EUROOPAN KOMISSIO

Bryssel 30.9.2010
KOM(2010) 521 lopullinen

2010/0275 (COD)

Ehdotus

EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS

Euroopan verkko- ja tietoturvavirastosta (ENISA)

{SEC(2010) 1126}
{SEC(2010) 1127}

PERUSTELUT

1. EHDOTUKSEN TAUSTA

1.1. Poliittinen tausta

Euroopan verkko- ja tietoturvavirasto ENISA perustettiin maaliskuussa 2004 asetuksella (EY) N:o 460/2004[1] aluksi viiden vuoden kaudeksi tärkeimpänä tavoitteena *”edistää korkeatasoista verkko- ja tietoturvaa [EU:ssa], (…) kehittää Euroopan unionin kansalaisia, kuluttajia, yrityksiä ja julkisen sektorin järjestöjä hyödyttävä verkko- ja tietoturvakulttuuri, ja siten edistää sisämarkkinoiden moitteetonta toimintaa*”. ENISAn toimikautta jatkettiin asetuksella (EY) N:o 1007/2008[2] maaliskuuhun 2012.

ENISAn toimikauden jatkaminen vuonna 2008 käynnisti keskustelun Euroopan verkko- ja tietoturvatoiminnan yleisestä suunnasta. Komissio osallistui keskusteluun käynnistämällä julkisen kuulemisen alan vahvemman EU-politiikan mahdollisista tavoitteista. Kuuleminen kesti marraskuusta 2008 tammikuuhun 2009 ja siinä saatiin lähes 600 lausuntoa[3].

Komissio antoi 30. maaliskuuta 2009 tiedonannon[4] kriittisten tietoinfrastruktuurien suojaamisesta. Tiedonannossa keskitytään Euroopan suojaamiseen tietoverkkohyökkäyksiltä ja -häiriöiltä parantamalla valmiutta, tietoturvaa ja verkkojen häiriösietoisuutta. Tiedonantoon sisältyvässä toimintasuunnitelmassa ENISAlle annetaan rooli, joka liittyy lähinnä jäsenvaltioiden tukemiseen. Toimintasuunnitelma sai laajan hyväksynnän kriittisten tietoinfrastruktuurien suojaamista käsitelleessä ministerikonferenssissa Tallinnassa 27.-28. huhtikuuta 2009[5]. EU:n puheenjohtajamaan päätelmissä korostetaan ENISAn operatiivisen vipuvaikutuksen merkitystä: päätelmissä todetaan, että ENISA "*toimii tärkeänä välineenä lisättäessä tämän alan EU-yhteistyötä*" ja viitataan tarpeeseen kehittää ja uudelleenmuotoilla viraston toimeksiantoa, jotta voidaan "*paremmin keskittyä EU:n painopisteisiin ja tarpeisiin*; *saavuttaa joustavammat reagointivalmiudet; kehittää taitoja ja osaamista; sekä lisätä viraston toimintatehokkuutta ja kokonaisvaikuttavuutta*" niin, että virastosta voidaan luoda "*pysyvä resurssi jokaiselle jäsenvaltiolle ja Euroopan unionille kokonaisuudessaan*".

Asiasta keskusteltiin 11. kesäkuuta 2009 viestintäministerineuvostossa, jossa jäsenvaltiot kannattivat verkko- ja tietoturvan tärkeyden ja alan esiin nousevien haasteiden vuoksi ENISAn toimeksiannon laajentamista ja sen resurssien lisäämistä. Tämän jälkeen asiasta tehtiin lopulliset päätelmät Ruotsin puheenjohtajakaudella. Yhteistoiminnallisesta eurooppalaisesta lähestymistavasta verkko- ja tietoturvallisuuden alalla 18 päivänä joulukuuta

---

1 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).

2 Euroopan parlamentin ja neuvoston asetus (EY) N:o 1007/2008, annettu 24 päivänä syyskuuta 2008, Euroopan verkko- ja tietoturvaviraston perustamisesta 10 päivänä maaliskuuta 2004 annetun Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 460/2004 muuttamisesta sen toimikauden keston osalta (EUVL L 293, 31.10.2008, s. 1).

3 Tiivistelmä julkisen kuulemisen ("Towards a Strengthened Network and Information Security Policy in Europe") tuloksista on tämän ehdotuksen vaikutustenarvioinnin liitteenä 11.

4 KOM(2009) 149, 30.3.2009.

5 Taustamuistio keskustelun pohjaksi: http://www.tallinnciip.eu/doc/discussion_paper_-_tallinn_ciip_conference.pdf
Puheenjohtajan päätelmät: http://www.tallinnciip.eu/doc/EU_Presidency_Conclusions_Tallinn_CIIP_Conference.pdf.

2009 annetussa neuvoston päätöslauselmassa[6] tunnustetaan ENISAn rooli ja potentiaali sekä tarve "*muokata ENISAsta tehokas elin*". Lisäksi siinä korostetaan tarvetta nykyaikaistaa ja vahvistaa virastoa niin, että se pystyy auttamaan komissiota ja jäsenvaltioita luomaan yhteyksiä teknologian ja politiikan välille ja toimimaan EU:n asiantuntijakeskuksena verkko- ja tietoturvaan liittyvissä kysymyksissä.

1.2. Yleinen tausta

Tieto- ja viestintäteknologiasta on tullut Euroopan talouden ja koko yhteiskunnan selkäranka. Siihen kohdistuu uhkia, jotka eivät enää kunnioita kansallisia rajoja ja jotka ovat muuttuneet teknologian ja markkinoiden kehityksen myötä. Koska erilaiset tieto- ja viestintäteknologiat ovat maailmanlaajuisia, yhteenliitettyjä ja keskinäisessä riippuvuussuhteessa muiden infrastruktuurien kanssa, niiden turvallisuutta ja sietokykyä ei voida varmistaa pelkästään kansallisilla ja koordinoimattomilla lähestymistavoilla. Samalla verkko- ja tietoturvaan liittyvät haasteet muuttuvat nopeasti. Verkot ja tietojärjestelmät on suojattava tehokkaasti kaikenlaisilta häiriöiltä ja vioilta, myös tahallisilta hyökkäyksiltä.

Verkko- ja tietoturvaan liittyvät toimet ovat keskeisellä sijalla Euroopan digitaalistrategiassa[7], joka on EU2020-strategian lippulaivahanke. Strategialla pyritään hyödyntämään ja lisäämään tieto- ja viestintäteknologian potentiaalia ja muuntamaan se kestäväksi kasvuksi ja innovaatioiksi. Strategian ydintavoitteisiin kuuluu tieto- ja viestintäteknologian käyttöönoton lisääminen sekä tietoyhteiskuntaan kohdistuvan luottamuksen lujittaminen.

ENISA luotiin aluksi varmistamaan, että EU:ssa vallitsee korkeatasoinen ja toimiva verkko- ja tietoturva. Viraston toiminnasta saadut kokemukset sekä todetut haasteet ja uhat ovat nostaneet esiin tarpeen uudenaikaistaa sen toimeksiantoa vastaamaan paremmin EU:n tarpeita. Tarpeet liittyvät seuraaviin seikkoihin:

- esiin nouseviin haasteisiin reagoidaan kansallisella tasolla eri tavoin
- verkko- ja tietoturvapolitiikan toteutuksesta puuttuu yhteistyömalleja
- uhkiin varautumisessa on puutteita, jotka johtuvat osittain Euroopan rajallisista varhaisvaroitus- ja reagointivalmiuksista
- Euroopasta puuttuu luotettavaa tutkimusdataa ja tietoa esiin nousevista ongelmista
- tietoisuus verkko- ja tietoturvariskeistä ja -haasteista on vähäistä
- verkko- ja tietoturvaan liittyvät näkökohdat on tietoverkkorikollisuuden torjumiseksi otettava tuloksellisemmin huomioon politiikan eri osa-alueilla.

1.3. Poliittiset tavoitteet

Ehdotetun asetuksen yleistavoitteena on luoda EU:lle, jäsenvaltioille ja eri sidosryhmille keinot kehittää korkeatasoiset valmiudet ja hyvä varautumisaste, jotta verkko- ja tietoturvaongelmia voidaan ehkäistä ja huomata ja niihin voidaan reagoida nykyistä

---

[6] Neuvoston päätöslauselma, annettu 18 päivänä joulukuuta 2009, yhteistoiminnallisesta eurooppalaisesta lähestymistavasta verkko- ja tietoturvallisuuden alalla (EUVL C 321, 29.12.2009, s. 1), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:321:0001:0004:FI:PDF.

[7] KOM(2010) 245, 19.5.2010.

paremmin. Tämä auttaa lisäämään tietoyhteiskunnan kehittymisen edellyttämää luottamusta, parantamaan eurooppalaisten yritysten kilpailukykyä ja varmistamaan sisämarkkinoiden käytännön toiminnan.

1.4. Voimassa olevat aiemmat säännökset

Ehdotus täydentää verkko- ja tietoturvaan liittyviä EU-tason sääntelyllisiä ja muita aloitteita, joilla pyritään parantamaan tieto- ja viestintäteknologian tietoturvaa ja varmatoimisuutta:

- Kriittisiä tietoinfrastruktuureja koskevalla tiedonannolla käynnistetyssä toimintasuunnitelmassa käsiteltiin seuraavien mekanismien perustamista:

  (1) Euroopan jäsenvaltiofoorumi, jolla pyritään vaalimaan keskustelua ja yhteydenpitoa hyvistä toimintamalleista ja jakamaan tietoa tieto- ja viestintäteknisen infrastruktuurin turvallisuuteen ja sietokykyyn liittyvistä poliittisista tavoitteista ja painopisteistä muun muassa hyödyntäen suoraan viraston tekemää työtä ja tarjoamaa tukea.

  (2) Sietokykyä käsittelevä eurooppalainen julkis-yksityinen kumppanuus (*European Public-Private Partnership for Resilience,* EP3R), joka on Euroopan laajuinen joustava ohjausjärjestelmä tieto- ja viestintäteknologiainfrastruktuurin varmatoimisuuden kehittämiseksi ja toimii edistämällä julkisen ja yksityisen sektorin yhteistyötä tietoturva- ja varmatoimisuustavoitteisiin, perusvaatimuksiin sekä hyviin käytänteisiin ja toimintatapoihin liittyvissä kysymyksissä.

- Eurooppa-neuvoston 11. joulukuuta 2009 hyväksymä ns. Tukholman ohjelma, jolla edistetään sellaisia politiikkoja, joilla varmistetaan verkkojen turvallisuus ja mahdollistetaan nopeampi reagointi tietoverkkohyökkäyksiin EU:ssa.

- Nämä aloitteet myötävaikuttavat Euroopan digitaalistrategian toteutumiseen. Verkko- ja tietoturvaan liittyvät politiikat ovat keskeisellä sijalla strategian niiden osien kannalta, joissa keskitytään tietoyhteiskunnan luotettavuuden ja tietoturvan parantamiseen. Niillä edesautetaan myös komission tukitoimia ja politiikkaa seuraavilla aloilla: yksityisyyden suoja (erityisesti pyrittäessä ottamaan eri ratkaisujen yksityisyyden suoja huomioon jo suunnitteluvaiheessa) ja henkilötietojen suoja (alan puitteiden tarkistus), kuluttajansuoja-alan yhteistyöverkosto, identiteetinhallinta ja internetin käyttöturvallisuuden parantamiseen tähtäävä Safer Internet -ohjelma.

1.5. Ehdotukseen liittyvät kehityssuuntaukset nykyisessä verkko- ja tietoturvapolitiikassa

Useille meneillään oleville verkko- ja tietoturvapolitiikan kehityssuuntauksille, erityisesti Euroopan digitaalistrategiassa vahvistetuille, on hyötyä ENISAn tuesta ja asiantuntemuksesta. Näitä ovat:

- Verkko- ja tietoturvapoliittisen yhteistyön lujittaminen tehostamalla toimintaa **Euroopan jäsenvaltiofoorumissa**. Tämä auttaa ENISAn suoralla tuella:

  – määrittelemään tapoja luoda toimiva eurooppalainen verkosto kansallisten tietotekniikan CERT-kriisiryhmien välisen, rajat ylittävän yhteistyön avulla,

– määrittelemään pitkän aikavälin tavoitteita ja painopisteitä yleiseurooppalaisille suuren mittakaavan verkko- ja tietoturvaharjoituksille,

– kehittämään vähimmäisvaatimuksia julkisille hankinnoille julkisen sektorin järjestelmien ja verkkojen tietoturvan ja vakauden edistämiseksi,

– määrittelemään tietoteknistä turvallisuutta ja varmatoimisuutta edistäviä taloudellisia ja sääntelyllisiä kannustimia,

– arvioimaan verkko- ja tietoturvan tilaa Euroopassa.

- Julkisen ja yksityisen sektorin yhteistyön ja kumppanuuksien vahvistaminen tukemalla **EP3R-toimintaa**. ENISAlla on kasvava rooli EP3R:n kokousten ja toiminnan mahdollistajana. EP3R tulee jatkossa:

  – keskustelemaan innovatiivisista toimenpiteistä ja keinoista, joilla voidaan parantaa turvallisuutta ja vakautta. Tähän kuuluvat muun muassa seuraavat seikat:

  (1) turvallisuuden ja varmatoimisuuden perusvaatimukset, erityisesti tieto- ja viestintäteknisten tuotteiden tai palvelujen julkisissa hankinnoissa, joilla voidaan taata tasavertaiset kilpailuolosuhteet, mutta samalla varmistaa riittävä varautumis- ja ennaltaehkäisytaso,

  (2) talouden toimijoiden vastuukysymysten selvittely, esimerkiksi niiden toteuttaessa tietoturvan vähimmäisvaatimuksia,

  (3) taloudelliset kannustimet riskinhallintakäytänteiden, tietoturvaprosessien ja tietoturvatuotteiden kehittämiseen ja käyttöönottoon,

  (4) riskinarviointi- ja -hallintamallit, joilla arvioidaan ja hallitaan merkittäviä turvallisuuspoikkeamia yhteisen näkemyksen pohjalta,

  (5) yksityisen ja julkisen sektorin yhteistyö laajamittaisissa ongelmatilanteissa,

  (6) **toimialan huippukokouksen** järjestäminen turvallisuuteen ja toimintavarmuuteen liittyvistä taloudellisista esteistä ja vaikuttimista.

- Sähköisen viestinnän lainsäädäntöpaketin tietoturvavaatimusten täytäntöönpano, jossa tarvitaan ENISAn asiantuntemusta ja apua seuraavien osalta:

  – jäsenvaltioiden ja komission tukeminen tarpeen mukaan yksityisen sektorin näkemykset huomioon ottaen laadittaessa puitteita säännöille ja menettelyille tietoturvaloukkausten ilmoitussäännösten (joista säädetään tarkistetun puitedirektiivin 13 artiklan a kohdassa) täytäntöönpanemiseksi,

  – vuosittain kokoontuvan foorumin luominen verkko- ja tietoturva-alan toimivaltaisille elimille / kansallisille sääntelyviranomaisille ja yksityisen sektorin sidosryhmille, jotta voidaan keskustella saaduista kokemuksista ja vaihtaa tietoja hyvistä toimintamalleista verkko- ja tietoturvaan liittyvien sääntelytoimien soveltamisessa.

- **EU:n laajuisten verkkoturvallisuuden valmiusharjoitusten** helpottaminen komission tuella ja ENISAn myötävaikutuksella pyrkimyksenä laajentaa tällaiset harjoitukset myöhemmin kansainväliselle tasolle.

- **Tietotekniikan CERT-kriisiryhmän perustaminen EU:n toimielimille**. Euroopan digitaalistrategian avaintoimenpide 6:n mukaan komissio esittää "korkean tason verkko- ja tietoturvapolitiikan lujittamiseen tähtääviä toimenpiteitä, joihin kuuluvat [...] toimenpiteet, jotka mahdollistavat entistä nopeamman reagoimisen verkkohyökkäyksiin, kuten EU:n toimielinten CERT"[8]. Tämä edellyttää, että komissio ja muut EU-toimielimet analysoivat tilanteen ja perustavat tietotekniikan CERT-kriisiryhmän, jolle ENISA voi tarjota teknistä tukea ja asiantuntemusta.

- Jäsenvaltioiden kannustaminen ja tukeminen niiden viimeistellessä tai perustaessa **kansallisia CERT-ryhmiä, jotta voidaan luoda hyvin toimiva koko Euroopan kattava CERT-verkosto**. Tämä toiminta on tärkeää myös kehitettäessä edelleen kansalaisille ja pk-yrityksille suunnattua eurooppalaista tiedonjako- ja hälytysjärjestelmää (EISAS), joka luodaan kansallisin resurssein ja valmiuksin vuoden 2012 loppuun mennessä.

- **Tietoisuuden lisääminen** verkko- ja tietoturvahaasteista, mihin kuuluvat seuraavat:

  – komissio laatii yhdessä ENISAn kanssa ohjeistusta verkko- ja tietoturvastandardien, hyvien toimintatapojen ja riskinhallintakulttuurin edistämisestä; tässä yhteydessä tuotetaan ensimmäinen näyte ohjeistuksesta,

  – ENISA järjestää yhteistyössä jäsenvaltioiden kanssa **Euroopan verkko- ja tietoturvakuukauden**, jonka yhteydessä järjestetään kansallisia/eurooppalaisia verkkoturvallisuuskilpailuja.

1.6. Johdonmukaisuus suhteessa unionin muuhun politiikkaan ja muihin tavoitteisiin

Ehdotus on johdonmukainen suhteessa EU:n muuhun politiikkaan ja muihin tavoitteisiin ja tukee täysin tavoitetta edesauttaa sisämarkkinoiden toimivuutta, koske se parantaa valmiuksia vastata verkko- ja tietoturvaan liittyviin haasteisiin.

2. KUULEMISTEN JA VAIKUTUSTEN ARVIOINNIN TULOKSET

2.1. Intressitahojen kuuleminen

Tämä poliittinen aloite on seurausta laajoista keskusteluista, joihin sai vapaasti osallistua ja joissa noudatettiin osallisuuden, avoimuuden, vastuullisuuden, tuloksellisuuden ja johdonmukaisuuden periaatteita. Tähän mittavaan prosessiin kuului vuosina 2006 ja 2007 suoritettu viraston arviointi, jonka jälkeen ENISAn hallintoneuvosto antoi asiasta suosituksensa ja järjestettiin kaksi julkista kuulemista (vuonna 2007 ja vuosina 2008–2009) sekä joukko seminaareja verkko- ja tietoturvaan liittyvistä kysymyksistä.

---

[8] Yhteistoiminnallisesta eurooppalaisesta lähestymistavasta verkko- ja tietoturvallisuuden alalla 18 päivänä joulukuuta 2009 annetussa neuvoston päätöslauselmassa todetaan lisäksi seuraavaa: *"Neuvosto […] korostaa, että […] on tärkeää tutkia, mitä strategisia vaikutuksia, riskejä ja mahdollisuuksia liittyisi tietotekniikan kriisiryhmien perustamiseen EU:n toimielimiin, ja pohtia ENISAn mahdollista tulevaa roolia tässä yhteydessä".*

Ensimmäinen julkinen kuuleminen käynnistettiin, kun komissio oli antanut tiedonantonsa ENISAn puoliväliarvioinnista. Kuulemisessa keskityttiin viraston tulevaisuuteen, ja se kesti 13. päivästä kesäkuuta 7. päivään syyskuuta 2007. Kuulemisessa saatiin internetin välityksellä 44 lausuntoa sekä lisäksi kaksi erikseen kirjallisesti toimitettua lausuntoa. Lausuntoja saatiin eri sidosryhmiltä ja intressitahoilta, kuten jäsenvaltioiden ministeriöiltä, sääntelyelimiltä, toimiala- ja kuluttajajärjestöiltä, korkeakouluilta, yrityksiltä ja yksityishenkilöiltä.

Vastauksissa esiin nostettuja kysymyksiä olivat uhkakuvan kehittyminen, tarve selkeyttää ja joustavoittaa asetusta, jotta ENISA voi mukautua haasteisiin, toimivan sidosryhmävuorovaikutuksen varmistamisen tärkeys sekä mahdollisuus viraston resurssien tietynasteiseen kasvattamiseen.

Toisessa julkisessa kuulemisessa, joka järjestettiin 7. marraskuuta 2008 – 9. tammikuuta 2009, pyrittiin määrittelemään Euroopan tasoisen vahvistetun verkko- ja tietoturvapolitiikan tärkeimmät tavoitteet ja keinot tavoitteisiin pääsemiseksi. Jäsenvaltioiden viranomaisilta, korkeakouluilta/tutkimuslaitoksilta, toimialajärjestöiltä, yrityksiltä ja muilta sidosryhmiltä, kuten tietosuojaorganisaatioilta ja -konsulttiyrityksiltä ja yksityishenkilöiltä saatiin lähes 600 lausuntoa.

Suuri enemmistö vastaajista[9] kannatti viraston toimikauden jatkamista ja tuki sen roolin vahvistamista verkko- ja tietoturvatoiminnan koordinoinnissa EU-tasolla, samoin kuin sen resurssien lisäämistä. Keskeisiä painopisteitä olivat tarve koordinoidummalle lähestymistavalle tietoverkkouhkien suhteen Euroopassa, ylikansallinen yhteistyö suuren mittakaavan verkkohyökkäyksiin reagoimisessa, luottamuksen rakentaminen sekä parempi tiedonvaihto sidosryhmien kesken.

Ehdotuksen vaikutusten arviointi käynnistettiin syyskuussa 2009, ja se perustui ulkopuolisella asiantuntijalla teetettyyn esiselvitykseen. Prosessiin osallistui laajasti eri sidosryhmiä ja asiantuntijoita. Näitä olivat muun muassa verkko- ja tietoturvasta vastaavat jäsenvaltioiden elimet, kansalliset sääntelyviranomaiset, teleoperaattorit ja internet-palveluntarjoajat ja niiden toimialajärjestöt, kuluttajajärjestöt, tieto- ja viestintätekniikan laitevalmistajat, CERT-ryhmät, tutkijat ja elinkeinoelämää edustavat järjestelmien käyttäjät. Vaikutustenarvioinnin tueksi perustettiin asianomaisten pääosastojen yhteinen komission yksiköiden ohjausryhmä.

2.2. Vaikutusten arviointi

Virastoa pidettiin tarkoituksenmukaisena ratkaisuna yleiseurooppalaisten tavoitteiden saavuttamiseksi[10]. Esivalintaprosessissa valittiin lisäanalyysiin viisi toimintavaihtoehtoa:

- Vaihtoehto 1 – Ei erityistä alan politiikkaa;
- Vaihtoehto 2 – Jatketaan entiseen malliin, eli samankaltaisella toimeksiannolla ja samantasoisilla resursseilla;
- Vaihtoehto 3 – Laajennetaan ENISAn tehtäviä ja lisätään lainvalvonta- ja tietosuojaviranomaiset täysivaltaisiksi sidosryhmiksi;

[9] Ks. vaikutusten arvioinnin liite XI.
[10] Ks. vaikutusten arvioinnin liite IV.

- Vaihtoehto 4 – Lisätään viraston tehtäviin tietoverkkohyökkäysten ehkäisy ja niihin reagointi;

- Vaihtoehto 5 – Lisätään viraston tehtäviin lainvalvonta- ja -käyttöviranomaisten tukeminen tietoverkkorikollisuuden vastaisessa toiminnassa.

Vaihtoehto 3 valittiin vertailevassa kustannus-hyötyanalyysissa kustannustehokkaimmaksi tavaksi saavuttaa poliittiset tavoitteet.

Vaihtoehdossa 3 ENISAn roolia laajennetaan siten, että se keskittyy seuraaviin tehtäviin:

- sidosryhmien välisen yhteydenpito- ja osaamisverkoston luominen ja ylläpito, jotta ENISA on kattavasti perillä Euroopan verkko- ja tietoturvatilanteesta,
- toimiminen verkko- ja tietoturva-asioiden tukikeskuksena politiikan laatimista ja toteuttamista varten (erityisesti yksityisyyden suojaan, sähköisiin allekirjoituksiin, sähköiseen identiteettiin ja verkko- ja tietoturvaa koskeviin julkisten hankintojen normeihin liittyvissä kysymyksissä),
- EU:n kriittisiä tietoinfrastruktuureja ja niiden suojaamista koskevan politiikan tukeminen (harjoitukset, EP3R, eurooppalainen tiedonjako- ja hälytysjärjestelmä EISAS jne.),
- EU:n yhteisten puitteiden luominen verkko- ja tietoturvaa koskevan tiedon keruuta varten, myös oikeudellisten tietojen raportointiin ja jakamiseen liittyvien menetelmien ja käytänteiden kehittäminen,
- verkko- ja tietoturvaan liittyvien taloudellisten näkökohtien tutkimus,
- yhteistyön aikaansaaminen EU:n ulkopuolisten maiden ja kansainvälisten organisaatioiden kanssa, jotta voidaan edistää yhteisiä maailmanlaajuisia verkko- ja tietoturvaperiaatteita ja lisätä korkean tason kansainvälisten aloitteiden vaikuttavuutta Euroopassa,
- muiden kuin operatiivisten tehtävien suorittaminen liittyen tietoverkkorikollisuutta koskevaan oikeudelliseen ja lainvalvontayhteistyöhön.

3. EHDOTUKSEEN LIITTYVÄT OIKEUDELLISET NÄKÖKOHDAT

3.1. Ehdotetun toimen lyhyt kuvaus

Ehdotetulla asetuksella pyritään vahvistamaan ja nykyaikaistamaan Euroopan verkko- ja tietoturvavirastoa (ENISA) ja säätämään sen uudesta toimeksiannosta viiden vuoden kaudeksi.

Ehdotus sisältää edelliseen asetukseen verrattuna muutamia keskeisiä muutoksia:

(1) **Lisää joustavuutta, mukautuvuutta ja fokusointikykyä**. Tehtävät päivitetään ja muotoillaan uudelleen löyhemmin, jotta virastolla on toimissaan enemmän liikkumavaraa. Tehtävät ovat kuitenkin riittävän täsmällisiä niiden keinojen kuvaamiseksi, joilla tavoitteet on saavutettava. Tämä fokusoi paremmin viraston toimenkuvaa, parantaa sen valmiuksia saavuttaa tavoitteensa ja vahvistaa sen tehtäviä EU-politiikan täytäntöönpanon tukemiseksi.

(2) **Viraston tiiviimpi osallistuminen EU:n poliittiseen ja sääntelyprosessiin**. EU:n toimielimet ja erillisvirastot voivat pyytää virastolta apua ja neuvontaa. Tämä on

linjassa politiikan ja sääntelyn kehityssuuntausten kanssa: neuvosto on alkanut päätöslauselmissaan viitata virastoon suoraan, ja parlamentti ja neuvosto ovat sähköisen viestinnän sääntelyjärjestelmässä antaneet virastolle verkko- ja tietoturvaan liittyviä tehtäviä.

(3) **Yhteydet tietoverkkorikollisuuden vastaiseen toimintaan**. Tavoitteisiinsa pyrkiessään virasto ottaa huomioon tietoverkkorikollisuuden ehkäisytoiminnan. Lainvalvonta- ja tietosuojaviranomaisista tulee viraston täysivaltaisia sidosryhmiä, erityisesti pysyvässä sidosryhmässä.

(4) **Vahvempi omistajaohjausrakenne**. Ehdotus vahvistaa viraston johtokunnan valvontaroolia. Johtokunnassa ovat edustettuina jäsenvaltiot ja komissio. Johtokunta voi asettaa suuntaviivoja esimerkiksi henkilöstöasioissa, jotka aiemmin kuuluivat yksinomaan pääjohtajan vastuulle. Se voi myös perustaa työryhmiä avukseen tehtäviensä suorittamisessa, muun muassa päätöstensä täytäntöönpanon seurantaa varten.

(5) **Menettelyt sujuvammiksi**. Tarpeettoman monimutkaisiksi osoittautuneita menettelyjä yksinkertaistetaan. Esimerkkejä tästä: a) johtokunnan työjärjestystä koskevaa menettelyä yksinkertaistetaan, b) komissio antaa lausuntonsa ENISAn työohjelmasta suoraan yksiköidensä kautta eikä erillisellä komission päätöksellä. Johtokunnalle annetaan myös riittävät resurssit sen varalta, että sen täytyy tehdä varsinaisia johtamispäätöksiä ja täytäntöönpanna niitä (esim. jos henkilöstön jäsen tekee valituksen pääjohtajasta tai itse johtokunnasta).

(6) **Resursseja lisätään asteittain**. Jotta virasto pystyy hoitamaan EU-tason entistä vahvemmat painopistealueet ja vastaamaan laajentuviin haasteisiin, sen taloudellisten ja henkilöstöresurssien ennakoidaan kasvavan asteittain vuosina 2012–2016, sanotun kuitenkaan rajoittamatta seuraavaa monivuotista rahoituskehystä koskevan komission ehdotuksen laatimista. Komissio esittää tarkistetun rahoitusselvityksen vuoden 2013 jälkeistä monivuotista rahoituskehystä koskevan asetusehdotuksensa pohjalta ottaen huomioon vaikutusten arvioinnin päätelmät.

(7) **Mahdollisuus jatkaa pääjohtajan toimikautta**. Johtokunta voi jatkaa pääjohtajan toimikautta kolmella vuodella.

3.2. Oikeusperusta

Ehdotus perustuu Euroopan unionin toiminnasta tehdyn sopimuksen[11] (SEUT-sopimus) 114 artiklaan.

EU-tuomioistuimen tuomion mukaan[12] ennen Lissabonin sopimuksen voimaantuloa asianmukaiseksi oikeusperustaksi elimen perustamiselle varmistamaan verkko- ja tietoturvan korkea ja toimiva taso EU:ssa oli katsottava **Euroopan yhteisön perustamissopimuksen 95 artikla**. Käyttämällä 95 artiklassa ilmaisua "toimenpiteet […] lähentämiseksi" perustamissopimuksen laatijat halusivat antaa EU-lainsäätäjälle päätäntävallan valita sopivin toimenpide toivotun tuloksen aikaansaamiseksi. Tieto- ja viestintäteknisten infrastruktuurien

---

11 EUVL C 115, 9.5.2008, s. 94.

12 Asia C-217/04, 2.5.2006, Ison-Britannian ja Pohjois-Irlannin Yhdistynyt kuningaskunta vastaan Euroopan parlamentti ja Euroopan unionin neuvosto.

turvallisuuden ja varmatoimisuuden parantaminen on tärkeä sisämarkkinoiden sujuvaan toimintaan vaikuttava tekijä.

Lissabonin sopimuksen mukaisesti **SEUT:n 114 artiklassa**[13] kuvataan – lähes identtisellä tavalla – sisämarkkinavelvollisuus. Edellä kuvatuista syistä se pysyy edelleen sovellettavana oikeusperustana verkko- ja tietoturvan parantamiseen tähtääville toimenpiteille. Sisämarkkinavelvollisuus kuuluu nyt EU:n ja jäsenvaltioiden jaettuun toimivaltaan (SEUT:n 4 artiklan 2 kohdan a alakohta). Tämä merkitsee, että EU ja jäsenvaltiot voivat antaa (sitovia) säädöksiä ja että jäsenvaltiot käyttävät toimivaltaansa siltä osin kuin unioni ei ole käyttänyt omaansa tai on päättänyt lakata käyttämästä omaansa (SEUT:n 2 artiklan 2 kohta).

Sisämarkkinavelvollisuuden piiriin kuuluvat toimenpiteet edellyttävät tavallista lainsäätämisjärjestystä (SEUT:n 289 ja 294 artikla), joka on samankaltainen[14] kuin aiempi yhteispäätösmenettely (yhteisön perustamissopimuksen 251 artikla).

Lissabonin sopimuksen myötä aiempi erottelu "pilarien" välillä on poistunut. Rikollisuuden ehkäiseminen ja torjunta on siirtynyt osaksi unionin jaettua toimivaltaa. Tämä suo ENISAlle tilaisuuden ottaa rooli tietoverkkorikollisuuden torjunnassa verkko- ja tietoturvaan liittyvissä kysymyksissä ja ryhtyä yhteydenpitoon näkemyksistä ja parhaista toimintatavoista tietoverkkoasioissa puolustus-, lainvalvonta- ja tietosuojaviranomaisten kanssa.

3.3. Toissijaisuusperiaate

Ehdotus on toissijaisuusperiaatteen mukainen: Verkko- ja tietoturvapolitiikka edellyttää yhteistoiminnallista lähestymistapaa, eivätkä jäsenvaltiot voi yksinään saavuttaa ehdotuksen tavoitteita.

Ellei EU millään lailla puuttuisi kansalliseen verkko- ja tietoturvapolitiikkaan, asia jäisi jäsenvaltioiden hoidettavaksi, mikä jättäisi täysin huomiotta tietojärjestelmien selkeät keskinäiset riippuvuussuhteet. Näin ollen on toissijaisuusperiaatteen mukaista säätää toimenpiteestä, jolla taataan jäsenvaltioiden riittävä koordinointi sen varmistamiseksi, että verkko- ja tietoturvariskit voidaan asianmukaisesti hallita rajat ylittävässä ympäristössä, jossa niitä esiintyy. EU-tason toiminta parantaisi myös kansallisen politiikan vaikuttavuutta ja toisi näin lisäarvoa.

Yhteensovitetulla ja yhteistoiminnallisella verkko- ja tietoturvapolitiikalla on lisäksi myönteinen vaikutus perusoikeuksien suojaan ja erityisesti henkilötietojen ja yksityisyyden suojaan. Henkilötietojen suojaamisen tarve on nyt erittäin ajankohtainen, koska eurooppalaiset luovuttavat yhä enemmän tietojaan monisäikeisiin tietojärjestelmiin joko omasta aloitteestaan tai koska se on välttämätöntä, kykenemättä välttämättä arvioimaan oikein asiaan liittyviä tietosuojariskejä. Mikäli ongelmia esiintyy, he eivät näin ollen välttämättä pysty ryhtymään tarvittaviin toimiin, eikä ole varmaa, pystyisivät jäsenvaltiot tuloksellisesti ratkaisemaan kansainvälisiä ongelmatilanteita ilman EU:n tasoista verkko- ja tietoturvakoordinointia.

---

13 Vrt. edellä.

14 Tavallinen lainsäätämisjärjestys eroaa siitä erityisesti neuvostossa ja Euroopan parlamentissa sovellettavien enemmistövaatimusten osalta.

3.4. Suhteellisuusperiaate

Ehdotus on suhteellisuusperiaatteen mukainen, koska siinä ei ylitetä sitä, mikä on tarpeen sen tavoitteen saavuttamiseksi.

3.5. Sääntelytavan valinta

Ehdotettu sääntelytapa: asetus, jota sovelletaan sellaisenaan kaikissa jäsenvaltioissa.

4. TALOUSARVIOVAIKUTUKSET

Ehdotuksella on vaikutuksia unionin talousarvioon.

Koska ENISAn uuteen toimeksiantoon sisältyvistä tehtävistä säädetään asetuksella, on oletettavaa, että virastolle annetaan sen toiminnan menestyksekkään harjoittamisen edellyttämät voimavarat. Virastosta tehty arviointi, sidosryhmien mittava kuuleminen kaikilla tasoilla sekä vaikutusten arviointi osoittavat yleisen yksimielisyyden siitä, että viraston koko on tällä hetkellä sen kriittistä massaa pienempi ja resursseja tarvitaan lisää. Viraston henkilöstömäärän ja budjetin kasvattamisen seurauksia ja vaikutuksia analysoidaan ehdotukseen liittyvässä vaikutusten arvioinnissa.

Vuoden 2013 jälkeistä EU-rahoitusta pohditaan koko komission laajuisessa keskustelussa kaikista vuoden 2013 jälkeistä aikaa koskevista ehdotuksista.

5. LISÄHUOMIOITA

5.1. Kesto

Asetus kattaa viiden vuoden kauden.

5.2. Uudelleentarkastelulauseke

Asetuksessa säädetään viraston toiminnan arvioinnista, joka kattaa jakson vuonna 2007 suoritetusta edellisestä arvioinnista lähtien. Siinä arvioidaan viraston tuloksellisuutta asetuksessa säädettyjen tavoitteiden saavuttamisessa ja sitä, onko se edelleen tehokas väline sekä sitä, olisiko viraston toimikautta edelleen jatkettava. Johtokunta antaa arvioinnin tulosten perusteella komissiolle suosituksia tähän asetukseen, virastoon ja sen toimintatapoihin tehtävistä muutoksista. Jotta komissio ehtii ajoissa laatimaan mahdollisen ehdotuksen toimikauden jatkamisesta, arviointi on tehtävä asetuksessa säädetyn toimikauden toisen vuoden loppuun mennessä.

5.3. Väliaikaistoimenpiteet

Komissio on tietoinen siitä, että lainsäädäntömenettely Euroopan parlamentissa ja neuvostossa saattaa edellyttää aikaa vieviä keskusteluja ehdotuksesta, ja on vaarassa syntyä oikeudellinen tyhjiö, ellei viraston uuttaa toimikautta vahvisteta riittävän ajoissa ennen nykyisen toimikauden päättymistä. Näin ollen komissio antaa tämän ehdotuksen yhteydessä toisen ehdotuksen asetukseksi, jolla jatketaan viraston toimikautta 18 kuukaudella, jotta keskustelulle ja lainsäädäntöprosessille jää riittävästi aikaa.

2010/0275 (COD)

Ehdotus

EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS

Euroopan verkko- ja tietoturvavirastosta (ENISA)

EUROOPAN PARLAMENTTI JA EUROOPAN UNIONIN NEUVOSTO, jotka

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

ottavat huomioon Euroopan komission ehdotuksen,

ottavat huomioon Euroopan talous- ja sosiaalikomitean lausunnon[15],

ottavat huomioon alueiden komitean lausunnon[16],

sen jälkeen, kun ehdotus on toimitettu kansallisille parlamenteille,

noudattavat tavallista lainsäätämisjärjestystä,

sekä katsovat seuraavaa:

(1) Sähköinen viestintä ja sähköiset infrastruktuurit ja palvelut ovat taloudellisen ja yhteiskunnallisen kehityksen olennainen tekijä. Niillä on yhteiskunnassa elintärkeä rooli ja niistä on tullut sähkö- ja vesihuollon lailla kaikkialla läsnä olevia hyödykkeitä. Niiden häiriöt voivat aiheuttaa huomattavaa taloudellista haittaa, mikä entisestään korostaa tarvetta toimille, joilla parannetaan niiden suojaa ja sietokykyä ja pyritään varmistamaan kriittisten palvelujen tarjonnan jatkuvuus. Sähköisen viestinnän ja sähköisten infrastruktuurien ja palvelujen tietoturvaan ja erityisesti niiden koskemattomuuteen ja saatavuuteen kohdistuu alati kasvavia haasteita. Tämä on yhteiskunnallisesti yhä suurempi huolenaihe, eikä vähiten siksi, että järjestelmien monimutkaisuuden, onnettomuuksien, inhimillisten virheiden ja vihamielisten hyökkäysten vuoksi saattaa aiheutua ongelmia, joilla voi olla vaikutuksia fyysiseen infrastruktuuriin, joka tuottaa Euroopan kansalaisten hyvinvoinnin kannalta kriittisiä palveluja.

(2) Uhkakuvasto muuttuu jatkuvasti ja tietoturvaongelmat saattavat heikentää käyttäjien luottamusta. Sähköisten viestintäjärjestelmien, infrastruktuurien ja palvelujen vakavilla häiriöillä voi olla mittavia taloudellisia ja yhteiskunnallisia vaikutuksia, mutta myös jokapäiväiset tietoturvarikkomukset, -ongelmat ja -haitat saattavat rapauttaa yleistä luottamusta teknologiaa, verkkoja ja palveluja kohtaan.

---

15 EUVL C , , s. .
16 EUVL C , , s. .

(3) Näin ollen politiikan laatijoille, elinkeinoelämälle ja käyttäjille on tärkeää, että verkko- ja tietoturvallisuuden tilaa Euroopassa arvioidaan säännöllisesti luotettavan eurooppalaisen tiedon pohjalta.

(4) Joulukuun 13 päivänä 2003 Eurooppa-neuvostossa kokoontuneet jäsenvaltioiden edustajat päättivät, että komission ehdotuksen pohjalta perustettavan Euroopan verkko- ja tietoturvaviraston (ENISA) toimipaikka sijaitsisi jossain Kreikan kaupungissa, jonka Kreikan hallitus valitsee.

(5) Vuonna 2004 Euroopan parlamentti ja neuvosto antoivat Euroopan verkko- ja tietoturvaviraston perustamisesta asetuksen (EY) N:o 460/2004[17], jolla pyrittiin osaltaan varmistamaan verkko- ja tietoturvan korkea taso EU:ssa ja kehittämään verkko- ja tietoturvakulttuuria kansalaisten, kuluttajien, yritysten ja hallintojen hyväksi. Vuonna 2008 Euroopan parlamentti ja neuvosto antoivat asetuksen (EY) N:o 1007/2008[18], jolla viraston toimikautta jatkettiin maaliskuuhun 2012.

(6) Viraston perustamisen jälkeen verkko- ja tietoturvaan liittyvät haasteet ovat muuttuneet teknologian, markkinoiden ja sosioekonomisten olosuhteiden kehityksen myötä ja niistä on käyty lisää keskustelua. Vastauksena muuttuviin haasteisiin EU on päivittänyt verkko- ja tietoturvapolitiikkansa painopisteitä useissa asiakirjoissa, joita ovat vuonna 2006 annettu komission tiedonanto *Turvallisen tietoyhteiskunnan strategia – "Lisää vuoropuhelua, yhteistyötä ja vaikutusmahdollisuuksia"*[19], neuvoston vuonna 2007 antama päätöslauselma Euroopan turvallisen tietoyhteiskunnan strategiasta[20], vuonna 2009 annettu tiedonanto elintärkeiden tietoinfrastruktuureiden suojaamisesta: *"Euroopan suojaaminen laajoilta tietoverkkohyökkäyksiltä ja häiriöiltä: valmiuden, turvallisuuden ja sietokyvyn parantaminen"*[21], kriittisten tietoinfrastruktuurien suojaamista käsitelleen ministerikonferenssin puheenjohtajan päätelmät sekä vuonna 2009 annettu neuvoston päätöslauselma yhteistoiminnallisesta eurooppalaisesta lähestymistavasta verkko- ja tietoturvallisuuden alalla[22]. Virastoa on tunnustetusti nykyaikaistettava ja vahvistettava, jotta se voi onnistuneesti edesauttaa EU:n toimielinten ja jäsenvaltioiden pyrkimyksiä kehittää Euroopan valmiuksia selviytyä verkko- ja tietoturvahaasteista. Komissio hyväksyi hiljattain Euroopan digitaalistrategian[23], joka on yksi Eurooppa 2020 -strategian lippulaivahankkeista. Tällä laaja-alaisella strategialla pyritään hyödyntämään ja lisäämään tieto- ja viestintäteknologian potentiaalia ja muuntamaan se kestäväksi kasvuksi ja innovaatioiksi. Strategian yhtenä päätavoitteena on tietoyhteiskuntaan kohdistuvan luottamuksen lujittaminen, ja siinä esiteltiin lukuisia toimenpiteitä, joita komissio aikoo toteuttaa tällä alalla; näihin lukeutuu myös tämä ehdotus.

(7) Sisämarkkinasäännökset sähköisen viestinnän turvallisuuden ja yleisemmin verkko- ja tietoturvan alalla edellyttävät erilaisia teknisiä ja organisatorisia soveltamisen muotoja jäsenvaltioilta ja komissiolta. Näiden vaatimusten epäyhtenäinen soveltaminen voi

---

17 EUVL L 77, 13.3.2004, s. 1.
18 EUVL L 293, 31.10.2008, s. 1.
19 KOM(2006) 251, 31.5.2006.
20 Neuvoston päätöslauselma, annettu 22 päivänä maaliskuuta 2007, Euroopan turvallisen tietoyhteiskunnan strategiasta (EUVL C 68, 24.3.2007, s. 1).
21 KOM(2009) 149, 30.3.2009.
22 Neuvoston päätöslauselma, annettu 18 päivänä joulukuuta 2009, yhteistoiminnallisesta eurooppalaisesta lähestymistavasta verkko- ja tietoturvallisuuden alalla (EUVL C 321, 29.12.2009, s. 1).
23 KOM(2010) 245, 19.5.2010.

johtaa tehottomiin ratkaisuihin ja luoda esteitä sisämarkkinoille. Tästä syystä jäsenvaltioiden ja EU:n toimielinten tueksi tarvitaan Euroopan tasoista osaamiskeskusta antamaan ohjeistusta, neuvoa ja pyydettäessä apua verkko- ja tietoturvaan liittyvissä kysymyksissä. Virasto voi vastata näihin tarpeisiin kehittämällä ja ylläpitämällä korkeaa osaamistasoa ja avustamalla jäsenvaltioita ja komissiota ja tätä kautta elinkeinoelämää vastaamaan verkko- ja tietoturvaan liittyviin lakisääteisiin ja sääntelyllisiin vaatimuksiin, ja edesauttaa näin sisämarkkinoiden sujuvaa toimintaa.

(8) Viraston olisi hoidettava voimassa olevassa sähköisen viestinnän EU-lainsäädännössä sille annettuja tehtäviä ja yleisemmin myötävaikutettava sähköisen viestinnän tietoturvan parantumiseen muun muassa tarjoamalla asiantuntemustaan ja neuvontaa sekä edistämällä tiedonvaihtoa hyvistä käytänteistä.

(9) Sähköisten viestintäverkkojen ja -palvelujen yhteisestä sääntelyjärjestelmästä 7 päivänä maaliskuuta 2002 annetussa Euroopan parlamentin ja neuvoston direktiivissä 2002/21/EY (puitedirektiivi)[24] edellytetään, että yleisten sähköisten viestintäverkkojen ja yleisesti saatavilla olevien sähköisen viestinnän palvelujen tarjoajat toteuttavat tarvittavat toimet turvatakseen niiden koskemattomuuden ja tietoturvan, sekä asetetaan tietoturva- ja koskemattomuusloukkauksiin liittyviä tiedotusvelvollisuuksia. Kansallisten sääntelyviranomaisten on tarvittaessa tiedotettava loukkauksista myös virastolle ja niiden on toimitettava komissiolle ja virastolle vuosittain tiivistelmä saaduista ilmoituksista ja niiden johdosta toteutetuista toimenpiteistä. Lisäksi direktiivissä 2002/21/EY annetaan virastolle tehtäväksi osallistua tarvittavien teknisten ja organisatoristen tietoturvatoimenpiteiden yhdenmukaistamiseen antamalla asiasta lausuntoja.

(10) Henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla 12 päivänä heinäkuuta 2002 annetussa Euroopan parlamentin ja neuvoston direktiivissä 2002/58/EY[25] (sähköisen viestinnän tietosuojadirektiivi) vaaditaan yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajia toteuttamaan asianmukaiset tekniset ja organisatoriset toimenpiteet varmistaakseen tarjoamiensa palvelujen turvallisuuden, minkä lisäksi siinä edellytetään, että viestintä ja siihen liittyvät liikennetiedot ovat luottamuksellisia. Lisäksi direktiivillä 2002/58/EY asetetaan sähköisen viestinnän palvelujen tarjoajille vaatimuksia, jotka liittyvät henkilötietojen suojan loukkauksia koskeviin tietoihin ja niistä ilmoittamiseen. Siinä edellytetään myös, että komissio kuulee virastoa kaikista teknisistä täytäntöönpanosäädöksistä, jotka liittyvät tieto- ja ilmoitusvaatimusten edellytyksiin, muotoon tai niihin liittyviin menettelyihin. Yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta 24 päivänä lokakuuta 1995 annetussa Euroopan parlamentin ja neuvoston direktiivissä 95/46/EY[26] vaaditaan jäsenvaltioita säätämään, että rekisterinpitäjän on toteutettava tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi vahingossa tapahtuvalta tai laittomalta tuhoamiselta, vahingossa tapahtuvalta häviämiseltä, muuttamiselta, luvattomalta luovuttamiselta tai tietojen antamiselta, erityisesti jos käsittelyyn liittyy tietojen siirtämistä verkossa, sekä kaikelta muulta laittomalta käsittelyltä.

---

24 EYVL L 108, 24.4.2002, s. 33.
25 EYVL L 201, 31.7.2002, s. 37.
26 EYVL L 281, 23.11.1995, s. 31.

(11) Viraston olisi osaltaan edistettävä korkeatasoista verkko- ja tietoturvaa EU:ssa sekä kehitettävä sen kansalaisia, kuluttajia, yrityksiä ja julkisen sektorin organisaatioita hyödyttävä verkko- ja tietoturvakulttuuri, ja siten edistää sisämarkkinoiden moitteetonta toimintaa.

(12) Viraston tehtävänannossa olisi ilmaistava, miten viraston on määrä saavuttaa tavoitteensa niin, että se pystyy toimimaan joustavasti. Viraston tehtäviin olisi kuuluttava tarvittavan tiedon keruu sähköisten viestintäjärjestelmien, infrastruktuurien ja palvelujen tietoturvaan ja vakaatoimisuuteen kohdistuvien riskien analysoimiseksi sekä verkko- ja tietoturvatilanteen arvioimiseksi Euroopassa yhteistyössä jäsenvaltioiden kanssa. Viraston olisi varmistettava koordinaatio jäsenvaltioiden kanssa ja lisättävä eri sidosryhmien yhteistyötä Euroopassa, erityisesti ottamalla toimintaansa mukaan verkko- ja tietoturva-alan toimivaltaisia kansallisia elimiä ja asiantuntijoita yksityiseltä sektorilta. Viraston olisi avustettava komissiota ja jäsenvaltioita niiden yhteydenpidossa yritysmaailman edustajien kanssa laitteistojen ja ohjelmistotuotteiden tietoturvaongelmien arvioimiseksi ja edesautettava näin osaltaan yhteistoiminnallisen lähestymistavan kehittymistä verkko- ja tietoturvan alalla.

(13) Viraston olisi toimittava alan kiintopisteenä ja vahvistettava luottamusta riippumattomuutensa, antamiensa lausuntojen ja levittämiensä tietojen laadun, menettelyjensä ja toimintatapojensa avoimuuden sekä sille annettujen tehtävien suorittamisessa osoitetun huolellisuuden ansiosta. Viraston olisi perustuttava kansallisille ja EU:n toimille ja suoritettava näin ollen tehtävänsä täydessä yhteistyössä jäsenvaltioiden kanssa, ja sen olisi oltava valmis ottamaan yhteyksiä teollisuuteen ja muihin asianomaisiin sidosryhmiin. Lisäksi viraston olisi hyödynnettävä yksityisen sektorin näkemyksiä ja yhteistyötä, jotka ovat tärkeässä asemassa turvattaessa sähköistä viestintää sekä sähköisiä infrastruktuureja ja palveluja.

(14) Komissio on perustanut sietokykyä käsittelevän eurooppalaisen julkis-yksityisen kumppanuuden (*European Public-Private Partnership for Resilience*, EP3R) joustavaksi Euroopan laajuiseksi ohjauskehykseksi tieto- ja viestintäteknisen infrastruktuurin suojan parantamiseksi. Viraston olisi toimittava tässä yhteydessä mahdollistavassa roolissa ja saatettava yhteen julkisen ja yksityisen sektorin sidosryhmiä keskustelemaan politiikan painopisteistä, haasteiden taloudellisista ja markkinaulottuvuuksista ja toimista tieto- ja viestintäteknisen infrastruktuurin toimintavarmuuden parantamiseksi sekä määrittelemään eri sidosryhmien vastuualueita.

(15) Viraston olisi komission pyynnöstä tai omasta aloitteestaan neuvottava komissiota tuottamalla lausuntoja ja teknisiä ja sosioekonomisia analyyseja verkko- ja tietoturva-alan politiikan laadinnan tueksi. Viraston olisi pyynnöstä avustettava myös jäsenvaltioita ja EU:n toimielimiä ja muita elimiä niiden pyrkimyksissä kehittää verkko- ja tietoturvapolitiikkaa ja -valmiuksia.

(16) Viraston olisi avustettava jäsenvaltioita ja EU:n toimielimiä niiden pyrkimyksissä luoda ja parantaa rajat ylittäviä valmiuksia ehkäistä, todeta ja lieventää verkko- ja tietoturvaongelmia ja -uhkia sekä vastata niihin; tässä yhteydessä viraston olisi helpotettava jäsenvaltioiden keskinäistä ja jäsenvaltioiden ja komission välistä yhteistyötä. Tätä varten viraston olisi aktiivisesti tuettava jäsenvaltioita niiden pyrkiessä parantamaan reagointivalmiuksiaan ja järjestämään ja toteuttamaan kansallisia ja Euroopan laajuisia tietoturvaharjoituksia.

(17) Tämän asetuksen nojalla tapahtuvaan henkilötietojen käsittelyyn sovelletaan direktiiviä 95/46/EY.

(18) Ymmärtääkseen paremmin verkko- ja tietoturva-alan haasteita, viraston olisi analysoitava nykyisiä ja esiin nousevia riskejä. Tätä varten viraston olisi yhteistyössä jäsenvaltioiden ja tarvittaessa tilastokeskusten kanssa kerättävä tarvittavaa tietoa. Lisäksi viraston olisi autettava jäsenvaltioita ja EU:n toimielimiä ja muita elimiä keräämään, analysoimaan ja levittämään verkko- ja tietoturvaan liittyvää tietoa.

(19) Harjoittaessaan EU:ssa tilanteen seurantaa viraston olisi helpotettava EU:n ja jäsenvaltioiden välistä yhteistyötä Euroopan verkko- ja tietoturvatilanteen analysoinnissa ja osallistuttava arviointiin yhteistyössä jäsenvaltioiden kanssa.

(20) Viraston olisi helpotettava jäsenvaltioiden toimivaltaisten elinten yhteistyötä erityisesti tukemalla koulutusohjelmiin ja tiedotushankkeisiin liittyvien hyvien toimintamallien ja normien kehittämistä ja niitä koskevaa tiedonvaihtoa. Tiedonvaihdon lisääminen jäsenvaltioiden kesken tulee helpottamaan tällaista tiedotustoimintaa. Viraston olisi tuettava julkisen ja yksityisen sektorin sidosryhmien yhteistyötä myös EU:n tasolla, osin edistämällä tiedonvaihtoa, tiedotuskampanjoita ja koulutusohjelmia.

(21) Tehokkaan tietoturvapolitiikan olisi perustuttava kehittyneisiin riskinarviointimenetelmiin niin julkisella kuin yksityiselläkin sektorilla. Riskinarviointimenetelmiä ja -menettelyjä käytetään eri tasoilla vailla yhteistä tehokasta soveltamiskäytäntöä. Riskinarvioinnin ja yhteentoimivien riskinarviointiratkaisujen parhaiden käytäntöjen edistäminen ja kehittäminen julkisen ja yksityisen sektorin organisaatioissa kohottaa verkkojen ja tietojärjestelmien turvallisuustasoa Euroopassa. Tätä varten viraston olisi tuettava julkisen ja yksityisen sektorin sidosryhmien yhteistyötä EU:n tasolla ja helpotettava niiden pyrkimyksiä laatia ja ottaa käyttöön normeja riskinhallintaa ja sähköisten tuotteiden, järjestelmien, verkkojen ja palvelujen tietoturvan mittaamista varten.

(22) Viraston työssä olisi hyödynnettävä meneillään olevia tutkimus-, kehittämis- ja teknologian arvioimistoimia ja erityisesti niitä, joita harjoitetaan EU:n eri tutkimusaloitteissa.

(23) Viraston olisi jaettava kokemuksia ja yleisiä tietoja Euroopan unionin oikeuden mukaisesti luotujen sellaisten elinten ja virastojen kanssa, jotka toimivat verkko- ja tietoturva-alalla, jos se on tarkoituksenmukaista viraston toimialan, tavoitteiden ja tehtävien kannalta.

(24) Ollessaan tietoverkkorikollisuuden tietoturvanäkökohtiin liittyen yhteydessä lainvalvontaviranomaisiin virasto käyttää olemassa olevia tiedonvaihtokanavia ja vakiintuneita verkostoja, kuten yhteyspisteverkostoa, joka mainitaan ehdotuksessa Euroopan parlamentin ja neuvoston direktiiviksi tietoverkkoihin kohdistuvista hyökkäyksistä ja puitepäätöksen 2005/222/JHA kumoamisesta, tai tietotekniikkarikosyksiköiden päälliköistä koostuvaa Europolin työryhmää.

(25) Tavoitteidensa saavuttamiseksi viraston olisi oltava yhteydessä lainvalvontaelimiin ja tietosuojaviranomaisiin nostaakseen esiin tietoverkkorikollisuuden ehkäisemiseen liittyviä verkko- ja tietoturvanäkökohtia ja puuttuakseen niihin. Näiden viranomaisten edustajista olisi tultava viraston täysivaltaisia sidosryhmiä ja niiden olisi oltava edustettuina viraston pysyvässä sidosryhmässä.

(26) Verkko- ja tietoturvaongelmat ovat maailmanlaajuisia. Tarvitaan tiiviimpää kansainvälistä yhteistyötä, jotta voidaan parantaa tietoturvanormeja ja tiedonvaihtoa sekä edistää yhteistä maailmanlaajuista lähestymistapaa verkko- ja tietoturvakysymyksissä. Tätä varten viraston olisi tuettava yhteistyötä EU:n ulkopuolisten maiden ja kansainvälisten organisaatioiden kanssa tarvittaessa yhteistyössä Euroopan ulkosuhdehallinnon kanssa.

(27) Viraston tehtävien suorittaminen ei saisi vaikuttaa seuraavien elinten toimivaltaan eikä se saisi olla etusijalla niiden asiaa koskeviin toimivaltuuksiin ja tehtäviin nähden eikä estää näitä tai olla päällekkäistä näiden kanssa: sähköisiä viestintäverkkoja ja -palveluita koskevissa direktiiveissä tarkoitetut kansalliset sääntelyviranomaiset sekä Euroopan parlamentin ja neuvoston asetuksella (EY) N:o 1211/2009[27] perustettu Euroopan sähköisen viestinnän sääntelyviranomaisten yhteistyöelin (BEREC), direktiivissä 2002/21/EY tarkoitettu viestintäkomitea, eurooppalaiset standardointielimet, kansalliset standardointielimet, teknisiä standardeja ja määräyksiä ja tietoyhteiskunnan palveluja koskevia määräyksiä koskevien tietojen toimittamisessa noudatettavasta menettelystä 22 päivänä kesäkuuta 1998 annetulla Euroopan parlamentin ja neuvoston direktiivillä 98/34/EY[28] perustettu pysyvä komitea sekä jäsenvaltioiden valvontaviranomaiset, jotka käsittelevät yksilöiden suojelua henkilötietojen käsittelyssä ja näiden tietojen vapaata liikkuvuutta.

(28) Viraston toiminnan tuloksellisuuden varmistamiseksi jäsenvaltioiden ja komission olisi oltava edustettuina johtokunnassa, jonka 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, vahvistaa viraston työohjelma, vahvistaa työjärjestyksensä ja viraston sisäiset toimintasäännöt sekä nimittää pääjohtaja ja päättää tämän toimikauden jatkamisesta tai päättymisestä. Johtokunnan olisi voitava perustaa työryhmiä avukseen tehtäviensä hoidossa; ryhmät voisivat esimerkiksi laatia johtokunnan päätökset ja seurata niiden täytäntöönpanoa.

(29) Viraston asianmukainen toiminta edellyttää, että sen pääjohtaja nimitetään ansioiden ja todistuksin osoitettujen hallinnollisten ja johtamistaitojen sekä verkko- ja tietoturvan kannalta merkityksellisen pätevyyden ja kokemuksen perusteella ja että hänellä on tehtäviensä hoitamisessa täysi riippumattomuus viraston sisäisen toiminnan organisoinnissa. Tätä varten pääjohtajan olisi laadittava ehdotus viraston työohjelmaksi kuultuaan ensin komission yksiköitä ja toteutettava kaikki tarvittavat toimenpiteet varmistaakseen viraston työohjelman asianmukaisen toteutumisen. Hänen olisi luonnosteltava vuosittain johtokunnalle esitettävä yleiskertomus, laadittava esitys viraston tuloja ja menoja koskevaksi ennakkoarvioksi ja vastattava talousarvion toteuttamisesta.

(30) Pääjohtajan olisi voitava perustaa tilapäisiä työryhmiä erityisesti luonteeltaan tieteellisiä, teknisiä, oikeudellisia tai sosioekonomia erityiskysymyksiä varten. Tilapäisiä työryhmiä perustaessaan pääjohtajan olisi pyrittävä hankkimaan tarvittavaa ulkopuolista asiantuntemusta, jotta virastolla olisi käytettävissään viimeisin tieto kehittyvän tietoyhteiskunnan tietoturvahaasteista. Viraston olisi varmistettava, että

---

[27] EUVL L 337, 18.12.2009, s. 1.
[28] EYVL L 204, 21.7.1998, s. 37.

tilapäisten työryhmien jäsenet valitaan huippuasiantuntemuksen perusteella ja ottaen asianmukaisesti huomioon tarvittaessa tarkasteltavan kysymyksen edellyttämällä tavalla edustuksellinen tasapaino jäsenvaltioiden julkishallintojen, yksityisen sektorin, yritykset mukaan luettuina, käyttäjien ja tutkimusmaailmaa edustavien verkko- ja tietoturva-asiantuntijoiden välillä. Virasto voi tarpeen mukaan tapauskohtaisesti kutsua kyseisellä alalla päteviksi tunnustettuja yksittäisiä asiantuntijoita osallistumaan työryhmien toimintaan. Viraston olisi vastattava heille aiheutuvista kustannuksista sisäisten toimintasääntöjensä ja voimassa olevien varainhoitosäännösten mukaisesti.

(31) Virastolla olisi oltava neuvoa-antavana elimenä pysyvä sidosryhmä, jotta voitaisiin varmistaa säännöllinen yhteydenpito yksityisen sektorin, kuluttajajärjestöjen ja muiden asianmukaisten sidosryhmien kanssa. Pysyvän sidosryhmän, jonka johtokunta perustaa pääjohtajan ehdotuksesta, olisi keskityttävä kaikkia sidosryhmiä koskeviin asioihin ja saatettava ne viraston tietoon. Pääjohtaja voi tarvittaessa ja kokousten esityslistan mukaisesti kutsua Euroopan parlamentin ja muiden asianomaisten elinten edustajia osallistumaan ryhmän kokouksiin.

(32) Viraston on toiminnassaan noudatettava i) toissijaisuusperiaatetta varmistamalla riittävä jäsenvaltioiden välinen koordinointi verkko- ja tietoturvakysymyksissä sekä parantamalla kansallisten toimien vaikuttavuutta ja tuottamalla niille näin lisäarvoa ja ii) suhteellisuusperiaatetta, eli oltava ylittämättä sitä, mikä on tarpeen tässä asetuksessa säädettyjen tavoitteiden saavuttamiseksi.

(33) Viraston olisi sovellettava asianmukaista EU-lainsäädäntöä asiakirjojen julkisuuden osalta siten kuin siitä säädetään Euroopan parlamentin ja neuvoston asetuksessa (EY) N:o 1049/2001[29] ja yksilöiden suojelun osalta henkilötietojen käsittelyssä siten kuin siitä säädetään yksilöiden suojelusta yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta 18 päivänä joulukuuta 2000 annetussa Euroopan parlamentin ja neuvoston asetuksessa (EY) N:o 45/2001[30].

(34) Viraston olisi toimialansa ja tavoitteidensa puitteissa sekä tehtäviään suorittaessaan noudatettava erityisesti arkaluonteisten asiakirjojen käsittelyä koskevia EU:n toimielimiin sovellettavia määräyksiä ja kansallista lainsäädäntöä. Johtokunnalla olisi oltava valtuudet päättää viraston oikeudesta käsitellä turvaluokiteltua tietoa.

(35) Viraston täydellisen itsemääräämisoikeuden ja riippumattomuuden varmistamiseksi pidetään tarpeellisena antaa sille itsenäinen talousarvio, jonka tulot koostuvat ensisijaisesti EU:n rahoitusosuudesta ja viraston työhön osallistuvien EU:n ulkopuolisten maiden rahoitusosuuksista. Viraston isäntävaltion tai minkä tahansa muun jäsenvaltion olisi voitava maksaa vapaaehtoisia rahoitusosuuksia virastolle. EU:n talousarviomenettelyä sovelletaan edelleen Euroopan unionin yleisestä talousarviosta maksettaviin tukiin. Lisäksi tilintarkastustuomioistuimen olisi vastattava viraston tilintarkastuksesta.

---

[29] 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).

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

(36) Viraston olisi jatkettava asetuksella (EY) N:o 460/2004 perustetun ENISAn toimintaa. Eurooppa-neuvostossa 13 päivänä joulukuuta 2003 kokoontuneiden jäsenvaltioiden edustajien päätöksen puitteissa isäntäjäsenvaltion olisi ylläpidettävä ja kehitettävä nykyisiä käytännön järjestelyjä viraston sujuvan ja tehokkaan toiminnan varmistamiseksi. Tässä sen olisi erityisesti otettava huomioon viraston yhteistyö komission, jäsenvaltioiden ja niiden toimivaltaisten elinten, muiden unionin toimielinten ja elinten sekä julkisten ja yksityisten sidosryhmien kanssa kaikkialla Euroopassa sekä viraston näille tahoille antama apu.

(37) Virasto olisi perustettava rajatuksi kaudeksi. Sen toimintaa olisi arvioitava tulosten saavuttamisen ja toimintamenetelmien kannalta, jotta voidaan tarkastaa viraston tavoitteiden pysyvä asianmukaisuus ja päättää tältä pohjalta, olisiko sen toimintaa edelleen jatkettava,

OVAT HYVÄKSYNEET TÄMÄN ASETUKSEN:

1 JAKSO TOIMIALA, TAVOITTEET JA TEHTÄVÄT

1 artikla

Kohde ja soveltamisala

1. Tällä asetuksella perustetaan Euroopan verkko- ja tietoturvavirasto, jäljempänä 'virasto', jonka tarkoituksena on osaltaan varmistaa korkeatasoinen ja toimiva verkko- ja tietoturva unionissa, lisätä asiaa koskevaa tietoisuutta ja luoda yhteiskuntaan erityinen verkko- ja tietoturvakulttuuri, josta on hyötyä kansalaisille, kuluttajille, yrityksille ja julkisen sektorin organisaatioille unionissa, millä edistetään myös sisämarkkinoiden moitteetonta toimintaa.

2. Viraston tavoitteet ja tehtävät eivät rajoita verkko- ja tietoturvaa koskevaa jäsenvaltioiden toimivaltaa, eivätkä missään tapauksessa toimia, jotka koskevat yleistä turvallisuutta, puolustusta, valtion turvallisuutta (mukaan lukien valtion taloudellinen hyvinvointi silloin kun kyseessä ovat valtion turvallisuutta koskevat asiat) tai valtion toimia rikosoikeuden alalla.

3. "*Verkko- ja tietoturvalla*" tarkoitetaan tässä asetuksessa verkon tai tietojärjestelmän kykyä suojautua tietyllä varmuudella onnettomuuksilta tai laittomilta taikka ilkivaltaisilta toimilta, jotka vaarantavat tallennettujen tai siirrettävien tietojen ja niihin liittyvien verkoissa ja tietojärjestelmissä tarjottujen tai välitettävien palvelujen saatavuuden, aitouden, eheyden ja luottamuksellisuuden.

2 artikla

Tavoitteet

1. Virasto auttaa komissiota ja jäsenvaltioita täyttämään nykyisessä ja tulevassa unionin lainsäädännössä asetetut verkko- ja tietoturvaan liittyvät oikeudelliset ja sääntelylliset vaatimukset edesauttaen näin sisämarkkinoiden moitteetonta toimintaa.

2. Virasto parantaa unionin ja jäsenvaltioiden valmiuksia ehkäistä, havaita ja ratkaista verkko- ja tietoturvaongelmia ja -uhkia.

3. Virasto luo ja ylläpitää korkeatasoista asiantuntemusta ja käyttää tätä asiantuntemusta edistääkseen julkisen ja yksityisen sektorin toimijoiden välistä laajaa yhteistyötä.

3 artikla

Tehtävät

1. Edellä 1 kohdassa kuvattua tarkoitusta varten virasto hoitaa seuraavia tehtäviä:

a) avustaa komissiota pyynnöstä tai oma-aloitteisesti verkko- ja tietoturvapolitiikan kehittämisessä antamalla sille neuvoja ja lausuntoja ja laatimalla sille teknisiä ja sosioekonomisia analyyseja sekä valmistelevaa materiaalia unionin lainsäädännön kehittämiseksi ja ajantasaistamiseksi verkko- ja tietoturvan alalla,

b) helpottaa jäsenvaltioiden keskinäistä ja jäsenvaltioiden ja komission välistä yhteistyötä niiden pyrkiessä rajat ylittävissä asioissa ehkäisemään, havaitsemaan ja ratkaisemaan verkko- ja tietoturvaongelmia,

c) auttaa jäsenvaltioita ja EU:n toimielimiä ja muita elimiä keräämään, analysoimaan ja levittämään verkko- ja tietoturvaan liittyvää tietoa,

d) arvioi säännöllisesti yhteistyössä jäsenvaltioiden ja EU:n toimielinten kanssa verkko- ja tietoturvan tilaa Euroopassa,

e) tukee toimivaltaisten julkisten elinten yhteistyötä Euroopassa ja erityisesti niiden pyrkimyksiä kehittää hyviä käytänteitä ja normeja ja vaihtaa tietoa näistä,

f) auttaa unionia ja jäsenvaltioita edistämään riskinhallinnan ja tietoturvan hyviä käytänteitä ja normeja sähköisissä tuotteissa, järjestelmissä ja palveluissa,

g) tukee julkisen ja yksityisen sektorin sidosryhmien yhteistyötä unionin tasolla muun muassa edistämällä tiedonvaihtoa ja tietoisuuden lisäämistä ja helpottamalla niiden pyrkimyksiä kehittää ja ottaa käyttöön normeja riskinhallintaa ja sähköisten tuotteiden, verkkojen ja palvelujen tietoturvaa varten,

h) helpottaa vuoropuhelua ja tiedonvaihtoa verkko- ja tietoturvaa, mukaan luettuina tietoverkkorikollisuuden torjuntaan liittyvät näkökohdat, koskevista hyvistä käytänteistä julkisen ja yksityisen sektorin sidosryhmien keskuudessa; avustaa komissiota sellaisen politiikan kehittämisessä, jossa otetaan huomioon tietoverkkorikollisuuden torjunnan verkko- ja tietoturvanäkökohdat,

i) avustaa pyynnöstä jäsenvaltioita ja EU:n toimielimiä ja muita elimiä niiden pyrkimyksissä kehittää verkko- ja tietoturvaan liittyviä havaitsemis-, analysointi- ja reagointivalmiuksia,

j) tukee unionin vuoropuhelua ja yhteistyötä EU:n ulkopuolisten maiden ja kansainvälisten organisaatioiden kanssa tarvittaessa yhteistyössä Euroopan ulkosuhdehallinnon kanssa kansainvälisen yhteistyön edistämiseksi ja yhteisen globaalin lähestymistavan luomiseksi verkko- ja tietoturvakysymyksissä,

k) hoitaa sille unionin lainsäädännössä annettuja tehtäviä.

2 JAKSO ORGANISAATIO

4 artikla

Viraston elimet

Virastoon kuuluu:

a) johtokunta,

b) pääjohtaja ja henkilöstö ja

c) pysyvä sidosryhmä.

5 artikla

Johtokunta

1. Johtokunta määrittelee viraston toiminnan yleisen suunnan ja varmistaa, että se toimii tässä asetuksessa säädettyjen sääntöjen ja periaatteiden mukaisesti. Se huolehtii myös viraston toiminnan johdonmukaisuudesta suhteessa jäsenvaltioiden toimintaan sekä unionin tason toimiin.

2. Johtokunta vahvistaa työjärjestyksensä asiaan liittyvien komission yksiköiden suostumuksella.

3. Johtokunta vahvistaa viraston sisäiset toimintasäännöt asiaan liittyvien komission yksiköiden suostumuksella. Säännöt on julkistettava.

4. Johtokunta nimittää pääjohtajan 10 artiklan 2 kohdan mukaisesti ja voi erottaa tämän. Johtokunnalla on pääjohtajaan nähden kurinpidollinen toimivalta.

5. Johtokunta vahvistaa viraston työohjelman 13 artiklan 3 kohdan mukaisesti ja edeltävän vuoden yleiskertomuksen viraston toiminnasta 14 artiklan 2 kohdan mukaisesti.

6. Johtokunta vahvistaa virastoon sovellettavat varainhoitosäännöt. Säännökset voivat poiketa Euroopan yhteisöjen yleiseen talousarvioon sovellettavasta varainhoitoasetuksesta annetun neuvoston asetuksen (EY, Euratom) N:o 1605/2002 185 artiklassa tarkoitettuja elimiä koskevasta varainhoidon puiteasetuksesta 23 päivänä joulukuuta 2002 annetusta komission asetuksesta (EY, Euratom) N:o 2343/2002[31] ainoastaan, jos viraston toiminta sitä nimenomaisesti vaatii ja jos komissio on antanut siihen etukäteen suostumuksensa.

7. Johtokunta antaa yhteisymmärryksessä komission kanssa tarvittavat soveltamissäännöt henkilöstösääntöjen 110 artiklan mukaisesti.

8. Johtokunta voi perustaa jäsenistään koostuvia työryhmiä avustamaan sitä tehtävien suorittamisessa, kuten päätösten valmistelussa ja niiden täytäntöönpanon seurannassa.

---

[31] EYVL L 357, 31.12.2002, s. 72.

9. *Johtokunta voi vahvistaa monivuotisen henkilöstösuunnitelman kuultuaan komission yksiköitä ja ilmoitettuaan siitä asianmukaisesti budjettivallan käyttäjälle.*

6 artikla

Johtokunnan kokoonpano

1. Johtokuntaan kuuluu yksi edustaja kustakin jäsenvaltiosta, kolme komission nimittämää edustajaa sekä kolme sellaista niin ikään komission nimittämää edustajaa, joilla ei ole äänioikeutta ja joista kukin edustaa yhtä seuraavista ryhmistä:

a) tieto- ja viestintätekniikkatoimiala,

b) kuluttajajärjestöt,

c) akateemiset verkko- ja tietoturva-asiantuntijat.

2. Johtokunnan jäsenet ja heidän sijaisensa nimitetään verkko- ja tietoturva-alaa koskevan kokemuksen ja asiantuntemuksen perusteella.

3. Edellä 1 kohdan a, b ja c kohdassa tarkoitettujen ryhmien edustajien toimikausi on neljä vuotta. Tätä toimikautta voidaan jatkaa kerran. Edustajan luopuessa sidosryhmän jäsenyydestä komissio nimittää hänelle korvaajan.

7 artikla

Johtokunnan puheenjohtaja

Johtokunta valitsee keskuudestaan puheenjohtajan ja varapuheenjohtajan kolmen vuoden toimikaudeksi, joka voidaan uusia. Varapuheenjohtaja toimii ilman eri toimenpiteitä puheenjohtajan sijaisena tämän ollessa estynyt.

8 artikla

Kokoukset

1. Johtokunta kokoontuu puheenjohtajansa kutsusta.

2. Johtokunta kokoontuu sääntömääräiseen istuntoon kahdesti vuodessa. Johtokunta kokoontuu myös ylimääräisiin istuntoihin puheenjohtajan aloitteesta tai jos vähintään kolmasosa sen äänioikeutetuista jäsenistä sitä pyytää.

3. Pääjohtaja osallistuu johtokunnan kokouksiin ilman äänioikeutta.

9 artikla

Äänestäminen

1. Johtokunta tekee päätöksensä äänioikeutettujen jäsentensä enemmistöllä.

2. Työjärjestyksen, viraston sisäisten toimintasääntöjen, talousarvion ja vuosittaisen työohjelman hyväksyminen sekä pääjohtajan nimittäminen, toimikauden jatkaminen ja erottaminen edellyttävät kaikkien johtokunnan äänioikeutettujen jäsenten kahden kolmasosan enemmistöä.

10 artikla

Pääjohtaja

1. Virastoa johtaa sen pääjohtaja, joka hoitaa tehtäväänsä riippumattomasti.

2. Pääjohtajan nimittää ja vapauttaa tehtävistään johtokunta. Nimitys tapahtuu komission ehdottamasta ehdokasluettelosta viiden vuoden kaudeksi ansioiden ja todistuksin osoitettujen hallinnollisten ja johtamistaitojen sekä erityisen pätevyyden ja kokemuksen perusteella. Johtokunnan valitsema ehdokas voidaan ennen nimittämistä kutsua antamaan lausuntonsa Euroopan parlamentin toimivaltaiselle valiokunnalle ja vastaamaan sen jäsenten esittämiin kysymyksiin.

3. Toimikauden päättymistä edeltävien yhdeksän kuukauden aikana komissio suorittaa arvioinnin. Arvioinnissa komissio tarkastelee erityisesti

– pääjohtajan saavuttamia tuloksia

– viraston tehtäviä ja siihen kohdistuvia vaatimuksia lähivuosina.

4. Johtokunta voi komission ehdotuksesta ja ottaen huomioon arviointikertomuksen jatkaa pääjohtajan toimikautta enintään kolmella vuodella ja ainoastaan niissä tapauksissa, joissa tämä on viraston tehtävien ja vaatimusten kannalta perusteltua.

5. Johtokunnan on ilmoitettava Euroopan parlamentille aikeestaan jatkaa pääjohtajan toimikautta. Pääjohtaja voidaan toimikauden jatkamista edeltävän kuukauden aikana kutsua antamaan lausuntonsa Euroopan parlamentin toimivaltaiselle valiokunnalle ja vastaamaan sen jäsenten esittämiin kysymyksiin.

6. Jos toimikautta ei jatketa, pääjohtaja jatkaa tehtävässään seuraajan nimittämiseen asti.

7. Pääjohtajan tehtävänä on:

a) viraston päivittäinen hallinto

b) työohjelmien ja johtokunnan tekemien päätösten täytäntöönpano

c) sen varmistaminen, että virasto toimii sen palvelujen käyttäjien vaatimusten mukaisesti erityisesti tarjottujen palvelujen tarkoituksenmukaisuuden osalta

d) vastata kaikista henkilöstöasioista varmistaen, että johtokunnan asettamia yleisiä suuntaviivoja ja sen tekemiä yleisluontoisia päätöksiä noudatetaan

e) yhteyksien luominen ja ylläpito EU:n toimielimiin ja muihin elimiin

f) yhteyksien luominen ja ylläpitäminen liikemaailmaan ja kuluttajajärjestöihin säännöllisen vuoropuhelun varmistamiseksi asiaankuuluvien sidosryhmien kanssa

g) muiden hänelle tällä asetuksella osoitettujen tehtävien hoito.

8. Tarpeen vaatiessa ja viraston tavoitteiden ja tehtävien puitteissa pääjohtaja voi perustaa asiantuntijoista koostuvia tilapäisiä työryhmiä. Tästä on ilmoitettava etukäteen johtokunnalle. Menettelyt, jotka koskevat erityisesti tilapäisten työryhmien kokoonpanoa, pääjohtajan suorittamaa asiantuntijoiden nimeämistä ja työryhmien toimintaa, on vahvistettava viraston sisäisissä toimintasäännöissä.

9. Pääjohtajan on tarvittaessa asetettava johtokunnan käyttöön hallinnollista tukihenkilöstöä ja muita resursseja.

11 artikla

Pysyvä sidosryhmä

1. Johtokunta perustaa pääjohtajan ehdotuksesta pysyvän sidosryhmän, joka koostuu asiaan liittyvien sidosryhmien, kuten tieto- ja viestintäteknologiatoimialan, kuluttajajärjestöjen, verkko- ja tietoturva-alan akateemisten asiantuntijoiden sekä lainvalvonta- ja tietosuojaviranomaisten, edustajista.

2. Menettelyt, jotka koskevat erityisesti ryhmän jäsenten lukumäärää, sen kokoonpanoa, johtokunnan suorittamaa ryhmän jäsenten nimeämistä, pääjohtajan ehdotusta sekä ryhmän toimintaa, on määriteltävä viraston sisäisissä toimintasäännöissä ja ne on julkistettava.

3. Ryhmän puheenjohtajana toimii pääjohtaja.

4. Ryhmän jäsenten toimikausi on kaksi ja puoli vuotta. Johtokunnan jäsenet eivät saa olla ryhmän jäseniä. Komission henkilöstöllä on oikeus olla läsnä ryhmän kokouksissa ja osallistua sen työhön.

5. Ryhmä neuvoo virastoa sen tehtävien hoidossa. Erityisesti ryhmä neuvoo pääjohtajaa tämän laatiessa ehdotusta viraston työohjelmaksi sekä yhteydenpidossa asianmukaisten sidosryhmien kanssa työohjelmaan liittyvissä kysymyksissä.

3 JAKSO TOIMINTA

12 artikla

Työohjelma

1. Viraston on toimittava noudattaen työohjelmaansa, jonka on sisällettävä kaikki sen suunniteltu toiminta. Työohjelma ei estä virastoa ryhtymästä ennakoimattomiin toimiin tavoitteidensa, tehtäviensä ja talousarvionsa puitteissa. Pääjohtajan on tiedotettava johtokunnalle viraston toimista, jotka eivät sisälly työohjelmaan.

2. Pääjohtaja vastaa viraston työohjelmaluonnoksen laatimisesta kuultuaan komission yksiköitä. Pääjohtajan on joka vuosi ennen 15 päivää maaliskuuta toimitettava seuraavan vuoden työohjelmaluonnos johtokunnalle.

3. Johtokunta hyväksyy komission yksiköitä kuullen kunkin vuoden marraskuun 30 päivään mennessä viraston työohjelman seuraavaa vuotta varten. Työohjelmaan on sisällyttävä

monivuotinen ennakoiva katsaus. Johtokunnan on varmistettava, että työohjelma on viraston tavoitteiden sekä unionin verkko- ja tietoturva-alan lainsäädännön ja politiikan painopisteiden mukainen.

4. Työohjelma on laadittava toimintoperusteisen johtamisen periaatteiden mukaisesti. Työohjelman on oltava viraston kyseisen varainhoitovuoden tuloja ja menoja koskevan ennakkoarvioesityksen ja talousarvion mukainen.

5. Johtokunnan hyväksyttyä työohjelman pääjohtaja toimittaa sen Euroopan parlamentille, neuvostolle, komissiolle ja jäsenvaltioille sekä julkistaa sen.

13 artikla

Yleiskertomus

1. Pääjohtaja toimittaa vuosittain johtokunnalle yleiskertomusluonnoksen, joka kattaa kaiken viraston toiminnan edellisenä vuonna.

2. Johtokunta hyväksyy ennen kunkin vuoden maaliskuun 31 päivää yleiskertomuksen viraston toiminnasta edellisenä vuonna.

3. Johtokunnan hyväksyttyä yleiskertomuksen pääjohtaja toimittaa sen Euroopan parlamentille, neuvostolle, komissiolle, tilintarkastustuomioistuimelle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle sekä julkistaa sen.

14 artikla

Virastolle esitettävät pyynnöt

1. Viraston tavoitteiden ja tehtävien piiriin kuuluvat neuvonta- ja avustamispyynnöt on osoitettava pääjohtajalle, ja niihin on liitettävä taustatiedot, joista selviää, mistä asiassa on kyse. Pääjohtaja ilmoittaa johtokunnalle saaduista pyynnöistä ja pyyntöjen johdosta toteutetuista toimenpiteistä. Jos virasto torjuu pyynnön, sen on perusteltava päätöksensä.

2. Edellä 1 kohdassa tarkoitettuja pyyntöjä voivat esittää:

a) Euroopan parlamentti

b) neuvosto

c) komissio

d) kaikki jäsenvaltioiden nimeämät toimivaltaiset elimet, kuten direktiivin 2002/21/EY 2 artiklassa määritellyt kansalliset sääntelyviranomaiset.

3. Johtokunta vahvistaa viraston sisäisissä toimintasäännöissä 1 ja 2 kohdan soveltamista koskevat käytännön järjestelyt erityisesti virastolle osoitettujen pyyntöjen esittämisen, tärkeysjärjestykseen asettamisen ja seurannan sekä johtokunnalle tiedottamisen osalta.

15 artikla

Etunäkökohtia koskeva ilmoitus

1. Pääjohtajan sekä niiden toimihenkilöiden, jotka on otettu palvelukseen jäsenvaltioiden väliaikaisesti lähettäminä virkamiehinä, on tehtävä sitoumuksistaan ja etunäkökohdistaan kirjallinen ilmoitus, jossa he toteavat, ettei heidän riippumattomuuttaan mahdollisesti vaarantavia välittömiä tai välillisiä etunäkökohtia ole.

2. Tilapäisiin työryhmiin osallistuvien ulkopuolisten asiantuntijoiden on ilmoitettava kussakin kokouksessa mahdolliset etunäkökohdat, jotka saattavat vaarantaa heidän riippumattomuutensa kokouksen esityslistalla olevien kohtien suhteen, sekä pidättäydyttävä osallistumasta kyseisiä kohtia koskevaan keskusteluun.

16 artikla

Läpinäkyvyys

1. Viraston on varmistettava, että sen toiminta on mahdollisimman avointa sekä 13 ja 14 artiklan mukaista.

2. Virasto varmistaa, että yleisölle ja kaikille asianomaisille osapuolille annetaan tarvittaessa puolueetonta ja luotettavaa tietoa, joka on helposti saatavissa, varsinkin jos on kyse viraston työn tuloksia koskevasta tiedosta. Sen on myös julkistettava pääjohtajan ja niiden toimihenkilöiden, jotka on otettu palvelukseen jäsenvaltioiden väliaikaisesti lähettäminä virkamiehinä, etunäkökohtia koskevat ilmoitukset sekä asiantuntijoiden etunäkökohtia koskevat ilmoitukset tilapäisten työryhmien kokousten esityslistalla olevien kohtien suhteen.

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

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

17 artikla

Luottamuksellisuus

1. Virasto ei saa paljastaa kolmansille osapuolille käsittelemäänsä ja saamaansa sellaista tietoa, jolle on pyydetty luottamuksellista käsittelyä, sanotun kuitenkaan rajoittamatta 14 artiklan soveltamista.

2. Johtokunnan jäsenet, pääjohtaja, pysyvän sidosryhmän jäsenet, tilapäisiin työryhmiin osallistuvat ulkopuoliset asiantuntijat sekä viraston muu henkilöstö, mukaan lukien ne toimihenkilöt, jotka on otettu palvelukseen jäsenvaltioiden väliaikaisesti lähettäminä virkamiehinä, ovat myös tehtäviensä päätyttyä perussopimuksen 339 artiklan mukaisten salassapitovelvollisuutta koskevien vaatimusten alaisia.

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

4. Johtokunta voi päättää antaa virastolle luvan käsitellä turvaluokiteltua tietoa. Tässä tapauksessa johtokunnan on yhteisymmärryksessä asianomaisten komission yksiköiden kanssa vahvistettava sisäiset toimintasäännöt soveltaen tietoturvaperiaatteita, jotka sisältyvät komission sisäisten menettelysääntöjen muuttamisesta 29 päivänä marraskuuta 2001 tehtyyn komission päätökseen 2001/844/EY, EHTY, Euratom[32]. Tämä koskee muun muassa turvaluokiteltujen tietojen vaihtamista, käsittelyä ja tallentamista.

18 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 perussopimuksen 228 artiklan nojalla tai nostaa kanne Euroopan unionin tuomioistuimessa perussopimuksen 263 artiklan nojalla.

4 JAKSO VARAINHOITOA KOSKEVAT SÄÄNNÖKSET

19 artikla

Talousarvion vahvistaminen

1. Viraston tulot koostuvat Euroopan unionin talousarviosta saatavasta rahoitusosuudesta, viraston työhön 29 artiklan mukaisesti osallistuvien kolmansien maiden rahoitusosuuksista ja jäsenvaltioiden rahoitusosuuksista.

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

3. Pääjohtaja laatii vuosittain 1 päivään maaliskuuta mennessä esityksen viraston seuraavan varainhoitovuoden tuloja ja menoja koskevaksi ennakkoarvioksi ja toimittaa sen sekä siihen liitetyn henkilöstötaulukkoehdotuksen johtokunnalle.

4. Tulojen ja menojen on oltava tasapainossa.

5. Johtokunta laatii pääjohtajan laatiman tuloja ja menoja koskevan ennakkoarvioesityksen pohjalta vuosittain viraston tulo- ja menoarvion seuraavaa varainhoitovuotta varten.

6. Johtokunta toimittaa 31 päivään maaliskuuta mennessä tämän arvion, johon sisältyy henkilöstötaulukkoehdotus ja työohjelmaluonnos, komissiolle ja niille valtioille, joiden kanssa Euroopan unioni on tehnyt 24 artiklassa tarkoitetut sopimukset.

---

[32] EYVL L 317, 3.12.2001, s. 1.

7. Komissio toimittaa arvion Euroopan parlamentille ja neuvostolle, jäljempänä yhteisesti 'budjettivallan käyttäjä', yhdessä Euroopan unionin yleistä talousarviota koskevan esityksen kanssa.

8. Komissio ottaa Euroopan unionin yleistä talousarviota koskevaan esitykseen kyseiseen ennakkoarvioon perustuvat arviot, joita se pitää henkilöstötaulukon ja yleisestä talousarviosta suoritettavan avustuksen määrän osalta välttämättöminä, ja toimittaa alustavan talousarvioesityksen budjettivallan käyttäjälle perussopimuksen 314 artiklan mukaisesti.

9. Budjettivallan käyttäjä hyväksyy virastolle annettavaa avustusta koskevat määrärahat.

10. Budjettivallan käyttäjä vahvistaa viraston henkilöstötaulukon.

11. Johtokunta vahvistaa työohjelman ohella viraston talousarvion. Siitä tulee lopullinen, kun Euroopan unionin yleinen talousarvio on lopullisesti vahvistettu. Johtokunta mukauttaa tarvittaessa viraston talousarviota ja työohjelmaa Euroopan unionin yleisen talousarvion mukaisesti. Johtokunta toimittaa sen viipymättä komissiolle ja budjettivallan käyttäjälle.

20 artikla

Petostentorjunta

1. Petosten, lahjonnan ja muun laittoman toiminnan torjumiseksi virastoon sovelletaan rajoituksetta Euroopan petostentorjuntaviraston (OLAF) tutkimuksista 25 päivänä toukokuuta 1999 annettua Euroopan parlamentin ja neuvoston asetusta (EY) N:o 1073/1999[33].

2. Virasto liittyy Euroopan petostentorjuntaviraston (OLAF) sisäisistä tutkimuksista 25 päivänä toukokuuta 1999 tehtyyn Euroopan parlamentin, Euroopan unionin neuvoston ja Euroopan yhteisöjen komission tekemään toimielinten väliseen sopimukseen[34] ja antaa viipymättä asiaan liittyvät määräykset, jotka koskevat kaikkia viraston työntekijöitä.

21 artikla

Talousarvion toteuttaminen

1. Pääjohtaja huolehtii viraston talousarvion toteuttamisesta.

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

3. Viraston tilinpitäjä toimittaa alustavan tilinpäätöksen ja selvityksen varainhoitovuoden talousarvio- ja varainhallinnosta komission tilinpitäjälle seuraavan varainhoitovuoden maaliskuun 1 päivään mennessä. Komission tilinpitäjä konsolidoi toimielinten ja hajautettujen elinten alustavat tilinpäätökset Euroopan yhteisöjen yleiseen talousarvioon sovellettavasta varainhoitoasetuksesta 25 päivänä kesäkuuta 2002 annetun neuvoston asetuksen (EY, Euratom) N:o 1605/2002[35], jäljempänä 'yleinen varainhoitoasetus', 128 artiklan mukaisesti.

---

33 EYVL L 136, 31.5.1999, s. 1.
34 EYVL L 136, 31.5.1999, s. 15.
35 EYVL L 248, 16.9.2002, s. 1.

4. Komission tilinpitäjä toimittaa viraston alustavan tilinpäätöksen ja selvityksen varainhoitovuoden talousarvio- ja varainhallinnosta tilintarkastustuomioistuimelle viimeistään kunkin varainhoitovuoden päättymistä seuraavan maaliskuun 31 päivänä. Selvitys varainhoitovuoden talousarvio- ja varainhallinnosta toimitetaan myös budjettivallan käyttäjälle.

5. Saatuaan tilintarkastustuomioistuimelta yleisen varainhoitoasetuksen 129 artiklassa tarkoitetut huomautukset viraston alustavasta tilinpäätöksestä pääjohtaja laatii viraston lopullisen tilinpäätöksen, josta hän vastaa, ja toimittaa sen johtokunnalle lausuntoa varten.

6. Johtokunta antaa lausunnon viraston lopullisesta tilinpäätöksestä.

7. Pääjohtaja toimittaa viimeistään kutakin varainhoitovuotta seuraavan vuoden heinäkuun 1 päivänä lopullisen tilinpäätöksen ja johtokunnan lausunnon Euroopan parlamentille, neuvostolle, komissiolle ja tilintarkastustuomioistuimelle.

8. Pääjohtaja julkistaa lopullisen tilinpäätöksen.

9. Pääjohtaja lähettää tilintarkastustuomioistuimelle vastauksen sen huomautuksiin 30 päivään syyskuuta mennessä. Hän lähettää tämän vastauksen myös johtokunnalle.

10. Pääjohtaja antaa yleisen varainhoitoasetuksen 146 artiklan 3 kohdan mukaisesti Euroopan parlamentille tämän pyynnöstä kaikki kyseistä varainhoitovuotta koskevan vastuuvapausmenettelyn moitteettoman toteuttamisen edellyttämät tiedot.

11. Euroopan parlamentti myöntää neuvoston suosituksesta pääjohtajalle vuoden N+2 huhtikuun 30 päivään mennessä vuoden N talousarvion toteuttamista koskevan vastuuvapauden.

5 JAKSO YLEISET SÄÄNNÖKSET

22 artikla

Oikeudellinen asema

1. Virasto on unionin elin. Se on oikeushenkilö.

2. Virastolla on kussakin jäsenvaltiossa laajin oikeushenkilölle kansallisen lainsäädännön mukaan kuuluva oikeuskelpoisuus. Se voi erityisesti hankkia ja luovuttaa irtainta ja kiinteää omaisuutta sekä esiintyä kantajana ja vastaajana oikeudenkäynneissä.

3. Pääjohtaja edustaa virastoa.

23 artikla

Henkilöstö

1. Viraston henkilöstöön, pääjohtaja mukaan luettuna, sovelletaan Euroopan unionin virkamiehiin ja muuhun henkilöstöön sovellettavia sääntöjä ja määräyksiä.

2. Johtokunta käyttää pääjohtajan suhteen niitä valtuuksia, jotka kuuluvat nimittävälle viranomaiselle henkilöstösääntöjen mukaan ja sopimusten tekemiseen toimivaltaiselle viranomaiselle palvelussuhteen ehtojen mukaan.

3. Pääjohtaja käyttää viraston henkilöstön suhteen niitä valtuuksia, jotka kuuluvat nimittävälle viranomaiselle henkilöstösääntöjen mukaan ja sopimusten tekemiseen toimivaltaiselle viranomaiselle palvelussuhteen ehtojen mukaan.

4. Virasto voi ottaa palvelukseensa jäsenvaltioista tilapäisesti lähetettyjä kansallisia asiantuntijoita. Virasto vahvistaa sisäisissä toimintasäännöissään käytännön järjestelyt tätä varten.

24 artikla

Erioikeudet ja vapaudet

Virastoon ja sen henkilöstöön sovelletaan Euroopan yhteisöjen erioikeuksia ja vapauksia koskevaa pöytäkirjaa.

25 artikla

Vastuu

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

Euroopan unionin tuomioistuimella on toimivalta antaa ratkaisu viraston tekemässä sopimuksessa mahdollisesti olevan välityslausekkeen nojalla.

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

Euroopan unionin tuomioistuimella on tuomiovalta tällaisten vahinkojen korvaamista koskevissa riidoissa.

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

26 artikla

Kielet

1. Virastoon sovelletaan säännöksiä, jotka on vahvistettu Euroopan talousyhteisössä käytettäviä kieliä koskevista järjestelyistä 15 päivänä huhtikuuta 1958 annetussa asetuksessa N:o 1[36]. Jäsenvaltiot ja niiden nimeämät muut elimet voivat kääntyä viraston puoleen ja saada siltä vastauksen valitsemallaan Euroopan unionin kielellä.

---

[36] EYVL L 17, 6.10.1958, s. 385/58. Asetus sellaisena kuin se on muutettuna vuoden 1994 liittymisasiakirjalla.

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

27 artikla

Henkilötietojen suoja

Kun virasto käsittelee henkilöihin liittyviä tietoja, sen on noudatettava asetuksen (EY) N:o 45/2001 säännöksiä.

28 artikla

Kolmansien maiden osallistuminen

1. Viraston toimintaan voivat osallistua ne kolmannet maat, jotka ovat tehneet Euroopan unionin kanssa sopimuksen, jonka mukaisesti ne ovat saattaneet voimaan tämän asetuksen soveltamisalaan kuuluvan unionin lainsäädännön ja soveltavat sitä.

2. Näiden sopimusten asianomaisten määräysten nojalla tehdään järjestelyjä, joissa täsmennetään erityisesti, miten laajasti ja millä tavoin nämä maat osallistuvat viraston toimintaan, sekä vahvistetaan määräykset, jotka koskevat osallistumista viraston toteuttamiin aloitteisiin, rahoitusosuuksia ja henkilöstöä.

6 JAKSO LOPPUSÄÄNNÖKSET

29 artikla

Arviointi

1. Komissio suorittaa kolmen vuoden kuluessa 34 artiklassa tarkoitetusta perustamispäivästä kaikkien asianomaisten sidosryhmien näkemykset huomioon ottaen sekä johtokunnan kanssa sovittujen perusteiden mukaisesti tätä asetusta koskevan arvioinnin. Arvioinnissa tarkastellaan viraston vaikuttavuutta ja tuloksellisuutta 2 artiklassa kuvattujen tavoitteiden saavuttamisessa sekä viraston toimintatapojen tehokkuutta. Komissio toteuttaa tämän arvioinnin erityisesti voidakseen todeta, onko virasto edelleen tuloksellinen toimintaväline ja olisiko viraston toimintaa jatkettava 34 artiklassa tarkoitetun toimikauden jälkeen.

2. Komissio toimittaa Euroopan parlamentille ja neuvostolle arvioinnin tulokset, ja ne julkistetaan.

3. Arviointi toimitetaan johtokunnalle, joka antaa tämän asetuksen, viraston ja sen toimintatapojen muuttamista koskevia suosituksia komissiolle. Johtokunnan ja pääjohtajan on otettava arvioinnin tulokset huomioon viraston monivuotissuunnitelmissa.

30 artikla

Yhteistyö isäntävaltion kanssa

Viraston isäntävaltion on huolehdittava siitä, että virastolla on parhaat mahdolliset toimintaedellytykset.

31 artikla

Hallinnollinen valvonta

Viraston toiminta kuuluu oikeusasiamiehen valvonnan alaisuuteen perussopimuksen 228 artiklan mukaisesti.

32 artikla

Kumoaminen ja seuraanto

1. Kumotaan asetus (EY) N:o 460/2004.

Viittaukset asetukseen (EY) N:o 460/2004 ja ENISAan katsotaan viittauksiksi tähän asetukseen ja virastoon.

2. Virasto toimii kaikkien omistusten, sopimusten, oikeudellisten velvoitteiden, työsopimusten, taloudellisten sitoumusten ja vastuiden osalta asetuksella (EY) N:o 460/2004 perustetun viraston seuraajana.

33 artikla

Kesto

Virasto perustetaan […] alkavaksi viiden vuoden kaudeksi.

34 artikla

Voimaantulo

Tämä asetus tulee voimaan sitä päivää seuraavana päivänä, jona se on julkaistu *Euroopan unionin virallisessa lehdessä*, ja sitä sovelletaan 14 päivästä maaliskuuta 2012 tai sen julkaisemista seuraavasta päivästä sen mukaan, kumpi näistä ajankohdista on myöhäisempi.

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

Tehty […],

Euroopan parlamentin puolesta	*Neuvoston puolesta*
Puhemies	*Puheenjohtaja*

SÄÄDÖSEHDOTUKSEEN LIITTYVÄ RAHOITUSSELVITYS

1. PERUSTIEDOT EHDOTUKSESTA/ALOITTEESTA

1.1. Ehdotuksen/aloitteen nimi

Ehdotus Euroopan parlamentin ja neuvoston asetukseksi Euroopan verkko- ja tietoturvavirastosta (ENISA)

1.2. Toimintalohko(t) toimintoperusteisessa johtamis- ja budjetointijärjestelmässä (ABM/ABB)[37]

Tietoyhteiskunta ja viestimet

Digitaalistrategian sääntelykehys

1.3. Ehdotuksen/aloitteen luonne

☐ Ehdotus/aloite liittyy **uuteen toimeen**.

☐ Ehdotus/aloite liittyy **uuteen toimeen, joka perustuu pilottihankkeeseen tai valmistelutoimeen**[38].

☑ Ehdotus/aloite liittyy **käynnissä olevan toimen jatkamiseen**.

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

1.4. Tavoitteet

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

Sääntelyperiaatteiden johdonmukaisuus – ohjeiden ja neuvojen antaminen komissiolle ja jäsenvaltioille kokonaisvaltaisten ja normatiivisten puitteiden ajantasaistamiseksi ja kehittämiseksi verkko- ja tietoturvan alalla.

Ennaltaehkäisy, havaitseminen ja reagointi – valmistautuneisuusasteen parantaminen kehittämällä eurooppalaisia varhaisvaroitus- ja reagointivalmiuksia, yleiseurooppalaisia varasuunnitelmia ja harjoituksia.

Tiedon tuottaminen päätöksentekijöille – avun ja neuvonnan tarjoaminen komissiolle ja jäsenvaltioille osaamistason parantamiseksi koko unionissa verkko- ja tietoturvaan ja sen toteuttamiseen sidosryhmien keskuudessa liittyvissä kysymyksissä. Tähän sisältyy myös sellaisen tiedon luominen, analysointi ja levittäminen, joka koskee verkko- ja tietoturvaloukkausten taloudellisia näkökohtia ja vaikutuksia, sidosryhmien kannustimia investoida verkko- ja tietoturvatoimiin, riskien tunnistamista, verkko- ja tietoturvan tilaa unionissa koskevia indikaattoreita jne.

---

37 ABM: toimintoperusteinen johtaminen; ABB: toimintoperusteinen budjetointi.

38 Sellaisina kuin nämä on määritelty varainhoitoasetuksen 49 artiklan 6 kohdan a ja b alakohdassa.

Sidosryhmien valtaistaminen – tietoturva- ja riskinhallintakulttuurin kehittäminen edistämällä julkisen ja yksityisen sektorin toimijoiden välistä tiedonvaihtoa ja laajaa yhteistyötä, myös kansalaisten suoraksi hyödyksi ja verkko- ja tietoturvatietoisuuden kulttuurin luomiseksi.

Euroopan suojaaminen kansainvälisiltä uhkilta – korkeatasoisen yhteistyön aikaansaaminen EU:n ulkopuolisten maiden ja kansainvälisten organisaatioiden kanssa, jotta voidaan edistää yhteisiä maailmanlaajuisia verkko- ja tietoturvaperiaatteita ja lisätä korkean tason kansainvälisten aloitteiden vaikuttavuutta Euroopassa.

Kohti yhteistyöpohjaista täytäntöönpanoa – yhteistoiminnan helpottaminen verkko- ja tietoturvapolitiikan toteuttamisessa.

Tietoverkkorikollisuuden torjunta – tietoverkkorikollisuuden verkko- ja tietoturvanäkökohtien sisällyttäminen julkisen ja yksityisen sektorin sidosryhmien keskusteluihin ja tiedonvaihtoon hyvistä käytänteistä, erityisesti yhteistyössä aiemmin toisen ja kolmannen pilarin piiriin kuuluneiden viranomaisten, kuten Europolin, kanssa.

1.4.2. Erityistavoite (erityistavoitteet) sekä toiminto (toiminnot) toimintoperusteisessa johtamis- ja budjetointijärjestelmässä

Erityistavoite

Parannetaan verkko- ja tietoturvaa, luodaan verkko- ja tietoturvakulttuuri kansalaisten, kuluttajien, yritysten ja julkisen sektorin organisaatioiden hyödyksi sekä yksilöidään tulevaisuuden verkkojen ja internetin myötä esiin nousevia poliittisia haasteita.

Toiminto (toiminnot) toimintoperusteisessa johtamis- ja budjetointijärjestelmässä

Sähköistä viestintää koskeva politiikka ja verkkoturvallisuus

1.4.3. Odotettavissa olevat tulokset ja vaikutukset

Aloitteella odotetaan olevan seuraavanlaisia taloudellisia vaikutuksia:

- saatavilla on enemmän tietoa tietoturvaan ja uhkilta suojautumiseen liittyvistä nykyisistä ja tulevista haasteista ja riskeistä

- kunkin yksittäisen jäsenvaltion harjoittamassa tiedonkeruussa riskeistä, uhkista ja haavoittuvuuksista esiintyy vähemmän turhaa päällekkäisyyttä

- päätöksentekijöillä on käytettävissään enemmän tietoa päätöksenteon tueksi

- verkko- ja tietoturvapolitiikan laatu jäsenvaltioissa paranee parhaiden käytänteiden leviämisen myötä

- reagoimalla uhkiin EU-tasolla saavutetaan mittakaavaetuja

- yhteiset EU-tason poliittiset tavoitteet ja normit tietoturvan ja varautuneisuuden alalla aikaansaavat lisää investointeja

- yritysten operatiiviset riskit pienenevät, kun tietoturvan ja suojautuneisuuden taso paranee

- tietoverkkorikollisuuden torjuntatoimista tulee keskenään entistä johdonmukaisempia.

Aloitteella odotetaan olevan seuraavanlaisia yhteiskunnallisia vaikutuksia:

- käyttäjien luottamus tietoyhteiskuntapalveluja ja -järjestelmiä kohtaa paranee

- luottamus EU:n sisämarkkinoiden toimintaa kohtaan lisääntyy kuluttajansuojan paranemisen myötä

- tiedonvaihto EU:n ulkopuolisten maiden kanssa lisääntyy

- EU:n perusoikeudet turvataan entistä paremmin, kun kansalaisten henkilötietojen ja yksityisyyden suoja taataan tasavertaisesti.

Odotetut ympäristövaikutukset ovat vähäisiä:

- hiilidioksidipäästöjen vaikutus pienenee esimerkiksi kun matkustaminen vähenee tieto- ja viestintäteknisten järjestelmien ja palvelujen käytön lisääntymisen myötä ja sähkönkulutuksen pienentyessä tietoturvavelvoitteiden noudattamisessa saavutettavien mittakaavahyötyjen ansiosta.

1.4.4. Tulos- ja vaikutusindikaattorit

Tavoitekohtaiset seurantaindikaattorit ovat seuraavat:

Sääntelyperiaatteiden johdonmukaisuus:

- niiden jäsenvaltioiden lukumäärä, jotka ovat hyödyntäneet viraston suosituksia politiikkansa laadinnassa

- sellaisten tutkimusten määrä, joilla pyritään löytämään puutteita ja epäjohdonmukaisuuksia verkko- ja tietoturvanormeissa

- jäsenvaltioiden verkko- ja tietoturvaperiaatteiden erojen vähentyminen.

Ennaltaehkäisy, havaitseminen ja reagointi:

- järjestetyn verkkoturvakoulutuksen määrä

- toimivan ennakkovaroitusjärjestelmän olemassaolo ilmeneviä riskejä ja hyökkäyksiä varten

- viraston koordinoimien EU-tason verkko- ja tietoturvaharjoitusten määrä.

Tiedon tuottaminen päätöksentekijöille:

- sellaisten tutkimusten määrä, joilla kerätään tietoa nykyisistä ja ennakoiduista verkko- ja tietoturvariskeistä ja riskien ennaltaehkäisyteknologioista

- verkko- ja tietoturvan parissa toimivien julkisten elinten kuulemisten määrä

- eurooppalaisen kehyksen olemassaolo verkko- ja tietoturvatiedon keruuta varten.

Sidosryhmien valtaistaminen:

- toimialan todettujen hyvien käytänteiden määrä

- yksityisen sektorin sidosryhmien tietoturvainvestointien määrä.

Euroopan suojaaminen kansainvälisiltä uhkilta:

- yhteisesti sovittujen verkko- ja tietoturvatavoitteiden määrittelemiseen tähtäävien, EU:n jäsenvaltioiden välisten konferenssien/kokousten määrä

- eurooppalaisten ja kansainvälisten verkko- ja tietoturva-asiantuntijoiden kokousten määrä.

Kohti yhteistyöpohjaista täytäntöönpanoa:

- säännöstenmukaisuuden arviointien määrä

- EU:n laajuisten verkko- ja tietoturvakäytänteiden määrä.

Tietoverkkorikollisuuden torjunta:

- yhteydenpidon säännöllisyys aiemmin toisen ja kolmannen pilarin piiriin kuuluneiden tahojen kanssa

- niiden rikostutkintatapausten määrä, joissa on annettu asiantuntija-apua.

1.5. Ehdotuksen/aloitteen perustelut

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

ENISA perustettiin alun perin vuonna 2004 käsittelemään verkko- ja tietoturvaan kohdistuvia uhkia ja mahdollisia loukkauksia. Verkko- ja tietoturvaan liittyvät haasteet ovat sittemmin kehittyneet teknologian ja markkinoiden myötä ja niihin on perehdytty lisää niin, että nyt kyetään tarkemmin ja ajantasaistetusti kuvailemaan todetut ongelmat ja se, miten verkko- ja tietoturvan muuttuva tilanne niihin vaikuttaa.

1.5.2. Unionin toiminnasta saatava lisäarvo

Verkko- ja tietoturvaongelmat eivät noudattele kansallisia rajoja, eikä niihin näin ollen voida tehokkaasti puuttua pelkästään kansallisen tason toimin. Samalla viranomaiset eri jäsenvaltioissa käsittelevät ongelmaa hyvin eri tavoin. Nämä erot voivat merkittävästi haitata tarvittavien EU:n laajuisten mekanismien toteuttamista verkko- ja tietoturvatilanteen kohentamiseksi Euroopassa. Tieto- ja viestintäteknisten infrastruktuurien keskinäisten riippuvuussuhteiden vuoksi on edelleen niin, että tietyn jäsenvaltion kansallisen tason toimien tuloksellisuus kärsii edelleen suuressa määrin riittämättömistä toimenpiteistä toisissa jäsenvaltioissa ja sitä heikentää järjestelmällisen rajat ylittävän yhteistyön puute. Ongelmiin

yhdessä jäsenvaltiossa johtavat riittämättömät verkko- ja tietoturvatoimet saattavat aiheuttaa palvelukatkoksia muissa jäsenvaltioissa.

Tietoturvavaatimusten hajanaisuus aiheuttaa myös lisäkustannuksia EU:n tasolla toimiville yrityksille ja johtaa pirstaleisuuteen ja kilpailukyvyn puutteeseen Euroopan sisämarkkinoilla.

Vaikka riippuvuus verkko- ja tietojärjestelmistä lisääntyy, valmistautuminen uhkatekijöiden varalta vaikuttaa riittämättömältä.

Nykyisissä kansallisissa varhaisvaroitus- ja reagointijärjestelmissä on vakavia puutteita. Verkkoturvan loukkausten valvontaan ja raportointiin liittyvät prosessit ja käytännöt poikkeavat suuresti toisistaan eri jäsenvaltioissa. Joissain maissa prosessit eivät ole säännönmukaisia ja toisissa ei ole nimetty toimivaltaista viranomaista käsittelemään loukkauksia koskevia ilmoituksia. Yhteiseurooppalaisia järjestelmiä ei ole. Tästä johtuu, että verkko- ja tietoturvaloukkaukset voisivat vakavasti keskeyttää perushyödykkeiden tarjonnan. Tähän olisi varauduttava riittävin vastatoimin. Kriittisistä tietoinfrastruktuureista annetussa komission tiedonannossa korostetaan, että Eurooppa tarvitsee varhaisvaroitus- ja reagointivalmiuksia, joita voitaisiin tukea Euroopan mittakaavassa toteutettavilla harjoituksilla.

On olemassa selkeä tarve poliittisille toimille, joilla pyritään ennakoivasti yksilöimään verkko- ja tietoturvariskejä ja haavoittuvuuksia, luodaan tarvittavat reagointimekanismit (esim. määrittelemällä hyviä käytänteitä ja levittämällä niiden käyttöä) ja varmistetaan, että kaikki sidosryhmät tuntevat nämä reagointimekanismit ja käyttävät niitä.

1.5.3. Vastaavista toimista saadut tärkeimmät kokemukset

Ks. kohdat 1.5.1 ja 1.5.2.

1.5.4. Yhteensopivuus muiden toimien kanssa ja mahdolliset synergiaedut

Tämä aloite on täysin johdonmukainen suhteessa yleiseen verkko- ja tietoturvakeskusteluun ja muihin poliittisiin aloitteisiin, joissa keskitytään verkko- ja tietoturvan tulevaisuuteen. Se on yksi tärkeimmistä osatekijöistä Euroopan digitaalistrategiassa, joka taas on yksi Eurooppa 2020 -strategian lippulaivahankkeista.

1.6. Toiminnan ja sen rahoitusvaikutusten kesto

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

– ☑ Viiden vuoden jatkoaika alkaa 14.3.2012 tai uuden asetuksen voimaatulopäivänä sen mukaan, kumpi ajankohdista on myöhäisempi.

– ☑ Rahoitusvaikutuksia vuosina 2012–2017.

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

– Käynnistysvaihe alkaa vuonna VVVV ja päättyy vuonna VVVV,

– minkä jälkeen toteutus täydessä laajuudessa.

1.7. Hallinnointitapa (hallinnointitavat)[39]

☐ komissio **hallinnoi suoraan keskitetysti**

☑ **epäsuora keskitetty hallinnointi**, jossa täytäntöönpanotehtävät on siirretty

– ☐ toimeenpanovirastoille

– ☑ yhteisöjen perustamille elimille[40]

– ☐ kansallisille julkisoikeudellisille yhteisöille tai julkisen palvelun tehtäviä suorittaville yhteisöille

– ☐ henkilöille, joille on annettu tehtäväksi toteuttaa Euroopan unionista tehdyn sopimuksen V osaston mukaisia erityistoimia ja jotka nimetään varainhoitoasetuksen 49 artiklan mukaisessa perussäädöksessä

☐ **hallinnointi yhteistyössä** jäsenvaltioiden kanssa

☐ **hajautettu hallinnointi** yhteistyössä kolmansien maiden kanssa

☐ **hallinnointi yhteistyössä** kansainvälisten järjestöjen kanssa (***tarkennettava***)

---

39 Kuvaukset eri hallinnointitavoista ja viittaukset varainhoitoasetukseen ovat saatavilla budjettipääosaston verkkosivuilla osoitteessa http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html.

40 Sellaisina kuin nämä on määritelty varainhoitoasetuksen 185 artiklassa.

2. HALLINNOINTI

2.1. Seuranta- ja raportointisäännöt

Pääjohtaja on vastuussa viraston toiminnan seurannasta ja edistyksen arvioinnista sen tavoitteisiin nähden ja raportoi siitä johtokunnalle vuosittain.

Pääjohtaja laatii yleiskertomuksen, jossa käsitellään kaikkia viraston edellisen vuoden toimia ja ennen kaikkea verrataan saavutettuja tuloksia vuosittaisen työohjelman tavoitteisiin. Kun johtokunta on hyväksynyt kertomuksen, se toimitetaan Euroopan parlamentille, neuvostolle, komissiolle, tilintarkastustuomioistuimelle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle ja julkaistaan.

2.2. Hallinnointi- ja valvontajärjestelmä

2.2.1. Todetut riskit

ENISA perustettiin vuonna 2004, minkä jälkeen siihen on kohdistettu sekä ulkoisia että sisäisiä arviointeja.

Ensimmäinen vaihe oli ENISAn perustamisasetuksen 25 artiklan mukainen ENISAn riippumaton arviointi, jonka suoritti ulkopuolinen asiantuntijapaneeli kaudella 2006–2007. Ulkoisen asiantuntijapaneelin raportissa[41] vahvistettiin, että ENISAn perustamiseen alun perin johtaneet syyt ja sen alkuperäiset tavoitteet ovat edelleen ajankohtaisia, ja siinä tuotiin myös esiin ongelmia, joihin on syytä puuttua.

Komissio raportoi maaliskuussa 2007 arvioinnista johtokunnalle, joka esitti sen jälkeen omat suosituksensa viraston tulevaisuudesta ja ENISAn perustamisasetukseen tehtävistä muutoksista[42].

Kesäkuussa 2007 komissio esitti oman arvionsa ulkoisen arvioinnin tuloksista ja johtokunnan suosituksista Euroopan parlamentille ja neuvostolle annetussa tiedonannossa[43]. Tiedonannon mukaan oli päätettävä, jatketaanko viraston toimeksiantoa vai korvataanko virasto jollain muulla järjestelyllä, kuten sidosryhmien pysyvällä foorumilla tai turvallisuusorganisaatioiden verkostolla. Tiedonannolla käynnistettiin myös julkinen kuuleminen aiheesta. Siinä eurooppalaisia sidosryhmiä pyydettiin vastaamaan kyselyyn, joka ohjaisi asiasta käytäviä jatkokeskusteluja[44].

41 http://ec.europa.eu/dgs/information_society/evaluation/studies/index_en.htm.

42 Kuten ENISA-asetuksen 25 artiklassa säädetään. ENISAn johtokunnan hyväksymä asiakirja, joka sisältää myös johtokunnan perustelut, on kokonaisuudessaan saatavissa seuraavasta internet-osoitteesta: http://enisa.europa.eu/pages/03_02.htm.

43 Komission tiedonanto Euroopan parlamentille ja neuvostolle: Euroopan verkko- ja tietoturvaviraston (ENISA) arviointi, KOM(2007) 285 lopullinen, 1.6.2007: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0285:FI:NOT.

44 http://ec.europa.eu/yourvoice/ipm/forms/dispatch?form=EnisaFuture&lang=en.

2.2.2. Valvontamenetelmä(t)

Ks. kohdat 2.1 ja 2.2.1 edellä.

2.3. Toimenpiteet petosten ja sääntöjenvastaisuuksien ehkäisemiseksi

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.).

3. EHDOTUKSEN/ALOITTEEN ARVIOIDUT RAHOITUSVAIKUTUKSET *

3.1. Kyseeseen tulevat monivuotisen rahoituskehyksen otsakkeet ja menopuolen budjettikohdat

- Talousarviossa jo olevat budjettikohdat

Moniv. rahoitus-kehyksen otsake	Budjettikohta	Menolaji	Rahoitusosuudet			
	Numero/kuvaus	JM/EI-JM (45)	EFTA-mailta[46]	ehdokas-mailta[47]	kolman-silta mailta	varainhoito-asetuksen 18 artiklan 1 kohdan aa alakohdassa tarkoitetut rahoitusosuudet
1 a. Kasvua ja työllisyyttä edistävä kilpailukyky	09 02 03 01 Euroopan verkko- ja tietoturvavirasto – Avustus osastoille 1 ja 2	JM	KYLLÄ	EI	EI	EI
	09 02 03 02 Euroopan verkko- ja tietoturvavirasto – Avustus osastoon 3	JM	KYLLÄ	EI	EI	EI
5 Hallintomenot	09 01 01 Menot tietoyhteiskunnan ja viestinten toimintalohkon palveluksessa olevasta henkilöstöstä	EI-JM	EI	EI	EI	EI
	09 01 02 11 Muut hallintomenot	EI-JM	EI	EI	EI	EI

* Tähän rahoitusselvitykseen eivät sisälly ehdotuksen arvioidut rahoitusvaikutukset nykyisen rahoitussuunnittelukauden 2007–2013 jälkeiseltä ajalta. Komissio esittää tarkistetun rahoitusselvityksen vuoden 2013 jälkeistä monivuotista rahoituskehystä koskevan asetusehdotuksensa pohjalta ottaen huomioon vaikutusten arvioinnin päätelmät.

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

46 EFTA: Euroopan vapaakauppaliitto.

47 Ehdokasmaat ja soveltuvin osin Länsi-Balkanin mahdolliset ehdokasmaat.

3.2. Arvioidut vaikutukset menoihin

3.2.1. Yhteenveto arvioiduista vaikutuksista menoihin

milj. euroa (kolmen desimaalin tarkkuudella)

Monivuotisen rahoituskehyksen otsake:	1.a	Kasvua ja työllisyyttä edistävä kilpailukyky

ENISA			1.1.–13.3.2012	14.3.–31.12.2012	2013	2014	2015	2016	1.1.–13.3.2017	**YHTEENSÄ 14.3.2012–13.3.2017**
Toimintamäärärahat										
09 02 03 02 Euroopan verkko- ja tietoturvavirasto – Avustus osastoon 3	Sitoumukset	(1)	0,454	1,976	2,470	--	--	--	--	--
	Maksut	(2)	0,454	1,976	2,470	--	--	--	--	--
Hallintomäärärahat										
09 02 03 01 Euroopan verkko- ja tietoturvavirasto – Avustus osastoille 1 ja 2		(3)	1,293	4,697	6,120	--	--	--	--	--
Määrärahat YHTEENSÄ Otsakkeessa 1 a	Sitoumukset	=1 +3	1,747	6,673	8,590	--	--	--	--	--
	Maksut	=2+3	1,747	6,673	8,590	--	--	--	--	--

Toimintamäärärahat YHTEENSÄ	Sitoumukset	(4)	0,454	1,976	2,470	--	--	--	--	---
	Maksut	(5)	0,454	1,976	2,470	--	--	--	--	--

Tiettyjen toimintaohjelmien määrärahoista katettavat hallintomäärärahat YHTEENSÄ		(6)	1,293	4,697	6,120	--	--	--	--	--
Määrärahat YHTEENSÄ Monivuotisen rahoituskehyksen **OTSAKKEESSA 1 A**	Sitoumukset	=4+6	1,747	6,673	8,590	--	--	--	--	--
	Maksut	=5+6	1,747	6,673	8,590	--	--	--	--	--

milj. euroa (kolmen desimaalin tarkkuudella)

Monivuotisen rahoituskehyksen otsake:	5	Hallintomenot

		1.1.–13.3.2012	14.3.–31.12.2012	2013	2014	2015	2016	1.1.–13.3.2017	Yhteensä
Henkilöresurssit		0,085	0,342	0,427	--	--	--	--	--
Muut hallintomenot		0,002	0,013	0,015	--	--	--	--	--
DG INFSO YHTEENSÄ	Määrärahat	0,087	0,355	0,442	--	--	--	--	--

Monivuotisen rahoituskehyksen **OTSAKKEESEEN 5 kuuluvat määrärahat YHTEENSÄ**	(Sitoumukset yhteensä = maksut yhteensä)	0,087	0,355	0,442	--	--	--	--	--

		1.1.–13.3.2012	14.3.–31.12.2012	2013	2014	2015	2016	1.1.–13.3.2017	Yhteensä
Monivuotisen rahoituskehyksen **OTSAKKEISIIN 1–5 kuuluvat määrärahat YHTEENSÄ**	Sitoumukset	1,834	7,028	9,032	--	--	--	--	--
	Maksut	1,834	7,028	9,032	--	--	--	--	--

3.2.2. Arvioidut vaikutukset toimintamäärärahoihin

– ☐ Ehdotus/aloite ei edellytä toimintamäärärahoja.

– ☑ Ehdotus/aloite edellyttää toimintamäärärahoja seuraavasti:

Maksusitoumusmäärärahat, milj. euroa (kolmen desimaalin tarkkuudella)

Tavoitteet ja tuotokset ⇩	1.1.–13.3.2012	14.3.–31.12.2012	2013	2014	2015	2016	1.1.–13.3.2017	**14.3.2012–13.3.2017 YHTEENSÄ**
Sääntelyperiaatteiden johdonmukaisuus	0,114	0,494	0,620	--	--	--	--	--
Ennaltaehkäisy, havaitseminen ja reagointi	0,114	0,494	0,620	--	--	--	--	--
Tiedon tuottaminen päätöksentekijöille	0,068	0,297	0,370	--	--	--	--	--
Sidosryhmien valtaistaminen	0,050	0,218	0,270	--	--	--	--	--
Euroopan suojaaminen kansainvälisiltä uhkilta	0,023	0,099	0,120	--	--	--	--	--
Kohti yhteistyöpohjaista täytäntöönpanoa	0,064	0,276	0,340	--	--	--	--	--
Tietoverkkorikollisuuden torjunta	0,023	0,098	0,120	--	--	--	--	--
KUSTANNUKSET YHTEENSÄ	0,454	1,976	2,460	--	--	--	--	--

3.2.3. Arvioidut vaikutukset hallintomäärärahoihin[48]

3.2.3.1. Yhteenveto

– ☐ Ehdotus/aloite ei edellytä hallintomäärärahoja.

– ☑ Ehdotus/aloite edellyttää hallintomäärärahoja seuraavasti:

a) Monivuotisen rahoituskehyksen otsakkeeseen 5 kuuluvat hallintomenot

milj. euroa (kolmen desimaalin tarkkuudella)

Monivuotisen rahoituskehyksen OTSAKE 5	1.1.–13.3.2012	14.3.–31.12.2012	2013	2014	2015	2016	1.1.–13.3.2017	**14.3.2012–13.3.2017 yhteensä**
Henkilöresurssit	0,085	0,342	0,427	--	--	--	--	--
Muut hallintomenot	0,002	0,013	0,015	--	--	--	--	--
YHTEENSÄ	0,087	0,355	0,442	--	--	--	--	--

b) ENISAan liittyvät hallintomenot – sisältyvät budjettikohtaan "09.020301 Euroopan verkko- ja tietoturvavirasto: osasto 1 – henkilöstö ja osasto 2 – viraston toiminta".

milj. euroa (kolmen desimaalin tarkkuudella)

	1.1.–13.3.2012	14.3.–31.12.2012	2013	2014	2015	2016	1.1.–13.3.2017	**14.3.2012–13.3.2017 yhteensä**
Henkilöresurssit - Osasto 1 – Henkilöstö	1,153	4,329	5,607	--	--	--	--	--
Muut hallintomenot – Osasto 2 – Viraston toiminta	0,140	0,368	0,513	--	--	--	--	--
YHTEENSÄ	**1,293**	**4,697**	**6,120**	--	--	--	--	--

3.2.3.2. Henkilöresurssien arvioitu tarve

Viraston henkilöstötaulukko selitetään ja perustellaan joka vuosi budjettivallan käyttäjälle toimitettavassa henkilöstösuunnitelmassa.

[48] Rahoitusselvityksen liitettä ei ole täytetty, koska se ei koske tätä ehdotusta.

– ☐ Ehdotus/aloite ei edellytä henkilöresursseja.

– ☑ Ehdotus/aloite edellyttää henkilöresursseja seuraavasti:

a) Henkilöresurssit komissiossa

	1.1.–13.3.2012	14.3.–31.12.2012	2013	2014	2015	2016	1.1.–13.3.2017
Henkilöstötaulukkoon sisältyvät virat/toimet (virkamiehet ja väliaikaiset toimihenkilöt)							
XX 01 01 01 (päätoimipaikka ja komission edustustot)	3,5	3,5	3,5	--	--	--	--
YHTEENSÄ	**3,5**	**3,5**	**3,5**	**--**	**--**	**--**	**--**

b) ENISAn henkilöresurssit

		1.1.–13.3.2012	14.3.–31.12.2012	2013	2014	2015	2016	1.1.–13.3.2017
ENISAn henkilöstötaulukko (kokoaikaiseksi muutettuna)								
Virkamiehet ja väliaikaiset toimihenkilöt	AD	29	31	31	--	--	--	--
	AST	15	16	16	--	--	--	--
Virkamiehet tai väliaikaiset toimihenkilöt YHTEENSÄ		44	47	47	--	--	--	--
Muu henkilöstö (kokoaikaiseksi muutettuna)								
Sopimussuhteiset toimihenkilöt		13	14	14	--	--	--	--
Kansalliset asiantuntijat		5	5	5	--	--	--	--
Muu henkilöstö yhteensä		18	19	19	--	--	--	--
YHTEENSÄ		**62**	**66**	**66**	**--**	**--**	**--**	**--**

Kuvaus viraston henkilöstön tehtävistä:

Virkamiehet ja väliaikaiset toimihenkilöt	Virasto – hoitaa edelleen neuvoa-antavia ja koordinoivia tehtäviä, joissa se **kerää ja analysoi** tietoturvaa koskevaa **tietoa**. Nykyisin sekä julkiset että yksityiset tahot keräävät erilaisia tarkoituksia varten tietoa tietoturvaloukkauksista ja muista tietoturvallisuuden kannalta tärkeistä asioista. Euroopan tasolla ei kuitenkaan ole keskitettyä kokonaisuutta, joka kattavasti keräisi ja analysoisi tietoja sekä antaisi

	lausuntoja ja neuvoja unionin verkko- ja tietoturvapolitiikan kehittämisen tueksi; – **toimii osaamiskeskuksena**, josta sekä jäsenvaltiot että EU:n toimielimet voivat pyytää **lausuntoja ja neuvoja turvallisuuteen liittyvissä teknisissä asioissa**; – osallistuu tietoturva-alan **eri toimijoiden väliseen yleiseen yhteistyöhön** esimerkiksi avustamalla tietoturvallisen sähköisen liiketoiminnan tukitoimien seurannassa. Tällainen yhteistyö on keskeinen edellytys verkkojen ja tietojärjestelmien turvalliselle toiminnalle Euroopassa. Kaikkien asianosaisten mukanaolo on tarpeen; – pyrkii osaltaan koordinoimaan tietoturva-ajattelua **tukemalla jäsenvaltioita** esimerkiksi **riskinarvioinnin edistämisessä** ja tiedotuskampanjoiden järjestämisessä; – varmistaa **verkkojen ja tietojärjestelmien yhteentoimivuuden** jäsenvaltioiden **soveltaessa** turvallisuuteen vaikuttavia teknisiä vaatimuksia; – kartoittaa **standardointitarpeita**, arvioi nykyisiä turvallisuusnormeja ja sertifiointijärjestelmiä ja edistää niiden mahdollisimman laajaa käyttöä eurooppalaisen lainsäädännön tukena; – tukee alan **kansainvälistä yhteistyötä**, joka on yhä välttämättömämpää verkko- ja tietoturvan maailmanlaajuisesta luonteesta johtuen.
Ulkopuolinen henkilöstö	Ks. edellä

3.2.4. Yhteensopivuus nykyisen monivuotisen rahoituskehyksen kanssa

– ☑ Ehdotus/aloite on nykyisen monivuotisen rahoituskehyksen mukainen.

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

– ☐ Ehdotus/aloite edellyttää joustovälineen varojen käyttöön ottamista tai monivuotisen rahoituskehyksen tarkistamista[49].

Vuoden 2013 jälkeistä EU-rahoitusta pohditaan koko komission laajuisessa keskustelussa kaikista vuoden 2013 jälkeistä aikaa koskevista ehdotuksista. Tämä merkitsee sitä, että sen jälkeen kun komissio on antanut seuraavaa monivuotista rahoituskehystä koskevan ehdotuksensa se esittää tarkistetun rahoitusselvityksen ottaen huomioon vaikutusten arvioinnin päätelmät.

3.2.5. Ulkopuolisten tahojen osallistuminen rahoitukseen

– ☐ Ehdotuksen/aloitteen rahoittamiseen ei osallistu ulkopuolisia tahoja.

– ☑ Ehdotuksen/aloitteen rahoittamiseen osallistuu ulkopuolisia tahoja seuraavasti:

Ohjeelliset määrärahat, milj. euroa (kolmen desimaalin tarkkuudella)

	1.1.–13.3.2012	14.3.–31.12.2012	2013	2014	2015	2016	1.1.–13.3.2017	**14.3.2012 – 13.3.2017 yhteensä**
EFTA	0,042	0,160	0,206	--	--	--	--	**--**

[49] Katso toimielinten sopimuksen 19 ja 24 kohta.

3.3. Arvioidut vaikutukset tuloihin

– ☑ Ehdotuksella/aloitteella ei ole vaikutuksia tuloihin.

– ☐ Ehdotuksella/aloitteella on vaikutuksia tuloihin seuraavasti:

  – ☐ vaikutukset omiin varoihin

  – ☐ vaikutukset sekalaisiin tuloihin