmitted under COM(2017) 477 final of 13.9.2017 and retransmitted (with corrections) under COM(2017) 477 final/2 of 4.10.2017

Ehdotus

EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS

EU:n kyberturvallisuusvirastosta ENISAsta ja asetuksen (EU) 526/2013 kumoamisesta sekä tieto- ja viestintätekniikan kyberturvallisuussertifioinnista (”kyberturvallisuusasetus”)

(ETA:n kannalta merkityksellinen teksti)

{SWD(2017) 500 final}
{SWD(2017) 501 final}
{SWD(2017) 502 final}

PERUSTELUT

1. EHDOTUKSEN TAUSTA

• Ehdotuksen perustelut ja tavoitteet

Euroopan unioni on päättänyt useista toimista kyberresilienssinsä ja varautumistasonsa parantamiseksi. EU:n ensimmäisessä 2013 hyväksytyssä kyberturvallisuusstrategiassa[1] esiteltiin strategiset tavoitteet ja konkreettiset toimet, joiden tarkoituksena on saavuttaa häiriönsietokyky (resilienssi), vähentää kyberrikollisuutta, kehittää kyberpuolustuspolitiikkaa ja -valmiuksia, kehittää teollisia ja teknologisia voimavaroja ja luoda EU:lle johdonmukainen kansainvälinen verkkotoimintapolitiikka. Tässä yhteydessä on sittemmin tapahtunut merkittävää kehitystä, mistä ovat esimerkkeinä Euroopan unionin verkko- ja tietoturvavirastolle (ENISA) annettu jatkomandaatti[2] ja Euroopan unionille hyväksytty **verkko- ja tietoturvadirektiivi**[3], jotka muodostavat perustan tälle ehdotukselle.

Lisäksi **Euroopan komissio hyväksyi vuonna 2016 tiedonannon Euroopan kyberresilienssijärjestelmän vahvistamisesta sekä kilpailukykyisen ja innovatiivisen kyberturvallisuustoimialan tukemisesta**[4]. Tiedonannossa ilmoitettiin toimenpiteistä lisätä yhteistyötä ja tiedon ja tietämyksen jakamista sekä parantaa EU:n resilienssiä ja varautumista, myös laajamittaisten turvallisuuspoikkeamien ja mahdollisen koko Euroopan laajuisen kyberturvallisuuskriisin tapauksessa. Tässä yhteydessä komissio ilmoitti, että se aikoo jouduttaa Euroopan parlamentin ja neuvoston asetuksesta (EY) N:o 526/2013 tehtävää **arviointia** ja **uudelleentarkastelua**. Kyseisellä asetuksella, jäljempänä ’ENISA-asetus’, jatkettiin ENISAn toimeksiantoa ja kumottiin asetus (EY) N:o 460/2004. Arviointi voi johtaa viraston toiminnan uudistamiseen ja sen valmiuksien ja resurssien lisäämiseen, jotta se voisi tukea jäsenvaltioita kestävällä tavalla. Tällöin se saisi operatiivisemman ja keskeisemmän roolin kyberresilienssin saavuttamisessa, ja sen tarkistettuun toimeksiantoon sisällytettäisiin viraston uudet verkko- ja tietoturvadirektiivin mukaiset vastuualueet.

Verkko- ja tietoturvadirektiivi on ensimmäinen tärkeä askel riskinhallintakulttuurin edistämisessä. Sillä otetaan käyttöön turvallisuusvaatimukset oikeudellisina velvoitteina keskeisille talouden toimijoille, varsinkin keskeisiä palveluja tarjoaville toimijoille (keskeisten palvelujen tarjoajat) ja joidenkin keskeisten digitaalisten palvelujen toimittajille (digitaalisen palvelun tarjoajat). Koska turvallisuusvaatimusten merkitys nähdään olennaisena yhteiskunnan kehittyvän digitalisoinnin hyötyjen turvaamiseksi ja koska verkkoon liitettyjen laitteiden määrä on kasvaa nopeasti (esineiden internet), vuoden 2016 tiedonannossa nostettiin myös esille ajatus puitteiden luomisesta tieto- ja viestintäteknologian tuotteiden ja palvelujen turvallisuussertifioinnille, jotta voidaan lisätä turvallisuutta digitaalisilla sisämarkkinoilla ja näitä markkinoita kohtaan tunnettua luottamusta. Tieto- ja viestintäteknologian kyberturvallisuussertifioinnin merkitys korostuu erityisesti, kun korkeaa kyberturvallisuuden tasoa edellyttävät teknologiat, kuten verkkoyhteyksillä varustetut ja automatisoidut autot,

---

1 Euroopan komission ja Euroopan ulkosuhdehallinnon yhteinen tiedonanto: Euroopan unionin kyberturvallisuusstrategia: Avoin, turvallinen ja vakaa verkkoympäristö, JOIN(2013)1.

2 Asetus (EU) 526/2013 Euroopan unionin verkko- ja tietoturvavirastosta (ENISA) ja asetuksen (EY) N:o 460/2004 kumoamisesta.

3 Direktiivi (EU) 2016/1148 toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa.

4 Komission tiedonanto Euroopan kyberresilienssijärjestelmän vahvistamisesta sekä kilpailukykyisen ja innovatiivisen kyberturvallisuustoimialan tukemisesta, COM/2016/0410 final.

sähköiset terveyspalvelut tai teollisuusautomaation ohjausjärjestelmät (IACS), tulevat yleisempään käyttöön.

Nämä poliittiset toimenpiteet ja esitykset saivat lisävahvistuksen vuonna 2016 annetuissa **neuvoston päätelmissä,** joissa todettiin, että ”kyberuhkat ja haavoittuvuudet muuttuvat ja kasvavat, mikä edellyttää jatkuvaa ja tiiviimpää yhteistyötä erityisesti laajamittaisten rajatylittävien kyberturvallisuuspoikkeamien käsittelemiseksi”. Päätelmissä vahvistettiin, että ”ENISA-asetus on EU:n kyberresilienssikehyksen keskeisimpiä elementtejä”[5], ja kehotettiin komissiota ryhtymään lisätoimiin sertifiointikysymyksessä Euroopan tasolla.

Sertifiointijärjestelmän perustaminen edellyttäisi asianmukaisen hallintojärjestelmän perustamista EU:n tasolla, mihin sisältyisi riippumattoman EU:n viraston tarjoama perusteellinen asiantuntemus. Tässä ehdotuksessa katsotaan, että ENISAlle lankeaa kyberturvallisuusasioiden toimivaltaisena EU-tason elimenä luonnostaan tällainen rooli toimia kansallisten toimivaltaisten elinten yhteistahona ja koordinoida niiden työtä sertifioinnin alalla.

Toukokuussa 2017 julkaisemassaan digitaalisten sisämarkkinoiden strategian väliarvioinnissa komissio täsmensi, että se aikoo tarkastella uudelleen ENISAn toimeksiantoa syyskuuhun 2017 mennessä. Tarkoituksena on määritellä sen roolia muuttuneessa kyberturvallisuuden toimintaympäristössä ja kehittää kyberturvallisuuden standardeihin, sertifiointiin ja merkintöihin kohdistuvia toimenpiteitä, jotta tieto- ja viestintätekniikkaan perustuvien järjestelmien, kuten verkkoon liitettyjen esineiden, kyberturvallisuutta voidaan parantaa[6]. **Eurooppa-neuvoston päätelmissä** kesäkuulta 2017[7] kannatettiin komission aikomusta tarkastella uudelleen kyberturvallisuusstrategiaa syyskuuhun mennessä ja ehdottaa uusia kohdennettuja toimia ennen vuoden 2017 loppua.

Ehdotettu asetus sisältää kattavan joukon toimenpiteitä, jotka perustuvat aiempiin toimiin ja edistävät toisiaan vahvistavia erityistavoitteita

- lisätä jäsenvaltioiden ja yritysten **valmiuksia ja varautumiskykyä**,
- parantaa **yhteistyötä ja koordinointia** jäsenvaltioiden ja EU:n toimielinten, virastojen ja elinten välillä,
- lisätä **EU-tason valmiuksia täydentää jäsenvaltioiden toimia** erityisesti rajat ylittävien kyberkriisien yhteydessä,
- lisätä kansalaisten ja yritysten **tietoisuutta** kyberturvallisuuteen liittyvistä kysymyksistä,
- lisätä yleistä **avoimuutta tieto- ja viestintäteknisten tuotteiden ja palvelujen kyberturvallisuuden varmistuksessa**[8], jotta voidaan lisätä luottamusta digitaalisiin sisämarkkinoihin ja digitaalisiin innovaatioihin, ja

---

5 Neuvoston päätelmät Euroopan kyberresilienssijärjestelmän vahvistamisesta sekä kilpailukykyisen ja innovatiivisen kyberturvallisuustoimialan tukemisesta, 15.11.2016.

6 Komission tiedonanto digitaalisten sisämarkkinoiden strategian täytäntöönpanon väliarvioinnista, COM(2017) 228.

7 Eurooppa-neuvoston istunto 22. ja 23.6.2017, päätelmät EUCO 8/17.

8 Avoimuudella kyberturvallisuuden varmistuksessa tarkoitetaan sitä, että käyttäjät saavat kyberturvallisuusominaisuuksista riittävät tiedot, joiden avulla käyttäjät voivat objektiivisesti määrittää tietyn tieto- ja viestintäteknisen tuotteen, palvelun tai prosessin turvallisuustason.

- välttää **hajanaisuutta sertifiointijärjestelmissä** ja niihin liittyvissä turvallisuusvaatimuksissa ja arviointiperusteissa jäsenvaltioissa ja eri aloilla.

Perustelujen seuraavassa osassa aloitetta perustellaan tarkastelemalla lähemmin ENISAn ja kyberturvallisuussertifioinnin osalta ehdotettuja toimia.

ENISA

ENISA toimii osaamiskeskuksena, jonka tehtävänä on tehostaa verkko- ja tietoturvaa unionissa ja tukea valmiuksien kehittämistä jäsenvaltioissa.

ENISA perustettiin vuonna 2004[9] tarkoituksenaan edistää yleistä tavoitetta varmistaa verkko- ja tietoturvan korkea taso EU:ssa. Vuonna 2013 virastolle annettiin asetuksella (EU) N:o 526/2013 jatkomandaatti seitsemäksi vuodeksi vuoteen 2020 saakka. Virasto sijaitsee Kreikassa. Hallinnollinen toimipaikka on Iráklion (Kreeta). Ydintoiminnot ovat Ateenassa.

ENISA on pieni virasto, jonka budjetti ja henkilöstö jäävät määrällisesti vähäisiksi verrattuna muihin EU:n virastoihin. Sen toimikausi on määräaikainen.

ENISA tukee Euroopan unionin toimielimiä, jäsenvaltioita ja yritysmaailmaa **verkko- ja tietoturvaongelmiin puuttumisessa ja reagoimisessa**. Erityisesti sen tehtävänä on pyrkiä **ehkäisemään verkko- ja tietoturvaongelmat**. Tätä varten se huolehtii eri toimista viidellä sen strategiassa[10] määritellyllä osa-alueella:

- asiantuntemus: tiedon ja asiantuntemuksen antaminen keskeisissä verkko- ja tietoturvakysymyksissä
- politiikka: tuki politiikanteolle ja politiikan täytäntöönpanolle unionissa
- valmiudet: tuki valmiuksien kehittämiselle kaikkialla unionissa (esim. koulutuksen, suositusten ja tietoisuuden lisäämisen avulla)
- yhteisöä palveleva toiminta: verkko- ja tietoturvayhteisön tukeminen (esim. tuki tietoturvaloukkauksiin ja niiden ennaltaehkäisyyn keskittyville ryhmille (CERT) ja yleiseurooppalaisten kyberharjoitusten koordinointi)
- toimintaedellytysten luominen (esim. sidosryhmien kanssa ja kansainvälisten suhteiden kautta).

Verkko- ja tietoturvadirektiivistä neuvoteltaessa EU:n lainsäätäjät päättivät antaa ENISAlle keskeisiä tehtäviä direktiivin täytäntöönpanossa. Erityisesti virasto tarjoaa sihteeristöpalvelut CSIRT-verkostolle (joka on perustettu edistämään yksittäisiin kyberturvallisuuspoikkeamiin kohdennettua nopeaa operatiivista yhteistyötä jäsenvaltioiden välillä sekä tietojen vaihtamista riskeistä). Viraston tehtävänä on myös avustaa verkko- ja tietoturvadirektiivin yhteistyöryhmää sen tehtävien suorittamisessa. Lisäksi direktiivi velvoittaa ENISAn avustamaan jäsenvaltioita ja komissiota tarjoamalla asiantuntemusta ja neuvontaa ja helpottamalla parhaiden käytäntöjen vaihtoa.

Komissio on ENISA-asetuksen mukaisesti tehnyt virastosta arvioinnin, johon on sisältynyt riippumaton tutkimus ja julkinen kuuleminen. Arvioinnissa tarkasteltiin viraston merkityksellisyyttä, vaikuttavuutta, toimivuutta ja tehokkuutta sekä sen toiminnan johdonmukaisuutta ja EU-tason lisäarvoa viraston suorituskyvyn, hallinnon, sisäisen organisaatiorakenteen ja työskentelytapojen suhteen vuosina 2013–2016.

---

9 Euroopan parlamentin ja neuvoston asetus (EY) N:o 460/2004, annettu 10 päivänä maaliskuuta 2004, Euroopan verkko- ja tietoturvaviraston perustamisesta, EUVL L 77, 13.3.2004, s. 1.

10 https://www.enisa.europa.eu/publications/corporate/enisa-strategy

Vastaajien enemmistö[11] (74 %) antoi julkisessa kuulemisessa myönteisen arvion ENISAn yleisestä suorituskyvystä. Enemmistö vastaajista katsoi ENISAn myös saavuttavan eri tavoitteensa (vähintään 63 % kunkin tavoitteen osalta). ENISAn palveluja ja tuotteita käyttää säännöllisesti (kuukausittain tai sitä useammin) lähes puolet vastaajista (46 %). Niitä pidetään arvossa, koska ne tulevat EU:n tason elimeltä (83 %) ja ovat laadukkaita (62 %).

Suuri enemmistö (88 %) vastaajista kuitenkin piti nykyisiä EU:n tasolla käytettävissä olevia välineitä ja mekanismeja riittämättöminä tai vain osittain soveltuvina vastaamaan kyberturvallisuuden nykyisiin haasteisiin. Samoin suuri enemmistö vastaajista (98 %) katsoi, että jonkin EU:n elimen olisi vastattava näihin tarpeisiin, ja näistä elimistä ENISAa piti oikeana organisaationa 99 prosenttia vastaajista. Lisäksi 67,5 prosenttia vastanneista katsoi, että ENISAlla voisi olla rooli luotaessa yhdenmukaistettuja puitteita tietotekniikkatuotteiden ja -palvelujen turvallisuussertifioinnille.

Yleisessä arvioinnissa (joka perustui julkisen kuulemisen lisäksi myös haastatteluihin, kohdennettuihin lisäkyselyihin ja työryhmätapaamisiin) tehtiin seuraavat päätelmät:

- ENISAn tavoitteet ovat edelleen ajankohtaisia. Ottaen huomioon tekniikan nopea kehitys ja kehittyvät uhat sekä kyberturvallisuuteen liittyvät kasvavat maailmanlaajuiset riskit EU:ssa on olemassa selkeä tarve edistää ja lujittaa edelleen korkean tason teknistä asiantuntemusta kyberturvallisuuteen liittyvissä kysymyksissä. Jäsenvaltioissa on tarpeen kehittää valmiuksia ymmärtää ja torjua uhkia, ja sidosryhmien on tarpeen toimia yhteistyössä eri temaattisten alojen ja instituutioiden välisesti.
- Rajoitetuista määrärahoistaan huolimatta virasto on ollut operatiivisesti tehokas resurssiensa käytössä ja tehtäviensä täytäntöönpanossa. Sijainti sekä Ateenassa että Iráklionissa on kuitenkin myös lisännyt hallinnollisia kustannuksia.
- Tehokkuutta tarkastellen ENISA on saavuttanut tavoitteensa osittain. Virasto on onnistuneesti kyennyt osaltaan parantamaan verkko- ja tietoturvallisuutta Euroopassa tukemalla valmiuksien kehittämistä 28 jäsenvaltiossa[12], tehostamalla jäsenvaltioiden ja verkko- ja tietoturvan sidosryhmien välistä yhteistyötä, tarjoamalla käyttöön asiantuntemusta sekä tukemalla yhteisöjen ja politiikan kehittämistä. Kaiken kaikkiaan ENISA on keskittynyt huolellisesti työohjelmansa täytäntöönpanoon ja toiminut luotettavana kumppanina sidosryhmilleen alalla, jonka vahva rajat ylittävä merkitys on tunnustettu vasta hiljattain.
- ENISA on kyennyt saamaan aikaan vaikutuksen, ainakin jossain määrin, verkko- ja tietoturvan laajalla toimintasaralla, mutta se ei ole täysin onnistunut kehittämään

[11] Kuulemiseen vastasi 90 sidosryhmää 19 jäsenvaltiosta (vastauksia saatiin 88 ja kannanottopapereita 2). Mukana oli kansallisia viranomaisia 15 jäsenvaltiosta sekä 8 kattojärjestöä, jotka edustavat merkittävää määrää eurooppalaisia yrityksiä.

[12] Julkiseen kuulemiseen vastanneita pyydettiin esittämään mielipiteensä ENISAn tärkeimmistä saavutuksista vuosina 2013–2016. Vastaajat kaikista ryhmistä (yhteensä 55, joista 13 kansallisia viranomaisia, 20 yksityiseltä sektorilta ja 22 ”muuta” vastaajaa) näkivät ENISAn tärkeimpinä saavutuksina seuraavat: 1) Cyber Europe -harjoitusten koordinointi, 2) tuen antaminen CERT-ryhmille ja CSIRT-toimijoille työpajojen ja koulutuksen avulla sekä edistämällä koordinointia ja tiedonvaihtoa, 3) ENISAn julkaisut (mm. ohjeet ja suositukset, kyberuhkaympäristöä koskevat raportit ja strategiat turvapoikkeamien raportointia ja kriisinhallintaa varten), joista katsottiin olevan hyötyä kansallisten turvallisuuskehysten luomiselle ja päivittämiselle sekä referensseinä poliittisille päättäjille ja kyberturvallisuuden toimijoille, 4) avustaminen verkko- ja tietoturvadirektiivin tukitoiminnassa ja 5) toimet tietoisuuden lisäämiseksi kyberturvallisuudesta (kyberturvallisuuskuukausi).

vahvaa brändiä ja riittävää näkyvyyttä alan ykkösosaamiskeskuksena Euroopassa. Tämä selittyy ENISAn laajalla toimeksiannolla, jonka tueksi sille ei ole annettu riittäviä resursseja vastaavassa suhteessa. Lisäksi ENISA on ainoa EU:n virasto, jonka toimikausi on määräaikainen, mikä rajoittaa sen mahdollisuuksia kehittää pitkän aikavälin visiota ja tukea sidosryhmiään kestävällä tavalla. Tämä on myös ristiriidassa verkko- ja tietoturvadirektiivin säännösten kanssa, joissa ENISAlle annetaan tehtäviä ilman päättymispäivää. Lisäksi arvioinnissa todettiin, että viraston vähäistä vaikutusta osittain selittävät suuri riippuvuus ulkoisesta asiantuntemuksesta sisäisen asiantuntemuksen sijasta sekä vaikeudet rekrytoida ja pitää palveluksessa erikoistunutta henkilöstöä.

- Arvioinnin keskeisiin päätelmiin kuuluu myös se, että ENISAn lisäarvo johtuu pääasiallisesti viraston mahdollisuuksista tehostaa yhteistyötä lähinnä jäsenvaltioiden välillä ja erityisesti kyseeseen tulevien verkko- ja tietoturvayhteisöjen kanssa (varsinkin CSIRT-toimijoiden välillä). Mikään muu toimija EU:n tasolla ei tue näin laajaa kirjoa verkko- ja tietoturva-alan sidosryhmiä. Koska ENISAn toimintaa joudutaan kuitenkin priorisoimaan tiukasti, viraston työohjelmaa ohjaavat pääosin jäsenvaltioiden tarpeet. Tämän vuoksi se ei riittävällä tavalla pysty vastaamaan muiden sidosryhmien, erityisesti toimialan, tarpeisiin. Tämä on myös tehnyt viraston toimintatavasta reaktiivisen, kun virasto on täyttänyt keskeisten sidosryhmiensä tarpeita pystymättä laajentamaan vaikutustaan. Näin ollen viraston tuoma lisäarvo vaihteli sidosryhmien eri tarpeiden mukaan ja riippuen siitä, missä määrin virasto pystyi vastaamaan niihin (esim. suuret v. pienet jäsenvaltiot tai jäsenvaltiot v. toimiala).

Yhteenvetona voidaan todeta, että sidosryhmien kuulemisten ja arvioinnin tulokset viittaavat tarpeeseen mukauttaa ENISAn resursseja ja toimeksiantoa, jotta se voisi riittävällä tavalla vastata nykyisiin ja tuleviin haasteisiin.

Näiden havaintojen pohjalta tässä ehdotuksessa tarkistetaan ENISAn tämänhetkistä toimeksiantoa ja määritellään uudelleen sen tehtäviä ja toimintoja, jotta se voisi tuloksekkaasti ja tehokkaasti tukea jäsenvaltioiden, EU:n toimielinten ja muiden sidosryhmien pyrkimyksiä turvallisen kyberavaruuden varmistamiseksi Euroopan unionissa. Ehdotetun uuden toimeksiannon tarkoituksena on antaa virastolle vahvempi ja keskeisempi rooli. Tavoitteena on erityisesti, että se tukee jäsenvaltioita verkko- ja tietoturvadirektiivin täytäntöönpanossa ja yksittäisten uhkien torjumisessa aiempaa aktiivisemmin (operatiiviset valmiudet) ja että siitä tulee jäsenvaltioiden ja komission kyberturvallisuussertifiointia tukeva omaamiskeskus. Tämän ehdotuksen mukaan

- ENISAlle myönnettäisiin pysyvä mandaatti, jonka myötä sen toiminta olisi vakaalla pohjalla tulevaisuudessa. Toimeksiantoa, tavoitteita ja tehtäviä tarkasteltaisiin jatkossakin uudelleen säännöllisesti.
- Ehdotetussa toimeksiannossa täsmennetään ENISAn roolia EU:n kyberturvallisuusvirastona ja EU:n kyberturvallisuusekosysteemin viitekeskuksena, joka toimii tiiviissä yhteistyössä tämän toimintaympäristön kaikkien muiden asiaankuuluvien elinten kanssa.
- Viraston organisaatiota ja hallintoa, jotka saivat arvioinnissa myönteisen arvion, tarkistettaisiin kevyesti erityisesti varmistamalla, että laajemman sidosryhmänyhteisön tarpeet voidaan ottaa paremmin huomioon viraston toiminnassa.

- Toimeksiannon ehdotettu soveltamisala on määritetty lujittamalla niitä osa-alueita, joilla viraston toiminnasta on ollut selvää lisäarvoa, ja lisäämällä sellaisia uusia aloja, joilla tukea tarvitaan uusien poliittisten painopisteiden ja välineiden vuoksi. Jälkimmäisiin kuuluvat erityisesti verkko- ja tietoturvadirektiivi, EU:n kyberturvallisuusstrategian tarkistus, tuleva EU:n kyberturvallisuussuunnitelma kyberkriiseissä tehtävää yhteistyötä varten sekä tieto- ja viestintäteknologian turvallisuussertifiointi.

    - **EU:n politiikan kehittäminen ja täytäntöönpano:** ENISAn tehtäväksi annettaisiin edistää aktiivisesti politiikan kehittämistä verkko- ja tietoturvan alalla sekä muita toimintapoliittisia aloitteita eri aloilla (esim. energia-, liikenne- ja finanssipolitiikassa) silloin kun niihin liittyy kyberturvallisuustekijöitä. Tätä varten sillä olisi vahva neuvoa-antava rooli, jonka se voisi täyttää antamalla riippumattomia lausuntoja ja huolehtimalla valmistelutyöstä politiikan ja lainsäädännön kehittämistä ja päivittämistä varten. ENISA myös tukisi EU:n politiikkaa ja lainsäädäntöä sähköisen viestinnän, sähköisen tunnistamisen ja luottamuspalvelujen aloilla tavoitteena parantaa kyberturvallisuustasoa. Täytäntöönpanovaiheessa ENISA avustaisi – erityisesti verkko- ja tietoturvadirektiivin yhteistyöryhmän puitteissa – jäsenvaltioita johdonmukaisen lähestymistavan kehittämisessä verkko- ja tietoturvadirektiivin täytäntöönpanoon eri maiden ja alojen välisesti sekä muilla asiaankuuluvilla politiikan ja lainsäädännön lohkoilla. Politiikan ja lainsäädännön säännöllisen uudelleentarkastelun tukemiseksi kyberturvallisuuden alalla ENISA myös raportoisi säännöllisesti EU:n lainsäädännön täytäntöönpanon tilasta.

    - **Valmiuksien kehittäminen:** ENISAn tehtävänä olisi osaltaan parantaa EU:n ja kansallisten viranomaisten valmiuksia ja asiantuntemusta muun muassa turvallisuuspoikkeamiin reagoimisessa ja kyberturvallisuuteen liittyvien sääntelytoimenpiteiden valvonnassa. Viraston tehtävänä olisi myös edistää tietojen jakamisen ja analysoinnin alakohtaisten keskusten (ISAC) perustamista eri aloilla tarjoamalla käyttöön parhaita käytäntöjä ja ohjeita saatavilla olevista välineistä ja menettelyistä sekä asianmukaisista tavoista ratkaista tietojen jakamiseen liittyviä sääntelykysymyksiä.

    - **Tietämys, tiedotus ja tietoisuuden lisääminen:** ENISAsta tulisi EU:n tietokeskus. Tämä merkitsisi parhaiden käytäntöjen ja aloitteiden edistämistä ja jakamista koko EU:ssa kokoamalla yhteen tietoa kyberturvallisuudesta EU:n toimielimiltä, virastoilta ja elimiltä sekä kansallisilta instituutioilta, virastoilta ja laitoksilta. Virasto antaisi myös käyttöön neuvoja, ohjeita ja hyviä käytäntöjä elintärkeiden infrastruktuurien turvallisuutta koskevissa kysymyksissä. Merkittävien rajatylittävien kyberturvallisuuspoikkeamien tapauksessa ENISA laatisi myös jälkiraportteja ohjeistuksen antamiseksi yrityksille ja kansalaisille eri puolilla EU:ta. Tähän työsarkaan sisältyisi myös säännöllisten tiedotuskampanjoiden järjestäminen koordinoiden toimintaa jäsenvaltioiden viranomaisten kanssa.

    - **Markkinoihin liittyvät tehtävät (standardointi ja turvallisuussertifiointi):** ENISAn tehtäväksi tulisi toimintoja, jotka erityisesti tukevat sisämarkkinoita. Se toimisi kyberturvallisuuteen keskittyvänä ”markkinoiden seurantakeskuksena” tehtävänään analysoida kyberturvallisuusmarkkinoiden kehityssuuntauksia, jotta kysyntä ja tarjonta saataisiin vastaamaan paremmin

toisiaan, sekä tukea EU:n politiikan kehittämistä tieto- ja viestintätekniikan standardoinnin ja kyberturvallisuussertifioinnin aloilla. Erityisesti standardointiin liittyen se helpottaisi kyberturvallisuusstandardien laatimista ja käyttöönottoa. ENISA huolehtisi myös tehtävistä, jotka sisältyvät tulevaan sertifiointia varten kaavailtuun kehykseen (ks. jäljempänä).

- **Tutkimus ja innovointi:** ENISA tarjoaisi käyttöön asiantuntemusta neuvomalla EU:n ja kansallisia viranomaisia tutkimuksen ja kehittämisen painopisteistä, muun muassa sopimusperusteisen julkisen ja yksityisen sektorin kyberturvallisuuskumppanuuden puitteissa. ENISAn tutkimusneuvonta tarjoaisi aineksia uuteen Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskukseen seuraavan monivuotisen rahoituskehyksen puitteissa. ENISA myös osallistuisi komission pyynnöstä EU:n tutkimuksen ja innovoinnin rahoitusohjelmien täytäntöönpanoon.
- **Operatiivinen yhteistyö ja kriisinhallinta:** Tämän työn lähtökohtana olisi nykyisten ennalta ehkäisevien operatiivisten valmiuksien vahvistaminen – erityisesti yleiseurooppalaisten kyberturvallisuusharjoitusten (Cyber Europe) tehostaminen pitämällä ne vuosittain. Virastolla olisi myös tukijan rooli operatiivisessa yhteistyössä CSIRT-verkoston sihteeristönä (verkko- ja tietoturvadirektiivin säännösten mukaisesti), joka varmistaisi muun muassa CSIRT-verkoston tietoteknisen infrastruktuurin ja viestintäkanavien toimivuuden. Tämä edellyttäisi jäsenneltyä yhteistyötä CERT-EU:n, Euroopan kyberrikostorjuntakeskuksen (EC3) ja muiden asiaankuuluvien EU:n elinten kanssa. CERT-EU:n kanssa tehtävä jäsennelty yhteistyö, jossa osapuolet ovat fyysisesti lähellä toisiaan, tarjoaisi käyttöön toiminnon teknisen avun antamiseksi merkittävien turvallisuuspoikkeamien tapauksessa ja niiden analysoinnin tueksi. Jäsenvaltiot saisivat pyynnöstä apua poikkeamien käsittelyyn ja tukea heikkouksien, artefaktien ja poikkeamien analysointiin, jotta ne voisivat vahvistaa omia ennaltaehkäiseviä ja reagointivalmiuksiaan.
- ENISAlla olisi tehtävä myös **EU:n kyberturvallisuussuunnitelmassa**. Suunnitelmassa, joka esitetään osana tätä pakettia, komissio antaa jäsenvaltioille suosituksensa koordinoiduista toimista laajamittaisissa rajatylittävissä kyberturvallisuuspoikkeamissa ja -kriiseissä EU:n tasolla[13]. ENISA helpottaisi yksittäisten jäsenvaltioiden välistä yhteistyötä hätätilanteisiin vastaamisessa analysoimalla ja kokoamalla yhteen kansallisia tilannekatsauksia jäsenvaltioiden ja muiden tahojen vapaaehtoisesti viraston käyttöön antamien tietojen pohjalta.

- **Tieto- ja viestintätekniikan tuotteiden ja palvelujen kyberturvallisuussertifiointi**

Tieto- ja viestintätekniikan tuotteisiin ja palveluihin on luottamuksen ja turvallisuuden luomiseksi ja ylläpitämiseksi tarpeen sisällyttää suoraan turvaominaisuudet varhaisessa vaiheessa niiden teknistä suunnittelua ja kehittämistä (sisäänrakennettu turvallisuus). Lisäksi

[13] Suunnitelmaa sovelletaan kyberturvallisuuspoikkeamiin, joiden aiheuttamat häiriöt ylittävät yksittäisen jäsenvaltion käsittelyvalmiudet tai jotka koskevat kahta tai useampaa jäsenvaltiota ja ovat vaikutuksiltaan tai poliittiselta merkitykseltään niin laajoja ja merkittäviä, että ne edellyttävät pikaista poliittista koordinointia ja reagointia unionin poliittisella tasolla.

asiakkaiden ja käyttäjien on voitava varmistua hankkimiensa tuotteiden ja palvelujen tietoturvavarmistustasosta.

Sertifioinnilla, jossa riippumaton ja akkreditoitu elin arvioi virallisesti tuotteet, palvelut ja prosessit määriteltyjä kriteereitä ja standardeja vasten ja jossa annetaan sertifikaatti vaatimustenmukaisuudesta, on tärkeä merkitys pyrittäessä lisäämään tuotteiden ja palvelujen turvallisuutta ja niitä kohtaan tunnettua luottamusta. Vaikka turvallisuuden arvioinnit ovat luonteeltaan varsin teknisiä, sertifiointi palvelee kuitenkin sitä, että ostajat ja käyttäjät saavat informaatiota ja voivat vakuuttua tieto- ja viestintäteknisten tuotteiden ja palvelujen turvallisuusominaisuuksista. Kuten edellä mainitaan, tämä koskee erityisesti uusia järjestelmiä, joissa hyödynnetään laajasti digitaaliteknologiaa ja jotka edellyttävät korkeatasoista turvallisuutta. Tällaisia ovat esimerkiksi verkkoyhteyksillä varustetut ja automatisoidut autot, sähköiset terveyspalvelut, teollisuusautomaation ohjausjärjestelmät (IACS)[14] ja älykkäät verkot.

Tieto- ja viestintätekniikan tuotteiden kyberturvallisuussertifioinnin tilanne on tällä hetkellä melko hajanainen EU:ssa. Alan kansainvälisiin aloitteisiin kuuluu ns. Common Criteria (CC) -tietoturvastandardi (Common Criteria (CC) for Information Technology Security Evaluation, ISO 15408), joka on tietokoneiden turvallisuusarviointiin sovellettava kansainvälinen standardi. Se perustuu kolmannen osapuolen arviointiin ja käsittää seitsemän varmuustasoa (Evaluation Assurance Level, EAL). CC-standardi ja siihen liittyvät yhteiset CEM-menetelmät (Common Methodology for Information Technology Security Evaluation) muodostavat teknisen perustan kansainväliselle CCRA-järjestelylle (Common Criteria Recognition Arrangement), jolla varmistetaan, että CC-sertifikaatit ovat kaikkien CCRA-järjestelyn allekirjoittajien tunnustamia. Nykyisen CCRA-järjestelyn mukaan arvioinnit tunnustetaan vastavuoroisesti kuitenkin vain EAL 2 -varmuustasolle asti. Lisäksi vain 13 jäsenvaltiota on allekirjoittanut järjestelyn.

Sertifiointiviranomaiset 12 jäsenvaltiosta ovat tehneet vastavuoroista tunnustamista koskevan sopimuksen koskien sertifikaatteja, jotka on myönnetty sopimuksen mukaisesti yhteisten CC-kriteerien perusteella[15]. Lisäksi jäsenvaltioissa on tehty tai tekeillä muita tieto- ja viestintätekniikan sertifiointiin liittyviä aloitteita. Vaikka nämä ovatkin tärkeitä, ne uhkaavat johtaa hajanaisuuteen markkinoilla ja yhteentoimivuusongelmiin. Yritys voi sen vuoksi joutua läpäisemään useita sertifiointimenettelyjä eri jäsenvaltioissa, jotta se voisi tarjota tuotettaan useilla eri markkinoilla. Esimerkiksi älymittareiden valmistaja, joka haluaa myydä tuotteitaan kolmessa jäsenvaltiossa (esim. Saksassa, Ranskassa ja Yhdistyneessä kuningaskunnassa), joutuu noudattamaan tällä hetkellä kolmen eri sertifiointijärjestelmän vaatimuksia. Nämä ovat Commercial Product Assurance (CPA) Yhdistyneessä kuningaskunnassa, Certification de Sécurité de Premier Niveau (CSPN) Ranskassa ja erityinen CC-kriteereihin perustuva suojausprofiili Saksassa.

Tämä tilanne lisää kustannuksia ja merkitsee huomattavaa hallinnollista rasitetta niille yrityksille, jotka toimivat useissa jäsenvaltioissa. Sertifioinnin kustannukset voivat vaihdella

---

[14] Komission pääosasto DG JRC on julkaissut raportin, jossa esitetään alustavat yhteiset eurooppalaiset vaatimukset ja yleiset suuntaviivat liittyen IACS-komponenttien kyberturvallisuussertifiointiin. Raportti on saatavilla osoitteesta https://erncip-project.jrc.ec.europa.eu/documents/introduction-european-iacs-components-cybersecurity-certification-framework-iccf

[15] Johtavien virkamiesten tietoturvallisuusryhmään (SOGIS) kuuluu 12 EU:n jäsenvaltiota sekä Norja. Se on kehittänyt suojausprofiileja rajatulle määrälle tuotteita, kuten digitaaliselle allekirjoitukselle, digitaaliselle ajopiirturille ja älykorteille. Osallistujat työskentelevät yhdessä koordinoidakseen CC-suojausprofiilien standardointia ja suojausprofiilien kehittämistä. Jäsenvaltiot pyytävät usein SOGIS-sertifiointia kansallisiin julkisia hankintoja koskeviin tarjouskilpailuihin.

paljon riippuen kyseessä olevasta tuotteesta tai palvelusta, halutusta varmuustasosta ja/tai muista tekijöistä. Sertifioinnista yrityksille aiheutuvat kustannukset ovat kuitenkin yleensä varsin huomattavat. Esimerkiksi BSI:n ”Smart Meter Gateway” -sertifikaatin kustannukset nousevat yli miljoonaan euroon (korkein testi- ja varmuustaso koskien yksittäisen tuotteen lisäksi myös koko ympäröivää infrastruktuuria). Älymittareiden sertifioinnin kustannukset ovat Yhdistyneessä kuningaskunnassa lähes 150 000 euroa ja Ranskassa samaa luokkaa, 150 000 euroa tai enemmän.

Keskeiset julkiset ja yksityiset sidosryhmät myönsivät, että ilman EU:n laajuista kyberturvallisuuden sertifiointijärjestelmää yritysten on monissa olosuhteissa hankittava erillinen sertifiointi kussakin jäsenvaltiossa, mikä johtaa markkinoiden hajanaisuuteen. Mikä tärkeintä, viestintäteknisiä tuotteita ja palveluja koskevan EU:n yhdenmukaistamislainsäädännön puuttuessa erot jäsenvaltioiden kyberturvallisuuden sertifiointistandardeissa ja -käytännöissä voivat luoda EU:hun käytännössä 28 erillistä markkina-aluetta, joista kullakin on omat tekniset vaatimuksena, testausmenetelmänsä ja sertifiointimenettelynsä. Nämä toisistaan poikkeavat kansalliset toimintamallit voivat aiheuttaa – jollei riittäviin toimiin ryhdytä EU:n tasolla – merkittävän takaiskun digitaalisten sisämarkkinoiden toteutumiselle, sillä ne hidastavat kasvuun ja työllisyyteen kohdistuvia myönteisiä sisämarkkinavaikutuksia tai estävät niitä toteutumasta.

Edellä selostetun kehityksen vuoksi esitetään, että ehdotettavalla asetuksella luodaan eurooppalainen kehys tieto- ja viestintätekniikan tuotteiden ja palvelujen kyberturvallisuussertifioinnille (”**sertifiointikehys**”) ja määritetään ENISAn keskeiset toiminnot ja tehtävät kyberturvallisuussertifioinnin alalla. Asetusehdotuksessa vahvistetaan yleiset puitteet säännöille, joita Euroopan kyberturvallisuuden sertifiointijärjestelmiin on määrä soveltaa. Ehdotuksella ei otettaisi käyttöön sellaisenaan toiminnallisia sertifiointijärjestelmiä, vaan luotaisiin yleinen järjestelmä (kehys) yksittäisten sertifiointijärjestelmien perustamiseksi erityisille tieto- ja viestintätekniikan tuotteille tai palveluille (jäljempänä ”eurooppalaiset kyberturvallisuuden sertifiointijärjestelmät”). Sertifiointikehyksen mukaisesti perustetuissa eurooppalaisissa kyberturvallisuuden sertifiointijärjestelmissä myönnetyt sertifikaatit olisivat voimassa ja tunnustettuja kaikissa jäsenvaltioissa, jolloin voitaisiin päästä markkinoiden nykyisestä hajanaisuudesta.

Yleisenä tavoitteena eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä on antaa vahvistus siitä, että tällaisen järjestelmän mukaisesti sertifioidut tieto- ja viestintätekniset tuotteet ja palvelut ovat niille määriteltyjen kyberturvallisuusvaatimusten mukaisia. Tähän sisältyisi esimerkiksi niiden kyky suojella (tallennettua, siirrettyä tai muuten käsiteltyä) dataa vahingossa tapahtuvalta tai luvattomalta tallentamiselta, käsittelyltä, käytöltä, paljastamiselta, tuhoamiselta, tahattomalta katoamiselta tai muuttamiselta. EU:n kyberturvallisuuden sertifiointijärjestelmissä käytettäisiin olemassa olevia standardeja teknisissä vaatimuksissa ja arviointimenettelyissä, joita tuotteissa on noudatettava, ilman että laadittaisiin teknisiä standardeja itse[16]. Esimerkiksi EU:n laajuinen sertifiointi vaikkapa älykorteille, joita testataan parhaillaan kansainvälisten CC-standardien pohjalta monenvälisessä SOGIS-järjestelmässä (edellä kuvatulla tavalla), merkitsisi sitä, että kyseisen järjestelmä tulisi päteväksi koko EU:n alueella.

Eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien suunnittelussa huomioon otettavien turvallisuustavoitteiden lisäksi ehdotuksessa esitetään myös, mikä tulisi olla

[16] Eurooppalaisten standardien tapauksessa tämä tapahtuu eurooppalaisten standardointiorganisaatioiden kautta ja Euroopan komission hyväksymänä ja julkaisemana *Euroopan unionin virallisessa lehdessä* (ks. asetus 1025/2012).

tällaisten järjestelmien vähimmäissisältö. Näissä järjestelmissä on määriteltävä muun muassa joukko erityistekijöitä kyberturvallisuussertifioinnin soveltamisalan ja kohteen määrittelemiseksi. Tähän sisältyvät soveltamisalaan kuuluvien tuotteiden ja palvelujen luokkien määrittely, yksityiskohtainen eritelmä kyberturvallisuusvaatimuksista (esim. viittaamalla sovellettaviin standardeihin tai teknisiin eritelmiin), erityiset arviointiperusteet ja -menetelmät sekä varmuustaso, joka niiden avulla on määrä varmistaa (perustaso, korotettu tai korkea).

Eurooppalaiset kyberturvallisuuden sertifiointijärjestelmät valmistelee ENISA, jota avustaa ja neuvoo Euroopan kyberturvallisuuden sertifiointiryhmä tiiviissä yhteistyössä sen kanssa (ks. jäljempänä), ja ne hyväksyy komissio täytäntöönpanosäädöksillä. Kun kyberturvallisuuden sertifiointijärjestelmän tarve on tunnistettu, komissio pyytää ENISAa valmistelemaan järjestelmän erityisiä tieto- ja viestintäteknisiä tuotteita tai palveluja varten. ENISA työskentelee järjestelmän parissa läheisessä yhteistyössä kansallisten sertifiointialan valvontaviranomaisten kanssa, jotka ovat edustettuina sertifiointiryhmässä. Jäsenvaltiot tai sertifiointiryhmä voivat ehdottaa komissiolle, että se pyytäisi ENISAa laatimaan jonkin yksittäisen järjestelmän.

Sertifiointi voi olla erittäin kallis prosessi, mikä vuorostaan voi johtaa korkeampiin hintoihin asiakkaille ja kuluttajille. Sertifiointitarve voi myös vaihdella paljon riippuen tuotteiden ja palvelujen käyttöyhteydestä ja teknologian nopeasta muutostahdista. Eurooppalaisen kyberturvallisuussertifioinnin käytön tulisi sen vuoksi edelleen olla vapaaehtoista, jollei toisin säädetä unionin lainsäädännössä, jossa määritetään turvallisuusvaatimukset tieto- ja viestintätekniikan tuotteille ja palveluille.

Jotta voidaan varmistaa yhdenmukainen lähestymistapa ja välttää hajanaisuus, kansallisia kyberturvallisuuden sertifiointijärjestelmiä tai -menettelyjä, joiden kattamat tieto- ja viestintätekniikan tuotteet ja palvelut kuuluvat jonkin eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän soveltamisalaan, ei enää sovelleta alkaen päivästä, joka vahvistetaan järjestelmästä tehtävässä täytäntöönpanosäädöksessä. Jäsenvaltiot eivät myöskään saisi ottaa käyttöön uusia kansallisia kyberturvallisuuden sertifiointijärjestelmiä sellaisille tieto- ja viestintätekniikan tuotteille ja palveluille, jotka kuuluvat jonkin voimassa olevan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän soveltamisalaan.

Kun eurooppalainen kyberturvallisuuden sertifiointijärjestelmä on hyväksytty, tieto- ja viestintäteknisten tuotteiden valmistajat tai tieto- ja viestintäteknisten palvelujen tarjoajat voivat jättää tuotteidensa tai palvelujensa sertifiointia koskevan hakemuksen valitsemalleen vaatimustenmukaisuuden arviointilaitokselle. Vaatimustenmukaisuuden arviointilaitosten olisi saatava akkreditointi akkreditointielimeltä, jos ne täyttävät tietyt erityiset vaatimukset. Akkreditointi myönnetään enintään viideksi vuodeksi, ja se voidaan uusia samoin edellytyksin, jos vaatimustenmukaisuuden arviointilaitos täyttää edelleen vaatimukset. Akkreditointielin peruuttaa vaatimustenmukaisuuden arviointilaitoksen akkreditoinnin, jos akkreditoinnin edellytykset eivät täyty tai eivät enää täyty tai jos vaatimustenmukaisuuden arviointilaitoksen toiminta rikkoo tämän asetuksen säännöksiä.

Ehdotuksen mukaan seuranta-, valvonta- ja täytäntöönpanotehtävät kuuluvat jäsenvaltioille ja jäsenvaltioilla on oltava yksi sertifioinnin valvontaviranomainen. Tämän viranomaisen tehtävänä on valvoa sitä, ovatko sen alueelle sijoittautuneet vaatimustenmukaisuuden arviointilaitokset ja niiden myöntämät sertifikaatit tämän asetuksen vaatimusten ja vastaavien eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien vaatimusten mukaisia. Kansallisilla sertifioinnin valvontaviranomaisilla on toimivalta käsitellä luonnollisten henkilöiden tai oikeushenkilöiden tekemät valitukset, jotka liittyvät niiden alueelle sijoittautuneiden vaatimustenmukaisuuden arviointilaitosten myöntämiin sertifikaatteihin. Ne

tutkivat asianmukaisessa määrin valituksen kohteen ja ilmoittavat valituksen tekijälle valituksen etenemisestä ja tutkinnan tuloksista kohtuullisen ajan kuluessa. Ne tekevät yhteistyötä muiden sertifioinnin valvontaviranomaisten tai muiden viranomaisten kanssa esimerkiksi jakamalla tietoa mahdollisista tapauksista, joissa tieto- ja viestintätekniikan tuotteet ja palvelut eivät vastaa tämän asetuksen tai yksittäisten eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien vaatimuksia.

Lisäksi ehdotuksella perustettaisiin Euroopan kyberturvallisuuden sertifiointiryhmä, jäljempänä ’sertifiointiryhmä’, joka koostuu kaikkien jäsenvaltioiden kansallisista sertifioinnin valvontaviranomaisista. Sertifiointiryhmän päätehtävänä on antaa komissiolle neuvoja kyberturvallisuuden sertifiointipolitiikkaan liittyvissä kysymyksissä ja työskennellä ENISAn kanssa eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien valmistelemiseksi. ENISA avustaa komissiota sertifiointiryhmän sihteeristönä ja pitää yllä ajantasaista julkista luetteloa eurooppalaisessa kyberturvallisuuden sertifiointikehyksessä hyväksytyistä järjestelmistä. ENISA pitää myös yhteyksiä standardointielimiin, jotta voidaan varmistaa hyväksytyissä järjestelmissä käytettävien standardien tarkoituksenmukaisuus ja määritellä osa-alueita, joilla tarvitaan kyberturvallisuusstandardeja.

Eurooppalainen kyberturvallisuuden sertifiointikehys tarjoaa useita etuja kansalaisille ja yrityksille, erityisesti seuraavat:

- EU:n laajuisten kyberturvallisuuden sertifiointijärjestelmien luominen erityisille tuotteille tai palveluille tuo yritysten käyttöön keskitetyn väylän kyberturvallisuussertifiointiin EU:ssa. Sitä käyttävien yritysten tarvitsee sertifioida tuotteensa vain kerran saadakseen sertifikaatin, joka on voimassa kaikissa jäsenvaltioissa. Niiden ei enää tarvitse hankkia tuotteilleen uutta sertifiointia muilta kansallisilta sertifiointilaitoksilta. Tämä vähentää huomattavasti yrityksille aiheutuvia kustannuksia, helpottaa rajatylittävää toimintaa ja siten viime kädessä vähentää ja ehkäisee sisämarkkinoiden hajanaisuutta kyseisten tuotteiden osalta.
- Eurooppalaisista kyberturvallisuuden sertifiointijärjestelmistä tulee ensisijaisia kansallisiin järjestelmiin nähden: tämän säännön nojalla pätee, että eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän hyväksyminen syrjäyttää kaikki olemassa olevat rinnakkaiset kansalliset järjestelmät, jotka koskevat samoja tieto- ja viestintätekniikan tuotteita tai palveluja tietyllä varmuustasolla. Tämä tuo selkeyttä vähentämällä nykyisiä päällekkäisiä ja mahdollisesti keskenään ristiriitaisia kansallisia kyberturvallisuuden sertifiointijärjestelmiä.
- Tämä ehdotus tukee ja täydentää verkko- ja tietoturvadirektiivin täytäntöönpanoa tarjoamalla yrityksille, joihin direktiiviä sovelletaan, hyödyllisen välineen osoittaa, että ne noudattavat direktiivin vaatimuksia koko unionissa. Uusien kyberturvallisuuden sertifiointijärjestelmien kehittämisessä komissio ja ENISA tulevat kiinnittämään erityistä huomiota tarpeeseen varmistaa, että verkko- ja tietoturvadirektiivin vaatimukset otetaan huomioon näissä järjestelmissä.
- Ehdotus tukee ja helpottaa eurooppalaisen kyberturvallisuuspolitiikan kehittämistä yhdenmukaistamalla ehtoja ja sisältövaatimuksia, joita tieto- ja viestintätekniikan tuotteiden ja palvelujen kyberturvallisuussertifiointiin sovelletaan EU:ssa. Eurooppalaisissa kyberturvallisuuden sertifiointijärjestelmissä viitataan yhteisiin arviointi- ja testausmenetelmien standardeihin tai kriteereihin. Tämä edistää merkittävästi, vaikkakin epäsuorasti, yhteisten turvallisuusratkaisujen käyttöönottoa EU:ssa ja sitä kautta myös poistaa esteitä sisämarkkinoiden toiminnalta.

- Sertifiointikehys on suunniteltu siten, että kyberturvallisuuden sertifiointijärjestelmille jää tarvittava joustavuus. Kyberturvallisuustarpeista riippuen tuote tai palvelu voidaan sertifioida ylemmän tai alemman turvallisuustason mukaisesti. Eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien suunnittelussa otetaan huomioon tämä liikkumavara, ja ne tarjoavat näin ollen eri varmuustasoja (eli perustaso, korotettu tai korkea), jolloin niitä voidaan käyttää eri tarkoituksiin ja eri yhteyksissä.
- Kaikkien edellä mainittujen osatekijöiden ansiosta kyberturvallisuussertifioinnista tulee houkuttavampaa yrityksille, koska se tarjoaa käyttöön tehokkaan keinon tieto- ja viestintäteknisten tuotteiden tai palvelujen kyberturvallisuustason ilmaisemiseen. Kun kyberturvallisuussertifioinnista tulee edullisempaa, tehokkaampaa ja taloudellisesti houkuttelevaa, yrityksillä on suuremmat kannustimet hankkia tuotteilleen sertifiointi kyberturvallisuusriskien varalta, mikä edistää parempien kyberturvallisuuskäytäntöjen leviämistä tieto- ja viestintätekniikan tuotteiden ja palvelujen suunnittelussa (sisäänrakennettu kyberturvallisuus).

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

Verkko- ja tietoturvadirektiivi velvoittaa toimijat aloilla, jotka ovat elintärkeitä talouden ja yhteiskunnan kannalta (esim. energia, liikenne, vesihuolto, pankkitoiminta, rahoitusmarkkinoiden infrastruktuurit, terveydenhuolto ja digitaalinen infrastruktuuri), sekä digitaalisen palvelun tarjoajat (esim. hakukoneet, pilvipalvelut ja verkossa toimivat markkinapaikat) toimenpiteisiin turvallisuusriskien hallitsemiseksi asianmukaisesti. Tämän ehdotuksen uudet säännöt täydentävät verkko- ja tietoturvadirektiivin säännöksiä ja varmistavat johdonmukaisuuden niiden kanssa pyrittäessä edelleen kehittämään EU:n kykyä sietää kyberuhkia (kyberresilienssi) parantamalla valmiuksia, yhteistyötä, riskinhallintaa ja kybertietoisuutta.

Lisäksi kyberturvallisuussertifiointia koskevat säännöt antavat käyttöön olennaisen välineen verkko- ja tietoturvadirektiivin kohteena oleville yrityksille, kun ne voivat hankkia tieto- ja viestintätekniikan tuotteilleen ja palveluilleen sertifioinnin kyberturvallisuusriskien varalta käyttämällä kyberturvallisuuden sertifiointijärjestelmiä, jotka ovat päteviä ja jotka tunnustetaan koko EU:n alueella. Ne myös täydentävät eIDAS-asetuksessa[17] ja radiolaitedirektiivissä[18] esitettyjä turvallisuusvaatimuksia.

- **Yhdenmukaisuus unionin muiden politiikkojen kanssa**

Asetuksessa (EU) 2016/679 (**yleinen tietosuoja-asetus**)[19] säädetään sertifiointimekanismeista sekä tietosuojasineteistä ja -merkeistä, joiden tarkoituksena on osoittaa, että rekisterinpitäjät ja

[17] 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.

[18] Euroopan parlamentin ja neuvoston direktiivi 2014/53/EU, annettu 16 päivänä huhtikuuta 2014, radiolaitteiden asettamista saataville markkinoilla koskevan jäsenvaltioiden lainsäädännön yhdenmukaistamisesta ja direktiivin 1999/5/EY kumoamisesta.

[19] Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä 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. 1–88).

henkilötietojen käsittelijät noudattavat kyseistä asetusta käsittelytoimia suorittaessaan. Nyt käsillä oleva asetus ei rajoita tietojenkäsittelytoimien sertifiointia yleisen tietosuoja-asetuksen nojalla, ei myöskään silloin, kun nämä toimet on sisällytetty tuotteisiin ja palveluihin.

Ehdotetulla asetuksella taataan yhteensopivuus akkreditointia ja markkinavalvontaa koskevista vaatimuksista annetun asetuksen 765/2008[20] kanssa viittaamalla kyseisen kehyksen sääntöihin, jotka koskevat kansallisia akkreditointielimiä ja vaatimustenmukaisuuden arviointilaitoksia. Mitä tulee valvontaviranomaisiin, ehdotettu asetus velvoittaa jäsenvaltiot nimeämään kansalliset sertifioinnin valvontaviranomaiset vastaamaan valvonnasta, seurannasta ja sääntöjen täytäntöönpanosta. Kyseiset elimet pidetään erillään asetuksessa 765/2008 tarkoitetuista vaatimustenmukaisuuden arviointilaitoksista.

2. OIKEUSPERUSTA, TOISSIJAISUUSPERIAATE JA SUHTEELLISUUSPERIAATE

- **Oikeusperusta**

Oikeusperusta EU:n toiminnalle on Euroopan unionin toiminnasta tehdyn sopimuksen (SEUT) 114 artikla, joka koskee jäsenvaltioiden lainsäädännön lähentämistä, jotta voidaan saavuttaa SEUT-sopimuksen 26 artiklan tavoitteet eli sisämarkkinoiden moitteeton toiminta.

Sisämarkkinoita koskeva oikeusperusta ENISAn perustamiselle on vahvistettu unionin tuomioistuimen oikeuskäytännössä (asia C-217/04, *Yhdistynyt kuningaskunta v. Euroopan parlamentti ja neuvosto*) ja käyttämällä sitä uudelleen vuoden 2013 asetuksessa viraston nykyisestä toimeksiannosta. Lisäksi toimet, jotka vastaisivat tavoitteita lisätä jäsenvaltioiden välistä yhteistyötä ja koordinointia sekä EU:n tason valmiuksia jäsenvaltioiden toimien täydentämiseksi, kuuluisivat ”operatiivisen yhteistyön” luokkaan. Tämä yksilöidään nimenomaisesti tavoitteeksi verkko- ja tietoturvadirektiivissä (jonka oikeusperusta on SEUT-sopimuksen 114 artikla) CSIRT-verkoston yhteydessä, jossa ”ENISA huolehtii sihteeristötehtävistä ja tukee aktiivisesti yhteistyötä” (12 artiklan 2 kohta). Direktiivin 12 artiklan 3 kohdan f alakohdassa esitetään tarkemmin muita operatiivisen yhteistyön muotoja CSIRT-verkostolle kuuluvina tehtävinä, myös seuraavien osalta: i) riskien ja poikkeamien luokat, ii) ennakkovaroitukset, iii) keskinäinen avunanto ja iv) periaatteet ja yksityiskohtaiset säännöt koordinointia varten tilanteisiin, joissa jäsenvaltiot reagoivat rajat ylittäviin riskeihin ja poikkeamiin.

- Tieto- ja viestintätekniikan tuotteiden ja palvelujen sertifiointijärjestelmien nykyinen hajanaisuus johtuu myös siitä, ettei käytössä ole yhteistä oikeudellisesti sitovaa ja tehokasta kehysprosessia, jota sovellettaisiin kaikissa jäsenvaltioissa. Tämä haittaa sisämarkkinoiden aikaansaamista tieto- ja viestintätekniikan tuotteille ja palveluille ja heikentää Euroopan teollisuuden kilpailukykyä tällä alalla. Tämän ehdotuksen tarkoituksena on puuttua nykyiseen hajanaisuuteen ja sen aiheuttamiin esteisiin sisämarkkinoilla tarjoamalla käyttöön yhteinen kehys kyberturvallisuuden sertifiointijärjestelmille, jotka ovat voimassa koko EU:n alueella.

[20] Asetus (EY) N:o 765/2008 tuotteiden kaupan pitämiseen liittyvää akkreditointia ja markkinavalvontaa koskevista vaatimuksista ja neuvoston asetuksen (ETY) N:o 339/93 kumoamisesta.

Toissijaisuusperiaate (muun kuin jaetun toimivallan osalta)

Toissijaisuusperiaate edellyttää EU:n toiminnan tarpeellisuuden ja lisäarvon arvioimista. Toissijaisuusperiaatteen noudattaminen tällä alalla todettiin jo nykyisen ENISA-asetuksen[21] hyväksymisen yhteydessä.

Kyberturvallisuus on unionin yhteisen edun mukainen kysymys. Verkkojen ja tietojärjestelmien keskinäiset riippuvuudet ovat sellaisia, että yksittäiset toimijat (olipa kysymys julkisista tai yksityisistä toimijoista, myös kansalaisista) eivät useinkaan kykene hallitsemaan kyberturvallisuuspoikkeamiin liittyviä uhkia, riskejä ja mahdollisia vaikutuksia itsenäisesti. Jäsenvaltioiden väliset riippuvuussuhteet muun muassa elintärkeiden infrastruktuurien toiminnassa (energiahuolto, liikenne ja vesihuolto ovat tästä vain muutamia esimerkkejä) merkitsevät sitä, että julkiset toimet Euroopan tasolla ovat paitsi myönteisiä myös tarpeen. EU:n toiminnasta voi olla myös myönteisiä seurannaisvaikutuksia johtuen siitä, että hyviä käytäntöjä jaetaan jäsenvaltioiden kesken, mikä voi johtaa unionin kyberturvallisuuden tehostumiseen.

Yhteenvetona voidaan todeta, että nykyisessä tilanteessa ja tulevaisuuden skenaarioita tarkastellen näyttää siltä, etteivät **EU:n jäsenvaltioiden yksittäiset toimet ja hajanainen lähestymistapa kyberturvallisuuteen** riittäisi, jotta unionin **kollektiivista kyberresilienssiä voitaisiin lisätä**.

EU:n toiminta katsotaan myös tarpeelliseksi, jotta voidaan puuttua kyberturvallisuuden sertifiointijärjestelmien nykyiseen hajanaisuuteen. Se antaisi valmistajille mahdollisuuden hyötyä täysimääräisesti sisämarkkinoista ja saada merkittäviä säästöjä testaukseen ja uudelleensuunnitteluun liittyvissä kustannuksissa. Vaikka esimerkiksi nykyisellä johtavien virkamiesten tietoturvallisuusryhmän (SOGIS) vastavuoroista tunnustamista koskevalla sopimuksella (MRA) on tältä osin saavutettu merkittäviä tuloksia, se on myös osoittanut merkittävät rajoituksensa, jotka haittaavat sen soveltuvuutta pitkän aikavälillä kestäviin ratkaisuihin sisämarkkinoiden täyden potentiaalin hyödyntämisessä.

EU:n tason toiminnasta saatava lisäarvo, erityisesti pyrittäessä tehostamaan yhteistyötä jäsenvaltioiden välillä samoin kuin verkko- ja tietoturvallisuusyhteisöjen välillä, on tunnustettu vuoden 2016 neuvoston päätelmissä[22] ja käy myös selvästi ilmi ENISAn arvioinnista.

- **Suhteellisuusperiaate**

Suunnitelluilla toimenpiteillä ei ylitetä sitä, mikä on tarpeen niiden poliittisten tavoitteiden saavuttamiseksi. EU:n toiminnan soveltamisala ei estä muita kansallisia toimia kansalliseen turvallisuuteen liittyvissä asioissa. EU:n toimet ovat siksi perusteltuja toissijaisuus- ja suhteellisuusperiaatteen nojalla.

[21] Euroopan parlamentin ja neuvoston asetus (EU) N:o 526/2013, annettu 21 päivänä toukokuuta 2013 , Euroopan unionin verkko- ja tietoturvavirastosta (ENISA) ja asetuksen (EY) N:o 460/2004 kumoamisesta.

[22] Neuvoston päätelmät Euroopan kyberresilienssijärjestelmän vahvistamisesta sekä kilpailukykyisen ja innovatiivisen kyberturvallisuustoimialan tukemisesta – 15. marraskuuta 2016.

- **Toimintatavan valinta**

Tällä ehdotuksella tarkistetaan asetusta (EU) N:o 526/2013, jossa vahvistetaan ENISAn nykyinen toimeksianto ja tehtävät. Kun lisäksi otetaan huomioon ENISAn tärkeä rooli EU:n kyberturvallisuuden sertifiointipuitteiden perustamisessa ja hallinnoinnissa, ENISAn uusi toimeksianto ja kyseinen sertifiointikehys on perusteltua vahvistaa yhdellä yksittäisellä oikeudellisella välineellä valitsemalla toimintatavaksi asetus.

3. JÄLKIARVIOINTIEN, SIDOSRYHMIEN KUULEMISTEN JA VAIKUTUSTENARVIOINTIEN TULOKSET

Voimassa olevan lainsäädännön jälkiarvioinnit/toimivuustarkastukset

Komissio on arviointia koskevan etenemissuunnitelman[23] mukaisesti arvioinut viraston **merkityksellisyyden, vaikuttavuuden, toimivuuden ja tehokkuuden sekä sen toiminnan johdonmukaisuuden ja lisäarvon** viraston suorituskyvyn, hallinnon, sisäisen organisaatiorakenteen ja työskentelytapojen suhteen vuosina 2013–2016. Pääasialliset havainnot voidaan tiivistää seuraavasti (ks. tarkemmat tiedot komission yksiköiden valmisteluasiakirjasta, joka on vaikutusten arvioinnin liitteenä).

- **Merkityksellisyys:** Kehittyvän teknologian ja muuttuvien uhkien tilanteessa ja ottaen huomioon merkittävä tarve lisätä kyberturvallisuutta EU:ssa ENISAn tavoitteet ovat osoittaneet merkityksensä. Jäsenvaltiot ja EU:n elimet nojautuvat sen laajaan asiantuntemukseen kyberturvallisuuskysymyksissä. Lisäksi jäsenvaltioissa on tarpeen kehittää valmiuksia ymmärtää ja torjua uhkia paremmin ja sidosryhmien on tarpeen toimia yhteistyössä eri temaattisten alojen ja instituutioiden välisesti. Kyberturvallisuus on edelleen EU:n keskeinen poliittinen prioriteetti, johon ENISAn odotetaan vastaavan. Toisaalta kuitenkin ENISAn toimeksianto EU:n virastona, jonka toimikausi on määräaikainen, i) ei mahdollista pitkän aikavälin suunnittelua ja kestävää tukea jäsenvaltioille ja EU:n toimielimille; ii) voi johtaa oikeudelliseen tyhjiöön, koska verkko- ja tietoturvadirektiivin säännöksillä ENISAlle annetaan luonteeltaan pysyviä tehtäviä[24]; iii) ei johdonmukaisesti vastaa visiota, joka kytkee ENISAn kyberturvallisuustoimintaympäristön parantamiseen EU:ssa.
- **Vaikuttavuus**: ENISA on yleisesti ottaen saavuttanut tavoitteensa ja täyttänyt tehtävänsä. Se on myötävaikuttanut verkko- ja tietoturvan lisäämiseen Euroopassa tärkeimmillä toiminnoillaan (valmiuksien kehittäminen, asiantuntemuksen tarjoaminen, yhteisöjen rakentaminen ja toimintapoliittinen tuki). On kuitenkin todettu, että sen toimintaa on mahdollista parantaa kussakin näistä. Arvioinnissa todettiin ENISAn vaikutuksen näkyvän siinä, miten se on pystynyt luomaan tiiviit ja luottamukseen perustuvat suhteet joihinkin sidosryhmiinsä, erityisesti jäsenvaltioihin ja CSIRT-yhteisöön. Valmiuksien kehittämiseen liittyvällä toiminnalla katsottiin olleen vaikutus erityisesti jäsenvaltioissa, joilla on vähäisemmät resurssit. Tärkeimpiin saavutuksiin kuuluu laajan yhteistyön edistäminen, ja sidosryhmät ovat paljolti samaa mieltä ENISAn myönteisestä roolista sidosryhmien saattamisessa yhteen. ENISAn on kuitenkin ollut hankalaa saada aikaan suurta vaikutusta verkko- ja tietoturvan hyvin laajalla alalla. Tämä on johtunut myös sitä, että sillä on ollut laaja-alaiseen toimeksiantoonsa nähden melko rajalliset henkilö- ja taloudelliset resurssit. Arvioinnissa pääteltiin myös, että ENISA on täyttänyt osittain tavoitteensa

[23] http://ec.europa.eu/smart-regulation/roadmaps/docs/2017_cnect_002_evaluation_enisa_en.pdf

[24] Viitataan verkko- ja tietoturvadirektiivin 7, 9, 11, 12 ja 19 artiklaan.

tarjota asiantuntemusta. Tavoitteen saavuttamiseen vaikuttivat asiantuntijoiden palkkaamiseen liittyvät vaikeudet (ks. ”Tehokkuus” jäljempänä).

- **Tehokkuus**: Pienistä määrärahoistaan huolimatta – ENISAn budjetti on kuuluu EU:n virastojen suppeimpiin – virasto on kyennyt edistämään kohdennettuja tavoitteita tavalla, joka osoittaa kaiken kaikkiaan tehokasta resurssien käyttöä. Arvioinnissa todettiin, että prosessit olivat yleisesti ottaen tehokkaita ja että organisaation sisäisen selkeän vastuunjaon ansiosta viraston työ suoritettiin hyvin. Yksi viraston suurimmista tehokkuushaasteista liittyy ENISAn vaikeuksiin rekrytoida ja pitää palveluksessaan erittäin päteviä asiantuntijoita. Havaintojen mukaan tämä voi johtua useista eri tekijöistä, kuten julkisen sektorin yleisistä vaikeuksista kilpailla yksityisen sektorin kanssa pitkälle erikoistuneiden asiantuntijoiden palkkaamisessa, sopimusten tyypistä, sillä virasto voi tarjota enimmäkseen vain määräaikaisia työsopimuksia, sekä ENISAn sijaintiin liittyvästä verrattain vähäisestä houkuttelevuudesta, johtuen esimerkiksi puolisoiden kohtaamista vaikeuksista löytää töitä. Sijainti sekä Ateenassa että Iráklionissa edellytti lisätoimia viraston toiminnan koordinoimiseksi ja aiheutti lisäkustannuksia, mutta ydintoimintaosaston siirtyminen Ateenaan vuonna 2013 on lisännyt viraston toiminnallista tehokkuutta.
- **Johdonmukaisuus**: Vaikka ENISAn toimet ovat yleisesti olleet johdonmukaisia suhteessa sen sidosryhmien politiikkaan ja toimintaan kansallisella ja EU:n tasolla, kyberturvallisuuteen on tarpeen omaksua koordinoidumpi lähestymistapa EU:n tasolla. Potentiaalia ENISAn ja muiden EU:n elinten väliseen yhteistyöhön ei ole hyödynnetty täysimääräisesti. EU:n oikeudellisen ja poliittisen toimintaympäristön kehittymisen vuoksi nykyinen toimeksianto ei ole yhtä johdonmukainen suhteessa siihen.
- **EU:n tason lisäarvo**: Viraston lisäarvo syntyy pääasiassa viraston mahdollisuuksista tehostaa yhteistyötä – pääasiallisesti jäsenvaltioiden välillä mutta myös verkko- ja tietoturva-alan yhteisöjen kanssa. Mikään muu toimija EU:n tasolla ei tue vastaavan sidosryhmäkirjon yhteistyötä verkko- ja tietoturva-alalla. Viraston tuoma lisäarvo vaihteli eri sidosryhmien erilaisten tarpeiden ja resurssien mukaan (esim. suuret v. pienet jäsenvaltiot tai jäsenvaltiot v. toimiala) ja riippuen viraston tarpeesta priorisoida toimiaan työohjelman mukaisesti. Arvioinnissa todettiin, että mahdollinen ENISAn lakkauttaminen olisi menetetty mahdollisuus kaikille jäsenvaltioille. Vastaavanlaajuista yhteisöjen rakentamista ja yhteistyötä ei voitaisi varmistaa pelkästään jäsenvaltioiden välillä kyberturvallisuuden alalla. Ilman keskitettyä EU:n virastoa tilanne olisi nykyistä hajanaisempi, kun ENISAn jälkeensä jättämä tyhjiö korvautuisi kahdenvälisellä tai alueellisella yhteistyöllä.

ENISAn aikaisempia suorituksia ja tulevaisuutta tarkastellen tärkeimmät vuoden 2017 sidosryhmäkuulemisessa esille tulleet trendit ovat seuraavat[25]:

[25] Kuulemiseen vastasi 90 sidosryhmää 19 jäsenvaltiosta (vastauksia saatiin 88 ja kannanottopapereja 2). Mukana oli kansallisia viranomaisia 15 jäsenvaltiosta, muun muassa Ranskasta, Italiasta, Irlannista ja Kreikasta, sekä 8 kattojärjestöä, jotka edustavat merkittävää määrää eurooppalaisia organisaatioita. Kuulemiseen vastasivat muun muassa Euroopan pankkiyhdistysten liitto, Digital Europe (joka edustaa digitaaliteknologia-alan teollisuutta Euroopassa) ja Euroopan kiinteän verkon operaattoreiden järjestö ETNO. ENISAa koskenutta julkista kuulemista täydennettiin useita muista lähteistä, joita olivat i) perusteelliset haastattelut, joita tehtiin noin 50:lle kyberturvallisuusyhteisön keskeiselle toimijalle, ii) CSIRT-verkostolle tehty kysely ja iii) ENISAn johtokunnalle, hallitukselle ja pysyvälle sidosryhmälle tehty kysely.

- Vastaajien enemmistö (74 %) antoi myönteisen arvion ENISAn yleisestä suorituskyvystä vuosina 2013–2016. Enemmistö vastaajista katsoi ENISAn myös saavuttavan eri tavoitteensa (vähintään 63 % kunkin tavoitteen osalta). ENISAn palveluja ja tuotteita käyttää säännöllisesti (kuukausittain tai sitä useammin) lähes puolet vastaajista (46 %). Niitä pidetään arvossa, koska ne tulevat EU:n tason elimeltä (83 %) ja ovat laadukkaita (62 %).
- Vastaajat määrittelivät useita toimintatarpeita ja haasteita kyberturvallisuuden tulevaisuudelle EU:ssa. Viisi tärkeintä (yhteensä 16:sta) olivat: yhteistyö jäsenvaltioiden välillä, valmiudet ehkäistä, havaita ja ratkaista laajamittaisia kyberhyökkäyksiä, jäsenvaltioiden välinen yhteistyö kyberturvallisuuteen liittyvissä kysymyksissä, yhteistyö ja tietojenvaihto eri sidosryhmien välillä, mukaan lukien julkisen ja yksityisen sektorin yhteistyö, sekä kriittisen infrastruktuurin suojaaminen kyberhyökkäyksiltä.
- Suuri enemmistö (88 %) vastaajista piti nykyisiä EU:n tasolla käytettävissä olevia välineitä ja mekanismeja riittämättöminä tai vain osittain soveltuvina vastaamaan kyberturvallisuuden nykyisiin haasteisiin. Samoin suuri enemmistö vastaajista (98 %) katsoi, että jonkin EU:n elimen olisi vastattava näihin tarpeisiin, ja näistä elimistä ENISAa piti oikeana organisaationa 99 prosenttia vastaajista.

Sidosryhmien kuuleminen

- Komissio järjesti julkisen kuulemisen ENISA-asetuksen tarkistamisesta 12. huhtikuuta – 5. heinäkuuta 2016 ja sai 421 vastausta[26]. Tulosten mukaan 67,5 prosenttia vastaajista katsoi, että ENISAlla voisi olla rooli luotaessa yhdenmukaistettuja puitteita tietotekniikkatuotteiden ja -palvelujen turvallisuussertifioinnille.

Vuonna 2016 järjestetyn kuulemisen tulokset kyberturvallisuutta koskevasta julkisen ja yksityisen sektorin sopimusperusteisesta kumppanuudesta[27] osoittavat, että

- 50,4 % vastaajista (121 yhteensä 240:stä) ei tiedä, ovatko kansalliset sertifiointijärjestelmät vastavuoroisesti tunnustettuja EU:n jäsenvaltioissa. 25,8 % (62 yhteensä 240:stä) vastasi ”ei” ja 23,8 % (57 yhteensä 240:stä) ”kyllä”.
- 37,9 % vastaajista (91 yhteensä 240:stä) on sitä mieltä, että nykyiset sertifiointijärjestelmät eivät tue Euroopan teollisuuden tarpeita. Toisaalta 17,5 % (42 yhteensä 240:stä) – pääasiallisesti oli kyse Euroopan markkinoilla toimivista maailmanlaajuisista yrityksistä – oli päinvastaisella kannalla.
- 49,6 % vastanneista (119 yhteensä 240:stä) sanoo, ettei ole helppoa osoittaa vastaavuutta standardien, sertifiointijärjestelmien ja merkintöjen välillä. 37,9 % (91 yhteensä 240:stä) vastasi ”en tiedä” ja vain 12,5 % (30 yhteensä 240:stä) ”kyllä”.

[26] Vastaajien jakauma: 162 vastausta kansalaisilta, 33 kansalais- ja kuluttajajärjestöiltä, 186 toimialalta ja 40 viranomaisilta, muun muassa sähköisen viestinnän tietosuojadirektiivin täytäntöönpanoon toimivaltaisilta viranomaisilta.

[27] Sertifiointia koskevaan osioon vastasi 240 sidosryhmää, jotka edustivat kansallisia julkishallintoja, suuryrityksiä, pk-yrityksiä, mikroyrityksiä ja tutkimuslaitoksia.

Asiantuntijatiedon käyttö

Komissio on nojautunut seuraavaan ulkopuoliseen asiantuntija-apuun:

- Tutkimus ENISAn arvioinnista (*Study on the Evaluation of ENISA*, Ramboll/Carsa 2017; SMART no. 2016/0077),
- Tutkimus tieto- ja viestintätekniikan turvallisuussertifioinnista ja merkinnöistä – näytön kerääminen ja vaikutusten arviointi (*Study on ICT Security Certification and Labelling – Evidence gathering and impact assessment*, PriceWaterhouseCoopers 2017; SMART no. 2016/0029).

Vaikutusten arviointi

- Käsillä olevaa aloitetta koskevassa vaikutustenarviointiraportissa todettiin seuraavat keskeiset ongelmakohdat:
- kyberturvallisuuspolitiikan ja -lähestymistapojen hajanaisuus jäsenvaltioissa,
- hajanaiset resurssit ja yhtenäisen linjan puute kyberturvallisuuslähestymistavoissa EU:n toimielimissä, virastoissa ja elimissä ja
- riittämätön tietoisuus ja tiedotus kansalaisten ja yritysten keskuudessa yhdistettynä yhä useampien erillisten kansallisten ja alakohtaisten sertifiointijärjestelmien käyttöönottoon.

ENISAn toimeksiannon osalta raportissa arvioitiin seuraavia mahdollisia vaihtoehtoja:

- nykytilanteen säilyttäminen eli jatkokausi, joka olisi edelleen määräaikainen (perusskenaario),
- ENISAn nykyisen toimikauden päättyminen ilman jatkokautta ja ENISAn lakkauttaminen (ei poliittisia toimia),
- ”uudistettu ENISA” ja
- EU:n kyberturvallisuusvirasto, jolla on täydet operatiiviset valmiudet.

Kyberturvallisuussertifiointiin liittyen raportissa arvioitiin seuraavia mahdollisia vaihtoehtoja:

- ei poliittisia toimia (perusskenaario),
- muut kuin lainsäädäntötoimet (ei-sitovat toimenpiteet),
- unionin säädös, jolla luodaan kaikille jäsenvaltioille pakollinen järjestelmä SOGIS-järjestelmän pohjalta, ja
- yleinen EU:n kehys tieto- ja viestintätekniikan kyberturvallisuussertifioinnille.

Analyysin perusteella voitiin päätellä, että parhaana pidetty vaihtoehto on ”uudistettu ENISA”, johon liittyy yleinen EU:n kehys tieto- ja viestintäteknologian kyberturvallisuussertifioinnille.

Parhaaksi katsottu vaihtoehto on arvioitu toimintatavaksi, jolla avulla EU voi tuloksekkaimmin saavuttaa asetetut tavoitteet eli lisätä kyberturvallisuusvalmiuksia, varautumista, yhteistyötä, tietoisuutta ja avoimuutta ja estää markkinoiden pirstaloitumisen. Sen on myös arvioitu johdonmukaisimmin soveltuvan EU:n kyberturvallisuusstrategian ja siihen liittyvän toimintapolitiikan (esim. verkko- ja tietoturvadirektiivin) sekä digitaalisten sisämarkkinoiden strategian poliittisiin painopisteisiin. Lisäksi kuulemisessa kävi ilmi, että tämä parhaaksi arvioitu vaihtoehto saa sidosryhmien enemmistön kannatuksen.

Vaikutustenarvioinnissa tehty analyysi osoitti, että parhaaksi arvioidulla vaihtoehdolla tavoitteet saavutettaisiin kohtuullisin resurssein.

Komission sääntelyntarkastelulautakunta antoi ensin kielteisen lausunnon 24. heinäkuuta ja arvioinnin uudelleentoimituksen jälkeen myönteisen lausunnon 25. elokuuta 2017. Tarkistettu vaikutustenarviointiraportti sisälsi lisänäyttöä, ENISAn arvioinnin lopulliset päätelmät ja lisäselvityksiä toimintavaihtoehdoista ja niiden vaikutuksista. Vaikutustenarviointiraportin liitteessä 1 esitetään tiivistetysti, miten sääntelyntarkastelulautakunnan toisessa lausunnossa tekemät huomautukset on otettu huomioon. Raporttia päivitettiin esittämällä yksityiskohtaisemmin EU:n kyberturvallisuuden toimintaympäristö, myös toimenpiteet, jotka sisältyvät yhteiseen tiedonantoon ”Resilienssi, pelote ja puolustus: vahvan kyberturvallisuuden rakentaminen EU:lle”, (JOIN(2017) 450) ja joilla on erityinen merkitys ENISAn kannalta: EU:n kyberturvallisuussuunnitelma ja Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskus, johon virasto ohjaisi neuvontansa EU:n tutkimustarpeista.

Raportissa selitetään, miten viraston uudistus, mukaan lukien uudet tehtävät, paremmat työehdot ja EU:n elinten kanssa tehtävä rakenteellinen yhteistyö tällä alalla, lisäsivät sen houkuttelevuutta työnantajana ja auttaisivat ratkaisemaan asiantuntijoiden rekrytointiin liittyviä ongelmia. Raportin liitteessä 6 esitetään myös tarkistettu arvio ENISAn toimintavaihtoehtoihin liittyvistä kustannuksista. Sertifiointiaihepiirin osalta raporttia on tarkistettu antamalla yksityiskohtaisempi selvitys parhaaksi arvioidusta vaihtoehdosta, myös graafisen esityksen avulla, ja arviot kustannuksista, joita jäsenvaltioille ja komissiolle aiheutuu uudesta sertifiointikehyksestä. Perusteita sille, että ENISA on valittu sertifiointikehyksen keskeiseksi toimijaksi, on selitetty tarkemmin vedoten sen asiantuntemukseen alalla ja siihen, että se on ainoa kyberturvallisuuden alalla toimiva EU-tason virasto. Sertifiointia käsitteleviä osioita myös tarkistettiin selventämällä näkökohtia koskien eroja verrattuna nykyiseen SOGIS-järjestelmään ja eri toimintavaihtoehtojen hyötyjä sekä selittämällä, että eurooppalaisen sertifiointijärjestelmän piiriin kuuluvan tieto- ja viestintätekniikan tuotteen ja palvelun tyyppi määritellään hyväksytyssä järjestelmässä itsessään.

Sääntelyn tila ja yksinkertaistaminen

Ei sovelleta

Vaikutus perusoikeuksiin

Kyberturvallisuudella on keskeinen merkitys yksilöiden yksityisyyden ja henkilötietojen suojelemisessa EU:n perusoikeuskirjan 7 ja 8 artiklan mukaisesti. Kyberturvallisuuspoikkeamat kohdistavat selvän uhan yksityisyyteen ja henkilötietojen suojaukseen. Kyberturvallisuus on näin ollen välttämätön edellytys yksityisyyden suojalle ja henkilötietojen luottamuksellisuudelle. Tältä kannalta ehdotus, jonka tavoitteena on tehostaa kyberturvallisuutta Euroopassa, täydentää tärkeällä tavalla nykyistä lainsäädäntöä, jolla suojataan perusoikeutta yksityisyyteen ja henkilötietojen suojaan. Kyberturvallisuus on myös edellytys sähköisen viestinnän luottamuksellisuuden suojaamiselle ja näin ollen sananvapauden ja tiedonvälityksen vapauden sekä niihin liittyvien oikeuksien, kuten ajatuksen, omantunnon ja uskonnon vapauden, käyttämiselle.

4. TALOUSARVIOVAIKUTUKSET

Ks. rahoitusselvitys

5. LISÄTIEDOT

- **Täytäntöönpanosuunnitelmat sekä seuranta-, arviointi- ja raportointijärjestelyt**

Komissio seuraa asetuksen soveltamista ja antaa arvioinnistaan kertomuksen Euroopan parlamentille, neuvostolle ja Euroopan talous- ja sosiaalikomitealle joka viides vuosi. Nämä tämän asetuksen käytännön soveltamista ja täytäntöönpanoa tarkastelevat kertomukset ovat julkisia.

- **Ehdotukseen sisältyvien säännösten yksityiskohtaiset selitykset**

Asetuksen I osasto sisältää yleiset säännökset asetuksen kohteesta (1 artikla) sekä määritelmät (2 artikla). Jälkimmäinen sisältää myös viittaukset muiden EU:n säädösten sovellettaviin määritelmiin. Näitä säädöksiä ovat Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/1148 toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa (verkko- ja tietoturvadirektiivi), Euroopan parlamentin ja neuvoston asetus (EY) N:o 765/2008 tuotteiden kaupan pitämiseen liittyvää akkreditointia ja markkinavalvontaa koskevista vaatimuksista ja asetuksen (ETY) N:o 339/93 kumoamisesta sekä Euroopan parlamentin ja neuvoston asetus (EU) N:o 1025/2012 eurooppalaisesta standardoinnista.

Asetuksen II osasto sisältää keskeiset EU:n kyberturvallisuusvirastoon ENISAan liittyvät säännökset.

Kyseisen osaston I luvussa esitetään viraston toimeksianto (3 artikla), tavoitteet (4 artikla) ja tehtävät (5–11 artikla).

Luvussa II esitetään ENISAn organisaatio ja keskeiset säännökset sen rakenteesta (12 artikla). Siinä säädetään johtokunnan koostumuksesta, äänestyssäännöistä ja tehtävistä (1 jakso, 13–17 artikla), hallituksesta (2 jakso, 18 artikla) ja pääjohtajasta (3 jakso, 19 artikla). Se sisältää myös säännökset pysyvän sidosryhmän kokoonpanosta ja roolista (4 jakso, 20 artikla). Kyseisen luvun 5 jaksossa määritellään lisäksi viraston toimintaa koskevat säännöt, mukaan lukien ohjelmasuunnittelu, eturistiriidat, avoimuus, luottamuksellisuus ja oikeus tutustua asiakirjoihin (21–25 artikla).

Luvussa III säädetään viraston talousarvion laatimisesta ja rakenteesta (26 ja 27 artikla) sekä sen täytäntöönpanoa ohjaavista säännöistä (28 ja 29 artikla). Se sisältää myös säännökset, joilla helpotetaan petosten, korruption ja muun laittoman toiminnan torjuntaa (30 artikla).

Luku IV koskee viraston henkilöstöä. Se sisältää yleiset säännökset henkilöstösäännöistä ja henkilöstöön sovellettavista palvelussuhteen ehdoista sekä erioikeuksista ja vapauksista (31 ja 32 artikla). Siinä säädetään myös viraston pääjohtajan valinnasta ja nimittämisestä (33 artikla). Lisäksi se sisältää säännökset, joiden mukaisesti virasto voi käyttää kansallisia asiantuntijoita ja muuta sellaisen henkilöstöä, joka ei ole viraston palveluksessa (34 artikla).

Luku V sisältää virastoa koskevat yleiset säännökset. Siinä esitetään oikeudellinen asema (35 artikla), säännökset vastuusta, kielijärjestelyistä ja henkilötietojen suojasta (36–38 artikla) sekä turvallisuusluokiteltujen tietojen ja arkaluonteisten turvallisuusluokittelemattomien tietojen suojelemista koskevat turvallisuussäännökset (40 artikla). Se sisältää myös säännöt viraston yhteistyöstä kolmansien maiden ja kansainvälisten organisaatioiden kanssa (39 artikla) sekä toimipaikasta, toimintaolosuhteista ja oikeusasiamiehen vastuulle kuuluvasta hallinnollisesta valvonnasta (41 ja 42 artikla).

Asetuksen III osastossa vahvistetaan eurooppalainen kehys tieto- ja viestintätekniikan tuotteiden ja palvelujen kyberturvallisuussertifioinnille (”**sertifiointikehys**”) nojautuen *lex generalis* -periaatteeseen (1 artikla). Siinä määritellään eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien yleinen tavoite varmistaa, että tieto- ja viestintätekniikan tuotteet ja palvelut täyttävät määritellyt kyberturvallisuusvaatimukset kykenemällä suojautumaan tietyllä varmuustasolla toimilta, jotka vaarantavat tallennettujen, siirrettyjen tai käsiteltyjen tietojen saatavuuden, aitouden, eheyden tai luottamuksellisuuden tai tähän liittyvät toiminnot tai palvelut (43 artikla). Lisäksi siinä luetellaan turvallisuustavoitteet, joihin eurooppalaisilla kyberturvallisuuden sertifiointijärjestelmillä pyritään (45 artikla), kuten valmius suojella tietoja tahattomalta tai luvattomalta käytöltä tai luovuttamiselta, tuhoamiselta tai muuttamiselta, sekä määritetään eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien sisältö (osatekijät), kuten yksityiskohtainen eritelmä niiden soveltamisalasta, turvallisuustavoitteista, arviointikriteereistä jne. (47 artikla).

Asetuksen III osastossa määritellään myös eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien tärkeimmät oikeudelliset vaikutukset eli i) velvollisuus panna järjestelmä täytäntöön kansallisella tasolla ja sertifioinnin vapaaehtoinen luonne sekä ii) eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien oikeusvaikutus, joka tekee kansalliset järjestelmät pätemättömiksi samojen tuotteiden tai palvelujen osalta (48 ja 49 artikla).

Kyseisessä osastossa vahvistetaan menettely eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien hyväksymiselle sekä tehtävänjako komission, ENISAn ja Euroopan kyberturvallisuuden sertifiointiryhmän välillä (44 artikla). Lisäksi siinä annetaan säännökset vaatimustenmukaisuuden arviointilaitoksista, mukaan lukien niiden vaatimukset, valtuudet ja tehtävät, kansallisista sertifioinnin valvontaviranomaisista sekä seuraamuksista.

Myös Euroopan kyberturvallisuuden sertifiointiryhmä perustetaan tämän osaston säännöksillä keskeisenä elimenä, joka koostuu kansallisten sertifioinnin valvontaviranomaisten edustajista ja jonka pääasiallisena tehtävänä on työskennellä yhdessä ENISAn kanssa eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien valmistelemiseksi ja antaa komissiolle neuvoja kyberturvallisuussertifioinnin toimintapolitiikkaan liittyvissä yleisissä tai erityisissä kysymyksissä.

Asetuksen IV osasto sisältää loppusäännökset siirretyn säädösvallan käyttämisestä, arviointivaatimuksista, kumoamisesta, seuraannosta ja voimaantulosta.

2017/0225 (COD)

Ehdotus

EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS

EU:n kyberturvallisuusvirastosta ENISAsta ja asetuksen (EU) 526/2013 kumoamisesta sekä tieto- ja viestintätekniikan kyberturvallisuussertifioinnista (”kyberturvallisuusasetus”)

(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[28],

ottavat huomioon alueiden komitean lausunnon[29],

noudattavat tavallista lainsäätämisjärjestystä,

sekä katsovat seuraavaa:

(1) Verkko- ja tietojärjestelmillä ja televiestintäverkoilla ja -palveluilla on yhteiskunnassa elintärkeä rooli, ja niistä on tullut talouskasvun selkäranka. Tieto- ja viestintätekniikka luo pohjaa monimutkaisille järjestelmille, jotka tukevat yhteiskunnan toimintoja, pitävät talouden pyörät pyörimässä keskeisillä aloilla, kuten terveydenhuollossa, energia-alalla, rahoitusalalla ja liikenteessä, ja erityisesti tukevat sisämarkkinoiden toimintaa

(2) Verkko- ja tietojärjestelmien käyttö on nykyisin laajalla levinnyttä kansalaisten, yritysten ja julkishallinnon piirissä kaikkialla unionissa. Digitoinnista ja verkkoyhteyksistä on tulossa keskeisiä ominaisuuksia yhä useammissa tuotteissa ja palveluissa, ja esineiden internetin myötä EU:ssa ennakoidaan otettavan käyttöön miljoonia, ellei miljardeja, verkkoon kytkettyjä digitaalisia laitteita seuraavan vuosikymmenen aikana. Yhä useammat laitteet liitetään internetiin huolehtimatta samalla siitä, että turvallisuus ja resilienssi ovat riittävällä tavalla sisäänrakennettuja, mikä johtaa puutteisiin kyberturvallisuudessa. Sertifioinnin vähäinen käyttö johtaa tässä yhteydessä siihen, että organisaatiot ja yksittäiset käyttäjät eivät saa riittävästi tietoa tieto- ja viestintätekniikan tuotteiden ja palvelujen kyberturvallisuusominaisuuksista, mikä heikentää luottamusta digitaalisiin ratkaisuihin.

[28] EUVL C , , s. .
[29] EUVL C , , s. .

(3) Digitalisoinnin ja verkkoyhteyksien yleistyminen lisää kyberturvallisuuteen liittyviä riskejä, jolloin koko yhteiskunta on haavoittuvampi kyberuhkille, ja pahentaa yksilöihin, myös heikommassa asemassa oleviin henkilöihin, kuten lapsiin, kohdistuvia vaaroja. Tämän yhteiskuntaan kohdistuvan riskin lieventämiseksi kyberturvallisuutta on tarpeen parantaa EU:ssa kaikin tarvittavin toimenpitein, jotta kansalaisten, hallintojen ja yritysten – pk-yrityksistä elintärkeiden infrastruktuureiden ylläpitäjiin – käyttämät verkko- ja tietojärjestelmät, televiestintäverkot, digitaaliset tuotteet, palvelut ja laitteet voidaan suojata paremmin kyberuhilta.

(4) Kyberhyökkäyksiä tapahtuu yhä enemmän, ja verkottunut talous ja yhteiskunta, jotka ovat alttiimpia kyberuhille ja -hyökkäyksille, edellyttävät vahvempaa puolustusvalmiutta. Vaikka kyberhyökkäykset ovat usein rajatylittäviä, kyberturvallisuusviranomaisten poliittiset vastatoimet ja lainvalvontavaltuudet ovat enimmäkseen kansallisia. Laajamittaiset kyberturvallisuuspoikkeamat voivat häiritä keskeisten palvelujen tarjoamista koko EU:ssa. Tämä edellyttää tehokasta EU-tason reagointia ja kriisinhallintaa, jossa nojaudutaan kohdennettuihin politiikkoihin ja laaja-alaisempiin eurooppalaisen yhteisvastuun ja keskinäisen avunannon välineisiin. Politiikan laatijoille, toimialalle ja käyttäjille on tärkeää, että kyberturvallisuuden ja resilienssin tilaa unionissa arvioidaan säännöllisesti luotettavan unionin tiedon pohjalta ja että laaditaan järjestelmällisesti ennusteita tulevista kehityskuluista, haasteista ja uhkista sekä unionin tasolla että maailmanlaajuisesti.

(5) Unioniin kohdistuvien kyberturvallisuushaasteiden lisääntymisen vuoksi tarvitaan kattava joukko toimenpiteitä, jotka pohjautuvat aiempaan unionin toimintaan ja edistävät toisiaan vahvistavia tavoitteita. Tähän sisältyy tarve lisätä jäsenvaltioiden ja yritysten valmiuksia ja varautumiskykyä sekä parantaa yhteistyötä ja koordinointia jäsenvaltioiden ja EU:n toimielinten, virastojen ja elinten välillä. Koska kyberuhkat ovat luonteeltaan rajattomia, on myös tarpeen lisätä valmiuksia unionin tasolla jäsenvaltioiden toimien täydentämiseksi erityisesti laajamittaisten rajatylittävien kyberturvallisuuspoikkeamien ja -kriisien tapauksessa. Tarvitaan myös lisätoimia kansalaisten ja yritysten tietoisuuden lisäämiseksi kyberturvallisuuteen liittyvistä kysymyksistä. Lisäksi digitaalisiin sisämarkkinoihin tunnettua luottamusta olisi edelleen parannettava tarjoamalla avointa tietoa tieto- ja viestintätekniikan tuotteiden ja palvelujen turvallisuustasosta. Tätä voidaan helpottaa EU:n laajuisella sertifioinnilla, joka tuo käyttöön yhteiset kyberturvallisuusvaatimukset ja arviointiperusteet kansallisille markkinoille ja sektoreille.

(6) Euroopan parlamentti ja neuvosto antoivat vuonna 2004 ENISAn perustamisesta asetuksen (EY) N:o 460/2004[30], jolla pyrittiin osaltaan varmistamaan korkeatasoinen verkko- ja tietoturva unionissa ja luomaan verkko- ja tietoturvakulttuuri, josta on hyötyä kansalaisille, kuluttajille, yrityksille ja julkishallinnoille. Vuonna 2008 Euroopan parlamentti ja neuvosto antoivat asetuksen (EY) N:o 1007/2008[31], jolla viraston toimikautta jatkettiin maaliskuuhun 2012. Asetuksella (EY) N:o 580/2011[32]

30 Euroopan parlamentin ja neuvoston asetus (EY) N:o 460/2004, annettu 10 päivänä maaliskuuta 2004, Euroopan verkko- ja tietoturvaviraston perustamisesta (EUVL L 77, 13.3.2004, s. 1).

31 Euroopan parlamentin ja neuvoston asetus (EY) N:o 1007/2008, annettu 24 päivänä syyskuuta 2008, Euroopan verkko- ja tietoturvaviraston perustamisesta annetun asetuksen (EY) N:o 460/2004 muuttamisesta sen toimikauden keston osalta (EUVL L 293, 31.10.2008, s. 1).

32 Euroopan parlamentin ja neuvoston asetus (EU) N:o 580/2011, annettu 8 päivänä kesäkuuta 2011, Euroopan verkko- ja tietoturvaviraston perustamisesta annetun asetuksen (EY) N:o 460/2004 muuttamisesta viraston toimikauden osalta (EUVL L 165, 24.6.2011, s. 3).

viraston toimikautta jatkettiin edelleen 13 päivään syyskuuta 2013. Vuonna 2013 Euroopan parlamentti ja neuvosto antoivat ENISAsta ja asetuksen (EY) N:o 460/2004 kumoamisesta asetuksen (EU) N:o 526/2013[33], jolla viraston toimikautta jatkettiin kesäkuuhun 2020 saakka.

(7) Unioni on jo toteuttanut merkittäviä toimia kyberturvallisuuden varmistamiseksi ja luottamuksen lisäämiseksi digitaaliteknologioihin. Vuonna 2013 hyväksyttiin EU:n kyberturvallisuusstrategia ohjaamaan unionin poliittisia vastatoimia kyberturvallisuusuhkiin ja -riskeihin. Tarjotakseen eurooppalaisille paremman suojan verkkoympäristössä unioni hyväksyi vuonna 2016 ensimmäisenä kyberturvallisuusalan säädöksenä direktiivin (EU) 2016/1148 toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa, jäljempänä ’verkko- ja tietoturvadirektiivi’. Verkko- ja tietoturvadirektiivillä otettiin käyttöön vaatimukset kansallisista valmiuksista kyberturvallisuuden alalla, ensimmäiset mekanismit jäsenvaltioiden strategisen ja operatiivisen yhteistyön tehostamiseksi sekä velvoitteet toteuttaa turvallisuustoimenpiteitä ja tehdä ilmoitukset poikkeamista talouden ja yhteiskunnan kannalta olennaisilla aloilla, kuten energia, liikenne, vesihuolto, pankkitoiminta, rahoitusmarkkinoiden infrastruktuurit, terveydenhuolto ja digitaalinen infrastruktuuri sekä keskeisten digitaalisten palvelujen (hakukoneet, pilvipalvelut ja verkossa toimivat markkinapaikat) tarjoajat. ENISAlle annettiin keskeinen rooli tukea direktiivin täytäntöönpanoa. Lisäksi kyberrikollisuuden tehokas torjunta on tärkeä prioriteetti Euroopan turvallisuusagendassa, joka tältä osin edistää yleistä tavoitetta saavuttaa kyberturvallisuuden korkea taso.

(8) Yleisesti tunnustetaan, että sen jälkeen, kun EU:n kyberturvallisuusstrategia hyväksyttiin vuonna 2013 ja viraston toimeksiantoa viimeksi tarkistettiin, yleinen poliittinen tilanne on muuttunut merkittävästi, myös epävarmemman ja vähemmän turvatun globaalin toimintaympäristön vuoksi. Tässä yhteydessä ja osana uutta unionin kyberturvallisuuspolitiikkaa on tarpeen tarkistaa ENISAn toimeksiantoa, jotta voidaan määritellä sen rooli muuttuneessa kyberturvallisuuden toimintaympäristössä ja varmistaa, että se auttaa tehokkaasti unionia vastaamaan tästä perusteellisesti muuttuneesta uhkaympäristöstä johtuviin kyberturvallisuushaasteisiin. Kuten viraston arvioinnissa todetaan, sen nykyinen toimeksianto ei ole riittävä näiden haasteiden kannalta.

(9) Tällä asetuksella perustettavan viraston olisi jatkettava asetuksella (EY) N:o 526/2013 perustetun ENISAn toimintaa. Viraston olisi hoidettava tehtäviä, jotka sille annetaan tässä asetuksessa ja unionin säädöksissä kyberturvallisuuden alalla, muun muassa tarjoamalla asiantuntemusta ja neuvontaa ja toimimalla unionin tietokeskuksena. Sen olisi edistettävä parhaiden käytäntöjen vaihtoa jäsenvaltioiden ja yksityisten sidosryhmien välillä antamalla toimintapoliittisia ehdotuksia Euroopan komissiolle ja jäsenvaltioille, toimimalla viitetahona unionin alakohtaisille toimintapoliittisille aloitteille kyberturvallisuuskysymyksissä ja edistämällä operatiivista yhteistyötä jäsenvaltioiden välillä sekä jäsenvaltioiden ja EU:n toimielinten, virastojen ja elinten välillä.

[33] Euroopan parlamentin ja neuvoston asetus (EU) N:o 526/2013, annettu 21 päivänä toukokuuta 2013, Euroopan unionin verkko- ja tietoturvavirastosta (ENISA) ja asetuksen (EY) N:o 460/2004 kumoamisesta (EUVL L 165, 18.6.2013, s. 41).

(10) Eurooppa-neuvoston kokouksessa 13 päivänä joulukuuta 2003 hyväksytyllä päätöksellä 2004/97/EY, Euratom, jäsenvaltioiden edustajat päättivät, että ENISAn kotipaikaksi tulee Kreikan hallituksen myöhemmin nimeämä kaupunki Kreikassa. Viraston isäntäjäsenvaltion olisi huolehdittava siitä, että virastolla on parhaat mahdolliset toimintaedellytykset. Viraston tehtävien moitteettoman ja tehokkaan suorittamisen, henkilöstön palvelukseenoton ja sitouttamisen sekä verkostoitumisen tehokkuuden kannalta on ehdottoman tärkeää, että virasto sijaitsee soveltuvassa paikassa, jossa on muun muassa toimivat liikenneyhteydet ja palveluja viraston henkilöstön mukana tuleville puolisoille ja lapsille. Tarvittavat järjestelyt olisi vahvistettava viraston ja isäntäjäsenvaltion välisessä sopimuksessa, joka tehdään sen jälkeen kun viraston johtokunta on antanut hyväksyntänsä.

(11) Unioniin kohdistuvien kyberturvallisuushaasteiden lisääntyessä viraston määrärahoja ja henkilöresursseja olisi lisättävä siten, että ne vastaavat sen uutta roolia ja tehtäviä sekä sen keskeistä asemaa eurooppalaista digitaalista toimintaympäristöä puolustavassa organisaatioiden ekosysteemissä.

(12) Viraston olisi kehitettävä ja ylläpidettävä korkealaatuista asiantuntemusta ja toimittava viitetahona, joka vahvistaa uskoa ja luottamusta sisämarkkinoihin riippumattomuutensa, antamansa neuvonnan ja levittämänsä tiedon laadun, menettelyjensä ja toimintatapojensa avoimuuden sekä tehtäviensä suorittamisessa osoittamansa huolellisuuden ansiosta. Viraston olisi aktiivisesti edistettävä kansallisia ja unionin toimia ja suoritettava tehtävänsä täydessä yhteistyössä unionin toimielinten, elinten, laitosten ja virastojen sekä jäsenvaltioiden kanssa. Lisäksi viraston olisi hyödynnettävä yksityisen sektorin ja muiden asiaankuuluvien sidosryhmien näkemyksiä ja niiden kanssa tehtävää yhteistyötä. Viraston tehtävänannossa olisi vahvistettava, miten viraston on määrä saavuttaa tavoitteensa niin, että se pystyy toimimaan joustavasti.

(13) Viraston olisi avustettava komissiota antamalla neuvoja, lausuntoja ja analyysejä kaikista unionin asioista, jotka liittyvät kyberturvallisuusalan toimintapolitiikan ja lainsäädännön kehittämiseen, päivittämiseen ja uudelleentarkasteluun, mukaan lukien kriittisen infrastruktuurin suojaaminen ja kyberresilienssi. Viraston olisi toimittava neuvonnan ja asiantuntemuksen viitetahona unionin alakohtaisille toimintapoliittisille ja lainsäädännöllisille aloitteille, kun niihin liittyy kyberturvallisuuskysymyksiä.

(14) Viraston lähtökohtaisena tehtävänä on edistää asianomaisen lainsäädännön johdonmukaista täytäntöönpanoa ja erityisesti verkko- ja tietoturvadirektiivin tehokasta täytäntöönpanoa, millä on olennainen merkitys kyberresilienssin lisäämisen kannalta. Koska kyberuhkaympäristö muuttuu nopeasti, on selvää, että jäsenvaltioita on tuettava omaksumalla kokonaisvaltaisempi, monialainen lähestymistapa kyberresilienssin rakentamiseen.

(15) Viraston olisi avustettava jäsenvaltioita sekä unionin toimielimiä, elimiä, laitoksia ja virastoja niiden pyrkimyksissä kehittää ja parantaa valmiuksia ja varautumiskykyä ehkäistä ja havaita kyberturvallisuusongelmia ja -poikkeamia ja reagoida niihin verkko- ja tietojärjestelmien turvallisuuden kannalta. Viraston olisi erityisesti tuettava kansallisten CSIRT-toimijoiden kehittämistä ja tehostamista, jotta niiden kypsyys olisi yhteisellä korkealla tasolla unionissa. Viraston olisi myös autettava kehittämään ja päivittämään unionin ja jäsenvaltioiden strategioita, jotka koskevat verkko- ja tietojärjestelmien turvallisuutta, erityisesti kyberturvallisuutta, sekä edistettävä niiden levittämistä ja seurattava niiden täytäntöönpanon edistymistä. Viraston olisi myös tarjottava koulutusta ja koulutusmateriaalia julkisille elimille ja tarvittaessa

”koulutettava kouluttajia”, jotta voidaan auttaa jäsenvaltioita kehittämään omia koulutusvalmiuksia.

(16) Viraston olisi avustettava verkko- ja tietoturvadirektiivillä perustettua yhteistyöryhmää sen tehtävien suorittamisessa erityisesti tarjoamalla asiantuntemusta ja neuvontaa sekä helpotettava parhaiden käytäntöjen vaihtoa muun muassa keskeisten palvelujen tarjoajien yksilöimisestä, myös rajat ylittävien riippuvuussuhteiden osalta, siltä osin kuin kyse on riskeistä ja poikkeamista.

(17) Pyrkien edistämään julkisen ja yksityisen sektorin välistä ja yksityisen sektorin sisäistä yhteistyötä, erityisesti kriittisten infrastruktuurien suojelun tukemiseksi, viraston olisi helpotettava tietojen jakamisen ja analysoinnin alakohtaisten keskusten (ISAC) perustamista tarjoamalla käyttöön parhaita käytäntöjä ja ohjeita käytettävissä olevista välineistä ja menettelyistä sekä ohjeita tietojen jakamiseen liittyvien sääntelykysymysten ratkaisemiseksi.

(18) Viraston olisi koottava ja analysoitava CSIRT-toimijoilta ja CERT-EU:lta saatavat kansalliset raportit ja otettava käyttöön yhteiset säännöt, kieli ja terminologia tiedonvaihtoa varten. Viraston olisi myös otettava yksityinen sektori mukaan verkko- ja tietoturvadirektiivin kehykseen, jossa vahvistettiin perusta vapaaehtoiselle teknisten tietojen vaihdolle operatiivisella tasolla perustamalla CSIRT-verkosto.

(19) Viraston olisi osallistuttava EU:n tason vastaukseen laajamittaisten rajatylittävien kyberturvallisuuspoikkeamien ja -kriisien tapauksessa. Tähän tehtävään olisi kuuluttava tarvittavan tiedon keruu ja toimiminen välittäjänä CSIRT-verkoston ja tekniikan alan toimijoiden sekä kriisinhallinnasta vastaavien päätöksentekijöiden välillä. Lisäksi virasto voisi tukea poikkeamien käsittelyä teknisestä näkökulmasta helpottamalla tarvittavien ratkaisujen teknistä vaihtoa jäsenvaltioiden välillä ja osallistumalla julkiseen viestintään. Viraston olisi tuettava tätä prosessia testaamalla tällaisen yhteistyön menettelyjä vuotuisissa kyberturvallisuusharjoituksissa.

(20) Operatiivisten tehtäviensä hoitamiseksi viraston olisi hyödynnettävä saatavilla olevaa CERT-EU:n asiantuntemusta jäsennellyssä yhteistyössä, jossa osapuolet ovat fyysisesti lähellä toisiaan. Jäsennelty yhteistyö helpottaa luomaan tarvittavaa synergiaa ja kehittämään ENISAn asiantuntemusta. Tarvittaessa tällaisen yhteistyön käytännön toteutus olisi määriteltävä erityisin järjestelyin näiden kahden organisaation välillä.

(21) Operatiivisten tehtäviensä mukaisesti viraston olisi voitava tarjota tukea jäsenvaltioille, esimerkiksi antamalla neuvoja tai teknistä apua tai varmistamalla analyysit uhkista ja poikkeamista. Komission suosituksessa koordinoidusta reagoinnista laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin suositellaan, että jäsenvaltiot tekisivät yhteistyötä vilpittömässä mielessä ja vaihtaisivat keskenään ja ENISAn kanssa tietoja laajamittaisista kyberturvallisuuspoikkeamista ja -kriiseistä ilman aiheetonta viivytystä. Tällainen tieto auttaisi ENISAa sen operatiivisten tehtävien suorittamisessa.

(22) Viraston olisi osana unionin tilannetietoisuutta tukevaa säännöllistä teknisen tason yhteistyötä laadittava poikkeamista ja uhkista säännöllisesti EU:n kyberturvallisuuden tekninen tilanneraportti, joka perustuu julkisesti saatavilla oleviin tietoihin, sen omaan analyysiin sekä raportteihin, joita se on saanut jäsenvaltioiden CSIRT-toimijoilta (vapaaehtoisuuden pohjalta) tai verkko- ja tietoturvadirektiivillä perustetuilta keskitetyiltä yhteyspisteiltä, Europolissa toimivalta Euroopan kyberrikostorjuntakeskukselta (EC3) ja CERT-EU:lta sekä tarvittaessa EU:n tiedusteluanalyysikeskukselta (INTCEN) ja Euroopan ulkosuhdehallinnolta (EUH).

Raportti olisi asetettava neuvoston, komission ja unionin ulkoasioiden ja turvallisuuspolitiikan korkean edustajan asianomaisten yksiköiden ja CSIRT-verkoston saataville.

(23) Useampaan kuin yhteen jäsenvaltioon merkittävästi vaikuttaneista poikkeamista jälkikäteen tehtävät tekniset tutkinnat, joita virasto tukee tai jotka se suorittaa asianomaisten jäsenvaltioiden pyynnöstä tai suostumuksella, olisi kohdistettava poikkeamien välttämiseen jatkossa ja suoritettava rajoittamatta mahdollisia oikeudellisia tai hallinnollisia menettelyjä syyllisyyden tai vastuun osoittamiseksi.

(24) Asianomaisten jäsenvaltioiden olisi annettava virastolle tarvittavat tiedot ja apu tutkintaa varten rajoittamatta Euroopan unionin toiminnasta tehdyn sopimuksen 346 artiklan soveltamista ja sulkematta pois muita yleiseen järjestykseen liittyviä syitä.

(25) Jäsenvaltiot voivat pyytää yrityksiä, joita poikkeama koskee, tekemään yhteistyötä antamalla tarvittavan tiedon ja avun virastolle, sanotun kuitenkaan rajoittamatta niiden oikeutta suojata kaupallisesti arkaluonteiset tiedot.

(26) Ymmärtääkseen paremmin kyberturvallisuuteen liittyviä haasteita ja tarjotakseen strategista pitkän aikavälin neuvontaa jäsenvaltioille ja unionin toimielimille viraston on tarpeen analysoida nykyisiä ja kehittymässä olevia riskejä. Tätä varten viraston olisi yhteistyössä jäsenvaltioiden ja tarvittaessa tilastokeskusten ja muiden elinten kanssa kerättävä tarvittavaa tietoa sekä tehtävä analyysejä uusista teknologioista ja aihekohtaisia arviointeja teknologisten innovaatioiden odotettavissa olevista yhteiskunnallisista, oikeudellisista, taloudellisista ja sääntelyyn liittyvistä vaikutuksista verkko- ja tietoturvallisuuden ja erityisesti kyberturvallisuuden kannalta. Viraston olisi myös tuettava jäsenvaltioita ja unionin toimielimiä, virastoja ja elimiä kyberturvallisuuteen liittyvien uusien kehityssuuntausten kartoittamisessa ja kyberturvallisuuteen liittyvien ongelmien ehkäisyssä tekemällä analyyseja uhkista ja poikkeamista.

(27) Unionin resilienssin lisäämiseksi viraston olisi kehitettävä internetinfrastruktuurin ja elintärkeiden infrastruktuurien turvallisuuteen liittyvää huippuosaamista tarjoamalla neuvontaa, ohjeita ja parhaita käytäntöjä. Jotta kyberturvallisuusriskeistä ja mahdollisista suojakeinoista saataisiin tietoa helpommin ja paremmin jäsennellyssä muodossa, viraston olisi kehitettävä unionin ”tietokeskus” ja ylläpidettävä sitä. Kyseessä on keskitetty verkkoportaali, josta yleisö saa EU:n ja kansallisilta toimielimiltä, virastoilta ja laitoksilta peräisin olevaa tietoa kyberturvallisuudesta.

(28) Viraston olisi autettava lisäämään yleisön tietoisuutta kyberturvallisuuteen liittyvistä riskeistä ja annettava yksittäisille käyttäjille ohjeita hyvistä toimintatavoista kansalaisten ja organisaatioiden käyttöön. Viraston pitäisi osaltaan edistää parhaita käytäntöjä ja ratkaisuja yksilöiden ja organisaatioiden tasolla keräämällä ja analysoimalla julkisesti saatavilla olevia tietoja merkittävistä poikkeamista ja kokoamalla raportteja ohjeistuksen antamiseksi yrityksille ja kansalaisille ja yleisen varautumis- ja resilienssitason parantamiseksi. Viraston olisi myös järjestettävä yhteistyössä jäsenvaltioiden sekä unionin toimielinten, elinten, virastojen ja laitosten kanssa säännöllisiä loppukäyttäjille suunnattuja tiedotus- ja valistuskampanjoita, joiden tarkoituksena on edistää turvallisempaa verkkokäyttäytymistä yksilötasolla ja lisätä tietoisuutta verkossa piilevistä mahdollisista uhkista, mukaan lukien verkkourkintayritysten, bottiverkkojen sekä talous- ja pankkipetosten kaltainen kyberrikollisuus, sekä edistää yleisluonteisen neuvonnan antamista aitouden todentamista ja tietosuojaa koskevissa kysymyksissä. Virastolla olisi oltava keskeinen rooli pyrittäessä lisäämään loppukäyttäjien tietoisuutta laitteiden turvallisuudesta.

(29) Kyberturvallisuuden alalla toimivien yritysten ja kyberturvallisuusratkaisujen käyttäjien tukemiseksi viraston olisi kehitettävä ”markkinoiden seurantakeskus” ja ylläpidettävä sitä tekemällä säännöllisiä analyyseja kyberturvallisuusmarkkinoiden tärkeimmistä suuntauksista sekä kysyntä- että tarjontapuolella ja levittämällä tietoa näistä suuntauksista.

(30) Varmistaakseen tavoitteidensa täysimittaisen saavuttamisen viraston olisi oltava yhteydessä asiaankuuluviin toimielimiin, virastoihin ja elimiin, mukaan lukien CERT-EU, Europolissa toimiva Euroopan kyberrikostorjuntakeskus (EC3), Euroopan puolustusvirasto (EDA), laaja-alaisten tietojärjestelmien operatiivisesta hallinnoinnista vastaava eurooppalainen virasto (eu-LISA), Euroopan lentoturvallisuusvirasto (EASA) sekä muut kyberturvallisuuteen liittyviä kysymyksiä käsittelevät EU:n virastot. Sen olisi oltava yhteydessä myös tietosuoja-asioita käsitteleviin viranomaisiin, jotta voidaan vaihtaa tietotaitoa ja parhaita käytäntöjä ja antaa neuvontaa kyberturvallisuusnäkökohdista, joilla voi olla vaikutusta niiden toimintaan. Kansallisten ja unionin lainvalvonta- ja tietosuojaviranomaisten edustajien olisi voitava olla edustettuina viraston pysyvässä sidosryhmässä. Ollessaan yhteydessä lainvalvontaviranomaisiin sellaisissa verkko- ja tietoturvakysymyksissä, joilla voi olla vaikutusta niiden toimintaan, viraston olisi käytettävä olemassa olevia tiedonvaihtokanavia ja vakiintuneita verkostoja.

(31) Viraston olisi CSIRT-verkoston sihteeristönä toimivana jäsenenä tuettava jäsenvaltioiden CSIRT-toimijoita ja CERT-EU:ta operatiivisessa yhteistyössä kaikkien asiaankuuluvien CSIRT-verkoston tehtävien lisäksi, sellaisina kuin ne määritellään verkko- ja tietoturvadirektiivissä. Viraston olisi lisäksi edistettävä ja tuettava yhteistyötä asianomaisten CSIRT-toimijoiden välillä tapauksissa, joissa CSIRT-toimijoiden hallinnoimiin tai suojaamiin verkkoihin tai infrastruktuureihin kohdistuu poikkeamia, hyökkäyksiä tai häiriöitä, jotka koskevat tai mahdollisesti koskevat vähintään kahta CERT-toimijaa, ottaen asianmukaisesti huomioon CSIRT-verkoston menettelyohjeet.

(32) Jotta voidaan lisätä unionin varautumista kyberturvallisuuspoikkeamiin vastaamisessa, viraston olisi järjestettävä vuosittain kyberturvallisuusharjoituksia unionin tasolla sekä tuettava jäsenvaltioita ja EU:n toimielimiä, virastoja ja elimiä niiden pyynnöstä harjoitusten järjestämisessä.

(33) Viraston olisi kehitettävä ja ylläpidettävä asiantuntemustaan kyberturvallisuussertifioinnissa, jotta voidaan tukea unionin politiikkaa tällä alalla. Viraston olisi edistettävä kyberturvallisuussertifioinnin käyttöä unionissa muun muassa osallistumalla kyberturvallisuuden sertifiointikehyksen perustamiseen ja ylläpitoon unionin tasolla, jotta voidaan lisätä avoimuutta tieto- ja viestintätekniikan tuotteiden ja palvelujen kyberturvallisuuden varmistuksessa ja tällä tavoin vahvistaa luottamusta digitaalisiin sisämarkkinoihin.

(34) Tehokkaan kyberturvallisuuspolitiikan olisi perustuttava kehittyneisiin riskinarviointimenetelmiin niin julkisella kuin yksityiselläkin sektorilla. Riskinarviointimenetelmiä käytetään eri tasoilla vailla yhteistä tehokasta soveltamiskäytäntöä. Riskinarvioinnin ja yhteentoimivien riskinhallintaratkaisujen parhaiden käytäntöjen edistäminen ja kehittäminen julkisen ja yksityisen sektorin organisaatioissa nostaa kyberturvallisuustasoa unionissa. Tätä varten viraston olisi tuettava sidosryhmien yhteistyötä unionin tasolla ja helpotettava niiden pyrkimyksiä laatia ja ottaa käyttöön eurooppalaisia ja kansainvälisiä standardeja riskinhallinnalle ja mitattavissa olevalle turvallisuudelle sähköisissä tuotteissa, järjestelmissä, verkoissa ja

palveluissa, jotka yhdessä ohjelmistojen kanssa muodostavat verkko- ja tietojärjestelmät.

(35) Viraston olisi kannustettava jäsenvaltioita ja palveluntarjoajia tiukentamaan yleisiä turvallisuusnormejaan, jotta kaikki internetin käyttäjät voivat toteuttaa tarvittavat toimenpiteet oman kyberturvallisuutensa varmistamiseksi. Erityisesti palveluntarjoajien ja tuotteiden valmistajien olisi poistettava tuotannosta tai kierrätettävä tuotteet ja palvelut, jotka eivät täytä kyberturvallisuusnormeja. ENISA voi yhteistyössä toimivaltaisten viranomaisten kanssa levittää tietoa sisämarkkinoilla tarjottavien tuotteiden ja palvelujen kyberturvallisuustasosta ja antaa varoituksia palveluntarjoajille ja valmistajille ja vaatia niitä parantamaan tuotteidensa ja palvelujensa turvallisuutta, mukaan lukien kyberturvallisuus.

(36) Viraston olisi otettava täysimääräisesti huomioon meneillään olevat tutkimus-, kehittämis- ja teknologian arviointitoimet erityisesti unionin eri tutkimusaloitteissa antaakseen unionin toimielimille, elimille, virastoille ja laitoksille sekä tarvittaessa jäsenvaltioille pyynnöstä neuvoja verkko- ja tietoturva-alan tutkimustarpeista varsinkin kyberturvallisuuskysymyksissä.

(37) Kyberturvallisuuteen liittyvät ongelmat ovat maailmanlaajuisia. Tarvitaan tiiviimpää kansainvälistä yhteistyötä turvallisuusstandardien parantamiseksi, mihin sisältyy myös yhteisten käyttäytymisnormien määrittely, sekä tiedonvaihtoa kansainvälisen yhteistoiminnan nopeuttamiseksi verkko- ja tietoturvakysymyksissä samoin kuin yhteistä maailmanlaajuista lähestymistapaa näihin kysymyksiin. Tätä varten viraston olisi tuettava unionin osallistumista kolmansien maiden ja kansainvälisten organisaatioiden kanssa harjoitettavaan yhteistyöhön ja tämän yhteistyön lisäämistä tarjoamalla käyttöön asianomaisten unionin toimielinten, elinten, virastojen ja laitosten mahdollisesti tarvitsemaa asiantuntemusta ja analysointivalmiuksia.

(38) Viraston olisi voitava vastata tapauskohtaisiin neuvonta- ja avustamispyyntöihin, joita jäsenvaltiot ja EU:n toimielimet, virastot ja elimet esittävät ja jotka ovat viraston tavoitteiden mukaisia.

(39) On tarpeen panna täytäntöön tiettyjä viraston hallintoa koskevia periaatteita, jotta voidaan noudattaa EU:n erillisvirastoja käsittelevässä toimielinten välisessä työryhmässä heinäkuussa 2012 hyväksyttyä yhteistä julkilausumaa ja yhteistä lähestymistapaa, joiden tarkoituksena on tehostaa virastojen toimintaa ja parantaa niiden tuloksellisuutta. Yhteisen julkilausuman ja yhteisen lähestymistavan tulisi näkyä asianmukaisella tavalla myös viraston työohjelmissa, viraston arvioinneissa ja viraston raportointi- ja hallintokäytännöissä.

(40) Johtokunnan, jossa ovat edustettuna jäsenvaltiot ja komissio, olisi määriteltävä viraston toiminnan yleinen suunta ja varmistettava, että se hoitaa tehtäviään tämän asetuksen mukaisesti. Johtokunnalle olisi annettava tarvittavat valtuudet hyväksyä talousarvio, valvoa sen toteuttamista, vahvistaa tarvittavat varainhoitoa koskevat säännöt, luoda avoimet menettelyt viraston päätöksentekoa varten, hyväksyä viraston yhtenäinen ohjelma-asiakirja, vahvistaa työjärjestyksensä, nimittää pääjohtaja sekä päättää tämän toimikauden jatkamisesta ja päättymisestä.

(41) Viraston moitteettoman ja tehokkaan toiminnan takaamiseksi komission ja jäsenvaltioiden olisi varmistettava, että johtokunnan jäseniksi nimitettävillä henkilöillä on riittävä ammatillinen asiantuntemus ja kokemus toiminnallisilta aloilta. Johtokunnan työn jatkuvuuden varmistamiseksi komission ja jäsenvaltioiden olisi pyrittävä rajoittamaan johtokunnassa olevien edustajiensa vaihtuvuutta.

(42) Viraston moitteeton toiminta edellyttää, että sen pääjohtaja nimitetään ansioiden ja todistuksin osoitettujen hallinnollisten taitojen ja johtamistaitojen sekä kyberturvallisuuden kannalta merkityksellisen pätevyyden ja kokemuksen perusteella ja että pääjohtajan tehtäviä hoidetaan täysin riippumattomasti. Pääjohtajan olisi laadittava ehdotus viraston työohjelmaksi kuultuaan ensin komissiota ja toteutettava kaikki tarvittavat toimenpiteet varmistaakseen viraston työohjelman asianmukaisen toteuttamisen. Pääjohtajan olisi laadittava johtokunnalle esitettävä vuosikertomus sekä esitys viraston tuloja ja menoja koskevaksi ennakkoarvioksi ja vastattava talousarvion toteuttamisesta. Pääjohtajan olisi voitava perustaa tilapäisiä työryhmiä erityisesti tieteellisiä, teknisiä, oikeudellisia tai sosioekonomisia erityiskysymyksiä varten. Pääjohtajan olisi varmistettava, että tilapäisten työryhmien jäsenet valitaan huippuasiantuntemuksen perusteella ja ottaen asianmukaisesti huomioon tarkasteltavan kysymyksen edellyttämällä tavalla edustuksellinen tasapaino jäsenvaltioiden julkishallintojen, unionin toimielinten ja yksityisen sektorin välillä, mukaan lukien toimiala, käyttäjät ja tiedeyhteisöä edustavat verkko- ja tietoturva-asiantuntijat.

(43) Hallituksen olisi edistettävä johtokunnan moitteetonta toimintaa. Osana johtokunnan päätöksiin liittyvää valmistelutyötään sen olisi tutkittava yksityiskohtaisesti asiaan liittyvät tiedot ja tarkasteltava käytettävissä olevia vaihtoehtoja sekä tarjottava neuvoja ja ratkaisuja johtokunnan päätösten valmistelemiseksi.

(44) Virastolla olisi oltava neuvoa-antavana elimenä pysyvä sidosryhmä, jotta voitaisiin varmistaa säännöllinen yhteydenpito yksityisen sektorin, kuluttajajärjestöjen ja muiden asianosaisten sidosryhmien kanssa. Pysyvän sidosryhmän, jonka johtokunta perustaa pääjohtajan ehdotuksesta, olisi keskityttävä sidosryhmiä koskeviin asioihin ja saatettava ne viraston tietoon. Pysyvän sidosryhmän kokoonpanossa ja tälle ryhmälle, jotka kuullaan erityisesti työohjelmaluonnoksesta, annettavissa tehtävissä olisi varmistettava sidosryhmien riittävä edustus viraston työskentelyssä.

(45) Virastolla olisi oltava säännöt eturistiriitojen ehkäisemisestä ja hallinnasta. Viraston olisi sovellettava asiakirjojen saamista yleisön tutustuttavaksi koskevia asiaankuuluvia unionin säännöksiä, sellaisina kuin ne on vahvistettu Euroopan parlamentin ja neuvoston asetuksessa (EY) N:o 1049/2001[34]. Viraston suorittamassa henkilötietojen käsittelyssä olisi noudatettava yksilöiden suojelusta yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta 18 päivänä joulukuuta 2000 annettua Euroopan parlamentin ja neuvoston asetusta (EY) N:o 45/2001[35]. Viraston olisi noudatettava tietojen käsittelyä koskevia unionin toimielimiin sovellettavia määräyksiä ja kansallista lainsäädäntöä, erityisesti kun on kyse arkaluonteisista turvallisuusluokittelemattomista ja EU:n turvallisuusluokitelluista tiedoista.

(46) Jotta voidaan varmistaa viraston täydellinen itsemääräämisoikeus ja riippumattomuus ja jotta virasto pystyy suorittamaan uusia ja täydentäviä tehtäviä, myös ennakoimattomia tehtäviä hätätilanteissa, virastolle olisi annettava riittävä ja itsenäinen talousarvio, jonka tulot koostuvat ensisijaisesti unionin rahoitusosuudesta ja viraston työhön osallistuvien kolmansien maiden rahoitusosuuksista. Viraston

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

[35] EYVL L 8, 12.1.2001, s. 1.

henkilöstön enemmistön työtehtävien olisi liityttävä suoraan viraston toimeksiannon operatiiviseen täytäntöönpanoon. Viraston isäntäjäsenvaltion tai minkä tahansa muun jäsenvaltion olisi voitava maksaa vapaaehtoisia rahoitusosuuksia virastolle. Unionin talousarviomenettelyä olisi sovellettava edelleen unionin yleisestä talousarviosta maksettaviin tukiin. Lisäksi tilintarkastustuomioistuimen olisi tarkastettava viraston tilit avoimuuden ja vastuuvelvollisuuden varmistamiseksi.

(47) Vaatimustenmukaisuuden arviointi on menettely sen osoittamiseksi, täyttyvätkö tuotteelle, prosessille, palvelulle, järjestelmälle, henkilölle tai elimelle asetetut erityiset vaatimukset. Tätä asetusta sovellettaessa sertifiointi olisi katsottava vaatimustenmukaisuuden arvioinnin tyypiksi, joka koskee tuotteen, prosessin, palvelun, järjestelmän tai näiden yhdistelmän, jäljempänä ’tieto- ja viestintätekniikan tuotteet ja palvelut’, kyberturvallisuusominaisuuksia ja jonka suorittaa riippumaton kolmas osapuoli, joka ei ole tuotteen valmistaja tai palvelun tarjoaja. Sertifiointi ei sinänsä takaa, että sertifioidut tieto- ja viestintätekniikan tuotteet ja palvelut ovat kyberturvallisia. Se on pikemminkin menettely ja tekninen menetelmä todistaa, että tieto- ja viestintätekniikan tuotteet ja palvelut on testattu ja että ne täyttävät tietyt kyberturvallisuusvaatimukset, jotka on vahvistettu muualla, esimerkiksi teknisissä standardeissa.

(48) Kyberturvallisuussertifioinnilla on tärkeä rooli lisättäessä tieto- ja viestintätekniikan tuotteiden ja palvelujen turvallisuutta ja niihin tunnettua luottamusta. Digitaaliset sisämarkkinat ja erityisesti datatalous ja esineiden internet voivat menestyä vain, jos vallitsee yleinen julkinen luottamus siihen, että tuotteissa ja palveluissa varmistetaan kyberturvallisuus tietyllä tasolla. Verkkoyhteyksillä varustetut ja automatisoidut autot, sähköiset terveyspalvelut, teollisuusautomaation ohjausjärjestelmät ja älykkäät verkot ovat joitakin esimerkkejä aloista, joilla sertifiointi on jo laajalti käytössä tai tulee todennäköisesti käyttöön lähitulevaisuudessa. Verkko- ja tietoturvadirektiivillä säännellyt alat ovat samalla aloja, joilla kyberturvallisuussertifioinnilla on ratkaiseva merkitys.

(49) Vuonna 2016 antamassaan tiedonannossa ”Euroopan kyberresilienssijärjestelmän vahvistaminen sekä kilpailukykyisen ja innovatiivisen kyberturvallisuustoimialan tukeminen” komissio linjasi tarpeen ottaa käyttöön laadukkaita, kohtuuhintaisia ja yhteentoimivia kyberturvallisuustuotteita ja -ratkaisuja. Tieto- ja viestintätekniikan tuotteiden ja -palvelujen tarjonta sisämarkkinoilla on edelleen maantieteellisesti hyvin hajanaista. Tämä johtuu siitä, että Euroopan kyberturvallisuusala on kehittynyt suurelta osin kansallisista valtiollisen kysynnän lähtökohdista. Kyberturvallisuuden sisämarkkinoiden toimintapuutteisiin kuuluu lisäksi yhteentoimivien ratkaisujen (teknisten standardien), toimintatapojen ja EU:n laajuisten sertifiointimekanismien puuttuminen. Tämä yhtäältä vaikeuttaa eurooppalaisten yritysten kilpailua niin kansallisella kuin Euroopan ja maailmanlaajuisellakin tasolla ja toisaalta vähentää yksilöiden ja yritysten saatavilla olevan hyödyllisen ja käyttökelpoisen kyberturvallisuusteknologian valinnanvaraa. Samoin myös digitaalisten sisämarkkinoiden strategian täytäntöönpanon väliarvioinnissa komissio korosti tarvetta huolehtia verkkoon liitettyjen tuotteiden ja järjestelmien turvallisuudesta ja totesi, että luomalla tieto- ja viestintätekniikan turvallisuudelle eurooppalaiset puitteet, joissa annetaan säännöt tieto- ja viestintäteknologian turvallisuussertifioinnin järjestämisestä unionissa, voitaisiin sekä ylläpitää luottamusta internetiin ja puuttua kyberturvallisuuden markkinoiden nykyiseen hajanaisuuteen.

(50) Tieto- ja viestintätekniikan tuotteiden ja palvelujen kyberturvallisuussertifiointia käytetään tällä hetkellä vain vähäisessä määrin. Kun sitä käytetään, käyttö rajoittuu

enimmäkseen jäsenvaltioiden tasolle tai teollisuuslähtöisten järjestelmien piiriin. Tässä yhteydessä yhden kansallisen kyberturvallisuusviranomaisen myöntämää sertifikaattia ei periaatteessa tunnusteta muissa jäsenvaltioissa. Yritykset voivat näin ollen joutua sertifioimaan tuotteensa ja palvelunsa useissa jäsenvaltioissa, joissa ne toimivat, esimerkiksi voidakseen osallistua kansallisiin hankintamenettelyihin. Syntymässä on uusia järjestelmiä, mutta vaikuttaa siltä, ettei ole olemassa johdonmukaista ja kokonaisvaltaista lähestymistapaa laaja-alaisiin kyberturvallisuuskysymyksiin esimerkiksi esineiden internetin alalla. Nykyisissä järjestelmissä on merkittäviä puutteita ja eroja, jotka liittyvät niiden tuotekatteeseen, varmuustasoihin, aineellisiin edellytyksiin ja tosiasialliseen käyttöön.

(51) Joillain toimilla on jo pyritty sertifikaattien vastavuoroiseen tunnustamiseen Euroopassa. Niiden tavoitteet on kuitenkin saavutettu vain osittain. Tärkein esimerkki tästä on johtavien virkamiesten tietoturvallisuusryhmän (SOGIS) vastavuoroista tunnustamista koskeva sopimus (MRA). SOGIS MRA on tärkein malli yhteistyölle ja vastavuoroiselle tunnustamiselle turvallisuussertifioinnin alalla, mutta siihen liittyy merkittäviä puutteita johtuen sen korkeista kustannuksista ja rajallisesta soveltamisalasta. Toistaiseksi on kehitetty vain muutamia suojausprofiileja digitaalisille tuotteille, kuten digitaaliselle allekirjoitukselle, digitaaliselle ajopiirturille ja älykorteille. Tärkein puute on se, SOGIS-ryhmään kuuluu vain osa unionin jäsenvaltioista. Tämä on rajoittanut SOGIS MRA:n toimivuutta sisämarkkinoiden kannalta.

(52) Edellä esitetyn perusteella on tarpeen perustaa eurooppalainen kyberturvallisuuden sertifiointikehys, jossa vahvistetaan tärkeimmät horisontaaliset vaatimukset kehitettäville eurooppalaisille kyberturvallisuuden sertifiointijärjestelmille ja jonka ansiosta tieto- ja viestintätekniikan tuotteita ja palveluja koskevat sertifikaatit voidaan tunnustaa ja ottaa käyttöön kaikissa jäsenvaltioissa. Eurooppalaisen sertifiointikehyksen tulisi palvella kahta tarkoitusta. Yhtäältä sen pitäisi lisätä luottamusta tieto- ja viestintätekniikan tuotteisiin ja palveluihin, jotka on sertifioitu tällaisten järjestelmien mukaisesti. Toisaalta sen avulla pitäisi välttää tilanne, jossa käytössä on monia keskenään ristiriitaisia tai päällekkäisiä kansallisia kyberturvallisuussertifiointeja, ja vähentää siten digitaalisilla sisämarkkinoilla yrityksille aiheutuvia kustannuksia. Järjestelmien olisi oltava syrjimättömiä ja kansainvälisiin ja/tai unionin standardeihin perustuvia, paitsi jos kyseiset standardit ovat tehottomia tai epäasianmukaisia EU:n oikeutettujen tavoitteiden saavuttamiseksi.

(53) Komissiolle olisi siirrettävä valta hyväksyä eurooppalaiset kyberturvallisuuden sertifiointijärjestelmät yksittäisille tieto- ja viestintätekniikan tuotteiden ja palvelujen ryhmille. Kansallisten sertifioinnin valvontaviranomaisten olisi vastattava näiden järjestelmien täytäntöönpanosta ja valvonnasta, ja näissä järjestelmissä myönnettyjen sertifikaattien olisi oltava voimassa ja tunnustettuja kaikkialla unionissa. Toimialan tai muiden yksityisten organisaatioiden ylläpitämien sertifiointijärjestelmien ei tulisi kuulua tämän asetuksen soveltamisalaan. Tällaisia järjestelmiä ylläpitävät elimet voivat kuitenkin ehdottaa, että komissio ottaa tällaiset järjestelmät lähtökohdaksi niiden hyväksymiseksi eurooppalaisena järjestelmänä.

(54) Tämän asetuksen säännökset eivät saisi vaikuttaa unionin lainsäädäntöön, jossa annetaan erityiset säännöt tieto- ja viestintätekniikan tuotteiden ja palvelujen sertifioinnista. Erityisesti yleisessä tietosuoja-asetuksessa säädetään sertifiointimekanismeista sekä tietosuojasineteistä ja -merkeistä, joiden tarkoituksena on osoittaa, että rekisterinpitäjät ja henkilötietojen käsittelijät noudattavat kyseistä asetusta käsittelytoimia suorittaessaan. Rekisteröityjen olisi tällaisten

sertifiointimekanismien ja tietosuojasinettien ja -merkkien avulla voitava nopeasti arvioida asianomaisten tuotteiden ja palvelujen tietosuojataso. Tämä asetus ei rajoita tietojenkäsittelytoimintojen sertifiointia yleisen tietosuoja-asetuksen mukaisesti, ei myöskään silloin, kun nämä toimet on sisällytetty tuotteisiin ja palveluihin.

(55) Eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien tarkoituksena olisi oltava varmistaa, että tällaisessa järjestelmässä sertifioidut tieto- ja viestintätekniikan tuotteet ja palvelut täyttävät määritellyt vaatimukset. Nämä vaatimukset koskevat kykyä suojautua tietyllä varmuustasolla toimilta, joiden tarkoituksena on vaarantaa tallennettujen, siirrettävien tai käsiteltävien tietojen tai niihin liittyvien kyseisissä tuotteissa, prosesseissa, palveluissa ja järjestelmissä tarjottavien tai välitettävien toimintojen tai palvelujen käytettävyys, aitous, eheys ja luottamuksellisuus tässä asetuksessa tarkoitetussa merkityksessä. Tässä asetuksessa ei ole mahdollista määritellä yksityiskohtaisesti kyberturvallisuusvaatimuksia kaikille tieto- ja viestintätekniikan tuotteille ja palveluille. Tieto- ja viestintätekniikan tuotteet ja palvelut ja niihin liittyvät kyberturvallisuustarpeet ovat niin moninaiset, että on hyvin vaikeaa määritellä yleisiä kyberturvallisuusvaatimuksia, jotka olisivat voimassa kaikkialla. Siksi kyberturvallisuus olisi määriteltävä laajasti ja yleisesti sertifiointitarkoituksia varten ja sitä olisi täydennettävä erityisillä kyberturvallisuustavoitteilla, jotka on tarpeen ottaa huomioon suunniteltaessa eurooppalaisia kyberturvallisuuden sertifiointijärjestelmiä. Se, miten tällaiset tavoitteet saavutetaan yksittäisissä tieto- ja viestintätekniikan tuotteissa ja palveluissa, olisi täsmennettävä yksityiskohtaisemmin komission hyväksymien yksittäisten sertifiointijärjestelmien tasolla, esimerkiksi viittaamalla standardeihin tai teknisiin eritelmiin.

(56) Komissiolle olisi annettava valtuudet pyytää ENISAa valmistelemaan yksittäisiä tieto- ja viestintätekniikan tuotteita tai palveluja varten ehdolla olevat järjestelmät. Edelleen komissiolle olisi annettava valtuudet hyväksyä ENISAn valmisteleman ehdolla olevan järjestelmän pohjalta eurooppalainen kyberturvallisuuden sertifiointijärjestelmä täytäntöönpanosäädöksillä. Kun otetaan huomioon tämän asetuksen yleinen tarkoitus ja siinä määritellyt turvallisuustavoitteet, komission hyväksymissä eurooppalaisissa kyberturvallisuuden sertifiointijärjestelmissä olisi määriteltävä tietyt vähimmäistekijät yksittäisen järjestelmän kohteen, soveltamisalan ja toiminnan osalta. Näihin olisi sisällyttävä muun muassa kyberturvallisuussertifioinnin soveltamisala ja kohde, mukaan lukien sertifioinnin kattamat tieto- ja viestintätekniikan tuotteiden ja palvelujen luokat, yksityiskohtainen eritelmä kyberturvallisuusvaatimuksista esimerkiksi viittaamalla standardeihin tai teknisiin eritelmiin, yksittäiset arviointiperusteet ja -menetelmät sekä aiottu varmuustaso: perustaso, korotettu ja/tai korkea.

(57) Eurooppalaisen kyberturvallisuussertifioinnin käytön tulisi edelleen olla vapaaehtoista, jollei toisin säädetä unionin tai kansallisessa lainsäädännössä. Jotta voitaisiin kuitenkin saavuttaa tämän asetuksen tavoitteet ja välttää hajanaisuus sisämarkkinoilla, sellaisten kansallisten kyberturvallisuuden sertifiointijärjestelmien tai -menettelyjen, joiden kattamat tieto- ja viestintätekniikan tuotteet ja palvelut kuuluvat jonkin eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän soveltamisalaan, olisi lakattava tuottamasta oikeusvaikutuksia alkaen päivästä, jonka komissio vahvistaa täytäntöönpanosäädöksessä. Jäsenvaltiot eivät myöskään saisi ottaa käyttöön uusia kansallisia kyberturvallisuuden sertifiointijärjestelmiä tieto- ja viestintätekniikan tuotteille ja palveluille, jotka kuuluvat jo jonkin olemassa olevan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän soveltamisalaan.

(58) Kun eurooppalainen kyberturvallisuuden sertifiointijärjestelmä on hyväksytty, tieto- ja viestintätekniikan tuotteiden valmistajien tai tieto- ja viestintätekniikan palvelujen tarjoajien olisi voitava jättää tuotteidensa tai palvelujensa sertifiointia koskeva hakemus valitsemalleen vaatimustenmukaisuuden arviointilaitokselle. Vaatimustenmukaisuuden arviointilaitosten olisi saatava akkreditointi akkreditointielimeltä, jos ne täyttävät tässä asetuksessa vahvistetut tietyt erityiset vaatimukset. Akkreditointi olisi myönnettävä enintään viideksi vuodeksi, ja se voidaan uusia samoin edellytyksin, jos vaatimustenmukaisuuden arviointilaitos täyttää vaatimukset. Akkreditointielimen olisi peruutettava vaatimustenmukaisuuden arviointilaitoksen akkreditointi, jos akkreditoinnin edellytykset eivät täyty tai eivät enää täyty tai jos vaatimustenmukaisuuden arviointilaitoksen toiminta rikkoo tämän asetuksen säännöksiä.

(59) On tarpeen velvoittaa kaikki jäsenvaltiot nimeämään yksi kyberturvallisuussertifioinnin valvontaviranomainen valvomaan sitä, ovatko niiden alueelle sijoittautuneet vaatimustenmukaisuuden arviointilaitokset ja niiden myöntämät sertifikaatit tämän asetuksen vaatimusten ja asianomaisten kyberturvallisuuden sertifiointijärjestelmien vaatimusten mukaisia. Kansallisten sertifioinnin valvontaviranomaisten olisi käsiteltävä luonnollisten tai oikeushenkilöiden tekemät valitukset, jotka liittyvät niiden alueelle sijoittautuneiden vaatimustenmukaisuuden arviointilaitosten myöntämiin sertifikaatteihin, tutkittava asianmukaisessa määrin valituksen kohde ja ilmoitettava valituksen tekijälle tutkinnan etenemisestä ja tuloksesta kohtuullisessa ajassa. Lisäksi niiden olisi tehtävä yhteistyötä muiden kansallisten sertifioinnin valvontaviranomaisten tai muiden viranomaisten kanssa esimerkiksi jakamalla tietoa mahdollisista tapauksista, joissa tieto- ja viestintätekniikan tuotteet ja palvelut eivät vastaa tämän asetuksen tai yksittäisten kyberturvallisjärjestelmien vaatimuksia.

(60) Eurooppalaisen kyberturvallisuuden sertifiointikehyksen johdonmukaisen soveltamisen varmistamiseksi olisi perustettava Euroopan kyberturvallisuuden sertifiointiryhmä, jäljempänä ’sertifiointiryhmä’, joka koostuu kansallisista sertifioinnin valvontaviranomaisista. Ryhmän päätehtävinä tulisi olla neuvoa ja avustaa komissiota sen pyrkiessä varmistamaan eurooppalaisen kyberturvallisuuden sertifiointikehyksen yhdenmukaisen täytäntöönpanon ja soveltamisen, avustaa virastoa ehdolla olevien kyberturvallisuuden sertifiointijärjestelmien valmistelussa tiiviissä yhteistyössä sen kanssa, suosittaa, että komissio pyytää virastoa valmistelemaan ehdolla olevan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän, sekä antaa komissiolle osoitettuja lausuntoja voimassa olevien eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien ylläpitämisestä ja tarkistamisesta.

(61) Tietoisuuden lisäämiseksi ja tulevien EU:n kyberturvallisuusjärjestelmien hyväksymisen helpottamiseksi Euroopan komissio voi antaa yleisiä tai alakohtaisia kyberturvallisuutta koskevia suuntaviivoja esimerkiksi hyvistä kyberturvallisuuskäytännöistä tai vastuullisesta kyberturvallisuuskäyttäytymisestä korostaen sertifioitujen tieto- ja viestintätekniikan tuotteiden ja palvelujen käytön myönteistä vaikutusta.

(62) Viraston kyberturvallisuussertifioinnille tarjoamaan tukeen olisi kuuluttava myös yhteydenpito neuvoston turvallisuuskomiteaan ja asianomaiseen kansalliseen elimeen, kun on kyse turvallisuusluokitellun aineiston verkoissa käytettävien tuotteiden kryptografisesta hyväksymisestä.

(63) Jotta voidaan täsmentää tarkemmin kriteerit vaatimustenmukaisuuden arviointilaitosten akkreditointia varten, komissiolle olisi siirrettävä valta hyväksyä säädösvallan siirron nojalla annettavia delegoituja säädöksiä Euroopan unionin toiminnasta tehdyn sopimuksen 290 artiklan mukaisesti. Komissio järjestää valmistelutyönsä aikana asianmukaisia kuulemisia, myös asiantuntijatasolla. Nämä kuulemiset toteutetaan paremmasta lainsäädännöstä 13 päivänä huhtikuuta 2016 tehdyssä toimielinten välisessä sopimuksessa 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.

(64) Jotta voidaan varmistaa tämän asetuksen yhdenmukainen täytäntöönpano, komissiolle olisi siirrettävä täytäntöönpanovalta tässä asetuksessa säädetyn mukaisesti. Tätä valtaa olisi käytettävä asetuksen (EU) N:o 182/2011 mukaisesti.

(65) Olisi sovellettava tarkastusmenettelyä hyväksyttäessä täytäntöönpanosäädöksiä, jotka koskevat tieto- ja viestintätekniikan tuotteiden ja palvelujen eurooppalaisia kyberturvallisuuden sertifiointijärjestelmiä, viraston tutkimusten toteuttamista koskevia yksityiskohtaisia sääntöjä sekä kansallisten sertifioinnin valvontaviranomaisten komissiolle tekemien, akkreditoituja vaatimustenmukaisuuden arviointilaitoksia koskevien ilmoitusten olosuhteita, muotoseikkoja ja menettelyjä.

(66) Viraston toimintaa olisi arvioitava riippumattomasti. Arvioinnissa olisi otettava huomioon viraston tavoitteiden saavuttaminen, sen toimintatavat ja sen tehtävien merkityksellisyys. Arvioinnissa olisi myös arvioitava eurooppalaisen kyberturvallisuuden sertifiointikehyksen vaikutusta, vaikuttavuutta ja tehokkuutta.

(67) Asetus (EU) N:o 526/2013 olisi kumottava.

(68) Jäsenvaltiot eivät voi riittävällä tavalla saavuttaa tämän asetuksen tavoitteita, vaan ne voidaan saavuttaa paremmin unionin tasolla, joten unioni voi toteuttaa toimenpiteitä Euroopan unionista tehdyn sopimuksen 5 artiklassa vahvistetun toissijaisuusperiaatteen mukaisesti. Mainitussa artiklassa vahvistetun suhteellisuusperiaatteen mukaisesti tässä asetuksessa ei ylitetä sitä, mikä on tarpeen tämän tavoitteen saavuttamiseksi,

OVAT HYVÄKSYNEET TÄMÄN ASETUKSEN:

I OSASTO

YLEISET SÄÄNNÖKSET

1 artikla
Kohde ja soveltamisala

Sisämarkkinoiden asianmukaisen toiminnan varmistamiseksi, pyrkien samalla kyberturvallisuuden, kyberresilienssin ja luottamuksen korkeaan tasoon unionissa, tässä asetuksessa

a) vahvistetaan ”EU:n kyberturvallisuusviraston” ENISAn, jäljempänä ’virasto’, tavoitteet, tehtävät ja organisatoriset näkökohdat ja

b) vahvistetaan kehys eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien perustamiselle, jotta voidaan varmistaa riittäväntasoinen kyberturvallisuus tieto- ja viestintätekniikan tuotteille ja palveluille unionissa. Tämän kehyksen soveltaminen ei rajoita niiden erityisten säännösten soveltamista, jotka koskevat vapaaehtoista tai pakollista sertifiointia muiden unionin säädösten nojalla.

2 *artikla*
Määritelmät

Tässä asetuksessa tarkoitetaan:

1) ’kyberturvallisuudella’ kaikkia toimia, joita tarvitaan verkko- ja tietojärjestelmien, niiden käyttäjien ja asianosaisten henkilöiden suojaamiseksi kyberuhilta;

2) ’verkko- ja tietojärjestelmällä’ direktiivin (EU) 2016/1148 4 artiklan 1 kohdassa tarkoitettua järjestelmää;

3) ’verkko- ja tietojärjestelmien turvallisuutta koskevalla kansallisella strategialla’ direktiivin (EU) 2016/1148 4 artiklan 3 kohdassa tarkoitettua kehystä;

4) ’keskeisten palvelujen tarjoajalla’ direktiivin (EU) N:o 2016/1148 4 artiklan 4 kohdassa määriteltyä julkista tai yksityistä toimijaa;

5) ’digitaalisen palvelun tarjoajalla’ direktiivin (EU) N:o 2016/1148 4 artiklan 6 kohdassa määriteltyä digitaalisen palvelun tarjoavaa oikeushenkilöä;

6) ’poikkeamalla’ direktiivin (EU) N:o 2016/1148 4 artiklan 7 kohdassa määriteltyä tapahtumaa;

7) ’poikkeamien käsittelyllä’ direktiivin (EU) N:o 2016/1148 4 artiklan 8 kohdassa määriteltyä menettelyä;

8) ’kyberuhalla’ potentiaalista tilannetta tai tapahtumaa, joka voi vaikuttaa haitallisesti verkko- ja tietojärjestelmiin, niiden käyttäjiin ja asianosaisiin henkilöihin;

9) ’eurooppalaisella kyberturvallisuuden sertifiointijärjestelmällä’ unionin tasolla määriteltyjä kattavia sääntöjä, teknisiä vaatimuksia, standardeja ja menettelyjä, joita sovelletaan kyseisen erityisen järjestelmän kattamien tieto- ja viestintätekniikan tuotteiden ja palvelujen sertifiointiin;

10) ’eurooppalaisella kyberturvallisuussertifikaatilla’ vaatimustenmukaisuuden arviointilaitoksen antamaa asiakirjaa, jolla todistetaan, että tietty tieto- ja

viestintätekniikan tuote tai palvelu täyttää eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä vahvistetut erityiset vaatimukset;

11) ’tieto- ja viestintätekniikan tuotteella tai palvelulla’ mitä tahansa verkko- ja tietojärjestelmien elementtiä tai elementtien ryhmää;

12) ’akkreditoinnilla’ asetuksen (EY) N:o 765/2008 2 artiklan 10 kohdassa määriteltyä akkreditointia;

13) ’kansallisella akkreditointielimellä’ asetuksen (EY) N:o 765/2008 2 artiklan 11 kohdassa määriteltyä kansallista akkreditointielintä;

14) ’vaatimustenmukaisuuden arvioinnilla’ vaatimustenmukaisen arviointia sellaisena kuin se on määritelty asetuksen (EY) N:o 765/2008 2 artiklan 12 alakohdassa;

15) ’vaatimustenmukaisuuden arviointilaitoksella’ asetuksen (EY) N:o 765/2008 2 artiklan 13 alakohdassa määriteltyä vaatimustenmukaisuuden arviointilaitosta;

16) ’standardilla’ asetuksen (EU) N:o 1025/2012 2 artiklan 1 kohdassa määriteltyä standardia.

II OSASTO
EU:n kyberturvallisuusvirasto ENISA

I LUKU
TOIMEKSIANTO, TAVOITTEET JA TEHTÄVÄT

3 artikla
Toimeksianto

1. Virasto hoitaa sille tämän asetuksen mukaisesti kuuluvia tehtäviä kyberturvallisuuden korkean tason edistämiseksi unionissa.

2. Virasto suorittaa tehtävät, jotka sille annetaan unionin säädöksissä, joissa vahvistetaan toimenpiteet jäsenvaltioiden lakien, asetusten ja hallinnollisten määräysten lähentämiseksi kyberturvallisuuden alalla.

3. Viraston tavoitteet ja tehtävät eivät rajoita kyberturvallisuutta koskevaa jäsenvaltioiden toimivaltaa eivätkä missään tapauksessa toimia, jotka koskevat yleistä turvallisuutta, puolustusta, kansallista turvallisuutta tai yksittäisen valtion toimia rikosoikeuden alalla.

4 artikla
Tavoitteet

1. Virasto on kyberturvallisuuden osaamiskeskus riippumattomuutensa, antamansa neuvonnan ja avun ja tarjoamansa tiedon tieteellisen ja teknisen laadun, toimintatapojensa ja -menettelyjensä avoimuuden sekä tehtäviensä suorittamisessa osoittamansa huolellisuuden ansiosta.

2. Virasto auttaa unionin toimielimiä, virastoja ja elimiä sekä jäsenvaltioita kehittämään ja panemaan täytäntöön kyberturvallisuutta koskevat toimintapolitiikat.

3. Virasto tukee valmiuksien kehittämistä ja varautumista kaikkialla unionissa avustamalla unionia, jäsenvaltioita sekä julkisia ja yksityisiä sidosryhmiä niiden verkko- ja tietojärjestelmien suojelun lisäämiseksi, ammattitaidon ja osaamisen kehittämiseksi kyberturvallisuuden alalla ja kyberresilienssin saavuttamiseksi.

4. Virasto edistää yhteistyötä ja koordinointia unionin tasolla jäsenvaltioiden, unionin toimielinten, virastojen ja elinten sekä asiaankuuluvien sidosryhmien välillä, mukaan lukien yksityinen sektori, kyberturvallisuuteen liittyvissä kysymyksissä.

5. Virasto lisää kyberturvallisuusvalmiuksia unionin tasolla jäsenvaltioiden toimien täydentämiseksi kyberuhkien ehkäisemisessä ja niihin vastaamisessa erityisesti rajat ylittävien poikkeamien tapauksessa.

6. Virasto edistää sertifioinnin käyttöä muun muassa osallistumalla kyberturvallisuuden sertifiointikehyksen perustamiseen ja ylläpitoon unionin tasolla tämän asetuksen III osaston mukaisesti, jotta voidaan lisätä avoimuutta tieto- ja viestintätekniikan tuotteiden ja palvelujen kyberturvallisuuden varmistuksessa ja tällä tavoin vahvistaa luottamusta digitaalisiin sisämarkkinoihin.

7. Virasto edistää tietoisuuden korkeaa tasoa kansalaisten ja yritysten keskuudessa kyberturvallisuuteen liittyvissä kysymyksissä.

5 artikla

Unionin politiikan ja lainsäädännön kehittämiseen ja täytäntöönpanoon liittyvät tehtävät

Virasto edistää unionin politiikan ja lainsäädännön kehittämistä ja täytäntöönpanoa tehtävänään

1. avustaa ja neuvoa erityisesti antamalla riippumattomia lausuntoja ja tekemällä valmistelutyötä unionin politiikan ja lainsäädännön kehittämisessä ja tarkistamisessa kyberturvallisuuden alalla sekä alakohtaisissa toimintapoliittisissa ja lainsäädännöllisissä aloitteissa, kun niihin liittyy kyberturvallisuuskysymyksiä;
2. auttaa jäsenvaltioita panemaan johdonmukaisesti täytäntöön erityisesti direktiiviin (EU) 2016/1148 liittyvää unionin kyberturvallisuuspolitiikkaa ja -lainsäädäntöä muun muassa antamalla lausuntoja, ohjeita ja neuvoja ja laatimalla parhaita käytäntöjä riskinhallinnan, poikkeamista raportoinnin ja tietojen jakamisen kaltaisista aiheista sekä helpottamalla parhaiden käytäntöjen vaihtoa toimivaltaisten viranomaisten välillä tältä osin;
3. edesauttaa yhteistyöryhmän työtä direktiivin (EU) 2016/1148 11 artiklan mukaisesti antamalla asiantuntemusta ja apua;
4. tukea
    1) unionin politiikan valmistelua ja täytäntöönpanoa sähköisen henkilöllisyyden ja sähköisten luottamuspalvelujen alalla erityisesti antamalla neuvoja ja teknisiä ohjeita sekä helpottamalla parhaiden käytäntöjen vaihtoa toimivaltaisten viranomaisten välillä;
    2) sähköisen viestinnän turvallisuuden parantamista muun muassa tarjoamalla asiantuntemusta ja neuvontaa sekä helpottamalla parhaiden käytäntöjen vaihtoa toimivaltaisten viranomaisten välillä;
5. tukea unionin poliittisten toimien säännöllistä uudelleentarkastelua antamalla vuosiraportti asianomaisen lainsäädännön täytäntöönpanosta liittyen seuraaviin:
    a) poikkeamista tehtävät jäsenvaltioiden ilmoitukset, jotka keskitetyt yhteyspisteet toimittavat yhteistyöryhmälle direktiivin (EU) 2016/1148 10 artiklan 3 kohdan mukaisesti;
    b) luottamuspalvelun tarjoajiin liittyvät tietoturvaloukkausta tai eheyden menetystä koskevat ilmoitukset, jotka valvontaelimet toimittavat virastolle asetuksen (EU) N:o 910/2014 19 artiklan 3 kohdan mukaisesti;
    c) yleisiä viestintäverkkoja tai yleisesti saatavilla olevia sähköisiä viestintäpalveluja tarjoavilta yrityksiltä saadut turvallisuuden loukkausta koskevat ilmoitukset, jotka toimivaltaiset viranomaiset toimittavat virastolle [eurooppalaisesta sähköisen viestinnän säännöstöstä annetun direktiivin] 40 artiklan mukaisesti.

6 artikla

Valmiuksien kehittämiseen liittyvät tehtävät

1. Virasto avustaa

a) jäsenvaltioita niiden pyrkiessä parantamaan kyberturvallisuusongelmien ja -poikkeamien ennaltaehkäisyä, havaitsemista ja analysointia sekä valmiuksia reagoida näihin ongelmiin ja poikkeamiin tarjoamalla jäsenvaltioille tarvittavaa osaamista ja asiantuntemusta;

b) unionin toimielimiä, elimiä, laitoksia ja virastoja niiden pyrkiessä parantamaan kyberturvallisuusongelmien ja -poikkeamien ennaltaehkäisyä, havaitsemista ja analysointia sekä valmiuksia reagoida näihin ongelmiin ja poikkeamiin antamalla CERTille asianmukaista tukea unionin toimielimiä, virastoja ja elimiä varten (CERT-EU);

c) pyynnöstä jäsenvaltioita niiden kehittäessä kansallisia tietoturvaloukkauksiin reagoivia ja niitä tutkivia yksiköitä (CSIRT-toimijoita) direktiivin (EU) 2016/1148 9 artiklan 5 kohdan mukaisesti;

d) pyynnöstä jäsenvaltioita niiden kehittäessä verkko- ja tietojärjestelmien turvallisuutta koskevia kansallisia strategioita direktiivin (EU) 2016/1148 7 artiklan 2 kohdan mukaisesti; virasto myös edistää tiedon levittämistä kyseisistä strategioista ja seuraa niiden täytäntöönpanon edistymistä kaikkialla unionissa parhaiden käytäntöjen edistämiseksi;

e) unionin toimielimiä niiden kehittäessä ja tarkastellessa uudelleen unionin strategioita kyberturvallisuuden alalla edistämällä niiden levittämistä ja seuraamalla niiden täytäntöönpanon edistymistä;

f) kansallisia ja unionin CSIRT-toimijoita niiden valmiustason nostamisessa muun muassa edistämällä vuoropuhelua ja tiedonvaihtoa, jotta voidaan varmistaa, että viimeisimmän teknisen kehityksen huomioon ottaen jokaisella CSIRT-toimijalla on yhteisesti määritellyt vähimmäisvalmiudet ja että se toimii parhaita käytäntöjä noudattaen;

g) jäsenvaltioita järjestämällä vuosittain 7 artiklan 6 kohdassa tarkoitettuja laajamittaisia kyberturvallisuusharjoituksia unionin tasolla ja antamalla poliittisia suosituksia harjoitusten arviointiprosessin ja niistä saatavien kokemusten pohjalta;

h) asianomaisia julkisia elimiä tarjoamalla kyberturvallisuuteen liittyvää koulutusta tarvittaessa yhteistyössä sidosryhmien kanssa;

i) yhteistyöryhmää vaihtamalla parhaita käytäntöjä erityisesti jäsenvaltioiden toteuttamasta keskeisten palvelujen tarjoajien määrittämisestä, myös rajat ylittävien riippuvuussuhteiden osalta, siltä osin kuin kyse on riskeistä ja poikkeamista ja direktiivin (EU) 2016/1148 11 artiklan 3 kohdan l alakohdan mukaisesti.

2. Virasto helpottaa tietojen jakamisen ja analysoinnin alakohtaisten keskusten (ISAC) perustamista ja antaa niille jatkuvaa tukea erityisesti direktiivin (EU) 2016/1148 liitteessä II mainituilla aloilla tarjoamalla käyttöön parhaita käytäntöjä ja ohjeita käytettävissä olevista välineistä ja menettelyistä sekä ohjeita tietojen jakamiseen liittyvien sääntelykysymysten ratkaisemiseksi.

7 artikla

Unionin tasolla tehtävään operatiiviseen yhteistyöhön liittyvät tehtävät

1. Virasto tukee operatiivista yhteistyötä toimivaltaisten julkisten elinten välillä sekä sidosryhmien välillä.

2. Virasto tekee yhteistyötä operatiivisella tasolla ja luo synergioita unionin toimielinten, elinten, laitosten ja virastojen kanssa, mukaan lukien CERT-EU, kyberrikollisuutta käsittelevät yksiköt sekä yksityisyyden ja henkilötietojen suojaa käsittelevät valvontaviranomaiset, yhteiseen etuun liittyvien ongelmien ratkaisemiseksi muun muassa

   a) vaihtamalla tietotaitoa ja parhaita käytäntöjä;

   b) tarjoamalla neuvoja ja ohjeita asiaankuuluvista kyberturvallisuuteen liittyvistä kysymyksistä;

   c) ottamalla käyttöön komissiota kuullen käytännön järjestelyt erityisten tehtävien toteuttamiseksi.

3. Virasto toimii CSIRT-verkoston sihteeristönä direktiivin (EU) 2016/1148 12 artiklan 2 kohdan mukaisesti ja aktiivisesti helpottaa tietojen jakamista ja yhteistyötä sen jäsenten kesken.

4. Virasto edistää operatiivista yhteistyötä CSIRT-verkostossa tukemalla jäsenvaltioita tehtävänään

   a) antaa neuvoja siitä, miten ne voivat parantaa valmiuksiaan ehkäistä ja havaita poikkeamia ja reagoida niihin;

   b) tarjoamalla pyynnöstä teknistä apua sellaisten poikkeamien yhteydessä, joilla on merkittävä vaikutus;

   c) analysoi haavoittuvuuksia, artefakteja ja poikkeamia.

Näiden tehtävien suorittamisessa virasto ja CERT-EU tekevät jäsenneltyä yhteistyötä hyötyäkseen synergioista erityisesti toiminnallisissa näkökohdissa.

5. Kahden tai useamman sellaisen jäsenvaltion pyynnöstä, jota asia koskee, ja pelkästään neuvonnan tarjoamiseksi uusien poikkeamien ehkäisemistä varten virasto antaa tukea jälkikäteen tehtävälle tekniselle tutkimukselle tai suorittaa tällaisen tutkimuksen sen jälkeen, kun vaikutukseltaan merkittävistä poikkeamista saadaan direktiivin (EU) 2016/1148 mukaisesti ilmoituksia yrityksiltä, joihin nämä poikkeamat ovat vaikuttaneet. Lisäksi virasto suorittaa tällaisen tutkimuksen asianmukaisesti perustellusta pyynnöstä, jonka komissio tekee yhteisymmärryksessä asianomaisten jäsenvaltioiden kanssa tapauksissa, joissa tällaiset poikkeamat vaikuttavat useampaan kuin kahteen jäsenvaltioon.

   Tutkimuksen laajuudesta ja sen suorittamisessa noudatettavasta menettelystä sovitaan asianomaisten jäsenvaltioiden ja viraston välillä, eikä se rajoita mahdollista samasta poikkeamasta käynnissä olevaa rikostutkintaa. Tutkimuksen päätteeksi virasto kokoaa erityisesti asianosaisten jäsenvaltioiden ja yritysten antamien tietojen ja kommenttien perusteella lopullisen teknisen raportin, jonka asianomaiset jäsenvaltiot hyväksyvät. Raportin yhteenveto, jossa keskitytään suosituksiin poikkeamien ehkäisemiseksi tulevaisuudessa, jaetaan CSIRT-verkoston kanssa.

6. Virasto järjestää vuosittain kyberturvallisuusharjoituksia unionin tasolla ja tukee jäsenvaltioita ja EU:n toimielimiä, virastoja ja elimiä harjoitusten järjestämisessä niiden pyynnöstä. Unionin tasolla järjestettävät vuotuiset harjoitukset sisältävät teknisiä, operatiivisia ja strategisia osatekijöitä ja auttavat valmistelemaan yhteistyöhön perustuvan vastauksen unionin tasolla laajamittaisiin rajatylittäviin kyberturvallisuuspoikkeamiin. Virasto myös edistää ja auttaa tarvittaessa järjestämään alakohtaisia kyberturvallisuusharjoituksia yhdessä ISAC-keskusten kanssa ja sallii ISAC-keskusten osallistumisen myös unionin tasolla järjestettäviin kyberturvallisuusharjoituksiin.

7. Virasto laatii poikkeamista ja uhista säännöllisesti EU:n kyberturvallisuuden teknisen tilanneraportin, joka perustuu julkisiin tietolähteisiin, sen omaan analyysiin ja raportteihin, jotka on saatu muun muassa CSIRT-toimijoilta (vapaaehtoisuuden pohjalta) tai verkko- ja tietoturvadirektiivillä perustetuilta keskitetyiltä yhteyspisteiltä (verkko- ja tietoturvadirektiivin 14 artiklan 5 kohdan mukaisesti), Europolissa toimivalta Euroopan kyberrikostorjuntakeskukselta (EC3) sekä CERT-EU:lta.

8. Virasto edistää yhteistyöhön perustuvan vastauksen kehittämistä unionin ja jäsenvaltioiden tasolla laajamittaisiin rajatylittäviin kyberturvallisuuspoikkeamiin tai -kriiseihin pääasiallisesti

   a) kokoamalla raportteja kansallisista lähteistä, jotta voidaan edistää yhteistä tilannetietoisuutta;

   b) varmistamalla tehokkaan tiedonkulun ja eskalointimekanismit CSIRT-verkoston sekä teknisten ja poliittisten päättäjien välillä unionin tasolla;

   c) tukemalla poikkeaman tai kriisin teknistä käsittelyä, muun muassa helpottamalla teknisten ratkaisujen jakamista jäsenvaltioiden välillä;

   d) tukemalla poikkeamaan tai kriisiin liittyvää julkista viestintää;

   e) testaamalla yhteistyösuunnitelmia tällaisiin poikkeamiin tai kriiseihin vastaamiseksi.

8 *artikla*

Markkinoihin, kyberturvallisuussertifiointiin ja standardointiin liittyvät tehtävät

Virasto

a) tukee ja edistää tieto- ja viestintätekniikan tuotteiden ja palvelujen kyberturvallisuussertifiointiin liittyvän, tämän asetuksen III osastolla käyttöön otettavan unionin politiikan kehittämistä ja täytäntöönpanoa tehtävänään

   1) valmistella ehdolla olevat eurooppalaiset kyberturvallisuuden sertifiointijärjestelmät tieto- ja viestintätekniikan tuotteille ja palveluille tämän asetuksen 44 artiklan mukaisesti;

   2) avustaa komissiota toimimalla Euroopan kyberturvallisuuden sertifiointiryhmän sihteeristönä tämän asetuksen 53 artiklan mukaisesti;

   3) koota ja julkaista ohjeita ja laatia hyviä käytäntöjä, jotka koskevat tieto- ja viestintätekniikan tuotteiden ja palvelujen kyberturvallisuusvaatimuksia, yhteistyössä kansallisten sertifioinnin valvontaviranomaisten ja toimialan kanssa;

b) helpottaa tieto- ja viestintäteknisten tuotteiden ja palvelujen riskinhallintaan ja turvallisuuteen liittyvien eurooppalaisten ja kansainvälisten standardien laatimista ja

käyttöönottoa sekä antaa yhteistyössä jäsenvaltioiden kanssa neuvoja ja suuntaviivoja keskeisten palvelujen tarjoajia ja digitaalisen palvelun tarjoajia koskeviin turvallisuusvaatimuksiin liittyvistä teknisistä aloista sekä jo olemassa olevista standardeista, mukaan lukien jäsenvaltioiden kansalliset standardit, direktiivin (EU) 2016/1148 19 artiklan 2 kohdan mukaisesti;

c) tekee säännöllisiä analyyseja kyberturvallisuusmarkkinoiden tärkeimmistä suuntauksista sekä kysyntä- että tarjontapuolella ja levittää näiden analyysien tuloksia kyberturvallisuusmarkkinoiden edistämiseksi unionissa.

9 artikla

Tietämykseen, tiedotukseen ja tietoisuuden lisäämiseen liittyvät tehtävät

Virasto

a) tekee analyyseja uusista teknologioista ja aihekohtaisia arviointeja teknologisten innovaatioiden odotettavissa olevista yhteiskunnallisista, oikeudellisista, taloudellisista ja sääntelyyn liittyvistä vaikutuksista kyberturvallisuuden kannalta;

b) tekee pitkän aikavälin strategisia analyyseja kyberturvallisuusuhista ja -poikkeamista kyberturvallisuuteen liittyvien uusien kehityssuuntausten kartoittamiseksi ja kyberturvallisuuteen liittyvien ongelmien ehkäisemiseksi;

c) tarjoaa yhteistyössä jäsenvaltioiden viranomaisten asiantuntijoiden kanssa neuvoja, ohjeita ja parhaita käytäntöjä, jotka koskevat verkko- ja tietojärjestelmien turvallisuutta ja erityisesti internetinfrastruktuurin ja direktiivin (EU) 2016/1148 liitteessä II mainittuja aloja tukevien infrastruktuurien turvallisuutta;

d) kokoaa, järjestää ja saattaa yleisön saataville erityisen portaalin kautta unionin toimielimiltä, virastoilta ja elimiltä saatavaa tietoa kyberturvallisuudesta;

e) lisää suuren yleisön tietoisuutta kyberturvallisuuteen liittyvistä riskeistä ja antaa yksittäisille käyttäjille ohjeita hyvistä käytännöistä kansalaisten ja organisaatioiden käyttöön;

f) kerää ja analysoi julkisesti saatavilla olevia tietoja merkittävistä poikkeamista ja kokoaa raportteja ohjeiden antamiseksi yrityksille ja kansalaisille kaikkialla unionissa;

g) järjestää yhteistyössä jäsenvaltioiden ja unionin toimielinten, elinten, laitosten ja virastojen kanssa säännöllisiä tiedotuskampanjoita kyberturvallisuuden ja sen näkyvyyden parantamiseksi unionissa.

10 artikla

Tutkimukseen ja innovointiin liittyvät tehtävät

Tutkimuksen ja innovoinnin osalta virasto

a) antaa unionille ja jäsenvaltioille neuvoja kyberturvallisuusalan tutkimustarpeista ja -painopisteistä, jotta nykyisiin ja kehittyviin riskeihin ja uhkiin, myös jos ne liittyvät uusiin ja kehittyviin tieto- ja viestintäteknologioihin, voitaisiin löytää toimivia ratkaisuja ja jotta riskinehkäisytekniikoita voitaisiin käyttää tehokkaasti;

b) osallistuu, jos komissio on siirtänyt sille toimivaltuudet, tutkimuksen ja innovoinnin rahoitusohjelmien täytäntöönpanovaiheeseen tai on näiden ohjelmien rahoituksen saajana.

11 artikla
Kansainväliseen yhteistyöhön liittyvät tehtävät

Virasto edesauttaa unionin pyrkimyksiä yhteistoimintaan kolmansien maiden ja kansainvälisten organisaatioiden kanssa kansainvälisen yhteistyön edistämiseksi kyberturvallisuuskysymyksissä muun muassa

a) toimimalla tarvittaessa tarkkailijana kansainvälisten harjoitusten järjestämisessä sekä analysoimalla harjoitusten tuloksia ja raportoimalla niistä johtokunnalle;

b) edistämällä komission pyynnöstä parhaiden käytäntöjen vaihtoa asiaankuuluvien kansainvälisten järjestöjen välillä;

c) antamalla pyynnöstä asiantuntemusta komission käyttöön.

II LUKU
VIRASTON ORGANISAATIO

12 artikla
Rakenne

Viraston hallinto- ja johtamisrakenne muodostuu seuraavista:

a) johtokunta, jonka tehtävät vahvistetaan 14 artiklassa;

b) hallitus, jonka tehtävät vahvistetaan 18 artiklassa;

c) pääjohtaja, jonka velvollisuudet vahvistetaan 19 artiklassa; ja

d) pysyvä sidosryhmä, jonka tehtävät vahvistetaan 20 artiklassa.

1 JAKSO
JOHTOKUNTA

13 artikla
Johtokunnan kokoonpano

1. Johtokuntaan kuuluu kustakin jäsenvaltiosta yksi edustaja ja kaksi komission nimittämää edustajaa. Kaikilla edustajilla on äänioikeus.

2. Kullakin johtokunnan jäsenellä on varajäsen, joka edustaa jäsentä tämän ollessa poissa.

3. Johtokunnan jäsenet ja varajäsenet nimitetään heidän kyberturvallisuusalaa koskevan tietämyksensä perusteella ottaen huomioon asianmukaiset johtamis-, hallinto- ja varainhoitotaidot. Johtokunnan toiminnan jatkuvuuden varmistamiseksi komission ja jäsenvaltioiden on pyrittävä rajoittamaan edustajiensa vaihtuvuutta johtokunnassa.

Komission ja jäsenvaltioiden on pyrittävä miesten ja naisten tasapuoliseen edustukseen johtokunnassa.

4. Johtokunnan jäsenten ja varajäsenten toimikausi on neljä vuotta. Toimikausi voidaan uusia.

14 artikla
Johtokunnan tehtävät

1. Johtokunta

a) määrittelee viraston toiminnan yleiset suuntaviivat ja varmistaa, että virasto toimii tässä asetuksessa vahvistettujen sääntöjen ja periaatteiden mukaisesti; Se myös huolehtii viraston toiminnan johdonmukaisuudesta suhteessa jäsenvaltioiden toimintaan sekä unionin tason toimiin.

b) hyväksyy luonnoksen viraston yhtenäiseksi ohjelma-asiakirjaksi 21 artiklan mukaisesti ennen sen toimittamista komissiolle lausuntoa varten;

c) komission lausunnon huomioon ottaen hyväksyy viraston yhtenäisen ohjelma-asiakirjan jäsentensä kahden kolmasosan enemmistöllä ja 17 artiklan mukaisesti;

d) hyväksyy jäsentensä kahden kolmasosan enemmistöllä viraston vuotuisen talousarvion ja hoitaa muita tehtäviä, jotka liittyvät viraston talousarvioon, III luvun mukaisesti;

e) arvioi ja hyväksyy viraston toimintaa koskevan vuotuisen konsolidoidun toimintakertomuksen ja toimittaa sen yhdessä arviointinsa kanssa seuraavan vuoden heinäkuun 1 päivään mennessä Euroopan parlamentille, neuvostolle, komissiolle ja tilintarkastustuomioistuimelle. Toimintakertomus sisältää tilinpäätöksen ja kuvauksen siitä, kuinka virasto on saavuttanut tulosindikaattorinsa. Toimintakertomus julkistetaan;

f) hyväksyy viraston varainhoitosäännöt 29 artiklan mukaisesti;

g) hyväksyy petostentorjuntastrategian, joka on oikeassa suhteessa petosriskeihin nähden, kun toteutettavien toimenpiteiden kustannus-hyötyanalyysi otetaan huomioon;

h) hyväksyy jäsentensä eturistiriitojen ehkäisemistä ja hallintaa koskevat säännöt;

i) huolehtii asianmukaisista jatkotoimista, joita toteutetaan Euroopan petostentorjuntaviraston (OLAF) tutkimuksiin ja erilaisiin sisäisen tai ulkoisen tarkastuksen raportteihin ja sisäisiin tai ulkoisiin arviointeihin perustuvien tulosten ja suositusten perusteella;

j) hyväksyy työjärjestyksensä;

k) käyttää 2 kohdan mukaisesti viraston henkilöstön suhteen Euroopan unionin virkamiehiin sovellettavissa henkilöstösäännöissä nimittävälle viranomaiselle ja unionin muuta henkilöstöä koskevissa palvelussuhteen ehdoissa työsopimusten tekemiseen valtuutetulle viranomaiselle annettuja valtuuksia, jäljempänä ’nimittävän viranomaisen valtuudet’;

l) vahvistaa henkilöstösääntöjen ja muuhun henkilöstöön sovellettavien palvelussuhteen ehtojen täytäntöönpanoa koskevat säännökset henkilöstösääntöjen 110 artiklassa säädettyä menettelyä noudattaen;

m) nimittää pääjohtajan ja jatkaa tarvittaessa tämän toimikautta tai erottaa tämän asetuksen 33 artiklan mukaisesti;

n) nimittää tilinpitäjän, joka voi olla komission tilinpitäjä ja joka hoitaa tehtäviään täysin riippumattomasti;

o) tekee kaikki päätökset viraston sisäisistä rakenteista ja tarvittaessa niiden muuttamisesta ottaen huomioon viraston toimintatarpeet ja moitteettoman varainhoidon;

p) hyväksyy työjärjestelyistä sopimisen 7 ja 39 artiklan mukaisesti.

2. Johtokunta tekee henkilöstösääntöjen 110 artiklan mukaisesti henkilöstösääntöjen 2 artiklan 1 kohtaan ja muuta henkilöstöä koskevien palvelussuhteen ehtojen 6 artiklaan perustuvan päätöksen, jolla siirretään nimittävän viranomaisen toimivalta pääjohtajalle ja määritellään olosuhteet, joissa toimivallan siirto voidaan keskeyttää. Pääjohtajalla on valtuudet siirtää tämä toimivalta edelleen.

3. Jos poikkeukselliset olosuhteet sitä edellyttävät, johtokunta voi tekemällään päätöksellä tilapäisesti keskeyttää pääjohtajalle siirretyn nimittävän viranomaisen toimivallan ja hänen edelleen siirtämänsä nimittävän viranomaisen toimivallan ja käyttää kyseistä toimivaltaa itse tai siirtää sen jollekin jäsenistään tai jollekulle henkilöstöön kuuluvalle, joka on muu kuin pääjohtaja.

15 artikla
Johtokunnan puheenjohtaja

Johtokunta valitsee keskuudestaan puheenjohtajan ja varapuheenjohtajan jäsentensä kahden kolmasosan enemmistöllä neljän vuoden toimikaudeksi, joka voidaan uusia kerran. Jos heidän jäsenyytensä johtokunnassa kuitenkin päättyy heidän toimikautensa aikana, myös heidän toimikautensa päättyy tuona päivänä ilman eri toimenpiteitä. Varapuheenjohtaja toimii viran puolesta puheenjohtajan sijaisena tämän ollessa estynyt.

16 artikla
Johtokunnan kokoukset

1. Johtokunta kokoontuu puheenjohtajansa kutsusta.

2. Johtokunta pitää vähintään kaksi sääntömääräistä kokousta vuodessa. Johtokunta kokoontuu myös ylimääräisiin kokouksiin puheenjohtajan, komission tai vähintään kolmasosan johtokunnan jäsenistä sitä pyytäessä.

3. Pääjohtaja osallistuu johtokunnan kokouksiin ilman äänioikeutta.

4. Pysyvän sidosryhmän jäsenet voivat osallistua puheenjohtajan kutsusta johtokunnan kokouksiin ilman äänioikeutta.

5. Johtokunnan jäsenillä ja varajäsenillä voi olla kokouksissa avustajinaan neuvonantajia tai asiantuntijoita, jollei työjärjestyksestä muuta johdu.

6. Virasto vastaa johtokunnan sihteeristön tehtävistä.

17 artikla

Johtokunnan äänestyssäännöt

1. Johtokunta tekee päätöksensä jäsentensä enemmistöllä.
2. Yhtenäisen ohjelma-asiakirjan ja vuotuisen talousarvion hyväksyminen sekä pääjohtajan nimittäminen, toimikauden jatkaminen ja erottaminen edellyttävät kaikkien johtokunnan jäsenten kahden kolmasosan enemmistöä.
3. Kullakin jäsenellä on yksi ääni. Jäsenen poissa ollessa varajäsenellä on oikeus käyttää äänioikeutta.
4. Puheenjohtaja osallistuu äänestykseen.
5. Pääjohtaja ei osallistu äänestykseen.
6. Johtokunnan työjärjestyksessä määritellään yksityiskohtaisemmat äänestystä koskevat järjestelyt, erityisesti olosuhteet, joissa jäsen voi toimia toisen jäsenen puolesta.

2 JAKSO
HALLITUS

18 artikla

Hallitus

1. Johtokuntaa avustaa hallitus.
2. Hallitus
   a) valmistelee päätökset johtokunnan hyväksyttäviksi;
   b) varmistaa yhdessä johtokunnan kanssa, että OLAFin tutkimuksissa sekä sisäisissä tai ulkoisissa tarkastuskertomuksissa ja arvioinneissa esitettyjen havaintojen ja suositusten johdosta toteutetaan asianmukaiset jatkotoimet:
   c) avustaa ja neuvoo pääjohtajaa hallinnollisia ja talousarvioasioita koskevien johtokunnan päätösten täytäntöönpanossa 19 artiklan mukaisesti, sanotun kuitenkaan rajoittamatta 19 artiklassa säädettyjä pääjohtajan tehtäviä.
3. Hallitukseen kuuluu viisi jäsentä, jotka nimitetään johtokunnan jäsenten keskuudesta ja joista yksi on johtokunnan puheenjohtaja, joka voi myös toimia hallituksen puheenjohtajana, ja yksi on komission edustaja. Pääjohtaja osallistuu hallituksen kokouksiin ilman äänioikeutta.
4. Hallituksen jäsenten toimikausi on neljä vuotta. Toimikausi voidaan uusia.
5. Hallitus kokoontuu vähintään kerran kolmessa kuukaudessa. Hallituksen puheenjohtaja kutsuu kokoon ylimääräisiä kokouksia hallituksen jäsenten pyynnöstä.
6. Johtokunta vahvistaa hallituksen työjärjestyksen.
7. Hallitus tekee tarvittaessa kiireellisissä tapauksissa tiettyjä väliaikaisia päätöksiä johtokunnan puolesta, erityisesti hallinnollisista kysymyksistä, mukaan lukien nimittävän viranomaisen toimivallan siirron keskeyttäminen, sekä talousarvioon liittyvistä kysymyksissä.

3 JAKSO
PÄÄJOHTAJA

19 artikla
Pääjohtajan tehtävät

1. Virastoa johtaa sen pääjohtaja, joka hoitaa tehtäväänsä riippumattomasti. Pääjohtaja on vastuussa johtokunnalle.

2. Pääjohtaja raportoi pyydettäessä Euroopan parlamentille tehtäviensä hoidosta. Neuvosto voi pyytää pääjohtajaa raportoimaan tehtäviensä hoidosta.

3. Pääjohtajan tehtävänä on

   a) viraston päivittäisen toiminnan hallinnointi;

   b) johtokunnan tekemien päätösten täytäntöönpano;

   c) yhtenäisen ohjelma-asiakirjan luonnoksen laatiminen ja sen toimittaminen johtokunnan hyväksyttäväksi ennen sen toimittamista komissiolle;

   d) yhtenäisen ohjelma-asiakirjan täytäntöönpano ja siitä raportointi johtokunnalle;

   e) viraston toimintaa koskevan vuotuisen konsolidoidun toimintakertomuksen laatiminen ja sen esittäminen johtokunnalle arvioitavaksi ja hyväksyttäväksi;

   f) toimintasuunnitelman laatiminen jälkiarviointien päätelmien perusteella ja edistymiskertomuksen laatiminen komissiolle kahden vuoden välein;

   g) toimintasuunnitelman laatiminen sisäisten tai ulkoisten tarkastuskertomusten päätelmiin sekä Euroopan petostentorjuntaviraston (OLAF) tutkimuksiin perustuvia jatkotoimia varten ja suunnitelman edistymisestä raportointi kahdesti vuodessa komissiolle ja säännöllisesti johtokunnalle;

   h) virastoon sovellettavien varainhoitosääntöjen luonnoksen valmistelu;

   i) viraston tuloja ja menoja koskevan ennakkoarvion luonnoksen laatiminen ja viraston talousarvion toteuttaminen;

   j) unionin taloudellisten etujen suojeleminen toteuttamalla petosten, lahjonnan ja muun laittoman toiminnan torjuntatoimia ja tehokkaita tarkastuksia ja, jos väärinkäytöksiä ilmenee, perimällä takaisin väärin perustein maksetut määrät sekä soveltamalla tarvittaessa tehokkaita, oikeasuhteisia ja varoittavia hallinnollisia ja taloudellisia seuraamuksia;

   k) petostentorjuntastrategian laatiminen virastolle ja sen esittäminen johtokunnalle hyväksyntää varten;

   l) yhteyksien luominen ja ylläpito liikemaailmaan ja kuluttajajärjestöihin säännöllisen vuoropuhelun varmistamiseksi asiaankuuluvien sidosryhmien kanssa;

m) muiden pääjohtajalle tällä asetuksella osoitettujen tehtävien hoito.

4. Tarpeen vaatiessa ja viraston toimeksiannon, tavoitteiden ja tehtävien puitteissa pääjohtaja voi perustaa muun muassa jäsenvaltioiden toimivaltaisten viranomaisten asiantuntijoista koostuvia tilapäisiä työryhmiä. Tästä on ilmoitettava etukäteen johtokunnalle. Menettelyt, jotka koskevat erityisesti työryhmien kokoonpanoa, pääjohtajan suorittamaa työryhmien asiantuntijoiden nimeämistä ja työryhmien toimintaa, vahvistetaan viraston sisäisissä toimintasäännöissä.

5. Toimitusjohtaja päättää, onko viraston tehtävien tehokkaan ja vaikuttavan suorittamisen kannalta tarpeellista sijoittaa toimihenkilöitä yhteen tai useampaan jäsenvaltioon. Ennen kuin toimitusjohtaja tekee päätöksen paikallistoimiston perustamisesta, hänen on hankittava ennakkosuostumus komissiolta, hallintoneuvostolta ja asianomaiselta jäsenvaltiolta (asianomaisilta jäsenvaltioilta). Päätöksessä on määriteltävä paikallistoimistossa toteutettavien toimien laajuus siten, että vältetään tarpeettomia kustannuksia ja viraston hallinnollisten tehtävien päällekkäisyyttä. Asianomaisen jäsenvaltion (asianomaisten jäsenvaltioiden) kanssa on tehtävä sopimus tarvittaessa tai pyydettäessä.

4 JAKSO
PYSYVÄ SIDOSRYHMÄ

20 artikla
Pysyvä sidosryhmä

1. Johtokunta perustaa pääjohtajan esityksestä pysyvän sidosryhmän, joka koostuu asiaan liittyviä sidosryhmiä, kuten tieto- ja viestintätekniikan alaa, sähköisten viestintäverkkojen tai yleisön saatavilla olevien palvelujen tarjoajia ja kuluttajajärjestöjä, edustavista tunnustetuista asiantuntijoista, tiedeyhteisöä edustavista kyberturvallisuusasiantuntijoista sekä [eurooppalaisesta sähköisen viestinnän säännöstöstä annetun direktiivin] mukaisesti ilmoitettujen toimivaltaisten viranomaisten sekä lainvalvonta- ja tietosuojaviranomaisten edustajista.

2. Pysyvän sidosryhmän menettelyt, jotka koskevat erityisesti ryhmän jäsenten lukumäärää, sen kokoonpanoa, johtokunnan suorittamaa ryhmän jäsenten nimeämistä, pääjohtajan tekemää esitystä sekä ryhmän toimintaa, määritellään viraston sisäisissä toimintasäännöissä ja julkaistaan.

3. Pysyvän sidosryhmän puheenjohtajana toimii pääjohtaja tai pääjohtajan tähän tehtävään tapauskohtaisesti nimeämä henkilö.

4. Pysyvän sidosryhmän jäsenten toimikausi on kaksi ja puoli vuotta. Johtokunnan jäsenet eivät saa olla pysyvän sidosryhmän jäseniä. Komission ja jäsenvaltioiden asiantuntijoilla on oikeus olla läsnä pysyvän sidosryhmän kokouksissa ja osallistua sen työhön. Muiden pääjohtajan tärkeiksi katsomien elinten edustajia, jotka eivät ole pysyvän sidosryhmän jäseniä, voidaan pyytää saapuville pysyvän sidosryhmän kokouksiin ja osallistumaan sen työhön.

5. Pysyvä sidosryhmä neuvoo virastoa sen tehtävien hoidossa. Erityisesti se neuvoo pääjohtajaa tämän laatiessa esitystä viraston työohjelmaksi sekä yhteydenpidossa asianmukaisten sidosryhmien kanssa kaikissa työohjelmaan liittyvissä kysymyksissä.

5 JAKSO
TOIMINTA

21 artikla
Yhtenäinen ohjelma-asiakirja

1. Virasto noudattaa toiminnassaan sen monivuotisen ja vuotuisen ohjelman suunnitelmat sisältävää yhtenäistä ohjelma-asiakirjaa, johon sisältyy kaikki sen suunniteltu toiminta.

2. Pääjohtaja laatii vuosittain luonnoksen yhtenäiseksi ohjelma-asiakirjaksi, joka sisältää monivuotisen ja vuotuisen ohjelman suunnitelmat ja vastaavan henkilöstö- ja resurssisuunnittelun, komission delegoidun asetuksen (EU) N:o 1271/2013[36] 32 artiklan mukaisesti ja ottaen huomioon komission esittämät ohjeet.

3. Johtokunta hyväksyy kunkin vuoden marraskuun 30 päivään mennessä 1 kohdassa tarkoitetun yhtenäisen ohjelma-asiakirjan ja toimittaa sen Euroopan parlamentille, neuvostolle ja komissiolle viimeistään seuraavan vuoden tammikuun 31 päivänä, samoin asiakirjan mahdolliset myöhemmät päivitetyt versiot.

4. Yhtenäisestä ohjelma-asiakirjasta tulee lopullinen, kun unionin yleinen talousarvio on lopullisesti vahvistettu, ja sitä on tarvittaessa mukautettava talousarviota vastaavasti.

5. Vuotuisessa työohjelmassa on esitettävä yksityiskohtaiset tavoitteet ja odotetut tulokset, suoritusindikaattorit mukaan lukien. Siinä on myös esitettävä kuvaus rahoitettavista toimista ja mainittava kuhunkin toimeen osoitetut taloudelliset ja henkilöstöresurssit toimintoperusteisen budjetoinnin ja hallinnoinnin periaatteiden mukaisesti. Vuotuisen työohjelman on oltava yhdenmukainen 7 kohdassa tarkoitetun monivuotisen työohjelman kanssa. Siinä on selkeästi ilmoitettava, mitä tehtäviä on lisätty, muutettu tai poistettu edelliseen varainhoitovuoteen verrattuna.

6. Johtokunta muuttaa hyväksyttyä vuotuista työohjelmaa tarvittaessa, jos virastolle annetaan uusi tehtävä. Vuotuiseen työohjelmaan tehtävät olennaiset muutokset on hyväksyttävä samaa menettelyä noudattaen kuin alkuperäinen vuotuinen työohjelma. Johtokunta voi siirtää pääjohtajalle valtuudet tehdä vuotuiseen työohjelmaan muita kuin olennaisia muutoksia.

7. Monivuotisessa työohjelmassa on esitettävä yleinen strateginen ohjelma, mukaan lukien tavoitteet, odotetut tulokset ja suoritusindikaattorit. Siinä on esitettävä myös resursseja koskeva ohjelmasuunnittelu, mukaan lukien monivuotinen talousarvio ja henkilöstösuunnitelma.

8. Resursseja koskeva ohjelmasuunnittelu saatetaan ajan tasalle vuosittain. Strategista ohjelmaa päivitetään tarvittaessa ja erityisesti 56 artiklassa tarkoitetun arvioinnin tulosten huomioon ottamiseksi.

---

36 Komission delegoitu asetus (EU) N:o 1271/2013, annettu 30 päivänä syyskuuta 2013, Euroopan parlamentin ja neuvoston asetuksen (EU, Euratom) N:o 966/2012 208 artiklassa tarkoitettuja elimiä koskevasta varainhoidon puiteasetuksesta(EUVL L 328, 7.12.2013, s. 42).

22 artikla

Ilmoitus sidonnaisuuksista

1. Jokaisen johtokunnan jäsenen, pääjohtajan sekä jokaisen toimihenkilön, joka on otettu palvelukseen jäsenvaltion tilapäisesti lähettämänä virkamiehenä, on tehtävä ilmoitus sitoumuksistaan sekä ilmoitus, jossa he toteavat, onko olemassa heidän riippumattomuuttaan mahdollisesti vaarantavia välittömiä tai välillisiä sidonnaisuuksia. Ilmoitusten on oltava tarkkoja ja täydellisiä, ne on tehtävä kirjallisesti vuosittain ja ne on tarvittaessa saatettava ajan tasalle.

2. Jokaisen johtokunnan jäsenen, pääjohtajan ja jokaisen tilapäisiin työryhmiin osallistuvan ulkopuolisen asiantuntijan on ilmoitettava viimeistään kunkin kokouksen alussa tarkasti ja täydellisesti mahdolliset sidonnaisuudet, jotka saattavat vaarantaa heidän riippumattomuutensa kokouksen esityslistalla olevien asioiden suhteen, sekä pidättäydyttävä osallistumasta kyseisiä kohtia koskevaan keskusteluun ja äänestykseen.

3. Virasto vahvistaa sisäisissä toimintasäännöissään 1 ja 2 kohdassa tarkoitettua sidonnaisuuksien ilmoittamista koskeviin sääntöihin liittyvät käytännön järjestelyt.

23 artikla

Avoimuus

1. Viraston toiminnan on oltava mahdollisimman avointa sekä 25 artiklan mukaista.

2. Virasto varmistaa, että suuri yleisö ja kaikki asianomaiset tahot saavat asianmukaista, puolueetonta, luotettavaa ja helposti saatavissa olevaa tietoa erityisesti viraston työn tuloksista. Sen on myös julkistettava 22 artiklan mukaisesti tehdyt sidonnaisuuksia koskevat ilmoitukset.

3. Johtokunta voi pääjohtajan ehdotuksesta sallia asianomaisten tahojen seurata joidenkin viraston toimien käsittelyä.

4. Virasto vahvistaa sisäisissä toimintasäännöissään 1 ja 2 kohdassa tarkoitettujen avoimuussääntöjen täytäntöönpanoa koskevat käytännön järjestelyt.

24 artikla

Luottamuksellisuus

1. Virasto ei saa paljastaa kolmansille osapuolille käsittelemiään ja saamiaan tietoja, joiden käsittelystä osittain tai kokonaisuudessaan luottamuksellisina on esitetty perusteltu pyyntö, sanotun kuitenkaan rajoittamatta 25 artiklan soveltamista.

2. Johtokunnan jäsenten, pääjohtajan, pysyvän sidosryhmän jäsenten, tilapäisiin työryhmiin osallistuvien ulkopuolisten asiantuntijoiden sekä viraston henkilöstön, mukaan lukien ne toimihenkilöt, jotka on otettu palvelukseen jäsenvaltioiden tilapäisesti lähettäminä virkamiehinä, on myös tehtäviensä päätyttyä noudatettava Euroopan unionin toiminnasta tehdyn sopimuksen 339 artiklan mukaista salassapitovelvollisuutta.

3. Virasto vahvistaa sisäisissä toimintasäännöissään 1 ja 2 kohdassa tarkoitettujen salassapitovelvollisuutta koskevien sääntöjen täytäntöönpanoa koskevat käytännön järjestelyt.

4. Johtokunta päättää antaa virastolle luvan käsitellä turvallisuusluokiteltua tietoa, jos viraston tehtävien suorittaminen sitä edellyttää. Tässä tapauksessa johtokunnan on yhteisymmärryksessä komission yksiköiden kanssa vahvistettava sisäiset toimintasäännöt soveltaen tietoturvan periaatteita, jotka on vahvistettu komission päätöksissä (EU, Euratom) 2015/443[37] ja 2015/444[38]. Nämä säännöt koskevat muun muassa turvallisuusluokiteltujen tietojen vaihtamista, käsittelyä ja tallentamista.

25 artikla
Asiakirjojen julkisuus

1. Viraston hallussaan pitämiin asiakirjoihin sovelletaan asetusta (EY) N:o 1049/2001.
2. Johtokunta vahvistaa järjestelyt asetuksen (EY) N:o 1049/2001 täytäntöönpanemiseksi kuuden kuukauden kuluessa viraston perustamisesta.
3. Asetuksen (EY) N:o 1049/2001 8 artiklan perusteella tehdyistä viraston päätöksistä voidaan kannella oikeusasiamiehelle Euroopan unionin toiminnasta tehdyn sopimuksen 228 artiklan nojalla tai nostaa kanne Euroopan unionin tuomioistuimessa Euroopan unionin toiminnasta tehdyn sopimuksen 263 artiklan nojalla.

III LUKU
TALOUSARVION LAATIMINEN JA RAKENNE

26 artikla
Talousarvion laatiminen

1. Pääjohtaja laatii vuosittain esityksen viraston seuraavan varainhoitovuoden tuloja ja menoja koskevaksi ennakkoarvioksi ja toimittaa sen sekä siihen liitetyn henkilöstötaulukkoehdotuksen johtokunnalle. Tulojen ja menojen on oltava tasapainossa.
2. Johtokunta laatii 1 kohdassa tarkoitetun tuloja ja menoja koskevan ennakkoarvioesityksen pohjalta vuosittain viraston tulo- ja menoarvion seuraavaa varainhoitovuotta varten.
3. Johtokunta toimittaa 2 kohdassa tarkoitetun tulo- ja menoarvion, joka on osa yhtenäisen ohjelma-asiakirjan luonnosta, vuosittain viimeistään tammikuun 31 päivänä komissiolle ja niille kolmansille maille, joiden kanssa unioni on tehnyt sopimukset 39 artiklan mukaisesti.
4. Komissio ottaa unionin talousarviota koskevaan esitykseen kyseiseen tulo- ja menoarvioon perustuvat arviot, joita se pitää henkilöstötaulukon ja yleisestä talousarviosta suoritettavan rahoitusosuuden määrän osalta välttämättöminä, ja toimittaa talousarvioesityksen Euroopan parlamentille ja neuvostolle Euroopan unionin toiminnasta tehdyn sopimuksen 313 ja 314 artiklan mukaisesti.

---

37 Komission päätös (EU, Euratom) 2015/443, annettu 13 päivänä maaliskuuta 2015, turvallisuudesta komissiossa (EUVL L 72, 17.3.2015, s. 41).

38 Komission päätös (EU, Euratom) 2015/444, annettu 13 päivänä maaliskuuta 2015, EU:n turvallisuusluokiteltujen tietojen suojaamista koskevista säännöistä (EUVL L 72, 17.3.2015, s. 53).

5. Euroopan parlamentti ja neuvosto hyväksyvät virastolle annettavaa rahoitusosuutta koskevat määrärahat.

6. Euroopan parlamentti ja neuvosto vahvistavat viraston henkilöstötaulukon.

7. Johtokunta vahvistaa yhtenäisen ohjelma-asiakirjan ohella viraston talousarvion. Siitä tulee lopullinen, kun unionin yleinen talousarvio on lopullisesti vahvistettu. Johtokunta mukauttaa tarvittaessa viraston talousarviota ja yhtenäistä ohjelma-asiakirjaa unionin yleisen talousarvion mukaisesti.

27 artikla
Talousarvion rakenne

1. Sulkematta pois muita tulonlähteitä viraston tulot koostuvat seuraavista:

   a) rahoitusosuus unionin talousarviosta;

   b) tiettyjen menoerien rahoittamiseen osoitettavat tulot 29 artiklassa tarkoitettuja varainhoitosääntöjä noudattaen;

   c) unionin rahoitus, joka annetaan valtuutussopimusten tai kertaluonteisten avustusten muodossa 29 artiklassa tarkoitettujen varainhoitosääntöjen ja unionin politiikkoja tukeviin asianomaisiin välineisiin sovellettavien säännösten mukaisesti;

   d) viraston toimintaan 39 artiklan mukaisesti osallistuvien kolmansien maiden rahoitusosuudet;

   e) mahdolliset jäsenvaltioiden vapaaehtoiset rahoitusosuudet rahana tai luontoissuorituksina. Vapaaehtoisia rahoitusosuuksia suorittavat jäsenvaltiot eivät voi vaatia erityisoikeuksia tai -palveluja suorituksensa perusteella.

2. Viraston menoihin kuuluvat henkilöstöstä, hallinnollisesta ja teknisestä tuesta, infrastruktuurista ja toiminnasta sekä kolmansien osapuolten kanssa tehdyistä sopimuksista aiheutuvat menot.

28 artikla
Talousarvion toteuttaminen

1. Pääjohtaja vastaa viraston talousarvion toteuttamisesta.

2. Komission sisäinen tilintarkastaja käyttää virastoon nähden samoja valtuuksia kuin komission yksiköihin.

3. Viraston tilinpitäjä toimittaa alustavan tilinpäätöksen komission tilinpitäjälle ja tilintarkastustuomioistuimelle viimeistään varainhoitovuoden päättymistä seuraavan maaliskuun 1 päivänä (vuoden N + 1 maaliskuun 1 päivä).

4. Saatuaan viraston alustavaa tilinpäätöstä koskevat tilintarkastustuomioistuimen huomautukset viraston tilinpitäjä laatii viraston lopullisen tilinpäätöksen omalla vastuullaan.

5. Pääjohtaja toimittaa lopullisen tilinpäätöksen johtokunnalle lausuntoa varten.

6. Pääjohtaja toimittaa selvityksen varainhoitovuoden talousarvio- ja varainhallinnosta Euroopan parlamentille, neuvostolle, komissiolle ja tilintarkastustuomioistuimelle viimeistään vuoden N + 1 maaliskuun 31 päivänä.

7. Tilinpitäjä toimittaa lopullisen tilinpäätöksen ja johtokunnan lausunnon Euroopan parlamentille, neuvostolle, komission tilinpitäjälle ja tilintarkastustuomioistuimelle viimeistään vuoden N + 1 heinäkuun 1 päivänä.

8. Tilinpitäjä toimittaa myös tilinpäätöstä koskevan vahvistuskirjeen tilintarkastustuomioistuimelle sekä tiedoksi komission tilinpitäjälle samana päivänä kuin lopullisen tilinpäätöksen.

9. Pääjohtaja julkistaa lopullisen tilinpäätöksen viimeistään seuraavan vuoden marraskuun 15 päivänä.

10. Pääjohtaja lähettää tilintarkastustuomioistuimelle vastauksen sen huomautuksiin viimeistään vuoden N + 1 syyskuun 30 päivänä ja lähettää jäljennöksen tästä vastauksesta myös johtokunnalle ja komissiolle.

11. Pääjohtaja antaa varainhoitoasetuksen 165 artiklan 3 kohdan mukaisesti Euroopan parlamentille tämän pyynnöstä kaikki kyseistä varainhoitovuotta koskevan vastuuvapausmenettelyn moitteettoman toteuttamisen edellyttämät tiedot.

12. Euroopan parlamentti myöntää neuvoston suosituksesta pääjohtajalle ennen vuoden N + 2 toukokuun 15 päivää vastuuvapauden vuoden N talousarvion toteuttamisen osalta.

29 artikla
Varainhoitosäännöt

Johtokunta hyväksyy virastoon sovellettavat varainhoitoa koskevat säännöt komissiota kuultuaan. Varainhoitosäännöt voivat poiketa asetuksesta (EU) N:o 1271/2013 ainoastaan, jos viraston toiminta sitä erityisesti edellyttää ja jos komissio on antanut siihen ennalta suostumuksensa.

30 artikla
Petostentorjunta

1. Helpottaakseen Euroopan parlamentin ja neuvoston asetuksen (EU, Euratom) N:o 883/2013[39] soveltamisalaan kuuluvien petosten, lahjonnan ja muiden laittomien toimien torjuntaa virasto liittyy kuuden kuukauden kuluessa päivästä, jona se aloittaa toimintansa, Euroopan petostentorjuntaviraston (OLAF) sisäisistä tutkimuksista 25 päivänä toukokuuta 1999 tehtyyn toimielinten väliseen sopimukseen ja antaa kaikkia viraston työntekijöitä koskevat asiaan liittyvät määräykset käyttäen kyseisen sopimuksen liitteessä olevaa mallia.

2. Tilintarkastustuomioistuimella on valtuudet tehdä kaikkien virastolta unionin rahoitusta saaneiden avustuksensaajien, toimeksisaajien ja alihankkijoiden osalta asiakirjoihin perustuvia ja paikan päällä suoritettavia tarkastuksia.

[39] Euroopan parlamentin ja neuvoston asetus (EU, Euratom) N:o 883/2013, annettu 11 päivänä syyskuuta 2013, Euroopan petostentorjuntaviraston (OLAF) tutkimuksista sekä Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 1073/1999 ja neuvoston asetuksen (Euratom) N:o 1074/1999 kumoamisesta (EUVL L 248, 18.9.2013, s. 1).

3. OLAF voi tehdä tarkastuksia, myös paikalla suoritettavia tarkastuksia ja todentamisia, Euroopan parlamentin ja neuvoston asetuksen (EU, Euratom) N:o 883/2013 ja komission paikan päällä suorittamista tarkastuksista ja todentamisista Euroopan yhteisöjen taloudellisiin etuihin kohdistuvien petosten ja muiden väärinkäytösten estämiseksi 11 päivänä marraskuuta 1996 annetun neuvoston asetuksen (Euratom, EY) N:o 2185/96[40] säännösten ja niissä säädettyjen menettelyjen mukaisesti sen selvittämiseksi, onko viraston rahoittamaan avustukseen tai sopimukseen liittynyt unionin taloudellisia etuja vahingoittavia petoksia, lahjontaa tai muuta laitonta toimintaa.

4. Viraston yhteistyösopimuksiin kolmansien maiden ja kansainvälisten järjestöjen kanssa, muihin sopimuksiin, avustussopimuksiin ja avustuspäätöksiin on sisällytettävä määräyksiä, joissa nimenomaisesti annetaan tilintarkastustuomioistuimelle ja OLAFille valtuudet tehdä tällaisia tarkastuksia ja tutkimuksia niiden oman toimivallan mukaisesti, sanotun kuitenkaan rajoittamatta 1, 2 ja 3 kohdan soveltamista.

IV LUKU
VIRASTON HENKILÖSTÖ

31 artikla
Yleiset säännökset

Virastoon henkilöstöön sovelletaan henkilöstösääntöjä ja muuta henkilöstöä koskevia palvelussuhteen ehtoja sekä unionin toimielinten yhteisellä päätöksellä annettuja henkilöstösääntöjen täytäntöönpanosäännöksiä.

32 artikla
Erioikeudet ja vapaudet

Virastoon ja sen henkilöstöön sovelletaan Euroopan unionista tehtyyn sopimukseen ja Euroopan unionin toiminnasta tehtyyn sopimukseen liitettyä Euroopan unionin erioikeuksista ja vapauksista tehtyä pöytäkirjaa N:o 7.

33 artikla
Pääjohtaja

1. Pääjohtaja otetaan palvelukseen viraston väliaikaisena toimihenkilönä muuta henkilöstöä koskevien palvelussuhteen ehtojen 2 artiklan a alakohdan mukaisesti.

2. Johtokunta nimittää pääjohtajan ehdokaslistalta, jonka komissio esittää avoimen valintamenettelyn päätteeksi.

3. Johtokunnan puheenjohtaja tekee pääjohtajan työsopimuksen viraston puolesta.

[40] Neuvoston asetus (Euratom, EY) N:o 2185/96, annettu 11 päivänä marraskuuta 1996, komission paikan päällä suorittamista tarkastuksista ja todentamisista Euroopan yhteisöjen taloudellisiin etuihin kohdistuvien petosten ja muiden väärinkäytösten estämiseksi (EYVL L 292, 15.11.1996, s. 2).

4. Johtokunnan valitsema ehdokas kutsutaan ennen nimittämistä antamaan lausuma Euroopan parlamentin asiasta vastaavan valiokunnan kokouksessa ja vastaamaan Euroopan parlamentin jäsenten esittämiin kysymyksiin.

5. Pääjohtajan toimikausi on viisi vuotta. Toimikauden lopussa komissio laatii arvion, jossa otetaan huomioon pääjohtajan tehtävän hoidon arviointi ja viraston tulevat tehtävät ja haasteet.

6. Johtokunta tekee päätökset pääjohtajan nimittämisestä, toimikauden jatkamisesta tai erottamisesta äänivaltaisten jäsentensä kahden kolmasosan enemmistöllä.

7. Johtokunta voi komission ehdotuksesta, jossa otetaan huomioon 5 kohdassa tarkoitettu arviointi, jatkaa pääjohtajan toimikautta kerran enintään viideksi vuodeksi.

8. Johtokunnan on ilmoitettava Euroopan parlamentille aikeestaan jatkaa pääjohtajan toimikautta. Pääjohtaja antaa toimikauden mahdollista jatkamista edeltävien kolmen kuukauden aikana pyydettäessä lausuman Euroopan parlamentin asiasta vastaavan valiokunnan kokouksessa ja vastaa Euroopan parlamentin jäsenten esittämiin kysymyksiin.

9. Pääjohtaja, jonka toimikautta on jatkettu, ei saa osallistua samaa tointa koskevaan valintamenettelyyn.

10. Pääjohtaja voidaan erottaa toimestaan ainoastaan johtokunnan päätöksellä, jonka se tekee komission ehdotuksen perusteella.

34 artikla
Kansalliset asiantuntijat ja muu henkilöstö

1. Virasto voi käyttää kansallisia asiantuntijoita tai muuta henkilöstöä, joka ei ole viraston palveluksessa. Näihin henkilöihin ei sovelleta henkilöstösääntöjä eikä muuta henkilöstöä koskevia palvelussuhteen ehtoja.

2. Johtokunta tekee päätöksen, jolla vahvistetaan säännöt kansallisten asiantuntijoiden tilapäisestä lähettämisestä viraston palvelukseen.

V LUKU
YLEISET SÄÄNNÖKSET

35 artikla
Viraston oikeudellinen asema

1. Virasto on unionin elin, ja se on oikeushenkilö.

2. Virastolla on kussakin jäsenvaltiossa laajin kansallisen oikeuden mukainen oikeushenkilöllä oleva oikeuskelpoisuus. Se voi erityisesti hankkia ja luovuttaa irtainta ja kiinteää omaisuutta sekä esiintyä kantajana ja vastaajana oikeudenkäynneissä.

3. Virastoa edustaa sen pääjohtaja.

36 artikla

Viraston vastuu

1. Sopimukseen perustuva viraston vastuu määräytyy kyseessä olevaan sopimukseen sovellettavan lain mukaan.

2. Euroopan unionin tuomioistuimella on viraston tekemässä sopimuksessa olevaan välityslausekkeeseen perustuva tuomiovalta.

3. Sopimussuhteen ulkopuolisen vastuun osalta viraston on korvattava viraston tai sen henkilöstön tehtäviään suorittaessaan aiheuttamat vahingot jäsenvaltioiden lainsäädännön yhteisten yleisten periaatteiden mukaisesti.

4. Euroopan unionin tuomioistuimella on tuomiovalta tällaisten vahinkojen korvaamista koskevissa riidoissa.

5. Viraston toimihenkilöiden henkilökohtaista vastuuta virastoa kohtaan säännellään sen henkilöstöön sovellettavissa asiaa koskevissa määräyksissä.

37 artikla

Kielijärjestelyt

1. Virastoon sovelletaan neuvoston asetusta N:o 1[41]. Jäsenvaltiot ja niiden nimeämät muut elimet voivat kääntyä viraston puoleen ja saada siltä vastauksen valitsemallaan unionin toimielinten virallisella kielellä.

2. Euroopan unionin elinten käännöskeskus huolehtii viraston toiminnan edellyttämistä käännöspalveluista.

38 artikla

Henkilötietojen suoja

1. Virastossa tapahtuvaan henkilötietojen käsittelyyn sovelletaan Euroopan parlamentin ja neuvoston asetusta (EY) N:o 45/2001[42].

2. Johtokunta hyväksyy asetuksen (EY) N:o 45/2001 24 artiklan 8 kohdassa tarkoitetut täytäntöönpanotoimenpiteet. Johtokunta voi hyväksyä lisätoimenpiteitä, jotka ovat tarpeen viraston soveltaessa asetusta (EY) N:o 45/2001.

39 artikla

Yhteistyö kolmansien maiden ja kansainvälisten järjestöjen kanssa

1. Siltä osin kuin on tarpeen tämän asetuksen tavoitteiden saavuttamiseksi virasto voi tehdä yhteistyötä kolmansien maiden toimivaltaisten viranomaisten ja/tai kansainvälisten järjestöjen kanssa. Virasto voi tätä varten vahvistaa työjärjestelyt näiden kolmansien maiden viranomaisten ja kansainvälisten järjestöjen kanssa, edellyttäen että komissio antaa tähän ennakkohyväksynnän. Näistä järjestelyistä ei seuraa oikeudellisia velvoitteita unionille ja sen jäsenvaltioille.

---

41 Asetus N:o 1 Euroopan atomienergiayhteisössä käytettäviä kieliä koskevista järjestelyistä (EYVL 17, 6.10.1958, s. 401).

42 Euroopan parlamentin ja neuvoston asetus (EY) N:o 45/2001, annettu 18 päivänä joulukuuta 2000, yksilöiden suojelusta yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta (EYVL L 8, 12.1.2001, s. 1).

2. Viraston toimintaan voivat osallistua kolmannet maat, jotka ovat tehneet tästä sopimuksen unionin kanssa. Mainittujen sopimusten määräysten mukaisesti laaditaan järjestelyjä, joissa määritellään kyseisten maiden osalta erityisesti viraston toimintaan osallistumisen luonne, laajuus ja tapa, mukaan lukien viraston tekemiin aloitteisiin osallistumista, rahoitusosuuksia ja henkilöstöä koskevat säännöt. Henkilöstöasioiden osalta näiden järjestelyjen on kaikilta osin oltava henkilöstösääntöjen mukaiset.

3. Johtokunta hyväksyy strategian, joka koskee viraston suhteita kolmansiin maihin tai kansainvälisiin järjestöihin asioissa, joissa virasto on toimivaltainen. Komissio varmistaa, että virasto toimii toimeksiantonsa ja olemassa olevien institutionaalisten puitteiden mukaisesti sopimalla asianmukaisesta työjärjestelystä viraston pääjohtajan kanssa.

40 artikla

Turvallisuusluokiteltujen tietojen ja arkaluonteisten turvallisuusluokittelemattomien tietojen suojelemista koskevat turvallisuussäännöt

Virasto hyväksyy komissiota kuullen turvallisuussääntönsä, joissa sovelletaan turvallisuutta koskevia periaatteita, jotka sisältyvät komission päätöksissä (EU, Euratom) 2015/443 ja 2015/444 vahvistettuihin Euroopan unionin turvallisuusluokiteltujen tietojen ja arkaluonteisten turvallisuusluokittelemattomien tietojen suojaamista koskeviin komission turvallisuussäännöksiin. Tämä koskee muun muassa tällaisten tietojen vaihtamista, käsittelyä ja tallentamista.

41 artikla

Toimipaikkaa koskeva sopimus ja toimintaedellytykset

1. Vastaanottavan jäsenvaltion virastolle tarjoamia tiloja ja palveluja koskevat tarvittavat järjestelyt sekä pääjohtajaan, johtokunnan jäseniin, viraston henkilöstöön ja heidän perheenjäseniinsä vastaanottavassa jäsenvaltiossa sovellettavat erityissäännöt vahvistetaan viraston ja vastaanottavan jäsenvaltion välisessä toimipaikkaa koskevassa sopimuksessa, joka tehdään sen jälkeen kun johtokunta on sen hyväksynyt ja viimeistään [2 vuotta tämän asetuksen voimaantulon jälkeen].

2. Viraston isäntäjäsenvaltion on tarjottava parhaat mahdolliset edellytykset viraston moitteettomalle toiminnalle, mukaan lukien toimivat liikenneyhteydet sijaintipaikalle, henkilöstön jäsenten lapsille soveltuvat koulunkäyntimahdollisuudet, puolisoiden mahdollisuudet päästä työmarkkinoille sekä riittävä sosiaaliturvan ja terveydenhuoltopalvelujen saatavuus lapsille ja puolisoille.

42 artikla

Hallinnollinen valvonta

Oikeusasiamies valvoo viraston toimintaa Euroopan unionin toiminnasta tehdyn sopimuksen 228 artiklan mukaisesti.

III OSASTO

KYBERTURVALLISUUDEN SERTIFIOINTIKEHYS

43 artikla

Eurooppalaiset kyberturvallisuuden sertifiointijärjestelmät

Eurooppalaisella kyberturvallisuuden sertifiointijärjestelmällä todistetaan, että tällaisen järjestelmän mukaisesti sertifioidut tieto- ja viestintätekniikan tuotteet ja palvelut täyttävät määritellyt vaatimukset, jotka koskevat niiden kykyä suojautua tietyllä varmuustasolla toimilta, joiden tarkoituksena on vaarantaa tallennettujen, siirrettävien tai käsiteltävien tietojen tai kyseisissä tuotteissa, prosesseissa, palveluissa ja järjestelmissä tarjottavien tai välitettävien toimintojen tai palvelujen käytettävyys, aitous, eheys ja luottamuksellisuus.

44 artikla

Eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän valmistelu ja hyväksyminen

1. Kun komissio on esittänyt asiaa koskevan pyynnön, ENISA valmistelee ehdolla olevan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän, joka täyttää tämän asetuksen 45, 46 ja 47 artiklassa esitetyt vaatimukset. Jäsenvaltiot tai 53 artiklalla perustettu Euroopan kyberturvallisuuden sertifiointiryhmä, jäljempänä ’sertifiointiryhmä’, voivat esittää komissiolle ehdolla olevan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän valmistelemista.
2. Valmistellessaan 1 kohdassa tarkoitettuja ehdolla olevia järjestelmiä ENISA kuulee kaikkia asiaankuuluvia sidosryhmiä ja tekee tiivistä yhteistyötä sertifiointiryhmän kanssa. Sertifiointiryhmä antaa ENISAlle apua ja asiantuntijaneuvontaa, jota ENISA tarvitsee ehdolla olevan järjestelmän valmistelussa, tarvittaessa myös antamalla lausuntoja.
3. ENISA toimittaa tämän artiklan 2 kohdan mukaisesti valmistellun ehdolla olevan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän komissiolle.
4. Komissio voi ENISA:n valmisteleman ehdolla olevan järjestelmän pohjalta hyväksyä 55 artiklan 1 kohdan mukaisesti täytäntöönpanosäädöksiä tieto- ja viestintätekniikan tuotteiden ja palvelujen eurooppalaisista kyberturvallisuuden sertifiointijärjestelmistä, jotka täyttävät tämän asetuksen 45, 46 ja 47 artiklan vaatimukset.
5. ENISA ylläpitää erityistä verkkosivustoa, joka tarjoaa eurooppalaisia kyberturvallisuuden sertifiointijärjestelmiä koskevaa tiedotusta ja julkisuutta.

45 artikla

Eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien turvallisuustavoitteet

Eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän suunnittelussa on otettava huomioon soveltuvin osin seuraavat turvallisuustavoitteet:

a) suojata tallennetut, siirretyt tai muulla tavoin käsitellyt tiedot vahingossa tapahtuvalta tai luvattomalta tallentamiselta, käsittelyltä, käytöltä tai luovuttamiselta;

b) suojata tallennetut, siirretyt tai muulla tavoin käsitellyt tiedot vahingossa tapahtuvalta tai luvattomalta tuhoamiselta, tahattomalta katoamiselta tai muuttamiselta;

c) varmistaa, että valtuutettujen henkilöiden, ohjelmien tai koneiden saatavilla on ainoastaan ne tiedot, palvelut tai toiminnot, joihin näillä on käyttöoikeudet;

d) tallentaa tieto siitä, mitkä tiedot, toiminnot tai palvelut on ilmoitettu, sekä ilmoituksen ajankohta ja tekijä;

e) varmistaa, että on mahdollista tarkastaa, mitä tietoja, palveluja tai toimintoja on käytetty, sekä käytön ajankohta ja käyttäjä;

f) palauttaa tietojen, palvelujen ja toimintojen saatavuus ja käytettävyys mahdollisimman pian fyysisen tai teknisen vian sattuessa;

g) varmistaa tieto- ja viestintätekniikan tuotteille ja palveluille ajantasainen ohjelmisto, joka ei sisällä tunnettuja haavoittuvuuksia, ja mekanismit, joilla varmistetaan ohjelmistojen turvalliset päivitykset.

46 artikla

Eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien varmuustasot

1. Eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä voidaan määritellä yksi tai useampi varmuustaso – perustaso, korotettu ja/tai korkea – kyseisessä järjestelmässä sertifioiduille tieto- ja viestintätekniikan tuotteille ja palveluille.

2. Varmuustasojen perustaso, korotettu ja korkea on täytettävä seuraavat vaatimukset:

a) perustasolla oleva varmuustaso viittaa eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän yhteydessä myönnettyyn sertifikaattiin, joka antaa rajallisen luottamustason tieto- ja viestintätekniikan tuotteen tai palvelun väitetyille tai esitetyille kyberturvallisuusominaisuuksille ja jota luonnehditaan suhteessa siihen liittyviin teknisiin eritelmiin, standardeihin ja menettelyihin sekä teknisiin tarkastuksiin, joiden tarkoituksena on vähentää kyberturvallisuuspoikkeamien riskiä;

b) korotettu varmuustaso viittaa eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän yhteydessä myönnettyyn sertifikaattiin, joka antaa korotetun luottamustason tieto- ja viestintätekniikan tuotteen tai palvelun väitetyille tai esitetyille kyberturvallisuusominaisuuksille ja jota luonnehditaan suhteessa siihen liittyviin teknisiin eritelmiin, standardeihin ja menettelyihin sekä teknisiin tarkastuksiin, joiden tarkoituksena on vähentää merkittävästi kyberturvallisuuspoikkeamien riskiä;

c) korkea varmuustaso viittaa eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän yhteydessä myönnettyyn sertifikaattiin, joka antaa korotettua varmuustasoa korkeamman luottamustason tieto- ja viestintätekniikan tuotteen tai palvelun väitetyille tai esitetyille kyberturvallisuusominaisuuksille ja jota luonnehditaan suhteessa siihen liittyviin teknisiin eritelmiin, standardeihin ja menettelyihin sekä teknisiin tarkastuksiin, joiden tarkoituksena on ehkäistä kyberturvallisuuspoikkeamat.

47 artikla

Eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien osatekijät

1. Eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän on sisällettävä seuraavat osatekijät:

   a) sertifioinnin kohde ja soveltamisala, mukaan lukien sen kattamien tieto- ja viestintätekniikan tuotteiden ja palvelujen tyyppi tai luokat;

   b) yksityiskohtainen erittely kyberturvallisuusvaatimuksista, joihin nähden erityiset tieto- ja viestintätekniikan tuotteet ja palvelut arvioidaan, esimerkiksi viittaamalla unionin tai kansainvälisiin standardeihin tai teknisiin eritelmiin;

   c) soveltuvin osin yksi tai useampi varmuustaso;

   d) yksittäiset arvioinnissa käytettävät perusteet ja menetelmät, mukaan lukien arvioinnin tyypit, jotta voidaan osoittaa, että 45 artiklassa tarkoitetut erityiset tavoitteet saavutetaan;

   e) sertifioinnin edellyttämät tiedot, jotka hakijan on toimitettava vaatimustenmukaisuuden arviointilaitoksille;

   f) jos järjestelmä tarjoaa käyttöön merkkejä tai merkintöjä, näiden merkkien tai merkintöjen käytön edellytykset;

   g) jos järjestelmään kuuluu valvonta, säännöt sertifikaattien vaatimusten noudattamisen seurantaa varten, mukaan lukien mekanismit sen osoittamiseksi, että määriteltyjä kyberturvallisuusvaatimuksia noudatetaan jatkuvasti;

   h) ehdot sertifioinnin myöntämiselle, voimassa pitämiselle ja jatkamiselle sekä sen soveltamisalan laajentamiselle ja supistamiselle;

   i) säännöt seurauksista tapauksissa, joissa sertifioidut tieto- ja viestintätekniikan tuotteet ja palvelut eivät vastaa sertifiointivaatimuksia;

   j) säännöt siitä, miten aiemmin tuntemattomat tieto- ja viestintätekniikan tuotteiden ja palvelujen kyberhaavoittuvuudet on määrä raportoida ja käsitellä;

   k) säännöt tietojen säilyttämisestä vaatimustenmukaisuuden arviointilaitoksissa;

   l) sellaisten kansallisten kyberturvallisuuden sertifiointijärjestelmien yksilöinti, jotka kattavat saman tyypin tai samojen luokkien tieto- ja viestintätekniikan tuotteita ja palveluja;

   m) myönnetyn sertifikaatin sisältö.

2. Järjestelmälle määritellyt vaatimukset eivät saa olla ristiriidassa sovellettavien oikeudellisten vaatimusten, erityisesti yhdenmukaistetusta unionin lainsäädännöstä johtuvien vaatimusten kanssa.

3. Jos unionin säädöksessä niin säädetään, eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän mukaista sertifiointia voidaan käyttää osoittamaan, että kyseisen säädöksen vaatimusten suhteen vallitsee vaatimustenmukaisuusolettama.

4. Jos yhdenmukaistettua unionin lainsäädäntöä ei ole, myös jäsenvaltioiden lainsäädännössä voidaan säätää, että eurooppalaista kyberturvallisuuden sertifiointijärjestelmää voidaan käyttää luomaan vaatimustenmukaisuusolettama oikeudellisiin vaatimuksiin nähden.

48 artikla

Kyberturvallisuussertifiointi

1. Tieto- ja viestintätekniikan tuotteet ja palvelut, jotka on sertifioitu jossain 44 artiklan mukaisesti hyväksytyssä eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä, katsotaan kyseisen järjestelmän vaatimusten mukaisiksi.

2. Sertifiointi on vapaaehtoinen, jollei unionin lainsäädännössä toisin säädetä.

3. Tämän artiklan mukaisen eurooppalaisen kyberturvallisuussertifikaatin antavat 51 artiklassa tarkoitetut vaatimustenmukaisuuden arviointilaitokset perustuen kriteereihin, jotka sisältyvät 44 artiklan mukaisesti hyväksyttyyn eurooppalaiseen kyberturvallisuuden sertifiointijärjestelmään.

4. Poiketen siitä, mitä 3 kohdassa säädetään, asianmukaisesti perustelluissa tapauksissa yksittäisessä eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä voidaan määrätä, että järjestelmästä saatavan eurooppalaisen kyberturvallisuussertifikaatin voi myöntää vain julkinen elin. Tämän julkisen elimen on oltava joko

   a) 50 artiklan 1 kohdassa tarkoitettu kansallinen sertifioinnin valvontaviranomainen,

   b) 51 artiklan 1 kohdan nojalla vaatimustenmukaisuuden arviointilaitoksena akkreditoitu elin tai

   c) asianomaisen jäsenvaltion lakien, määräysten tai muiden virallisten hallintomenettelyjen mukaisesti perustettu elin, joka täyttää tuotteiden, prosessien ja palvelujen sertifiointielimiä koskevat vaatimukset ISO/IEC 17065:2012 -standardin mukaisesti.

5. Luonnollisen tai oikeushenkilön, joka jättää tieto- ja viestintätekniikan tuotteensa tai palvelunsa sertifioitaviksi, on toimitettava 51 artiklassa tarkoitetulle vaatimustenmukaisuuden arviointilaitokselle kaikki sertifiointimenettelyn suorittamiseen tarvittavat tiedot.

6. Sertifikaatit voidaan myöntää enintään kolmeksi vuodeksi, ja ne voidaan uusia samoin edellytyksin, jos sovellettavat vaatimukset täyttävät edelleen.

7. Tämän artiklan mukaisesti myönnetty eurooppalainen kyberturvallisuussertifikaatti on tunnustettava kaikissa jäsenvaltioissa.

49 artikla

Kansalliset kyberturvallisuuden sertifiointijärjestelmät ja sertifikaatit

1. Sellaisia tieto- ja viestintätekniikan tuotteita ja palveluja varten voimassa olevat kansalliset kyberturvallisuuden sertifiointijärjestelmät ja niihin liittyvät menettelyt, jotka kuuluvat jonkin eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän soveltamisalaan, lakkaavat tuottamasta oikeusvaikutuksia alkaen päivästä, joka vahvistetaan 44 artiklan 4 kohdan nojalla hyväksytyssä täytäntöönpanosäädöksessä, sanotun kuitenkaan rajoittamatta 3 kohdan soveltamista. Sellaisia tieto- ja viestintätekniikan tuotteita ja palveluja varten voimassa olevat kansalliset kyberturvallisuuden sertifiointijärjestelmät ja niihin liittyvät menettelyt, jotka eivät kuulu jonkin eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän soveltamisalaan, pysyvät edelleen voimassa.

2. Jäsenvaltiot eivät saa ottaa käyttöön uusia kansallisia kyberturvallisuuden sertifiointijärjestelmiä tieto- ja viestintätekniikan tuotteille ja palveluille, jotka kuuluvat jonkin voimassa olevan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän soveltamisalaan.

3. Kansallisissa kyberturvallisuuden sertifiointijärjestelmissä myönnetyt voimassa olevat sertifikaatit pysyvät voimassa niiden voimassaolon päättymispäivään asti.

50 artikla

Kansalliset sertifioinnin valvontaviranomaiset

1. Kunkin jäsenvaltion on nimettävä kansallinen sertifioinnin valvontaviranomainen.

2. Kunkin jäsenvaltion on ilmoitettava nimetty viranomainen komissiolle.

3. Kunkin kansallisen sertifioinnin valvontaviranomaisen on oltava organisaatioltaan, rahoituspäätöksiltään, oikeudelliselta rakenteeltaan ja päätöksenteoltaan riippumaton yksiköistä, joita ne valvovat.

4. Jäsenvaltioiden on varmistettava, että kansallisilla sertifioinnin valvontaviranomaisilla on riittävät resurssit käyttää valtuuksiaan ja suorittaa tuloksekkaasti ja tehokkaasti niille osoitetut tehtävät.

5. Tämän asetuksen tehokkaan täytäntöönpanon varmistamiseksi on aiheellista, että kyseiset viranomaiset osallistuvat 53 artiklan nojalla perustettuun Euroopan kyberturvallisuuden sertifiointiryhmään aktiivisella, tehokkaalla ja turvallisella tavalla.

6. Kansallisten sertifioinnin valvontaviranomaisten on

   a) valvottava tämän osaston säännösten soveltamista ja huolehdittava niiden täytäntöönpanosta kansallisella tasolla sekä valvottava sitä, ovatko niiden alueelle sijoittautuneiden vaatimustenmukaisuuden arviointilaitosten myöntämät sertifikaatit tämän osaston vaatimusten ja vastaavan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän vaatimusten mukaisia;

   b) seurattava ja valvottava vaatimustenmukaisuuden arviointilaitosten toimintaa tämän asetuksen soveltamiseksi, mukaan lukien vaatimustenmukaisuuden arviointilaitoksista ilmoittaminen ja siihen liittyvät tehtävät tämän asetuksen 52 artiklan mukaisesti;

   c) käsiteltävä luonnollisten tai oikeushenkilöiden tekemät valitukset, jotka liittyvät niiden alueelle sijoittautuneiden vaatimustenmukaisuuden arviointilaitosten myöntämiin sertifikaatteihin, tutkittava asianmukaisessa määrin valituksen kohde ja ilmoitettava valituksen tekijälle tutkinnan etenemisestä ja tuloksesta kohtuullisessa ajassa;

   d) tehtävä yhteistyötä muiden kansallisten sertifioinnin valvontaviranomaisten tai muiden viranomaisten kanssa esimerkiksi jakamalla tietoa mahdollisista tapauksista, joissa tieto- ja viestintätekniikan tuotteet ja palvelut eivät vastaa tämän asetuksen tai yksittäisten eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien vaatimuksia;

   e) seurattava merkityksellistä kehitystä kyberturvallisuussertifioinnin alalla.

7. Kullakin kansallisella sertifioinnin valvontaviranomaisella on oltava ainakin valtuudet

a) pyytää vaatimustenmukaisuuden arviointilaitoksilta ja eurooppalaisen kyberturvallisuussertifikaatin haltijoilta kaikki tiedot, jotka se tarvitsee tehtävänsä suorittamiseksi;

b) tehdä tarkastusten avulla tutkimuksia vaatimustenmukaisuuden arviointilaitoksista ja eurooppalaisen kyberturvallisuussertifikaatin haltijoista III osaston säännösten noudattamisen valvomiseksi;

c) toteuttaa asianmukaisia toimenpiteitä kansallisen lainsäädännön mukaisesti varmistaakseen, että vaatimustenmukaisuuden arviointilaitokset tai sertifikaattien haltijat noudattavat tämän asetuksen tai eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän vaatimuksia;

d) päästä vaatimustenmukaisuuden arviointilaitosten ja eurooppalaisen kyberturvallisuussertifikaatin haltijoiden tiloihin tutkimusten tekemiseksi unionin tai jäsenvaltion prosessioikeuden mukaisesti;

e) peruuttaa kansallisen lainsäädännön mukaisesti sertifikaatit, jotka eivät täytä tämän asetuksen tai eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän vaatimuksia;

f) määrätä seuraamuksia 54 artiklassa säädetyllä tavalla kansallisen lainsäädännön mukaisesti ja vaatia lopettamaan tässä asetuksessa säädettyjen velvoitteiden rikkominen välittömästi.

8. Kansallisten sertifioinnin valvontaviranomaisten on tehtävä yhteistyötä keskenään ja komission kanssa ja erityisesti vaihdettava tietoja, kokemuksia ja hyviä käytäntöjä tieto- ja viestintätekniikan tuotteiden ja palvelujen kyberturvallisuussertifioinnista ja niiden kyberturvallisuuteen liittyvistä teknisistä kysymyksistä.

51 artikla

Vaatimustenmukaisuuden arviointilaitokset

1. Asetuksen (EY) N:o 765/2008 mukaisesti nimetyn kansallisen akkreditointielimen on akkreditoitava vaatimustenmukaisuuden arviointilaitokset vain, jos ne täyttävät tämän asetuksen liitteessä esitetyt vaatimukset.

2. Akkreditointi myönnetään enintään viideksi vuodeksi, ja se voidaan uusia samoin edellytyksin, jos vaatimustenmukaisuuden arviointilaitos täyttää tässä artiklassa säädetyt vaatimukset. Akkreditointielimen on peruutettava tämän artiklan 1 kohdan nojalla myönnetty vaatimustenmukaisuuden arviointilaitoksen akkreditointi, jos akkreditoinnin edellytykset eivät täyty tai eivät enää täyty tai jos vaatimustenmukaisuuden arviointilaitoksen toiminta rikkoo tämän asetuksen säännöksiä.

52 artikla

Ilmoittaminen

1. Kansallisten sertifioinnin valvontaviranomaisten on jokaisen 44 artiklan mukaisesti hyväksytyn eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän osalta ilmoitettava komissiolle vaatimustenmukaisuuden arviointilaitoksista, jotka on akkreditoitu myöntämään sertifikaatteja 46 artiklassa tarkoitetuilla määritellyillä

varmuustasoilla, ja ilman aiheetonta viivytystä kaikista niiden myöhemmistä muutoksista.

2. Vuoden kuluttua eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän voimaantulosta komissio julkaisee luettelon ilmoitetuista vaatimustenmukaisuuden arviointilaitoksista *Euroopan unionin virallisessa lehdessä*.

3. Jos komissio saa ilmoituksen 2 kohdassa tarkoitetun ajanjakson päättymisen jälkeen, se julkaisee *Euroopan unionin virallisessa lehdessä* muutokset 2 kohdassa tarkoitettuun luetteloon kahden kuukauden kuluessa kyseisen ilmoituksen vastaanottamisesta.

4. Kansallinen sertifioinnin valvontaviranomainen voi esittää komissiolle pyynnön poistaa kyseisen kansallisen sertifioinnin valvontaviranomaisen ilmoittama vaatimustenmukaisuuden arviointilaitos tämän artiklan 2 kohdassa tarkoitetusta luettelosta. Komissio julkaisee *Euroopan unionin virallisessa lehdessä* vastaavat tarkistukset luetteloon kuukauden kuluessa kansallisen sertifioinnin valvontaviranomaisen pyynnön vastaanottamisesta.

5. Komissio voi täytäntöönpanosäädöksillä määritellä olosuhteet, muotoseikat ja menettelyt tämän artiklan 1 kohdassa tarkoitetuille ilmoituksille. Nämä täytäntöönpanosäädökset hyväksytään 55 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

53 artikla

Euroopan kyberturvallisuuden sertifiointiryhmä

1. Perustetaan Euroopan kyberturvallisuuden sertifiointiryhmä, jäljempänä ’sertifiointiryhmä’.

2. Ryhmä koostuu kansallisista sertifioinnin valvontaviranomaisista. Kansallisten sertifioinnin valvontaviranomaisten on oltava edustettuina johtajatasolla tai muulla korkealla tasolla.

3. Sertifiointiryhmän tehtävänä on

   a) neuvoa ja avustaa komissiota sen pyrkiessä varmistamaan tämän osaston johdonmukainen täytäntöönpano ja soveltaminen erityisesti kyberturvallisuussertifioinnin toimintapoliittisissa kysymyksissä, toimintaperiaatteiden yhteensovittamisessa ja eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien valmistelemisessa;

   b) avustaa ja neuvoa ENISAa ja tehdä sen kanssa yhteistyötä ehdolla olevan järjestelmän valmistelemisessa tämän asetuksen 44 artiklan mukaisesti;

   c) esittää komissiolle, että se pyytää virastoa valmistelemaan ehdolla olevan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän tämän asetuksen 44 artiklan mukaisesti;

   d) antaa komissiolle osoitettuja lausuntoja voimassa olevien eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien ylläpitämisestä ja tarkistamisesta;

   e) tarkastella merkityksellistä kehitystä kyberturvallisuussertifioinnin alalla ja vaihtaa hyviä käytäntöjä kyberturvallisuuden sertifiointijärjestelmistä;

   f) helpottaa kansallisten sertifioinnin valvontaviranomaisten välistä, tämän osaston mukaista yhteistyötä tiedonvaihdon avulla erityisesti ottamalla

käyttöön menetelmiä tietojen vaihtamiseksi tehokkaasti kaikista kyberturvallisuussertifiointia koskevista kysymyksistä.

4. Sertifiointiryhmän puheenjohtajana ja sihteeristönä toimii komissio ENISAn avustuksella siten kuin 8 artiklan a alakohdassa säädetään.

54 artikla
Seuraamukset

Jäsenvaltioiden on annettava säännöt seuraamuksista, joita sovelletaan tämän osaston ja eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien säännösten rikkomiseen, ja toteutettava kaikki tarvittavat toimenpiteet sen varmistamiseksi, että ne pannaan täytäntöön. Säädettyjen seuraamusten on oltava tehokkaita, oikeasuhteisia ja varoittavia. Jäsenvaltioiden on ilmoitettava nämä säännöt ja toimenpiteet komissiolle [viimeistään ... / viipymättä] ja ilmoitettava sille niihin vaikuttavista myöhemmistä muutoksista.

IV OSASTO
LOPPUSÄÄNNÖKSET

55 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 4 artiklaa.

56 artikla
Arviointi ja uudelleentarkastelu

1. Komissio arvioi viimeistään viiden vuoden kuluttua 58 artiklassa tarkoitetusta päivämäärästä ja sen jälkeen viiden vuoden välein viraston ja sen työtapojen vaikutuksen, tehokkuuden ja tuloksellisuuden sekä mahdollisen tarpeen muuttaa viraston toimeksiantoa ja tällaisten muutosten taloudelliset vaikutukset. Arvioinnissa otetaan huomioon viraston toiminnastaan mahdollisesti saama palaute. Jos komissio katsoo, ettei viraston toiminnan jatkaminen ole enää perusteltua sille asetettuihin tavoitteisiin, toimeksiantoon ja tehtäviin nähden, se voi ehdottaa, että tätä asetusta muutetaan virastoa koskevien säännösten osalta.
2. Arvioinnissa arvioidaan myös III osaston säännösten vaikutusta, tehokkuutta ja tuloksellisuutta suhteessa tavoitteisiin varmistaa tieto- ja viestintätekniikan tuotteiden ja palvelujen kyberturvallisuuden riittävä taso unionissa ja parantaa sisämarkkinoiden toimintaa.
3. Komissio toimittaa arviointikertomuksen ja päätelmänsä Euroopan parlamentille, neuvostolle ja johtokunnalle. Arvioinnin tulokset julkistetaan.

57 artikla
Kumoaminen ja seuraanto

1. Kumotaan asetus (EY) N:o 526/2013 [...] alkaen.
2. Viittaukset asetukseen (EY) N:o 526/2013 ja ENISAan katsotaan viittauksiksi tähän asetukseen ja virastoon.
3. Virasto toimii kaikkien omistusten, sopimusten, oikeudellisten velvoitteiden, työsopimusten, taloudellisten sitoumusten ja vastuiden osalta asetuksella (EY) N:o 526/2013 perustetun viraston seuraajana. Kaikki johtokunnan ja hallituksen voimassa olevat päätökset pysyvät voimassa edellyttäen, että ne eivät ole ristiriidassa tämän asetuksen säännösten kanssa.
4. Virasto perustetaan määrittelemättömäksi toimiajaksi [...] alkaen.
5. Asetuksen (EY) N:o 526/2013 24 artiklan 4 kohdan mukaisesti nimitetty pääjohtaja toimii viraston pääjohtajana jäljellä olevan toimikautensa ajan.

6. Asetuksen (EY) N:o 526/2013 6 artiklan mukaisesti nimitetyt johtokunnan jäsenet ja varajäsenet toimivat viraston johtokunnan jäseninä ja varajäseninä jäljellä olevan toimikautensa ajan.

58 artikla

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

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

Tehty Brysselissä

Euroopan parlamentin puolesta	*Neuvoston puolesta*
Puhemies	*Puheenjohtaja*

RAHOITUSSELVITYS

1. PERUSTIEDOT EHDOTUKSESTA/ALOITTEESTA

1.1. Ehdotuksen/aloitteen nimi

Ehdotus Euroopan parlamentin ja neuvoston asetukseksi EU:n kyberturvallisuusvirastosta ENISAsta ja asetuksen (EU) 526/2013 kumoamisesta sekä tieto- ja viestintätekniikan kyberturvallisuussertifioinnista (”kyberturvallisuusasetus”)

1.2. Toimintalohko(t)

Toimintalohko: 09 – Viestintäverkot, sisällöt ja teknologia

Toiminto: 09.02 Digitaaliset sisämarkkinat

1.3. Ehdotuksen/aloitteen luonne

☒ Ehdotus/aloite liittyy **uuteen toimeen (III osasto – Sertifiointi).**

☐ Ehdotus aloite liittyy **uuteen toimeen, joka perustuu pilottihankkeeseen tai valmistelutoimeen**[43]**.**

☒ Ehdotus/aloite liittyy **käynnissä olevan toimen jatkamiseen** (**II osasto – ENISAn toimeksianto).**

☐ Ehdotus/aloite liittyy **toimeen, joka on suunnattu uudelleen.**

1.4. Tavoite (Tavoitteet)

1.4.1. Komission monivuotinen strateginen tavoite (monivuotiset strategiset tavoitteet), jonka (joiden) saavuttamista ehdotus/aloite tukee

1. Jäsenvaltioiden, yritysten ja koko EU:n resilienssin lisääminen.

2. EU:n sisämarkkinoiden asianmukaisen toiminnan varmistaminen tieto- ja viestintätekniikan tuotteita ja palveluja varten.

3. Tieto- ja viestintätekniikan alalla toimivien EU:n yritysten maailmanlaajuisen kilpailukyvyn lisääminen.

4. Jäsenvaltioiden lakien, asetusten ja hallinnollisten määräysten lähentäminen kyberturvallisuuden tarpeisiin.

1.4.2. Erityistavoitteet

Yleisten tavoitteiden pohjalta ja tarkistetun kyberturvallisuusstrategian laajemmassa yhteydessä aloitteella pyritään – linjaamalla ENISAn toimintakenttää ja toimeksiantoa ja perustamalla eurooppalainen sertifiointikehys tieto- ja viestintätekniikan tuotteille ja palveluille – seuraaviin erityistavoitteisiin:

1. jäsenvaltioiden ja yritysten **valmiuksien ja varautumiskyvyn** lisääminen;
2. **yhteistyön ja koordinoinnin** parantaminen jäsenvaltioiden ja EU:n toimielinten, virastojen ja elinten välillä;
3. **EU-tason valmiuksien lisääminen jäsenvaltioiden toimien täydentämiseksi** erityisesti rajat ylittävien kyberkriisien yhteydessä;
4. kansalaisten ja yritysten **tietoisuuden** lisääminen kyberturvallisuuteen liittyvistä

[43] Sellaisina kuin nämä on määritelty varainhoitoasetuksen 54 artiklan 2 kohdan a ja b alakohdassa.

kysymyksistä;

5. yleisen **avoimuuden lisääminen tieto- ja viestintäteknisten tuotteiden ja palvelujen kyberturvallisuuden varmistuksessa**[44], jotta voidaan lisätä luottamusta digitaalisiin sisämarkkinoihin ja digitaalisiin innovaatioihin.

ENISA auttaa saavuttamaan edellä esitetyt tavoitteet seuraavasti:

Tehostettu päätöksenteon tuki – Virasto antaa ohjeita ja neuvoja komissiolle ja jäsenvaltioille, jotta voidaan kehittää ja pitää ajan tasalla kokonaisvaltaista ja normatiivista kehystä kyberturvallisuuden alalla sekä alakohtaisia toimintapoliittisia ja oikeudellisia aloitteita silloin kun niihin liittyy kyberturvallisuuskysymyksiä. Virasto edesauttaa yhteistyöryhmän työtä (direktiivin (EU) 2016/1148 11 artikla) antamalla asiantuntemusta ja apua, tukee politiikan valmistelua ja täytäntöönpanoa sähköisen henkilöllisyyden ja sähköisten luottamuspalvelujen alalla ja edistää parhaiden toimintatapojen vaihtoa toimivaltaisten viranomaisten välillä.

Tehostettu tuki valmiuksien kehittämiselle – Virasto tukee jäsenvaltioita sekä unionin toimielimiä, elimiä, laitoksia ja virastoja kehittämään ja tehostamaan kyberturvallisuusongelmien ja -poikkeamien ehkäisyä, havaitsemista ja analyysia sekä valmiuksia reagoida niihin. Virasto avustaa pyynnöstä jäsenvaltioita niiden kehittäessä kansallisia CSIRT-toimijoita ja kansallisia kyberturvallisuusstrategioita, avustaa unionin toimielimiä niiden kehittäessä ja tarkastellessa uudelleen unionin kyberturvallisuusstrategioita, tarjoaa kyberturvallisuuskoulutusta, avustaa yhteistyöryhmän kautta jäsenvaltioita parhaiden käytäntöjen vaihtamisessa sekä helpottaa tietojen jakamisen ja analysoinnin alakohtaisten keskusten (ISAC) perustamista.

Operatiivisen yhteistyön ja kriisinhallinnan tuki – Virasto tukee toimivaltaisten julkisten elinten keskinäistä ja sidosryhmien välistä yhteistyötä järjestelmällisessä yhteistoiminnassa unionin toimielinten, elinten, toimistojen ja virastojen kanssa kyberturvallisuuteen, kyberrikollisuuteen ja yksityisyyden ja henkilötietojen suojaan liittyvissä asioissa. Virasto toimii CSIRT-verkoston sihteeristönä (direktiivin (EU) 2016/1148 12 artiklan 2 kohta) ja edistää verkoston kanssa tehtävää operatiivista yhteistyötä antamalla yhdessä CERT-EU:n kanssa tukea jäsenvaltioille niiden pyynnöstä. Virasto järjestää säännöllisiä kyberturvallisuusharjoituksia, edistää yhteistyöhön perustuvan vastauksen kehittämistä laajamittaisiin rajatylittäviin kyberturvallisuuspoikkeamiin ja -kriiseihin sekä tekee yhteistyössä CSIRT-verkoston kanssa teknisiä jälkikäteistutkimuksia merkittävistä poikkeamista ja antaa suosituksia jatkotoimista.

Markkinoihin liittyvät tehtävät (standardointi, sertifiointi) – Virasto huolehtii useista tehtävistä, joilla tuetaan erityisesti sisämarkkinoita. Virasto pitää yllä ”markkinoiden seurantakeskusta” analysoimalla kyberturvallisuusmarkkinoiden tärkeimpiä suuntauksia, jotta kysyntä ja tarjonta saadaan vastaamaan paremmin toisiaan. Virasto tukee ja edistää tieto- ja viestintätekniikan tuotteiden ja palvelujen kyberturvallisuussertifiointiin liittyvän unionin politiikan kehittämistä ja täytäntöönpanoa valmistelemalla ehdolla olevat eurooppalaiset kyberturvallisuuden sertifiointijärjestelmät tieto- ja viestintätekniikan tuotteita ja palveluja varten, toimimalla unionin kyberturvallisuuden sertifiointiryhmän sihteeristönä ja tarjoamalla käyttöön ohjeita ja hyviä käytäntöjä tieto- ja viestintätekniikan tuotteiden ja palvelujen turvallisuusvaatimuksista yhteistyössä kansallisten sertifioinnin

[44] Avoimuudella kyberturvallisuuden varmistuksessa tarkoitetaan sitä, että käyttäjät saavat kyberturvallisuusominaisuuksista riittävät tiedot, joiden avulla käyttäjät voivat objektiivisesti määrittää tietyn tieto- ja viestintäteknisen tuotteen, palvelun tai prosessin turvallisuustason.

valvontaviranomaisten ja toimialan kanssa. **Tietämyksen, tiedotuksen ja tietoisuuden lisääminen** – Virasto antaa komissiolle ja jäsenvaltioille apua ja neuvontaa, jotta koko unionissa saavutettaisiin korkea osaamistaso asioissa, jotka liittyvät verkko- ja tietoturvaan ja sen soveltamiseen toimialan sidosryhmien keskuudessa. Tähän sisältyy myös verkko- ja tietojärjestelmien turvallisuutta [kyberturvallisuutta] koskevan tiedon kokoaminen, järjestäminen ja yleisön saataville asettaminen erityisen portaalin kautta. Toinen tärkeä tekijä ovat suurelle yleisölle suunnatut tietoisuutta lisäävät toimet ja tiedotuskampanjat kyberturvallisuusriskeistä.

Tehostettu tutkimus- ja innovointituki – Virasto tarjoaa neuvontaa tutkimustarpeista ja tutkimuksen painopisteistä kyberturvallisuuden alalla.

Tuki kansainväliselle yhteistyölle – Virasto tukee unionin pyrkimyksiä tehdä yhteistyötä kolmansien maiden ja kansainvälisten organisaatioiden kanssa, jotta voidaan edistää kansainvälistä yhteistyötä kyberturvallisuuden alalla.

SERTIFIOINTI

Sertifiointikehys auttaa saavuttamaan tavoitteet lisäämällä yleistä avoimuutta tieto- ja viestintäteknisten tuotteiden ja palvelujen kyberturvallisuuden varmistuksessa[45], jotta voidaan lisätä luottamusta digitaalisiin sisämarkkinoihin ja digitaalisiin innovaatioihin. Tällä tavoin voidaan myös välttää hajanaisuutta sertifiointijärjestelmissä EU:ssa ja niihin liittyvissä turvallisuusvaatimuksissa ja arviointiperusteissa jäsenvaltioissa ja eri aloilla.

1.4.3. Odotettavissa olevat tulokset ja vaikutukset

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

ENISAlle annetaan vahvempi rooli, jossa se tukee valmiuksien kehittämistä, ennaltaehkäisyä, yhteistyötä ja tietoisuutta EU:n tasolla pyrkimyksenä lisätä EU:n yleistä kyberresilienssiä sekä tukee EU:n sertifiointikehystä tieto- ja viestintätekniikan tuotteille ja palveluille, mistä odotetaan seuraavanlaisia vaikutuksia (luettelo ei ole tyhjentävä):

Kokonaisvaikutus:

– Vaikutus on sisämarkkinoilla on kaiken kaikkiaan positiivinen, koska voidaan korjata markkinoiden hajanaisuutta ja rakentaa luottamusta digitaaliteknologiaan sitä kautta, että yhteistyö parantuu, kyberturvallisuuteen EU:ssa omaksutut toimintamallit yhdenmukaistuvat ja valmiudet lisääntyvät EU:n tasolla. Tämän pitäisi johtaa myönteiseen talousvaikutukseen, koska se auttaisi vähentämään kyberturvallisuuspoikkeamista ja kyberrikollisuudesta aiheutuvia kustannuksia, joiden arvioitu taloudellinen vaikutus on Euroopan unionissa 0,41 % EU:n bruttokansantuotteesta (eli noin 55 miljardia euroa).

Erityiset tulokset:

Jäsenvaltioiden ja yritysten kyberturvallisuusvalmiuksien ja varautumiskyvyn paraneminen

– Jäsenvaltioiden kyberturvallisuusvalmiudet ja varautumiskyky paranevat, tukenaan pitkän aikavälin strategiset analyysit kyberuhkista ja -poikkeamista, ohjeet ja raportit, asiantuntemuksen ja hyvien käytäntöjen vaihto, koulutuksen ja koulutusmateriaalin saatavuus ja tehostetut CyberEurope-harjoitukset.

[45] Avoimuudella kyberturvallisuuden varmistuksessa tarkoitetaan sitä, että käyttäjät saavat kyberturvallisuusominaisuuksista riittävät tiedot, joiden avulla käyttäjät voivat objektiivisesti määrittää tietyn tieto- ja viestintäteknisen tuotteen, palvelun tai prosessin turvallisuustason.

– Yksityisten toimijoiden valmiudet paranevat tietojen jakamisen ja analysoinnin alakohtaisten keskusten (ISAC) perustamiselle eri aloilla annettavan tuen kautta.

– EU:n ja jäsenvaltioiden varautumistaso paranee, koska käyttöön tulee hyvin valmistellut ja sovitut suunnitelmat laajamittaisten rajaylittävien kyberturvallisuuspoikkeamien varalta CyberEurope-harjoituksissa testatulla tavalla.

Yhteistyön ja koordinoinnin lisääntyminen jäsenvaltioiden ja EU:n toimielinten, virastojen ja elinten välillä

– Yhteistyö paranee julkisen ja yksityisen sektorin sisäisesti ja niiden välillä.

– Verkko- ja tietoturvadirektiivin täytäntöönpano johdonmukaistuu maiden ja hallinnonalojen rajojen yli.

– Yhteistyö paranee sertifioinnin alalla, tukenaan institutionaalinen kehys, joka mahdollistaa eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien ja yhteisen politiikan kehittämisen tällä alalla.

EU:n tason valmiuksien lisääminen jäsenvaltioiden toimien täydentämiseksi

– EU saa paremmat operatiiviset valmiudet, joilla täydennetään jäsenvaltioiden toimintaa ja tuetaan niitä pyynnöstä ja rajoitettujen ja ennalta määriteltyjen palvelujen osalta. Tämän odotetaan vaikuttavan myönteisesti siihen, miten poikkeamien ennaltaehkäisy ja havaitsemisen ja niihin reagointi onnistuvat sekä jäsenvaltioiden että unionin tasolla.

Kansalaisten ja yritysten tietoisuuden lisääminen kyberturvallisuuteen liittyvistä kysymyksistä

– Kansalaisten ja yritysten yleinen tietoisuus kyberturvallisuuskysymyksistä lisääntyy.

– Kyberturvallisuussertifiointi parantaa valmiuksia tehdä tietoon perustuvia ostopäätöksiä tieto- ja viestintätekniikan tuotteista ja palveluista.

Yleisen avoimuuden tehostaminen tieto- ja viestintäteknisten tuotteiden ja palvelujen kyberturvallisuuden varmistuksessa, mikä lisää luottamusta digitaalisiin sisämarkkinoihin ja digitaalisiin innovaatioihin

– Avoimuus lisääntyy tieto- ja viestintätekniikan tuotteiden ja palvelujen kyberturvallisuuden varmistuksessa[46], kun turvallisuussertifioinnin menettelyt yksinkertaistuvat EU:n laajuisessa kehyksessä.

– Tieto- ja viestintätekniikan tuotteiden ja palvelujen turvallisuusominaisuuksien varmuustaso paranee.

– Turvallisuussertifiointi tulee laajempaan käyttöön kannusteinaan yksinkertaistetut menettelyt, alhaisemmat kustannukset ja EU:n laajuiset liiketoimintamahdollisuudet, joita markkinoiden hajanaisuus ei heikennä.

– Kilpailukyky paranee EU:n kyberturvallisuusmarkkinoilla, kun pk-yrityksille aiheutuvat kustannukset ja hallinnollinen taakka pienenevät ja markkinoille tulon esteet, joita kansallisten sertifiointijärjestelmien monilukuisuus saattaa aiheuttaa, poistuvat.

Muut tulokset

– Tavoitteista ei ennakoida koituvan merkittäviä ympäristövaikutuksia.

[46] Avoimuudella kyberturvallisuuden varmistuksessa tarkoitetaan sitä, että käyttäjät saavat kyberturvallisuusominaisuuksista riittävät tiedot, joiden avulla käyttäjät voivat objektiivisesti määrittää tietyn tieto- ja viestintäteknisen tuotteen, palvelun tai prosessin turvallisuustason.

– EU:n talousarvioon liittyviä tehokkuushyötyjä voidaan ennakoida tulokseksi EU:n toimielinten, virastojen ja elinten välisen yhteistyön ja toiminnan koordinoinnin lisäämisestä.

1.4.4. Tulos- ja vaikutusindikaattorit

Selvitys siitä, millaisin indikaattorein ehdotuksen/aloitteen toteuttamista seurataan

a)

Tavoite: Jäsenvaltioiden ja yritysten valmiuksien ja varautumiskyvyn lisääminen:

- ENISAn järjestämien koulutusten määrä
- ENISAn suoraan tarjoaman avun maantieteellinen kattavuus (maiden ja alueiden lukumäärä)
- Jäsenvaltioiden saavuttama varautumistaso, kun huomioon otetaan CSIRT-toiminnan saavuttama kypsyysaste ja kyberturvallisuuteen liittyvien sääntelyllisten toimenpiteiden valvonta
- EU:n laajuisten hyvien toimintatapojen määrä, jotka ENISA tarjoaa käyttöön kriittisiä infrastruktuureja varten
- EU:n laajuisten hyvien toimintatapojen määrä, jotka ENISA tarjoaa käyttöön pk-yrityksille
- ENISAn vuosittain julkaisema strateginen analyysi kyberuhista ja -poikkeamista uusien kehityssuuntausten tunnistamiseksi
- ENISAn säännöllinen osallistuminen Euroopan standardointiorganisaatioiden kyberturvallisuustyöryhmien työhön

Tavoite: Yhteistyön ja koordinoinnin lisääntyminen jäsenvaltioiden ja EU:n toimielinten, virastojen ja elinten välillä:

- Niiden jäsenvaltioiden lukumäärä, jotka ovat hyödyntäneet ENISAn suosituksia ja lausuntoja poliittisessa päätöksentekoprosessissaan
- Niiden EU:n toimielinten, virastojen ja elinten lukumäärä, jotka ovat hyödyntäneet ENISAn suosituksia ja lausuntoja poliittisessa päätöksentekoprosessissaan
- CSIRT-verkoston työohjelman säännöllinen täytäntöönpano ja CSIRT-verkoston tietoteknisen infrastruktuurin ja viestintäkanavien hyvä toimivuus
- Yhteistyöryhmän saataville asetetut ja sen hyödyntämät tekniset raportit
- Verkko- ja tietoturvadirektiivin johdonmukainen täytäntöönpano maiden ja hallinnonalojen rajojen yli
- ENISAn suorittamien säännöstenmukaisuuden arviointien määrä
- Eri aloilla käytössä olevien ISAC-keskusten määrä, erityisesti kriittisten infrastruktuurien osalta
- Tiedotusportaalin käyttöönotto ja jatkuva ylläpito EU:n toimielimiltä, virastoilta ja laitoksilta peräisin olevan kyberturvallisuuteen liittyvän tiedon levittämiseksi
- Säännöllinen osallistuminen EU:n tutkimus- ja innovointiohjelmien

valmisteluun

- Voimassa oleva ENISAn, EC3:n ja CERT-EU:n välinen yhteistyösopimus
- Sertifiointikehykseen sisältyvien ja sen puitteissa kehitettyjen sertifiointijärjestelmien määrä

Tavoite: EU-tason valmiuksien lisääminen jäsenvaltioiden toimien täydentämiseksi erityisesti rajat ylittävien kyberkriisien yhteydessä:

- ENISAn vuosittain julkaisema strateginen analyysi kyberuhista ja -poikkeamista uusien kehityssuuntausten tunnistamiseksi
- Koottujen tietojen julkaiseminen poikkeamista, joista raportoidaan verkko- ja tietoturvadirektiivin mukaisesti ENISAlle
- Viraston koordinoimien yleiseurooppalaisten harjoitusten ja niihin osallistuvien jäsenvaltioiden ja organisaatioiden lukumäärä
- Hätätilanteen tukea koskevien pyyntöjen määrä, jotka jäsenvaltiot esittävät ENISAlle ja jotka virasto täyttää
- ENISAn yhteistyössä CERT-EU:n kanssa suorittamien haavoittuvuuksia, artefakteja ja poikkeamia koskevien analyysien määrä
- Käytettävissä olevat EU:n laajuiset tilanneraportit, jotka perustuvat tietoon, jota jäsenvaltiot ja muut tahot antavat ENISAn käyttöön laajamittaisten rajatylittävien kyberpoikkeamien osalta

Tavoite: Kansalaisten ja yritysten tietoisuuden lisääminen kyberturvallisuuteen liittyvistä kysymyksistä:

- EU:n laajuisten ja kansallisten valistuskampanjoiden säännöllinen järjestäminen ja aiheiden säännöllinen päivittäminen kehittyvien oppimistarpeiden mukaan
- Kybertietoisuuden lisääminen EU:n kansalaisten keskuudessa
- Kyberturvallisuustietoisuuteen liittyvän tietovisan säännöllinen järjestäminen ja oikeiden vastausten prosentuaalisen osuuden kasvu ajan myötä
- Työntekijöille ja organisaatioille osoitettujen kyberturvallisuuden ja kyberhygienian hyvien käytäntöjen säännöllinen julkaiseminen

Tavoite: Yleisen avoimuuden lisääminen tieto- ja viestintäteknisten tuotteiden ja palvelujen kyberturvallisuuden varmistuksessa[47], jotta voidaan lisätä luottamusta digitaalisiin sisämarkkinoihin ja digitaalisiin innovaatioihin:

- EU:n kehyksen mukaisten järjestelmien määrä
- Tieto- ja viestintätekniikan turvallisuussertifikaatin saaminen pienemmin kustannuksin
- Tieto- ja viestintätekniikan sertifiointiin erikoistuneiden vaatimustenmukaisuuden arviointilaitosten määrä jäsenvaltioissa
- Euroopan kyberturvallisuuden sertifiointiryhmän perustaminen ja kokousten järjestäminen säännöllisesti

[47] Avoimuudella kyberturvallisuuden varmistuksessa tarkoitetaan sitä, että käyttäjät saavat kyberturvallisuusominaisuuksista riittävät tiedot, joiden avulla käyttäjät voivat objektiivisesti määrittää tietyn tieto- ja viestintäteknisen tuotteen, palvelun tai prosessin turvallisuustason.

- Saatavilla olevat ohjeet EU:n kehyksen mukaiselle sertifioinnille
- Säännöllinen analyysien julkaiseminen EU:n kyberturvallisuusmarkkinoiden tärkeimmistä suuntauksista
- Tieto- ja viestintätekniikan eurooppalaisen turvallisuussertifiointikehyksen säännöin sertifioitujen tieto- ja viestintätekniikan tuotteiden ja palvelujen määrä
- Tieto- ja viestintätekniikan tuotteiden ja palvelujen turvallisuusominaisuuksista tietoisten loppukäyttäjien määrän kasvaminen

b)

1.4.5. Tarpeet, joihin ehdotuksella/aloitteella vastataan lyhyellä tai pitkällä aikavälillä

Ottaen huomioon sääntelylliset vaatimukset ja nopeasti kehittyvä kyberturvallisuuden uhkaympäristö ENISAn toimeksiantoa on tarpeen tarkistaa ja sen tehtäviä ja toimintoja määritellä uudelleen, jotta se voisi tuloksekkaasti ja tehokkaasti tukea jäsenvaltioiden, EU:n toimielinten ja muiden sidosryhmien pyrkimyksiä turvallisen kyberavaruuden varmistamiseksi Euroopan unionissa. Toimeksiannon ehdotettu soveltamisala on määritetty lujittamalla niitä osa-alueita, joilla viraston toiminnasta on ollut selvää lisäarvoa, ja lisäämällä sellaisia uusia aloja, joilla viraston tukea tarvitaan uusien poliittisten painopisteiden ja välineiden vuoksi. Jälkimmäisiin kuuluvat erityisesti verkko- ja tietoturvadirektiivi, EU:n kyberturvallisuusstrategian tarkistus, EU:n kyberturvallisuussuunnitelma kyberkriiseissä tehtävää yhteistyötä varten sekä tieto- ja viestintäteknologian turvallisuussertifiointi. Ehdotetun uuden toimeksiannon tarkoituksena on antaa virastolle vahvempi ja keskeisempi rooli. Tarkoituksen on erityisesti, että se tukee jäsenvaltioita erityisten uhkien torjumisessa aiempaa aktiivisemmin (operatiiviset valmiudet) ja että siitä tulee jäsenvaltioiden ja komission kyberturvallisuussertifiointia tukeva omaamiskeskus.

Ehdotettavalla asetuksella luodaan samalla eurooppalainen kehys tieto- ja viestintätekniikan tuotteiden ja palvelujen kyberturvallisuussertifioinnille ja määritellään ENISAn keskeiset toiminnot ja tehtävät kyberturvallisuussertifioinnin alalla. Sertifiointikehyksessä vahvistetaan yhteiset säännöt ja menettelyt, joiden avulla voidaan luoda EU:n laajuisia kyberturvallisuuden sertifiointijärjestelmiä erityisille tieto- ja viestintätekniikan tuotteille ja palveluille tai yksittäisten kyberturvallisuusriskien osalta. Sertifiointikehyksen mukaisesti perustetuissa eurooppalaisissa kyberturvallisuuden sertifiointijärjestelmissä annetut sertifikaatit olisivat voimassa ja tunnustettuja kaikissa jäsenvaltioissa, mikä korjaisi markkinoiden nykyistä hajanaisuutta.

1.4.6. Unionin osallistumisesta saatava lisäarvo

Kyberturvallisuus on aidosti globaali kysymys, joka on luonteeltaan rajat ylittävä ja yhä monialaisempi verkkojen ja tietojärjestelmien keskinäisten riippuvuussuhteiden vuoksi. Kyberturvallisuuspoikkeamien määrä, kompleksisuus ja laajuus ja niiden vaikutukset talouteen ja yhteiskuntaan kasvavat ajan mittaan, ja niiden odotetaan lisääntyvän edelleen samaan tahtiin teknologian kehityksen kanssa, esimerkiksi esineiden internetin yleistymisen myötä. Tämä merkitsee sitä, että tarve jäsenvaltioiden, EU:n toimielinten ja yksityisten sidosryhmien yhteisille lisäponnisteluille kyberturvallisuusuhkiin vastaamiseksi ei oletettavasti vähene tulevaisuudessa.

Sen jälkeen, kun ENISA perustettiin vuonna 2004, se on pyrkinyt edistämään jäsenvaltioiden ja verkko- ja tietoturvadirektiivin sidosryhmien välistä yhteistyötä ja myös

tukemaan julkisen ja yksityisen sektorin yhteistyötä. Tähän yhteistyötä palvelevaan tukeen on sisältynyt luonteeltaan tekninen työ EU:n laajuisen kuvan muodostamiseksi uhkaympäristöstä, asiantuntijaryhmien perustaminen sekä kyberpoikkeamia ja kriisinhallintaa simuloivien yleiseurooppalaisten harjoitusten järjestäminen julkista ja yksityistä sektoria varten (erityisesti ”Cyber Europe”). Verkko- ja tietoturvadirektiivissä ENISAlle annettiin lisätehtäviä, kuten sihteeristöpalveluista huolehtiminen CSIRT-verkostolle jäsenvaltioiden välistä operatiivista yhteistyötä varten.

EU:n tason toiminnasta saatava lisäarvo, erityisesti pyrittäessä tehostamaan yhteistyötä jäsenvaltioiden välillä samoin kuin verkko- ja tietoturvallisuusyhteisöjen välillä, on tunnustettu neuvoston päätelmissä vuonna 2016[48] ja käy myös selvästi ilmi vuonna 2017 tehdystä ENISAn arvioinnista. Arviointi osoittaa, että virasto lisäarvo liittyy ensisijaisesti sen kykyyn tehostaa yhteistyötä sidosryhmien välillä. Mikään muu toimija EU:n tasolla ei tue vastaavan sidosryhmäkirjon yhteistyötä verkko- ja tietoturva-alalla.

ENISAn lisäarvo kyberturvallisuusyhteisöjen ja -sidosryhmien saattamisessa yhteen pätee myös sertifioinnin alalla. Kyberrikollisuuden ja turvallisuusuhkien lisääntyminen on synnyttänyt kansallisia aloitteita, joissa asetetaan korkean tason kyberturvallisuus- ja sertifiointivaatimuksia perinteisessä infrastruktuurissa käytettäville tieto- ja viestintätekniikan komponenteille. Vaikka nämä aloitteet ovat tärkeitä, ne uhkaavat luoda hajanaisuutta ja yhteentoimivuuden esteitä sisämarkkinoille. Tieto- ja viestintätekniikan myyjä voi joutua läpikäymään useita sertifiointimenettelyjä, jotta se voisi myydä tuotteitaan eri jäsenvaltioissa. Nykyisistä sertifiointijärjestelmistä johtuvaan tehottomuuteen ja rajalliseen kattavuuteen tuskin voidaan puuttua ilman EU:n toimia. Jos mitään ei tehdä, markkinoiden hajanaisuus hyvin todennäköisesti kasvaa lyhyellä tai keskipitkällä aikavälillä (5–10 vuoden kuluessa), kun käyttöön tulee uusia sertifiointijärjestelmiä. Koordinoinnin ja yhteentoimivuuden puute tällaisten järjestelmien välillä on tekijä, joka vähentää digitaalisten sisämarkkinoiden tarjoamia mahdollisuuksia. Tämä osoittaa lisäarvon, joka saataisiin perustamalla tieto- ja viestintätekniikan tuotteille ja palveluille eurooppalainen kyberturvallisuuden sertifiointikehys. Tällainen kehys tarjoaisi oikeat edellytykset puuttua tehokkaasti ongelmaan, joka aiheutuu eri jäsenvaltioissa käytössä olevien erillisten sertifiointimenettelyjen rinnakkaisuudesta. Se myös vähentäisi sertifioinnin kustannuksia, mikä lisäisi EU:n sertifioinnin yleistä houkuttelevuutta kaupan ja kilpailun kannalta.

1.4.7. Vastaavista toimista saadut kokemukset

Komissio on ENISAn oikeusperustan mukaisesti tehnyt virastosta arvioinnin, johon sisältyi riippumaton tutkimus sekä myös julkinen kuuleminen. Arvioinnissa tultiin siihen tulokseen, että ENISAn tavoitteet ovat edelleen ajankohtaisia. Kehittyvän teknologian ja muuttuvien uhkien tilanteessa, jossa vallitsee merkittävä tarve lisätä verkko- ja tietoturvallisuutta EU:ssa, käyttöön tarvitaan verkko- ja tietoturvakysymysten kehitykseen kohdistuvaa teknistä asiantuntemusta. Jäsenvaltioissa on tarpeen kehittää valmiuksia ymmärtää ja torjua uhkia, ja sidosryhmien on tarpeen toimia yhteistyössä eri temaattisten alojen ja instituutioiden välisesti.

Virasto on onnistuneesti parantanut verkko- ja tietoturvallisuutta Euroopassa tukemalla valmiuksien kehittämistä 28 jäsenvaltiossa, tehostamalla jäsenvaltioiden ja verkko- ja

[48] Neuvoston päätelmät Euroopan kyberresilienssijärjestelmän vahvistamisesta sekä kilpailukykyisen ja innovatiivisen kyberturvallisuustoimialan tukemisesta, 15.11.2016.

tietoturvan sidosryhmien välistä yhteistyötä, tarjoamalla käyttöön asiantuntemusta sekä tukemalla yhteisöjen ja politiikan kehittämistä.

ENISA on kyennyt saamaan aikaan vaikutuksen, ainakin jossain määrin, verkko- ja tietoturvan laajalla toimintasaralla, mutta se ei ole täysin onnistunut kehittämään vahvaa brändiä ja riittävää näkyvyyttä alan ykkösosaamiskeskuksena Euroopassa. Tämä selittyy ENISAn laajalla toimeksiannolla, jonka tueksi sille ei ole annettu riittäviä resursseja vastaavassa suhteessa. Lisäksi ENISA on ainoa EU:n virasto, jonka toimikausi on määräaikainen, mikä rajoittaa sen mahdollisuuksia kehittää pitkän aikavälin visiota ja tukea sidosryhmiään kestävällä tavalla. Tämä on myös ristiriidassa verkko- ja tietoturvadirektiivin säännösten kanssa, joissa ENISAlle annetaan tehtäviä ilman päättymispäivää.

Tietotekniikan tuotteiden ja palvelujen kyberturvallisuussertifioinnille ei tällä hetkellä ole olemassa eurooppalaista toimintakehystä. Kyberrikollisuuden ja turvallisuusuhkien lisääntyminen on kuitenkin synnyttänyt kansallisia aloitteita, jotka uhkaavat johtaa hajanaisuuteen sisämarkkinoilla.

1.4.8. Yhteensopivuus muiden kyseeseen tulevien välineiden kanssa ja mahdolliset synergiaedut

Aloite on hyvin linjassa nykyisten politiikkojen kanssa, erityisesti sisämarkkinoiden alalla. Sen suunnittelussa on noudatettu kyberturvallisuuteen omaksuttua yleistä, digitaalisten sisämarkkinoiden strategian uudelleentarkastelussa määriteltyä lähestymistapaa, jotta voidaan täydentää kattavaa toimenpidekokonaisuutta, johon sisältyvät EU:n kyberturvallisuusstrategian tarkistus, kyberturvallisuussuunnitelma kyberkriiseissä tehtävää yhteistyötä varten sekä aloitteet kyberrikollisuuden torjumiseksi. Tällä tavoin voidaan varmistaa yhdenmukaisuus voimassa olevan kyberturvallisuuslainsäädännön ja erityisesti verkko- ja tietoturvadirektiivin säännösten kanssa kyberresilienssin edelleenkehittämiseksi EU:ssa parantamalla valmiuksia, yhteistyötä, riskinhallintaa ja kybertietoisuutta.

Ehdotetuilla sertifiointitoimenpiteillä voitaisiin ehkäistä hajanaisuutta, jota jo käytössä olevat ja uudet kansalliset sertifiointijärjestelmät voivat aiheuttaa, ja näin edistää digitaalisten sisämarkkinoiden kehitystä. Tämä aloite myös tukee ja täydentää verkko- ja tietoturvadirektiivin täytäntöönpanoa tarjoamalla yrityksille, joihin direktiiviä sovelletaan, välineen osoittaa, että ne noudattavat direktiivin vaatimuksia koko unionissa.

Eurooppalainen tieto- ja viestintätekniikan kyberturvallisuuden sertifiointikehys ei ehdotetussa muodossaan rajoita yleisen tietosuoja-asetuksen[49] soveltamista, ei myöskään sertifiointia koskevien säännösten[50] soveltamista tietoturvaan henkilötietojen käsittelyssä. Tulevassa eurooppalaisessa kehyksessä ehdotettavissa järjestelmissä tulisi nojautua mahdollisuuksien mukaan kansainvälisiin standardeihin, jotta vältetään kaupan esteet ja varmistetaan johdonmukaisuus kansainvälisten aloitteiden kanssa.

[49] Asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus).

[50] Esim. artiklat 42 (”Sertifiointi”) ja 43 (”Sertifiointielimet”) sekä artiklat 57, 58 ja 70, jotka koskevat riippumattomien valvontaviranomaisten tehtäviä ja valtuuksia sekä Euroopan tietosuojaneuvoston tehtäviä.

1.5. Toiminnan ja sen rahoitusvaikutusten kesto

☐ Ehdotuksen/aloitteen mukaisen toiminnan **kesto on rajattu**.

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

– ☐ Rahoitusvaikutukset alkavat vuonna VVVV ja päättyvät vuonna VVVV.

☒ Ehdotuksen/aloitteen mukaisen toiminnan **kestoa ei ole rajattu**.

– Käynnistysvaihe alkaa vuonna 2019 ja päättyy vuonna 2020,

– minkä jälkeen toteutus täydessä laajuudessa.

1.6. Hallinnointitapa (Hallinnointitavat)[51]

☒ **Suora hallinnointi,** jonka komissio toteuttaa käyttämällä (III osasto – Sertifiointi)

– ☐ toimeenpanovirastoja

☐ **Hallinnointi yhteistyössä** jäsenvaltioiden kanssa

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

☐ kansainvälisille järjestöille ja niiden erityisjärjestöille (tarkennettava)

☐ Euroopan investointipankille ja Euroopan investointirahastolle

☒ 208 ja 209 artiklassa tarkoitetuille elimille (II osasto – ENISA)

☐ 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

Asetuksen – II osastossa säädetään Euroopan unionin verkko- ja tietoturvaviraston (ENISA) toimeksiannon tarkistamisesta ja annetaan sillä tärkeä rooli sertifioinnissa ja – III osastossa vahvistetaan kehys eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien luomiselle tieto- ja viestintätekniikan tuotteita ja palveluja varten, missä ENISAlla on tärkeä rooli.

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

2. HALLINNOINTI

2.1. Seuranta- ja raportointisäännöt

Ilmoitetaan sovellettavat aikavälit ja edellytykset.

Seuranta alkaa heti sen jälkeen, kun säädös on hyväksytty, ja siinä keskitytään sen soveltamiseen. Komissio järjestää kokouksia ENISAn, jäsenvaltioiden edustajien (esim. asiantuntijaryhmän) ja asiaankuuluvien sidosryhmien kanssa helpottaakseen erityisesti sertifiointia koskevien sääntöjen täytäntöönpanoa muun muassa johtokunnan kokoonpanoon liittyen.

Ensimmäinen arviointi on määrä tehdä 5 vuoden kuluttua säädöksen voimaantulosta, jos tietoja on käytettävissä riittävästi. Säädökseen sisältyy nimenomainen arviointi- ja uudelleentarkastelulauseke [XXX artikla], jonka nojalla komissio suorittaa riippumattoman arvioinnin. Komissio laatii arvioinnista kertomuksen Euroopan parlamentille ja neuvostolle ja liittää siihen tarvittaessa ehdotuksen asetuksen tarkistamiseksi. Tarkoituksena on määrittää asetuksen vaikutus ja sen tuoma lisäarvo. Sen jälkeen arviointi on määrä suorittaa viiden vuoden välein. Arviointiin sovelletaan komission paremman säädöskäytännön menetelmiä. Nämä arvioinnit perustuvat kohdennettuihin asiantuntijakeskusteluihin, tutkimuksiin ja laajaan sidosryhmien kuulemiseen.

ENISAn pääjohtajan on määrä esittää johtokunnalle ENISAn toimintaa koskeva jälkiarviointi kahden vuoden välein. Viraston olisi myös laadittava toimintasuunnitelma jälkiarviointien päätelmistä johtuville jatkotoimille ja raportoitava edistymisestä komissiolle kahden vuoden välein. Johtokunnan olisi valvottava sitä, että päätelmien johdosta toteutetaan asianmukaiset jatkotoimet.

Euroopan oikeusasiamies voi tutkia viraston toiminnassa ilmenneeksi väitetyt epäkohdat perussopimuksen 228 artiklan määräysten mukaisesti.

Suunnitellun seurannan tärkeimmät tietolähteet ovat ENISA, Euroopan kyberturvallisuuden sertifiointiryhmä, yhteistyöryhmä, CSIRT-verkosto ja jäsenvaltioiden viranomaiset. ENISAn raporteista (ml. vuotuiset toimintakertomukset), Euroopan kyberturvallisuuden sertifiointiryhmältä, yhteistyöryhmältä ja CSIRT-verkostolta saatavien tietojen ohella käytetään tarpeen mukaan erityisiä tiedonkeruuvälineitä (esim. kansallisille viranomaisille tehtyjä kyselyjä, Eurobarometri-tutkimuksia sekä kyberturvallisuuskuukauden tiedotuskampanjasta ja yleiseurooppalaisista harjoituksista laadittuja raportteja).

2.2. Hallinnointi- ja valvontajärjestelmä

2.2.1. Todetut riskit

Todetut riskit ovat vähäiset. Unionin virasto on jo toiminnassa, ja sen toimeksianto määritellään uudelleen lujittamalla niitä osa-alueita, joilla viraston toiminnasta on ollut selvää lisäarvoa, ja lisäämällä sellaisia uusia aloja, joilla viraston tukea tarvitaan uusien poliittisten painopisteiden ja välineiden vuoksi. Jälkimmäisiin kuuluvat erityisesti verkko- ja tietoturvadirektiivi, EU:n kyberturvallisuusstrategian tarkistus, tuleva EU:n kyberturvallisuussuunnitelma kyberkriiseissä tehtävää yhteistyötä varten sekä tieto- ja viestintäteknologian turvallisuussertifiointi.

Ehdotus näin ollen linjaa viraston tehtäviä ja tuo tehokkuushyötyjä. Operatiivisten toimivaltuuksien ja tehtävien lisäämiseen ei liity todellista riskiä, sillä niillä täydennettäisiin jäsenvaltioiden toimintaa ja tuettaisiin niitä pyynnöstä ja rajoitettujen ja ennalta määriteltyjen palvelujen osalta.

Virastolle ehdotetulla mallilla, joka vastaisi erillisvirastoja koskevaa yhteistä lähestymistapaa, varmistettaisiin riittävä valvonta sen varmistamiseksi, että ENISA työskentelee kohti tavoitteitaan. Ehdotettuihin muutoksiin liittyvät operatiiviset ja rahoitukselliset riskit vaikuttavat vähäisiltä.

Samalla on tarpeen varmistaa riittävät taloudelliset resurssit, jotta ENISA voisi hoitaa uudessa toimeksiannossaan saamansa tehtävät muun muassa sertifioinnin alalla.

2.2.2. Valvontamenetelmä(t)

Viraston tilit toimitetaan tilintarkastustuomioistuimen tarkastettaviksi, ja niihin sovelletaan vastuuvapausmenettelyä. Tarkastuksiin kuuluvat myös paikalla suoritettavat tarkastukset.

Viraston toiminta kuuluu oikeusasiamiehen valvonnan alaisuuteen perustamissopimuksen 228 artiklan määräysten mukaisesti.

Ks. myös kohdat 2.1 ja 2.2.1 edellä.

2.3. Toimenpiteet petosten ja sääntöjenvastaisuuksien ehkäisemiseksi

Ilmoitetaan käytössä olevat ja suunnitellut torjunta- ja suojatoimenpiteet

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 11 päivänä syyskuuta 2013 annetun Euroopan parlamentin ja neuvoston asetuksen (EU, Euratom) N:o 883/2013 säännöksiä.

– Virasto liittyy kuuden kuukauden kuluessa tämän asetuksen voimaantulosta 25 päivänä toukokuuta 1999 tehtyyn Euroopan parlamentin, Euroopan unionin neuvoston ja Euroopan yhteisöjen komission tekemään toimielinten väliseen sopimukseen Euroopan petostentorjuntaviraston (OLAF) sisäisistä tutkimuksista ja vahvistaa viipymättä asianmukaiset määräykset, 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	Määrä-rahalaji	Rahoitusosuudet			
		JM/EI-JM[52]	EFTA-mailta[53]	ehdokasmailta[54]	kolmansilta mailta	varainhoitoasetuksen 21 artiklan 2 kohdan b alakohdassa tarkoitetut rahoitusosuudet
1a Kasvua ja työllisyyttä tukeva kilpailukyky	09.0203 ENISA ja tieto- ja viestintätekniikan turvallisuussertifiointi	Jaks.	KYLLÄ	EI	EI	EI
5 Hallintomenot]	09.0101 Menot viestintäverkkojen, sisältöjen ja teknologian toimintalohkon palveluksessa olevasta henkilöstöstä 09.0102 Menot viestintäverkkojen, sisältöjen ja teknologian toimintalohkon palveluksessa olevasta ulkopuolisesta henkilöstöstä	EI-JM	EI	EI	EI	EI

52 JM = jaksotetut määrärahat; EI-JM = jaksottamattomat määrärahat.

53 EFTA: Euroopan vapaakauppaliitto.

54 Ehdokasmaat ja soveltuvin osin Länsi-Balkanin mahdolliset ehdokasmaat.

	09.010211 Muut hallintomenot					

3.2. Arvioidut vaikutukset menoihin

3.2.1. Yhteenveto arvioiduista vaikutuksista menoihin

milj. euroa (kolmen desimaalin tarkkuudella)

Monivuotisen rahoituskehyksen otsake	1a	Kasvua ja työllisyyttä tukeva kilpailukyky.

ENISA			**Vertailutaso 2017 (31.12.2016)**		**2019** ***(1.7.2019 alkaen)***	**2020**	**2021**	**2022**	**YHTEENSÄ**
Osasto 1: Henkilöstömenot *(mukaan lukien henkilöstön rekrytointiin, koulutukseen, sosiaali- ja terveyspalveluihin ja ulkoisiin palveluihin liittyvät kustannukset)*	Sitoumukset	(1)	6,387		9,899	12,082	13,349	13,894	**49,224**
	Maksut	(2)	6,387		9,899	12,082	13,349	13,894	**49,224**
Osasto 2: Infrastruktuuri- ja toimintamenot	Sitoumukset	(1a)	1,770		1,957	2,232	2,461	2,565	**9,215**
	Maksut	(2 a)	1,770		1,957	2,232	2,461	2,565	**9,215**
Osasto 3: Toimintamenot	Sitoumukset	(3a)	3,086		4,694	6,332	6,438	6,564	**24,028**
	Maksut	(3b)	3,086		4,694	6,332	6,438	6,564	**24,028**
ENISAn määrärahat YHTEENSÄ	Sitoumukset	= 1+1a +3a	**11,244**		16,550	20,646	22,248	23,023	**82,467**
	Maksut	= 2+2a +3b	**11,244**		**16,550**	**20,646**	**22,248**	**23,023**	**82,467**

Monivuotisen rahoituskehyksen otsake	**5**	”Hallintomenot”

milj. euroa (kolmen desimaalin tarkkuudella)

		2019 *(1.7.2019 alkaen)*	**2020**	**2021**	**2022**	**YHTEENSÄ**
PO: CNECT						
•Henkilöresurssit		0,216	0,846	0,846	0,846	**2,754**
•Muut hallintomenot		0,102	0,235	0,238	0,242	**0,817**
PO CNECT **YHTEENSÄ**	Määrärahat	0,318	1,081	1,084	1,088	**3,571**

Henkilöstökulut laskettiin suunnitellusta palvelukseenotosta (ENISAn palveluksessa 1.7.2019 alkaen).

Vuoden 2020 jälkeiset resurssinäkymät ovat ohjeellisia, eivätkä ne rajoita komission ehdotuksia vuoden 2020 jälkeistä monivuotista rahoituskehystä varten.

Monivuotisen rahoituskehyksen **OTSAKKEESEEN 5 kuuluvat määrärahat YHTEENSÄ**	(Sitoumukset yhteensä = maksut yhteensä)	0,318	1,081	1,084	1,088	**3,571**

milj. euroa (kolmen desimaalin tarkkuudella)

		2019	**2020**	**2021**	**2022**	**YHTEENSÄ**
Monivuotisen rahoituskehyksen	Sitoumukset	16,868	21,727	23,332	24,11	**86,038**

OTSAKKEISIIN 1–5 kuuluvat määrärahat YHTEENSÄ	Maksut	16,868	21,727	23,332	24,11	**86,038**

3.2.2. Arvioidut vaikutukset viraston määrärahoihin

– ☐ Ehdotus/aloite ei edellytä toimintamäärärahoja.

– ☒ Ehdotus/aloite edellyttää toimintamäärärahoja seuraavasti:

Maksusitoumusmäärärahat, milj. euroa (kolmen desimaalin tarkkuudella)

Tavoitteet ja tuotokset[55] ⇩	**2019**	**2020**	**2021**	**2022**	**YHTEENSÄ**
Jäsenvaltioiden ja yritysten valmiuksien ja varautumiskyvyn lisääminen	1,408	1,900	1,931	1,969	7,208
Yhteistyön ja koordinoinnin lisääminen jäsenvaltioiden ja EU:n toimielinten, virastojen ja elinten välillä	0,939	1,266	1,288	1,313	4,806
EU:n tason valmiuksien lisääminen jäsenvaltioiden toimien täydentämiseksi erityisesti rajat ylittävien kyberkriisien yhteydessä.	0,704	0,950	0,965	0,985	3,604
Kansalaisten ja yritysten tietoisuuden lisääminen kyberturvallisuuteen liittyvistä kysymyksistä.	0,704	0,950	0,965	0,985	3,604
Yleisen avoimuuden lisääminen tieto- ja viestintäteknisten tuotteiden ja palvelujen kyberturvallisuuden varmistuksessa, jotta voidaan lisätä luottamusta digitaalisiin sisämarkkinoihin ja digitaalisiin innovaatioihin.	0,939	1,266	1,288	1,313	4,806
KUSTANNUKSET YHTEENSÄ	4,694	6,332	6,437	6,565	24,028

[55] Tässä taulukossa esitetään ainoastaan osastoa 3 koskevat toimintamenot

3.2.3. Arvioidut vaikutukset viraston henkilöresursseihin

3.2.3.1. Yhteenveto

– ☐ Ehdotus/aloite ei edellytä hallintomäärärahoja.

– ☒ Ehdotus/aloite edellyttää hallintomäärärahoja seuraavasti:

milj. euroa (kolmen desimaalin tarkkuudella)

	Vuoden 2019 kolmas/neljäs neljännes	**2020**	**2021**	**2022**
Väliaikaiset toimihenkilöt (AD-ura-alue)	4,242	5,695	6,381	6,709
Väliaikaiset toimihenkilöt (AST-ura-alue)	1,601	1,998	2,217	2,217
Sopimussuhteiset toimihenkilöt	2,041	2,041	2,041	2,041
Kansalliset asiantuntijat	0,306	0,447	0,656	0,796
YHTEENSÄ	**8,190**	**10,181**	**11,295**	**11,763**

Henkilöstökulut laskettiin suunnitellusta palvelukseenotosta (ENISAn nykyisen henkilöstön osalta täysimääräisesti 1.1.2019 alkaen). Uuden henkilöstön palvelukseenotto laskettiin asteittain 1.7.2019 alkaen ja täysimääräisesti vuodesta 2022. Vuoden 2020 jälkeiset resurssinäkymät ovat ohjeellisia, eivätkä ne rajoita komission ehdotuksia vuoden 2020 jälkeistä monivuotista rahoituskehystä varten.

Arvioidut vaikutukset henkilöstöön (kokoaikaisten työntekijöiden lisäys) – ENISAn henkilöstötaulukko

Tehtäväryhmä ja palkkaluokka	2017 **Nykyinen ENISA**	Vuoden 2019 kolmas/neljäs neljännes	2020	2021	2022
AD16					
AD15	1				
AD14					
AD13					
AD12	3	3			
AD11					
AD10	5				
AD9	10	2			
AD8	15	4	2		1
AD7			3	3	2
AD6			3	3	
AD5					

AD yhteensä	34	9	8	6	3
AST11 AST10 AST9 AST8 AST7 AST6 AST5 AST4 AST3 AST2 AST1	 2 5 5 2	 1 2	 1 1	 1	
AST yhteensä	14	3	2	1	
AST/SC 6 AST/SC 5 AST/SC 4 AST/SC 3 AST/SC 2 AST/SC 1					
AST/SC yhteensä					
KAIKKI YHTEENSÄ	48	12	10	7	3

Uuden AD/AST-henkilöstön tehtävät ehdotuksen/aloitteen tavoitteiden saavuttamiseksi 1.4.2 kohdan mukaisesti:

Tehtävät	AD	AST	KANSALLISET ASIANTUNTIJAT	Yhteensä
Politiikan ja valmiuksien kehittäminen	8	1		9
Operatiivinen yhteistyö	8	1	7	16
Sertifiointi (markkinoihin liittyvät tehtävät)	9	3	2	14
Tietämys, tiedotus ja tietoisuuden lisääminen	1	1		2
YHTEENSÄ	26	6	9	41

Kuvaus henkilöstön tehtävistä:

Tehtävät	**Lisäresurssien tarve**
EU:n politiikan kehittäminen ja täytäntöönpano sekä valmiuksien kehittäminen	Tehtäviin kuuluu yhteistyöryhmän avustaminen, verkko- ja tietoturvadirektiivin johdonmukaisen täytäntöönpanon tukeminen yli rajojen, säännöllinen raportointi EU:n oikeudellisen kehyksen täytäntöönpanon tilasta, alakohtaisiin kyberturvallisuusaloitteisiin liittyvä neuvonta ja

	koordinointi muun muassa energia-alalla, liikenteessä (esim. ilmailu, maantie- ja meriliikenne ja verkkoon liitetyt ajoneuvot), terveydenhuollossa ja rahoitusalalla sekä tietojen jakamisen ja analysoinnin alakohtaisten keskusten (ISAC) perustamisen tukeminen eri aloilla.
Operatiivinen yhteistyö ja kriisinhallinta:	**Tehtäviin kuuluisivat seuraavat:** Toimiminen CSIRT-verkoston sihteeristönä varmistaen muun muassa CSIRT-verkoston tietoteknisen infrastruktuurin ja viestintäkanavien toimivuus. Jäsennellyn yhteistyön varmistaminen CERT-EU:n, EC3:n ja muiden asiaankuuluvien EU:n elinten kanssa. **Cyber Europe -harjoitusten**[56] järjestäminen ja laajentaminen muuttamalla ne kahden vuoden välein pidettävistä jokavuotisiksi ja varmistamalla, että harjoitukset kattavat kyberpoikkeaman alusta loppuun. **Tekninen apu** – Tehtäviin kuuluisi jäsennelty yhteistyö CERT-EU:n kanssa teknisen avun antamiseksi merkittävien kyberpoikkeamien tapauksessa ja poikkeamien analyysin tukemiseksi. Tähän sisältyisi jäsenvaltioiden avustaminen poikkeamien käsittelyssä ja haavoittuvuuksien, artefaktien ja poikkeamien analyysissa. Tehtävänä olisi myös helpottaa yksittäisten jäsenvaltioiden välistä yhteistyötä hätätilanteisiin vastaamisessa analysoimalla ja kokoamalla yhteen kansallisia tilannekatsauksia jäsenvaltioiden ja muiden tahojen viraston käyttöön antamien tietojen pohjalta. **Suunnitelma koordinoidusta reagoinnista laajamittaisiin rajat ylittäviin kyberturvallisuuspoikkeamiin** – Virasto edistää yhteistyöhön perustuvan vastauksen kehittämistä unionin ja jäsenvaltioiden tasolla laajamittaisiin rajatylittäviin kyberturvallisuuspoikkeamiin tai -kriiseihin huolehtimalla eri tehtävistä, jotka vaihtelevat tilannetietoisuuden kehittämisestä unionin tasolla yhteistyösuunnitelmien testaamiseen poikkeamien varalta.

[56] Cyber Europe on toistaiseksi tärkein ja kattavin EU:n kyberturvallisuusharjoitus, johon osallistuu yli 700 kyberturvallisuuden ammattilaista kaikista 28 jäsenvaltiosta. Se järjestetään joka toinen vuosi. ENISAn arviointi ja vuonna 2013 hyväksytty EU:n kyberturvallisuusstrategia viittaavat siihen, että kyberuhkien nopeasti muuttuvan luonteen vuoksi monet sidosryhmät kannattavat Cyber Europe -harjoitusten muuttamista vuotuiseksi tapahtumaksi. Tämä ei kuitenkaan ole tällä hetkellä mahdollista viraston rajallisten resurssien vuoksi.

	Poikkeamista jälkikäteen tehtävät tekniset tutkimukset – Virasto suorittaa tai tukee yhteistyössä CSIRT-verkoston kanssa teknisiä tutkimuksia, jotka poikkeamista tehdään jälkikäteen. Tarkoituksena on antaa suosituksia ja lujittaa valmiuksia julkisten raporttien muodossa, jotta voidaan paremmin ehkäistä uusia turvapoikkeamia.
Markkinoihin liittyvät tehtävät (standardointi ja sertifiointi):	Tehtäviin kuuluu tukea aktiivisesti sertifiointikehyksen puitteissa tehtävää työtä muun muassa antamalla teknistä asiantuntemusta ehdolla olevien eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien valmistelemiseksi. Tehtävänä on myös tukea unionin politiikan kehittämistä ja täytäntöönpanoa standardointiin, sertifiointiin ja markkinoiden seurantakeskukseen liittyen. Tätä varten viraston on määrä helpottaa tieto- ja viestintäteknisten tuotteiden, verkkojen ja palvelujen riskinhallintaan kohdistuvien standardien käyttöönottoa sekä neuvoa keskeisten palvelujen tarjoajia ja digitaalisen palvelun tarjoajia teknisistä turvallisuusvaatimuksista. Tehtäviin kuuluu myös analyysien laatiminen kyberturvallisuusmarkkinoiden tärkeimmistä suuntauksista.
Tietämys, tiedotus ja tietoisuuden lisääminen:	Jotta kyberturvallisuusriskeistä ja mahdollisista suojakeinoista saataisiin tietoa helpommin ja paremmin jäsennellyssä muodossa, ehdotuksessa annetaan virastolle uusi tehtävä kehittää unionin ”tietokeskus” ja ylläpitää sitä. Tätä varten se kokoaisi, järjestäisi ja saattaisi yleisön saataville erityisen portaalin kautta EU:n toimielimiltä, virastoilta ja elimiltä peräisin olevaa tietoa verkko- ja tietojärjestelmien turvallisuudesta, erityisesti kyberturvallisuudesta. Tehtäviin kuuluisi myös ENISAn toiminnan tukeminen tietoisuuden lisäämisessä, jotta virasto voisi laajentaa tätä toimintaa.

3.2.3.2. Henkilöresurssien arvioitu tarve vastuullisessa pääosastossa

– ☐ Ehdotus/aloite ei edellytä henkilöresursseja.

– ☒ Ehdotus/aloite edellyttää henkilöresursseja seuraavasti:

arvio kokonaislukuina (tai enintään yhden desimaalin tarkkuudella)

		Lisähenkilöstö			
	Lähtötaso 2017	Vuoden 2019 kolmas/neljäs neljännes	2020	2021	2020
• **Henkilöstötaulukkoon sisältyvät virat/toimet (virkamiehet ja väliaikainen henkilöstö)**					
09 01 01 01 (päätoimipaikka ja komission edustustot EU:ssa)	1	2	3		
• **Ulkopuolinen henkilöstö (kokoaikaiseksi muutettuna)**[57]					
09 01 02 01 (kokonaismäärärahoista katettavat sopimussuhteiset toimihenkilöt, kansalliset asiantuntijat ja vuokrahenkilöstö)	1	2			
YHTEENSÄ		**4**	**3**		

Kuvaus henkilöstön tehtävistä:

Virkamiehet ja väliaikaiset toimihenkilöt	Edustaa komissiota viraston johtokunnassa. Laatia komission lausunto ENISAn yhtenäisestä ohjelma-asiakirjasta ja valvoa sen täytäntöönpanoa. Valvoa viraston talousarvion valmistelua ja seurata talousarvion toteuttamista. Avustaa virastoa sen toiminnan kehittämisessä EU:n toimintalinjojen mukaisesti, muun muassa osallistumalla asiaankuuluviin kokouksiin. Valvoa eurooppalaisen kyberturvallisuuden sertifiointikehyksen täytäntöönpanoa tieto- ja viestintätekniikan tuotteita ja palveluja varten. Pitää yhteyttä jäsenvaltioihin ja muihin asiaankuuluviin sidosryhmiin sertifiointitoimintaa koskevissa kysymyksissä. Tehdä yhteistyötä ENISAn kanssa ehdolla oleviin sertifiointijärjestelmiin liittyen. Valmistella ehdolla

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

	olevat eurooppalaiset kyberturvallisuuden sertifiointijärjestelmät.
Ulkopuolinen henkilöstö	Kuten edellä

3.2.4. Yhteensopivuus nykyisen monivuotisen rahoituskehyksen kanssa

– ☐ Ehdotus/aloite on nykyisen monivuotisen rahoituskehyksen mukainen.

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

Ehdotus edellyttää rahoitussuunnitelman muuttamista momentissa 09 02 03. Syynä on ENISAn toimeksiannon tarkistaminen ja sille annettavat uudet tehtävät, jotka liittyvät muun muassa verkko- ja tietoturvadirektiivin täytäntöönpanoon ja eurooppalaiseen kyberturvallisuuden sertifiointikehykseen. Kyseeseen tulevat määrät:

Vuosi	Suunniteltu	Esitys
2019	10,739	16,550
2020	10,954	20,646
2021	Ei sovelleta	22,248*
2022	Ei sovelleta	23,023*

* Tämä on arvio. Vuoden 2020 jälkeistä EU-rahoitusta pohditaan koko komission laajuisessa keskustelussa kaikista vuoden 2020 jälkeistä aikaa koskevista ehdotuksista. Tämä tarkoittaa, että kun komissio on esittänyt ehdotuksensa seuraavaksi monivuotiseksi rahoituskehykseksi, komissio esittää tarkistetun rahoitusselvityksen ottaen huomioon vaikutusten arvioinnin päätelmät[58].

– ☐ Ehdotus/aloite edellyttää joustovälineen varojen käyttöön ottamista tai monivuotisen rahoituskehyksen tarkistamista[59].

3.2.5. Ulkopuolisten tahojen rahoitusosuudet

– ☐ Ehdotuksen/aloitteen rahoittamiseen ei osallistu ulkopuolisia tahoja.

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

[58] Linkki vaikutusten arvioinnin sivustolle

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

	Vuosi **2019**	Vuosi **2020**	Vuosi **2021**	Vuosi **2022**
EFTA	p.m[60].	p.m.	p.m.	p.m.

3.3. Arvioidut vaikutukset tuloihin

– ☒ Ehdotuksella/aloitteella ei ole vaikutuksia tuloihin.

– ☐ Ehdotuksella/aloitteella on vaikutuksia tuloihin seuraavasti:

  – ☐ vaikutukset omiin varoihin

  – ☐ vaikutukset sekalaisiin tuloihin

[60] Tarkka määrä seuraaviksi vuosiksi on tiedossa, kun EFTA-maiden suhdeluku vahvistetaan kyseiseksi vuodeksi.