EUROOPAN
KOMISSIO

Bryssel 7.2.2013
COM(2013) 48 final

2013/0027 (COD)

Ehdotus

EUROOPAN PARLAMENTIN JA NEUVOSTON DIREKTIIVI

toimenpiteistä yhteisen korkeatasoisen verkko- ja tietoturvan varmistamiseksi koko unionissa

{SWD(2013) 31 final}
{SWD(2013) 32 final}

PERUSTELUT

Ehdotetun direktiivin tavoitteena on varmistaa verkko- ja tietoturvan yhteinen korkea taso. Tämä tarkoittaa internetin turvallisuuden sekä yhteiskunnan ja talouden toimintaa tukevien yksityisten verkkojen ja tietojärjestelmien turvallisuuden parantamista. Tähän päästään velvoittamalla jäsenvaltiot nostamaan varautumistasoaan ja parantamaan keskinäistä yhteistyötään sekä edellyttämällä, että elintärkeiden infrastruktuurien (mm. energia ja liikenne) operaattorit ja keskeisten tietoyhteiskunnan palvelujen (sähköisen kaupankäynnin alustojen, verkkoyhteisöpalvelujen jne.) tarjoajat sekä julkishallinnot ryhtyvät tarvittaviin toimiin turvariskien hallitsemiseksi ja raportoivat vakavista turvapoikkeamista kansallisille toimivaltaisille viranomaisille.

Tämä ehdotus esitetään yhdessä komission ja unionin ulkoasioiden ja turvallisuuspolitiikan korkean edustajan yhteisen eurooppalaisen kyberturvallisuusstrategian kanssa. Strategian tavoitteena on varmistaa turvallinen ja luotettava digitaaliympäristö sekä edistää ja suojata perusoikeuksia ja muita EU:n perusarvoja. Tämä ehdotus on strategian tärkein toimi. Sen muut toimet keskittyvät tietoisuuden lisäämiseen, kyberturvallisuuteen liittyvien tuotteiden ja palvelujen sisämarkkinoiden kehittämiseen sekä t&k-investointien edistämiseen. Näitä toimia täydennetään muilla toimilla, joiden tavoitteena on tehostaa verkkorikollisuuden torjuntaa ja kehittää kansainvälistä kyberturvallisuuspolitiikkaa EU:lle.

1.1. Ehdotuksen perustelut ja tavoitteet

Verkko- ja tietoturvalla on kasvava merkitys taloudelle ja yhteiskunnalle. Verkko- ja tietoturva on myös tärkeä ennakkoehto luotettavan ympäristön luomiselle maailmanlaajuisessa palvelukaupassa. Tietojärjestelmät ovat kuitenkin alttiina turvapoikkeamille, kuten inhimillisille virheille, luonnon tapahtumille, teknisille vioille tai ilkivaltaisille hyökkäyksille. Turvapoikkeamat ovat yhä yleisempiä, laajempia ja monimutkaisempia. Verkko- ja tietoturvan parantamisesta EU:ssa järjestetyssä komission julkisessa verkkokuulemisessa[1] kävi ilmi, että 57 prosenttia vastaajista oli kokenut edellisvuoden aikana verkko- ja tietoturvapoikkeamia, joilla oli ollut vakava vaikutus niiden toimintoihin. Verkko- ja tietoturvan puutteet voivat vaarantaa elintärkeät palvelut, jotka ovat riippuvaisia verkko- ja tietojärjestelmien eheydestä. Tämä voi estää yritysten toiminnan, aiheuttaa merkittäviä taloudellisia tappioita EU:n taloudelle ja vaikuttaa kielteisesti yhteiskunnan hyvinvointiin.

[1] Julkinen verkkokuuleminen *Improving network and information security in the EU* järjestettiin 23. heinäkuuta – 15. lokakuuta 2012.

Lisäksi digitaaliset tietojärjestelmät, erityisesti internet, ovat rajat ylittäviä ja jäsenvaltioiden välillä yhteenliitettyjä viestintävälineitä, jotka helpottavat olennaisesti tavaroiden, palvelujen ja ihmisten liikkumista rajojen yli. Näiden järjestelmien vakavat häiriöt yhdessä jäsenvaltiossa voivat vaikuttaa myös muihin jäsenvaltioihin ja koko EU:hun. Verkko- ja tietojärjestelmien sietokyky ja vakaus ovat olennaisen tärkeitä digitaalisten sisämarkkinoiden toteuttamisen ja sisämarkkinoiden moitteettoman toiminnan kannalta. Turvapoikkeamien todennäköisyys ja yleisyys sekä kyvyttömyys taata tehokas suoja heikentävät myös yleisön luottamusta verkko- ja tietopalveluihin. Esimerkiksi Eurobarometrin vuoden 2012 kyberturvallisuuskyselyn mukaan 38 prosenttia internetin käyttäjistä EU:ssa on huolissaan verkkomaksujen turvallisuudesta ja on muuttanut käyttäytymistään turvallisuuskysymyksiin liittyvien huolenaiheiden vuoksi. Vastaajista 18 prosenttia ilmoitti aikovansa vähentää tavaroiden ostoa verkon kautta ja 15 prosenttia internet-pankkipalvelujen käyttöä[2].

Tämänhetkinen tilanne EU:ssa, joka on tulosta toistaiseksi harjoitetusta täysin vapaaehtoisesta lähestymistavasta, ei tarjoa riittävää suojaa verkko- ja tietoturvapoikkeamilta ja -riskeiltä kaikkialla EU:ssa. Tämänhetkiset verkko- ja tietoturvavalmiudet ja -mekanismit eivät yksinkertaisesti riitä vastaamaan nopeasti muuttuviin uhkiin ja varmistamaan korkeatasoista ja yhtenäistä suojaa kaikissa jäsenvaltioissa.

Toteutetuista aloitteista huolimatta jäsenvaltioiden valmiudet ja varautumistaso vaihtelevat paljon, mikä johtaa lähestymistapojen hajanaisuuteen eri puolilla EU:ta. Koska verkot ja järjestelmät ovat yhteenliitettyjä, EU:n yleinen verkko- ja tietoturva heikentyy sellaisten jäsenvaltioiden takia, joissa turvataso on riittämätön. Tämä tilanne vaikeuttaa myös luottamuksen luomista vertaisryhmien välille, mikä on ennakkoedellytys yhteistyölle ja tiedonvaihdolle. Yhteistyötä harjoitetaan vain niiden vähemmistönä olevien jäsenvaltioiden kesken, joissa valmiustaso on korkea.

EU:n tasolla ei tällä hetkellä ole toimivaa mekanismia tulokselliselle yhteistyölle ja luotettavalle jäsenvaltioiden väliselle tiedonjaolle verkko- ja tietoturvapoikkeamista ja -riskeistä. Tämä voi johtaa epäyhtenäisiin sääntelyllisiin toimiin, epäjohdonmukaisiin strategioihin ja erilaisiin standardeihin, mikä puolestaan johtaa riittämättömään verkko- ja tietoturvaan koko EU:ssa. Myös sisämarkkinoille voi syntyä esteitä, mikä lisää säännösten noudattamisesta aiheutuvia kustannuksia sellaisille yrityksille, jotka toimivat useammassa kuin yhdessä jäsenvaltiossa.

Lisäksi toimijoita, jotka ylläpitävät elintärkeää infrastruktuuria tai tarjoavat yhteiskunnan toiminnan kannalta olennaisia palveluja, ei ole velvoitettu riskinhallintatoimenpiteisiin ja tiedonvaihtoon asianomaisten viranomaisten kanssa. Tämän vuoksi yrityksiltä ensinnäkin puuttuvat toimivat kannusteet vakavien riskien hallintaan, joka sisältäisi turvariskien arvioinnin ja tarvittavat toimenpiteet verkko- ja tietoturvan varmistamiseksi. Toiseksi suuri osa tapauksista ei tule toimivaltaisten viranomaisten tietoon ja jää huomiotta. Turvapoikkeamia koskevat tiedot ovat kuitenkin olennaisen tärkeitä, jotta viranomaiset voisivat reagoida, ryhtyä tarvittaviin toimenpiteisiin turvariskien lieventämiseksi ja asettaa riittävät strategiset painopisteet verkko- ja tietoturvalle.

Nykyinen sääntelykehys velvoittaa ainoastaan teleyritykset riskinhallintatoimenpiteisiin ja raportoimaan vakavista verkko- ja tietoturvapoikkeamista. Kuitenkin myös monet muut alat ovat riippuvaisia tieto- ja viestintätekniikasta (TVT) toimintansa mahdollistajana, minkä vuoksi myös niiden tulisi huolehtia verkko- ja tietoturvasta. Tiettyjen infrastruktuurien ja palvelujen tarjoajat ovat erityisen haavoittuvassa asemassa, koska ne ovat hyvin riippuvaisia moitteettomasti toimivista verkko- ja tietojärjestelmistä. Nämä sektorit tarjoavat keskeisiä tukipalveluja taloudelle ja yhteiskunnalle, ja niiden järjestelmien turvallisuudella on erityinen

[2] Eurobarometri 390/2012.

merkitys sisämarkkinoiden toiminnan kannalta. Niitä ovat pankkitoiminta, pörssit, energian tuotanto, siirto ja jakelu, liikenne (lento-, rautatie- ja meriliikenne), terveydenhuolto, internet-palvelut sekä julkishallinnot.

Tämän vuoksi on muutettava olennaisesti tapaa, jolla verkko- ja tietoturvallisuutta käsitellään EU:ssa. Sääntelyllisiä velvoitteita tarvitaan tasapuolisten toimintaedellytysten luomiseksi ja nykyisten lainsäädännön porsaanreikien paikkaamiseksi. Jotta näihin ongelmiin voitaisiin puuttua ja nostaa verkko- ja tietoturvatasoa Euroopan unionissa, ehdotetulla direktiivillä pyritään seuraavaan.

Ensinnäkin ehdotus velvoittaisi kaikki jäsenvaltiot varmistamaan kansallisten valmiuksien vähimmäistason nimeämällä toimivaltaiset viranomaiset verkko- ja tietoturvaa varten, perustamalla tietotekniikan kriisiryhmiä (CERT) ja vahvistamalla kansallisia verkko- ja tietoturvastrategioita ja kansallisia verkko- ja tietoturvan yhteistyösuunnitelmia.

Toiseksi kansallisten toimivaltaisten viranomaisten olisi tehtävä yhteistyötä verkostossa, jossa voidaan varmistaa turvattu ja tuloksellinen koordinointi, muun muassa koordinoitu tiedonvaihto sekä havaitseminen ja reagointi EU:n tasolla. Jäsenvaltioiden olisi tämän verkoston kautta vaihdettava tietoja ja tehtävä yhteistyötä verkko- ja tietoturvauhkien ja -poikkeamien torjumiseksi Euroopan verkko- ja tietoturvan yhteistyösuunnitelman mukaisesti.

Kolmanneksi ehdotuksella pyritään varmistamaan sähköisen viestinnän puitedirektiivin mallin pohjalta riskinhallintakulttuurin kehittyminen ja tiedonjako yksityisen ja julkisen sektorin välillä. Edellä mainituilla kriittisillä sektoreilla toimivat yritykset ja julkishallinto velvoitetaan arvioimaan niihin kohdistuvat turvariskit ja toteuttamaan asianmukaiset ja oikeasuhteiset toimenpiteet verkko- ja tietoturvan varmistamiseksi. Nämä tahot velvoitetaan raportoimaan toimivaltaisille viranomaisille kaikista turvapoikkeamista, jotka vaarantavat vakavasti niiden verkot ja tietojärjestelmät ja vaikuttavat merkittävästi kriittisten palvelujen ja hyödykkeiden toimituksen jatkuvuuteen.

1.2. Yleinen tausta

Jo vuonna 2001 antamassaan tiedonannossa *Verkko- ja tietoturva: Ehdotus eurooppalaiseksi lähestymistavaksi* komissio korosti verkko- ja tietoturvan kasvavaa merkitystä[3]. Sitä seurasi vuonna 2006 annettu *Turvallisen tietoyhteiskunnan strategia*[4], jonka tavoitteena oli kehittää verkko- ja tietoturvakulttuuria Euroopassa. Sen keskeiset osatekijät hyväksyttiin neuvoston päätöslauselmassa[5].

Komissio antoi 30. maaliskuuta 2009 elintärkeiden tietoinfrastruktuurien suojaamista koskevan tiedonannon[6], jossa käsiteltiin Euroopan suojaamista tietoverkkohäiriöiltä parantamalla turvallisuutta. Tiedonannolla käynnistettiin toimintasuunnitelma, jolla tuettiin jäsenvaltioiden toimia ennaltaehkäisyn ja reagoinnin varmistamiseksi. Toimintasuunnitelma hyväksyttiin elintärkeiden infrastruktuurien suojaamista käsitelleen ministerikonferenssin puheenjohtajan päätelmissä Tallinnassa vuonna 2009. Neuvosto antoi 18. joulukuuta 2009 päätöslauselman yhteistoiminnallisesta eurooppalaisesta lähestymistavasta verkko- ja tietoturvallisuuden alalla[7].

---

3 KOM(2001) 298.
4 KOM(2006) 251 http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0251en01.pdf.
5 2007/068/01.
6 KOM(2009) 149.
7 2009/C 321/01.

Toukokuussa 2010 hyväksytyn Euroopan digitaalistrategian[8] ja sitä koskevien neuvoston päätelmien[9] myötä kävi ilmi yhteinen näkemys siitä, että luottamus ja tietoturva ovat ehdottomia perusedellytyksiä TVT:n laajalle käyttöönotolle ja tätä kautta Eurooppa 2020 -strategian ”älykäs kasvu” -tavoitteiden saavuttamiselle[10]. Digitaalistrategian luottamusta ja turvallisuutta koskevassa luvussa painotettiin tarvetta sille, että kaikki sidosryhmät yhdistävät voimansa kokonaisvaltaisella tavalla, jotta voidaan varmistaa TVT-infrastruktuurien suoja ja sietokyky keskittymällä ennaltaehkäisyyn, varautumiseen ja tietoisuuden lisäämiseen sekä kehittää tuloksellisia ja koordinoituja turvamekanismeja. Erityisesti digitaalistrategian avaintoiminnossa 6 peräänkuulutetaan korkean tason verkko- ja tietoturvapolitiikan lujittamiseen tähtääviä toimenpiteitä.

Maaliskuussa 2011 julkaistussa elintärkeitä tietoinfrastruktuureja koskevassa tiedonannossaan *Saavutukset ja seuraavat vaiheet: kohti maailmanlaajuista verkkoturvallisuutta*[11] komissio teki katsauksen tuloksiin, jotka oli saavutettu sen jälkeen, kun elintärkeiden tietoinfrastruktuurien suojaamista koskeva toimintasuunnitelma hyväksyttiin vuonna 2009. Komissio totesi suunnitelman täytäntöönpanon osoittavan, että puhtaasti kansalliset lähestymistavat turvallisuuden ja sietokyvyn asettamiin haasteisiin vastaamiseksi eivät ole riittäviä ja että Euroopan olisi jatkettava pyrkimyksiään luoda johdonmukainen ja yhteistyöhön perustuva lähestymistapa koko EU:ssa. Tässä vuoden 2011 tiedonannossa komissio ilmoitti useista toimista ja kehotti jäsenvaltioita luomaan verkko- ja tietoturvavalmiuksia ja rajat ylittävää yhteistyötä. Useimmat näistä toimista oli määrä saattaa päätökseen viimeistään vuonna 2012, mutta niitä ei ole vielä pantu täytäntöön.

Elintärkeiden tietoinfrastruktuurien suojaamisesta 27. toukokuuta 2011 antamissaan päätelmissä Euroopan unionin neuvosto korosti tarvetta vahvistaa tietoteknisten järjestelmien ja verkkojen sietokykyä ja suojausta kaikilta mahdollisilta häiriöiltä, olivatpa nämä tahattomia tai tahallisia, kehittää varautumiskyvyn, turvallisuusvalmiuden ja sietokyvyn korkeaa tasoa koko EU:ssa, parantaa teknistä osaamista niin, että Eurooppa voi vastata verkkojen ja tietoteknisen infrastruktuurin suojaamisen haasteeseen sekä edistää jäsenvaltioiden välistä yhteistyötä kehittämällä niiden välisiä häiriötilanteiden yhteistyömekanismeja.

1.3. Voimassa olevat aiemmat Euroopan unionin ja kansainväliset säännökset

Euroopan yhteisö perusti vuonna 2004 asetuksella (EY) N:o 460/2004 Euroopan verkko- ja tietoturvaviraston (ENISA)[12], jonka tehtävänä on osaltaan varmistaa korkeatasoinen verkko- ja tietoturva ja kehittää verkko- ja tietoturvakulttuuria EU:ssa. ENISAn toimeksiannon uudistamista koskeva ehdotus annettiin 30. syyskuuta 2010[13], ja se on nyt neuvoston ja Euroopan parlamentin käsiteltävänä. Tarkistetussa sähköisen viestinnän sääntelyjärjestelmässä[14], joka on ollut voimassa marraskuusta 2009 lähtien, asetetaan turvallisuusvelvoitteita sähköisten viestintäpalvelujen tarjoajille[15]. Kyseiset velvoitteet oli määrä saattaa osaksi kansallista lainsäädäntöä viimeistään toukokuussa 2011.

Tietosuojan sääntelykehys[16] velvoittaa kaikki toimijat, jotka ovat rekisterinpitäjiä (esim. pankit tai sairaalat), ottamaan käyttöön turvatoimenpiteet henkilötietojen suojaamiseksi.

---

8 KOM(2010) 245.

9 Neuvoston päätelmät, annettu 31 päivänä toukokuuta 2010, Euroopan digitaalistrategiasta (10130/10).

10 KOM(2010) 2020 ja Eurooppa-neuvoston päätelmät, 25.–26. maaliskuuta 2010 (EUCO 7/10).

11 KOM(2011) 163.

12 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML.

13 KOM(2010) 521.

14 Ks. http://ec.europa.eu/information_society/policy/ecomm/doc/library/regframeforec_dec2009.pdf.

15 Puitedirektiivin 13 a ja 13 b artikla.

16 Direktiivi 2002/58/EY, annettu 12 päivänä heinäkuuta 2002.

Lisäksi komission vuonna 2012 antama ehdotus yleiseksi tietosuoja-asetukseksi[17] velvoittaisi rekisterinpitäjät raportoimaan henkilötietojen loukkauksista kansallisille valvontaviranomaisille. Tämä tarkoittaa, että esimerkiksi sellaisista verkko- ja tietoturvan loukkauksista, jotka vaikuttavat palvelun tarjoamiseen vaarantamatta henkilötietojen suojaa (esim. sähkökatkokseen johtavasta TVT:n käyttökatkosta sähkövoimalaitoksessa), ei tarvitsisi ilmoittaa.

Euroopan elintärkeän infrastruktuurin määrittämisestä ja nimeämisestä sekä arvioinnista, joka koskee tarvetta parantaa sen suojaamista, annetun direktiivin 2008/114/EY alaisuuteen kuuluvassa Euroopan elintärkeiden infrastruktuureiden suojaamisohjelmassa (EPCIP)[18] esitetään kokonaisvaltainen lähestymistapa elintärkeiden infrastruktuurien suojaamiseen EU:ssa. EPCIPin tavoitteet ovat kaikilta osin johdonmukaisia nyt käsillä olevan ehdotuksen kanssa, ja direktiiviä soveltaminen ei saisi rajoittaa direktiivin 2008/114/EY soveltamista. EPCIP ei velvoita operaattoreita ilmoittamaan merkittävistä turvaloukkauksista eikä luo mekanismeja jäsenvaltioiden yhteistyötä ja turvapoikkeamiin reagoimista varten.

Lainsäädäntövallan käyttäjät keskustelevat parhaillaan komission ehdotuksesta direktiiviksi tietojärjestelmiin kohdistuvista hyökkäyksistä[19], jonka tarkoituksena on yhdenmukaistaa tietyntyyppisten toimintojen kriminalisoiminen. Se kattaa pelkästään tiettyjen toimintojen kriminalisoimisen, eikä siinä käsitellä verkko- ja tietoturvariskien ja -poikkeamien ennaltaehkäisyä, verkko- ja tietoturvapoikkeamiin reagoimista eikä niiden vaikutusten lieventämistä. Tämän direktiivin soveltaminen ei saisi rajoittaa tietojärjestelmiin kohdistuvista hyökkäyksistä annettavan direktiivin soveltamista.

Komissio antoi 28. maaliskuuta 2012 tiedonannon Euroopan verkkorikostorjuntakeskuksen (EC3) perustamisesta[20]. Tämä 11. tammikuuta 2013 perustettu keskus on osa Euroopan poliisivirastoa (Europol) ja toimii linkkinä verkkorikollisuuden torjunnassa EU:ssa. EC3:n on määrä koota yhteen eurooppalaista verkkorikollisuuteen liittyvää asiantuntemusta jäsenvaltioiden valmiuksien kehittämisen tueksi, tarjota jäsenvaltioille tukea tietoverkkorikosten tutkinnoissa sekä toimia yhteistyössä Eurojustin kanssa yhteisenä äänenä eurooppalaisille tietoverkkorikollisuuden tutkijoille sekä poliisi- että tuomioistuintoiminnassa.

EU:n toimielimet, virastot ja muut elimet ovat perustaneet oman tietotekniikan kriisiryhmänsä, nimeltään CERT-EU.

Kansainvälisesti EU toimii kyberturvallisuuden alalla sekä kahden- että monenvälisissä yhteyksissä. EU:n ja Yhdysvaltojen huippukokouksessa[21] vuonna 2010 perustettiin EU:n ja Yhdysvaltojen välinen kyberturvallisuutta ja -rikollisuutta käsittelevä työryhmä. EU toimii aktiivisesti myös muilla monenvälisillä foorumeilla, joita ovat Taloudellisen yhteistyön ja kehityksen järjestö OECD, Yhdistyneiden Kansakuntien yleiskokous, Kansainvälinen televiestintäliitto ITU, Euroopan turvallisuus- ja yhteistyöjärjestö ETYJ, tietoyhteiskuntahuippukokous WSIS ja Internetin hallintofoorumi IGF.

---

17 KOM(2012) 11.

18 KOM(2006) 786 http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0786en01.pdf.

19 KOM(2010) 517, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:EN:PDF.

20 COM(2012) 140 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0140:FIN:EN:PDF.

21 http://europa.eu/rapid/press-release_MEMO-10-597_en.htm.

2. KUULEMISTEN JA VAIKUTUSTENARVIOINTIEN TULOKSET

2.1. Intressitahojen kuuleminen ja asiantuntijatiedon käyttö

Verkko- ja tietoturvan parantamisesta järjestettiin 23. heinäkuuta – 15. lokakuuta 2012 julkinen verkkokuuleminen *Improving network and information security in the EU*. Komissio sai yhteensä 160 kannanottoa verkkokyselyyn.

Tärkein tulos oli se, että sidosryhmät antoivat yleisesti tukensa tarpeelle parantaa verkko- ja tietoturvaa koko EU:ssa. Yksityiskohtaisemmin mainittakoon, että vastaajista 82,6 prosenttia katsoi, että EU:n hallitusten pitäisi tehdä enemmän verkko- ja tietoturvan korkean tason varmistamiseksi; 82,8 prosenttia katsoi, etteivät tiedon ja järjestelmien käyttäjät ole tietoisia tämänhetkisistä verkko- ja tietoturvaan kohdistuvista uhkista ja vaaratilanteista; 66,3 prosenttia periaatteessa kannattaisi sääntelyllisten vaatimusten käyttöönottoa verkko- ja tietoturvariskien hallitsemiseksi; ja 84,8 prosenttia katsoi, että tällaisia vaatimuksia olisi vahvistettava EU:n tasolla. Suuri osa vastaajista oli sitä mieltä, että verkko- ja tietoturvavaatimuksia olisi tärkeää ottaa käyttöön erityisesti seuraavilla aloilla: pankki- ja rahoitustoimi (91,1 %), energiahuolto (89,4 %), liikenne (81,7 %), terveydenhuolto (89,4 %), internet-palvelut (89,1 %) ja julkishallinto (87,5 %). Vastaajat katsoivat myös, että jos käyttöön otetaan velvollisuus ilmoittaa verkko- ja tietoturvaloukkauksista kansalliselle toimivaltaiselle viranomaiselle, se tulisi asettaa EU:n tasolla (65,1 %), ja toivoi, että sitä sovellettaisiin myös julkishallintoihin (93,5 %). Vastaajat totesivat, että vaatimus verkko- ja tietoturvan riskinhallinnan toteuttamisesta uusimmalla tekniikalla ei aiheuttaisi niille merkittäviä lisäkustannuksia (63,4 %) ja että vaatimus tietoturvaloukkausten raportoinnista ei aiheuttaisi merkittäviä lisäkustannuksia (72,3 %).

Jäsenvaltioita kuultiin asiaa käsitelleissä neuvoston kokoonpanoissa, Euroopan jäsenvaltiofoorumin (EFMS) yhteydessä, komission ja Euroopan ulkosuhdehallinnon 6. heinäkuuta 2012 järjestämässä EU:n kyberturvallisuuskonferenssissa sekä yksittäisten jäsenvaltioiden pyynnöstä järjestetyissä kahdenvälisissä kokouksissa.

Yksityisen sektorin kanssa keskusteltiin myös järjestelmien sietokyvyn parantamiseen tähtäävän eurooppalaisen julkis-yksityisen kumppanuuden[22] yhteydessä sekä kahdenvälisissä tapaamisissa. Julkisen sektorin taholla komission kävi keskusteluja ENISAn sekä EU:n toimielinten CERT-kriisiryhmän kanssa.

2.2. Vaikutusten arviointi

Komissio on tehnyt vaikutusarvioinnin kolmesta toimintavaihtoehdosta:

Vaihtoehto 1: Ei lisätoimenpiteitä (perusskenaario): nykyiseen kehitykseen perustuva lähestymistapa.

Vaihtoehto 2: Sääntelyyn perustuva lähestymistapa: säädösehdotus yhteisestä EU:n verkko- ja tietoturvan sääntelyjärjestelmästä, joka koskee jäsenvaltioiden valmiuksia, EU-tason yhteistyömekanismeja ja keskeisille yksityissektorin toimijoille ja julkishallinnoille asetettavia vaatimuksia.

[22] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r.

Vaihtoehto 3: Yhdistetty lähestymistapa, jossa jäsenvaltioiden verkko- ja tietoturvavalmiuksiin ja EU-tason yhteistyömekanismeihin liittyviä vapaaehtoisia aloitteita täydennetään keskeisille yksityissektorin toimijoille ja julkishallinnoille asetettavilla sääntelyllisillä vaatimuksilla.

Komissio tuli siihen tulokseen, että vahvimmat myönteiset vaikutukset olisi vaihtoehdolla 2, koska se parantaisi huomattavasti EU:n kuluttajien, yritysten ja julkishallintojen suojaa verkko- ja tietoturvapoikkeamilta. Erityisesti jäsenvaltioille asetettavat vaatimukset takaisivat riittävän varautumistason kansallisella tasolla ja edistäisivät keskinäisen luottamuksen ilmapiiriä, joka on ennakkoedellytys tulokselliselle yhteistyölle EU:n tasolla. Mekanismien luominen verkoston kautta tehtävälle EU-tason yhteistyölle mahdollistaisi johdonmukaisen ja koordinoidun ennaltaehkäisyn ja reagoinnin rajat ylittävien verkko- ja tietoturvapoikkeamien ja -riskien tapauksessa. Julkishallinnoille ja keskeisille yksityissektorin toimijoille asetettavat vaatimukset verkko- ja tietoturvan riskinhallinnasta muodostaisivat vahvan kannusteen hallita turvariskejä tehokkaasti. Velvollisuus ilmoittaa vaikutuksiltaan merkittävistä verkko- ja tietoturvapoikkeamista parantaisi kykyä reagoida turvapoikkeamiin ja edistäisi avoimuutta. Huolehtimalla oman verkko- ja tietoturvansa korkeasta tasosta EU:n voisi lisäksi laajentaa kansainvälistä vaikutusvaltaansa ja toimia entistä uskottavampana kumppanina kahden- ja monenvälisissä yhteyksissä. EU:lla olisi tällöin myös paremmat edellytykset edistää perusoikeuksia ja EU:n perusarvoja kansainvälisesti.

Kvantitatiivinen arviointi osoitti, ettei vaihtoehdosta 2 aiheutuisi suhteetonta taakkaa jäsenvaltioille. Myös yksityissektorille koituvat kustannukset olisivat rajalliset, koska monet kyseeseen tulevista toimijoista joutuvat jo nyt noudattamaan voimassa olevia turvavaatimuksia (nimittäin rekisterinpitäjien velvoitetta tietosuojan varmistaviin teknisiin ja organisatorisiin toimenpiteisiin, joihin sisältyvät myös verkko- ja tietoturvatoimenpiteet). Tämänhetkiset yksityissektorin turvatoimenpiteiden menot on myös otettu huomioon.

Tässä ehdotuksessa kunnioitetaan Euroopan unionin perusoikeuskirjassa tunnustettuja periaatteita, kuten oikeutta yksityiselämän ja viestinnän yksityisyyden kunnioittamiseen, oikeutta henkilötietojen suojaan, elinkeinovapautta, omistusoikeutta, oikeutta tehokkaisiin oikeussuojakeinoihin tuomioistuimessa ja oikeutta tulla kuulluksi. Tämä direktiivi on pantava täytäntöön näiden oikeuksien ja periaatteiden mukaisesti.

3. EHDOTUKSEN OIKEUDELLINEN SISÄLTÖ

3.1. Oikeusperusta

Euroopan unionilla on toimivalta hyväksyä toimenpiteitä, joiden tarkoituksena on toteuttaa sisämarkkinat tai varmistaa niiden toiminta noudattaen asiaa koskevia perussopimusten määräyksiä (Euroopan unionin toiminnasta tehdyn sopimuksen (SEUT) 26 artikla). SEUT-sopimuksen 114 artiklan mukaan EU voi toteuttaa ”sisämarkkinoiden toteuttamista ja toimintaa koskevat toimenpiteet jäsenvaltioiden lakien, asetusten ja hallinnollisten määräysten lähentämiseksi”.

Kuten edellä mainitaan, verkko- ja tietojärjestelmät helpottavat olennaisella tavalla tavaroiden, palvelujen ja ihmisten liikkumista rajojen yli. Ne ovat usein yhteenliitettyjä, ja internet on luonteeltaan globaali. Tämän ylikansallisen ulottuvuuden vuoksi häiriö yhdessä jäsenvaltiossa voi vaikuttaa myös muihin jäsenvaltioihin ja koko EU:hun. Verkko- ja tietojärjestelmien sietokyky ja vakaus ovat sen vuoksi olennaisen tärkeitä sisämarkkinoiden moitteettomalle toiminnalle.

EU:n lainsäädännössä on jo tunnustettu tarve yhdenmukaistaa verkko- ja tietoturvan sääntöjä sisämarkkinoiden kehityksen varmistamiseksi. Tämä koskee erityisesti Euroopan verkko- ja

tietoturvaviraston perustamisesta annettua asetusta (EY) N:o 460/2004[23], joka perustuu SEUT-sopimuksen 114 artiklaan.

Verkko- ja tietoturvan kansallisten valmiuksien, toimintamallien ja suojatason epätasaisuudesta johtuvat erot jäsenvaltioiden välillä johtavat sisämarkkinoiden toimintaa haittaaviin esteisiin, minkä vuoksi EU:n toiminta on perusteltua.

3.2. Toissijaisuusperiaate

EU:n toimet verkko- ja tietoturvan alalla ovat perusteltuja toissijaisuusperiaatteen kannalta.

Ensinnäkin verkko- ja tietoturvan rajat ylittävän luonteen vuoksi toiminnan puute EU:n tasolla johtaisi tilanteeseen, jossa kukin jäsenvaltio toimisi yksinään ottamatta huomioon EU:n verkko- ja tietojärjestelmien keskinäisiä riippuvuussuhteita. Asianmukaisen laaja koordinointi jäsenvaltioiden välillä varmistaisi, että verkko- ja tietoturvariskit voitaisiin hallita rajat ylittävissä yhteyksissä, joissa niitä ilmenee. Verkko- ja tietoturvalainsäädännön erot muodostavat esteen sellaisille yrityksille, jotka haluavat toimia useissa maissa, ja estävät saavuttamasta kokonaisvaltaisia mittakaavaetuja.

Toiseksi EU:n tasolla tarvitaan sääntelyllisiä velvoitteita, jotta voidaan luoda tasapuoliset toimintaedellytykset ja paikata lainsäädännön porsaanreikiä. Täysin vapaaehtoinen lähestymistapa on johtanut yhteistyöhön vain sellaisissa vähemmistönä olevissa jäsenvaltioissa, joiden valmiudet ovat korkealla tasolla. Jotta kaikki jäsenvaltiot voisivat osallistua yhteistyöhön, on tarpeen varmistaa, että niiden kaikkien valmiudet ovat vaaditulla vähimmäistasolla. Valtioiden toteuttamien verkko- ja tietoturvatoimenpiteiden on oltava keskenään johdonmukaisia ja koordinoituja, jotta verkko- ja tietoturvapoikkeamien seuraukset voidaan hallita ja minimoida. Toimivaltaiset viranomaiset ja komissio tekevät verkostossa yhteistyötä ENISAn jatkuvalla tuella ja vaihtamalla tietoa parhaista toimintatavoista, jotta voidaan helpottaa direktiivin johdonmukaista täytäntöönpanoa koko EU:ssa. Yhdenmukaistetuilla verkko- ja tietoturvapoliittisilla toimilla voi olla vahva myönteinen vaikutus myös tehokkaaseen perusoikeuksien suojaan ja erityisesti henkilötietojen ja yksityisyyden suojaan. Tämän vuoksi EU-tason toiminta parantaisi nykyisten kansallisten toimintamallien tuloksellisuutta ja helpottaisi niiden kehitystä.

Ehdotetut toimet ovat perusteltuja myös suhteellisuusperiaatteen kannalta. Jäsenvaltioihin kohdistuvat vaatimukset asetetaan minimitasolle, joka on tarpeen riittävän varautumistason saavuttamiseksi ja luottamukseen perustuvan yhteistyön harjoittamiseksi. Tällöin jäsenvaltiot voivat ottaa asianmukaisesti huomioon kansalliset erikoispiirteet. Tämä myös takaa, että yhteisiä EU:n periaatteita voidaan soveltaa oikeasuhteisella tavalla. Laaja soveltamisala mahdollistaa sen, että jäsenvaltiot voivat panna direktiivin täytäntöön kansallisessa verkko- ja tietoturvastrategiassa määriteltyjen, kansallisella tasolla tosiasiallisesti esiintyvien riskien mukaan. Riskinhallintaa koskevat vaatimukset kohdistuvat vain kriittisiin toimijoihin ja velvoittavat toimenpiteisiin, jotka ovat oikeassa suhteessa riskeihin. Julkisessa kuulemisessa painotettiin merkitystä, joka näiden kriittisten toimijoiden turvallisuuden varmistamisella on. Raportointivaatimukset koskisivat vain vaikutuksiltaan merkittäviä turvapoikkeamia. Kuten edellä todetaan, toimenpiteistä ei aiheutuisi kohtuuttomia kustannuksia, koska monilla näistä toimijoista on rekisterinpitäjinä jo nykyisten tietosuojasääntöjen nojalla velvollisuus varmistaa henkilötietojen suoja.

Jotta vältettäisiin pienille toimijoille, erityisesti pk-yrityksille, aiheutuva kohtuuton rasite, vaatimukset ovat oikeassa suhteessa kulloisenkin verkon tai tietojärjestelmän riskiin eikä niitä sovelleta lainkaan mikroyrityksiin. Riskien määrittelystä vastaavat ensi kädessä näiden

[23] 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).

velvoitteiden kohteena olevat toimijat, joiden on päätettävä toimenpiteistä riskien lieventämiseksi.

Verkko- ja tietoturvapoikkeamien ja -riskien rajatylittävien näkökohtien vuoksi edellä mainitut tavoitteet voidaan saavuttaa paremmin EU:n tasolla kuin jäsenvaltioiden omin toimin. Näin ollen EU voi toteuttaa toimenpiteitä Euroopan unionista tehdyn sopimuksen 5 artiklassa vahvistetun toissijaisuusperiaatteen mukaisesti. Suhteellisuusperiaatteen mukaisesti tässä ehdotetussa direktiivissä ei ylitetä sitä, mikä on näiden tavoitteiden saavuttamiseksi tarpeen.

Tavoitteiden saavuttamiseksi komissiolle olisi siirrettävä valta antaa SEUT-sopimuksen 290 artiklan mukaisesti delegoituja säädöksiä, joilla täydennetään tai muutetaan joitakin perussäädöksen muita kuin keskeisiä osia. Komission ehdotus pyrkii myös tukemaan suhteellisuusperiaatteen toteutumista yksityisille ja julkisille toimijoille määrättyjen velvoitteiden täytäntöönpanossa.

Yhtenäisten olosuhteiden saavuttamiseksi perussäädöksen täytäntöönpanolle komissiolle olisi siirrettävä valta antaa SEUT-sopimuksen 291 artiklan mukaisesti täytäntöönpanosäädöksiä.

Erityisesti kun otetaan huomioon ehdotetun direktiivin laaja soveltamisala, sen kohteena olevat tiukasti säännellyt alat sekä sen IV luvusta johtuvat oikeudelliset velvoitteet, selittävät asiakirjat olisi liitettävä mukaan ilmoitettaessa toimenpiteistä, joilla direktiivi saatetaan osaksi kansallista lainsäädäntöä. Jäsenvaltiot ovat selittävistä asiakirjoista 28 päivänä syyskuuta 2011 annetun jäsenvaltioiden ja komission yhteisen poliittisen lausuman mukaisesti sitoutuneet perustelluissa tapauksissa liittämään ilmoitukseen toimenpiteistä, jotka koskevat direktiivin saattamista osaksi kansallista lainsäädäntöä, yhden tai useamman asiakirjan, joista käy ilmi direktiivin osien ja kansallisen lainsäädännön osaksi saattamiseen tarkoitettujen välineiden vastaavien osien suhde. Tämän direktiivin osalta lainsäätäjä katsoo tällaisten asiakirjojen toimittamisen olevan perusteltua.

4. TALOUSARVIOVAIKUTUKSET

Jäsenvaltioiden välistä yhteistyötä ja tiedonvaihtoa varten olisi oltava käytössä suojattu infrastruktuuri. Ehdotuksella on vaikutuksia EU:n talousarvioon vain, jos jäsenvaltiot päättävät mukauttaa olemassa olevaa infrastruktuuria (esim. sTESTA) ja antavat komissiolle tehtäväksi tämän täytäntöönpanon monivuotisessa rahoituskehyksessä 2014–2020. Kertaluonteiset kustannukset on arvioitu 1 250 000 euroksi, ja ne katettaisiin EU:n talousarvion budjettikohdasta 09.03.02 (jolla edistetään kansallisten julkisten palvelujen verkkoon liittämistä ja yhteentoimivuutta sekä pääsyä tällaisiin verkkoihin — Luku 09.03, ”Verkkojen Eurooppa ” -väline — televerkot) sillä ehdolla, että ”Verkkojen Eurooppa” -välineestä on tarjolla riittävästi varoja. Vaihtoehtoisesti jäsenvaltiot voivat joko jakaa nykyisen infrastruktuurin mukauttamisesta aiheutuvat kertaluonteiset kustannukset tai päättää luoda uuden infrastruktuurin ja vastata sen kustannuksista, joiden arvioidaan olevan noin 10 miljoonaa euroa vuodessa.

2013/0027 (COD)

Ehdotus

EUROOPAN PARLAMENTIN JA NEUVOSTON DIREKTIIVI

toimenpiteistä yhteisen korkeatasoisen verkko- ja tietoturvan varmistamiseksi koko unionissa

EUROOPAN PARLAMENTTI JA EUROOPAN UNIONIN NEUVOSTO, jotka

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

ottavat huomioon Euroopan komission ehdotuksen,

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

ottavat huomioon Euroopan talous- ja sosiaalikomitean lausunnon[1],

ovat kuulleet Euroopan tietosuojavaltuutettua,

noudattavat tavallista lainsäätämisjärjestystä,

sekä katsovat seuraavaa:

(1) Verkko- ja tietojärjestelmillä ja -palveluilla on elintärkeä tehtävä yhteiskunnassa. Niiden luotettavuus ja turvallisuus ovat olennaisen tärkeitä talouden toiminnalle ja sosiaaliselle hyvinvoinnille ja erityisesti sisämarkkinoiden toiminnalle.

(2) Tahallisten tai tahattomien turvapoikkeamien laajuus ja esiintymistiheys kasvavat ja muodostavat merkittävän uhan verkko- ja tietojärjestelmien toiminnalle. Tällaiset turvapoikkeamat voivat toimia esteenä taloudelliselle toiminnalle, tuottaa huomattavia taloudellisia tappioita, heikentää käyttäjien luottamusta ja aiheuttaa merkittävää vahinkoa unionin taloudelle.

(3) Digitaaliset tietojärjestelmät, ensisijaisesti internet, ovat rajat ylittäviä viestintävälineitä, jotka helpottavat olennaisesti tavaroiden, palvelujen ja ihmisten liikkumista rajojen yli. Tämän ylikansallisen luonteen vuoksi näiden järjestelmien merkittävä häiriö yhdessä jäsenvaltiossa voi vaikuttaa myös muihin jäsenvaltioihin ja koko EU:hun. Verkko- ja tietojärjestelmien sietokyky ja vakaus on sen vuoksi olennaisen tärkeää sisämarkkinoiden moitteettomalle toiminnalle.

(4) Olisi otettava käyttöön unionin tason yhteistyömekanismi, joka mahdollistaa verkko- ja tietoturvaan liittyvän tiedonvaihdon sekä koordinoidun havaitsemisen ja reagoinnin. Jotta tämä mekanismi olisi tehokas ja kaikkien jäsenvaltioiden käytettävissä, on olennaisen tärkeää, että kaikilla jäsenvaltioilla on vähimmäisvalmiudet ja strategia, joilla varmistetaan korkeatasoinen verkko- ja tietoturva niiden alueella. Vähimmäistason turvallisuusvaatimuksia olisi sovellettava myös julkishallintoihin ja elintärkeän tietoinfrastruktuurin operaattoreihin, jotta voidaan edistää riskinhallintakulttuuria ja varmistaa raportointi vakavimmista turvapoikkeamista.

[1] EUVL C […], […], s. […].

(5) Jotta tämä direktiivi kattaisi kaikki merkitykselliset turvapoikkeamat ja -riskit, sitä olisi sovellettava kaikkiin verkko- ja tietojärjestelmiin. Julkishallinnoille ja markkinatoimijoille asetettavia velvoitteita ei kuitenkaan pitäisi soveltaa yrityksiin, jotka tarjoavat käyttöön sähköisten viestintäverkkojen ja -palvelujen yhteisestä sääntelyjärjestelmästä (puitedirektiivi) 7 päivänä maaliskuuta 2002 annetussa Euroopan parlamentin ja neuvoston direktiivissä 2002/21/EY[2] tarkoitettuja yleisiä viestintäverkkoja tai yleisesti saatavilla olevia sähköisiä viestintäpalveluja, joihin sovelletaan mainitun direktiivin 13 a artiklassa vahvistettuja erityisiä turvallisuutta ja eheyttä koskevia vaatimuksia, eikä niitä pitäisi soveltaa luottamuspalvelun tarjoajiin.

(6) Nykyiset valmiudet eivät riitä varmistamaan korkeatasoista verkko- ja tietoturvaa unionissa. Jäsenvaltioiden valmiudet ovat tasoltaan hyvin erilaisia, mikä johtaa hajanaisiin lähestymistapoihin eri puolilla unionia. Tämä johtaa epätasaiseen suojaan kuluttajille ja yrityksille ja heikentää yleistä verkko- ja tietoturvan tasoa unionissa. Julkishallintoja ja markkinatoimijoita koskevien yhteisten vähimmäisvaatimusten puuttuminen puolestaan merkitsee sitä, ettei unionin tasolla ole mahdollista luoda kokonaisvaltaista ja tuloksellista yhteistyömekanismia.

(7) Tehokas reagointi verkko- ja tietojärjestelmien turvallisuuden asettamiin haasteisiin edellyttää sen vuoksi unionin tason kokonaisvaltaista lähestymistapaa, joka kattaa yhteisten vähimmäisvalmiuksien luomista ja suunnittelua koskevat vaatimukset, tiedonvaihdon ja toimien koordinoinnin sekä yhteiset vähimmäisturvavaatimukset kaikille kyseeseen tuleville markkinatoimijoille ja julkishallinnoille.

(8) Tämän direktiivin säännökset eivät saisi rajoittaa kunkin jäsenvaltion mahdollisuutta toteuttaa tarvittavat toimenpiteet, joilla varmistetaan sen olennaisten turvallisuusetujen suojelu, taataan yleinen järjestys ja turvallisuus ja mahdollistetaan rikosten tutkinta, selvittäminen ja syytteeseenpano. SEUT-sopimuksen 346 artiklan mukaisesti mitään jäsenvaltiota ei pitäisi velvoittaa antamaan tietoja, joiden ilmaisemisen se katsoo keskeisten turvallisuusetujensa vastaiseksi.

(9) Verkko- ja tietoturvan yhteisen korkean tason saavuttamiseksi ja ylläpitämiseksi kullakin jäsenvaltiolla olisi oltava kansallinen verkko- ja tietoturvastrategia, jossa määritellään strategiset tavoitteet ja toteutettavat konkreettiset toimet. Kansallisella tasolla on tarpeen kehittää olennaiset vaatimukset täyttäviä verkko- ja tietoturvan yhteistyösuunnitelmia, jotta saavutetaan valmiudet ja reagointikyky sellaisella tasolla, että voidaan toimia tuloksellisesti yhteistyössä kansallisella ja unionin tasolla turvapoikkeamien sattuessa.

(10) Jotta tämän direktiivin nojalla annetut säännökset voitaisiin panna tehokkaasti täytäntöön, kunkin jäsenvaltion olisi perustettava tai yksilöitävä elin vastaamaan verkko- ja tietoturvakysymysten koordinoinnista ja toimimaan keskuspisteenä yhteistyölle rajojen yli unionin tasolla. Näille elimille olisi annettava riittävät tekniset, taloudelliset ja inhimilliset voimavarat, jotta ne voivat toteuttaa tehokkaasti ja tuloksekkaasti niille osoitetut tehtävät ja siten saavuttaa tämän direktiivin tavoitteet.

(11) Kaikilla jäsenvaltioilla olisi oltava käytössään riittävät sekä tekniset että organisatoriset valmiudet, jotta voidaan ehkäistä ja havaita verkko- ja tietojärjestelmien turvapoikkeamia ja -riskejä, reagoida niihin ja lieventää niiden vaikutuksia. Tämän vuoksi kaikkiin jäsenvaltioihin olisi perustettava hyvin toimivat ja olennaiset vaatimukset täyttävät tietotekniikan kriisiryhmät (CERT), jotta voidaan

[2] EYVL L 108, 24.04.2002, s. 33.

taata toimivat ja yhteensopivat valmiudet turvapoikkeamien ja -riskien varalta ja varmistaa tehokas yhteistyö unionin tasolla.

(12) Euroopan jäsenvaltiofoorumilla (EFMS) on viety merkittävästi eteenpäin keskustelua ja tiedonvaihtoa hyvistä toimintamalleista, myös kehitetty periaatteita eurooppalaiselle kyberkriisejä koskevalle yhteistyölle. Jäsenvaltioiden olisi tätä edistystä hyödyntäen muodostettava verkosto, jonka kautta ne voivat olla jatkuvasti yhteydessä toisiinsa ja tukea yhteistyötään. Tämän turvatun ja tuloksellisen yhteistyömekanismin olisi mahdollistettava jäsennetty ja koordinoitu tiedonvaihto, havaitseminen ja reagointi unionin tasolla.

(13) Euroopan verkko- ja tietoturvaviraston (ENISA) olisi avustettava jäsenvaltioita ja komissiota antamalla asiantuntemusta ja neuvontaa ja helpottamalla parhaiden käytäntöjen vaihtamista. Komission olisi erityisesti kuultava ENISAa tämän direktiivin soveltamisesta. Jotta voidaan varmistaa toimiva ja oikea-aikainen tiedonsaanti jäsenvaltioille ja komissiolle, yhteistyöverkostossa olisi annettava varhaisvaroitukset turvapoikkeamista ja -riskeistä. Jotta voidaan kehittää valmiuksia ja tietämystä jäsenvaltioiden välillä, yhteistyöverkoston avulla olisi myös levitettävä parhaita toimintatapoja, avustettava sen jäseniä valmiuksien kehittämisessä sekä ohjattava vertaisarviointien ja verkko- ja tietoturvaharjoitusten organisointia.

(14) Arkaluonteisten ja luottamuksellisten tietojen vaihtamiseksi verkostossa olisi otettava käyttöön suojattu tiedonjakoinfrastruktuuri. Rajoittamatta velvollisuutta ilmoittaa yhteistyöverkostolle unionin kannalta merkittävistä turvapoikkeamista ja -riskeistä pääsy muista jäsenvaltioista tuleviin luottamuksellisiin tietoihin olisi annettava jäsenvaltioille vain, jos ne voivat näyttää toteen, että niiden tekniset, taloudelliset ja inhimilliset voimavarat ja prosessit sekä niiden viestintäinfrastruktuuri takaavat, että ne voivat osallistua verkostoon tehokkaasti, tuloksekkaasti ja turvallisesti.

(15) Koska useimmat verkko- ja tietojärjestelmät ovat yksityisten ylläpitämiä, julkisen ja yksityisen sektorin välinen yhteistyö on olennaisen tärkeää. Markkinatoimijoita olisi kannustettava kehittämään omia epävirallisia yhteistyömekanismejaan verkko- ja tietoturvan varmistamiseksi. Niiden olisi myös tehtävä yhteistyötä julkisen sektorin kanssa sekä jaettava tietoa ja parhaita toimintatapoja vastineeksi operatiivisesta tuesta turvapoikkeamien tapauksessa.

(16) Avoimuuden varmistamiseksi ja EU:n kansalaisten ja markkinatoimijoiden informoimiseksi asianmukaisesti toimivaltaisten viranomaisten olisi perustettava yhteinen verkkosivusto, jolla julkaistaan ei-luottamukselliset tiedot turvapoikkeamista ja -riskeistä.

(17) Jos tietoja pidetään luottamuksellisina liikesalaisuuksia koskevien unionin ja kansallisten sääntöjen mukaisesti, tällainen luottamuksellisuus on varmistettava tässä direktiivissä vahvistettujen toimien ja tavoitteiden toteuttamisen yhteydessä.

(18) Erityisesti kansallisten kriisinhallintakokemusten perusteella ja yhteistyössä ENISAn kanssa komission ja jäsenvaltioiden olisi luotava unionin verkko- ja tietoturvan yhteistyösuunnitelma, jossa määritellään yhteistyömekanismit turvariskien ja -poikkeamien torjumiseksi. Tämä suunnitelma olisi otettava asianmukaisesti huomioon varhaisvaroitusten tekemisessä yhteistyöverkostossa.

(19) Verkostossa tehtävää varhaisvaroitusta olisi edellytettävä ainoastaan silloin kun turvapoikkeaman tai -riskin laajuus ja vakavuus ovat niin merkittäviä tai niistä voi tulla niin merkittäviä, että niistä on tarpeen antaa tietoa tai niihin on tarpeen reagoida unionin tasolla. Varhaisvaroitukset olisi sen vuoksi rajoitettava sellaisiin todellisiin tai

mahdollisiin turvapoikkeamiin tai -riskeihin, jotka leviävät nopeasti, ylittävät kansallisen reagointivalmiuden tai vaikuttavat useampaan kuin yhteen jäsenvaltioon. Asianmukaisen arvioinnin mahdollistamiseksi yhteistyöverkostolle olisi ilmoitettava kaikki tiedot, joilla on merkitystä turvariskin tai -poikkeaman arvioinnin kannalta.

(20) Saatuaan varhaisvaroituksen ja sen arvioinnin toimivaltaisten viranomaisten olisi sovittava koordinoidusta reagoinnista unionin verkko- ja tietoturvan yhteistyösuunnitelman mukaisesti. Sekä toimivaltaisille viranomaisille että komissiolle olisi ilmoitettava toimenpiteistä, jotka kansallisella tasolla on toteutettu koordinoidun reagoinnin tuloksena.

(21) Verkko- ja tietoturvaongelmien maailmanlaajuisen luonteen vuoksi tarvitaan tiiviimpää kansainvälistä yhteistyötä, jolla voidaan parantaa turvallisuusstandardeja ja tiedonvaihtoa sekä edistää yhteistä maailmanlaajuista lähestymistapaa verkko- ja tietoturvakysymyksiin.

(22) Vastuu verkko- ja tietoturvan varmistamisesta lankeaa paljolti julkishallinnoille ja markkinatoimijoille. Riskinhallintakulttuuria, johon sisältyy riskinarviointi ja riskeihin suhteutettujen turvatoimenpiteiden toteuttaminen, olisi edistettävä ja kehitettävä asianmukaisten sääntelyllisten vaatimusten ja toimialojen vapaaehtoisten käytäntöjen kautta. Tasavertaisten toimintaedellytysten luominen on myös olennaista yhteistyöverkoston tehokkaan toiminnan kannalta, jotta voidaan varmistaa tuloksellinen yhteistyö kaikkien jäsenvaltioiden taholta.

(23) Direktiivissä 2002/21/EY velvoitetaan yritykset, jotka tarjoavat käyttöön yleisiä viestintäverkkoja tai yleisesti saatavilla olevia sähköisiä viestintäpalveluja, toteuttamaan aiheelliset toimenpiteet niiden eheyden ja turvallisuuden varmistamiseksi ja otetaan käyttöön ilmoitusvaatimukset turvallisuuden loukkausten ja eheyden menetysten varalta. Henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla (sähköisen viestinnän tietosuojadirektiivi) 12 päivänä heinäkuuta 2002 annettu Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY[3] velvoittaa yleisesti saatavilla olevan sähköisen viestintäpalvelun tarjoajat toteuttamaan asianmukaiset tekniset ja organisatoriset toimenpiteet varmistaakseen tarjoamiensa palvelujen turvallisuuden.

(24) Nämä velvollisuudet olisi laajennettava sähköisen viestinnän sektorin ulkopuolelle teknisiä standardeja ja määräyksiä ja tietoyhteiskunnan palveluja koskevia määräyksiä koskevien tietojen toimittamisessa noudatettavasta menettelystä 22 päivänä kesäkuuta 1998 annetussa Euroopan parlamentin ja neuvoston direktiivissä 98/34/EY[4] määriteltyjen sellaisten tietoyhteiskunnan palvelujen keskeisiin tarjoajiin, jotka tukevat loppukäyttäjille suunnattuja tietoyhteiskunnan palveluja tai verkkotoimintoja, kuten sähköisen kaupankäynnin alustoja, internet-välitteisiä maksupalveluja, verkkoyhteisöpalveluja, hakukoneita, pilvipalveluja ja sovelluskauppoja. Häiriöt näissä tietoyhteiskunnan mahdollistavissa palveluissa estävät tarjoamasta muita tietoyhteiskunnan palveluja, jotka ovat niistä keskeisesti riippuvaisia. Ohjelmistojen kehittäjät ja laitevalmistajat eivät ole tietoyhteiskunnan palvelujen tarjoajia, minkä vuoksi ne jäävät direktiivin soveltamisalan ulkopuolelle. Edellä mainitut velvollisuudet olisi laajennettava koskemaan myös julkishallintoja ja elintärkeiden infrastruktuurien operaattoreita, sillä ne ovat vahvasti riippuvaisia tieto- ja viestintäteknologiasta ja olennaisia elintärkeiden talouden ja yhteiskunnan toimintojen, kuten sähkön ja kaasun jakelun, liikenteen, luottolaitosten, pörssien ja

[3] EYVL L 201, 31.7.2002, s. 37.
[4] EYVL L 204, 21.7.1998, s. 37.

terveydenhuollon, ylläpitämiselle. Häiriö näissä verkko- ja tietojärjestelmissä vaikuttaisi sisämarkkinoihin.

(25) Julkishallinnoille ja markkinatoimijoille määrättävät tekniset ja organisatoriset toimenpiteet eivät saisi edellyttää jonkin tietyn kaupallisen tieto- ja viestintäteknologiatuotteen suunnittelua, kehittämistä tai valmistamista tietyllä tavalla.

(26) Julkishallintojen ja markkinatoimijoiden olisi varmistettava valvonnassaan olevien verkkojen ja järjestelmien turvallisuus. Näitä ovat ensisijaisesti yksityiset verkot ja järjestelmät, joita hallinnoi joko niiden oma tietotekninen henkilöstö tai joiden tietoturvahallinto on ulkoistettu. Turvallisuus- ja ilmoitusvaatimuksia olisi sovellettava kyseeseen tuleviin markkinatoimijoihin ja julkishallintoihin riippumatta siitä, huolehtivatko ne verkko- ja tietojärjestelmiensä ylläpidosta sisäisesti vai ulkoistavatko ne sen.

(27) Jotta pienille toimijoille ja käyttäjille ei aiheutuisi suhteetonta taloudellista ja hallinnollista rasitetta, vaatimusten olisi oltava oikeassa suhteessa kulloisenkin verkon tai tietojärjestelmän turvariskiin ottaen huomioon tällaisiin toimenpiteisiin käytettävä uusin tekniikka. Näitä vaatimuksia ei pitäisi soveltaa mikroyrityksiin.

(28) Toimivaltaisten viranomaisten olisi kiinnitettävä asianmukaista huomiota epävirallisten ja luotettavien tiedonjakokanavien säilyttämiseen markkinatoimijoiden välillä ja julkisen ja yksityisen sektorin välillä. Toimivaltaisille viranomaisille raportoitujen turvapoikkeamien julkistamisessa olisi otettava asianmukaisesti ja tasapainoisesti huomioon yleisön yleinen etu saada tietoa uhista sekä mahdollinen turvapoikkeamista raportoivien julkishallintojen ja markkinatoimijoiden maineen vahingoittuminen ja niille koituva taloudellinen vahinko. Ilmoitusvelvoitteiden täytäntöönpanossa toimivaltaisten viranomaisten olisi kiinnitettävä erityistä huomiota tarpeeseen pitää tuotteiden haavoittuvuutta koskevat tiedot tiukasti luottamuksellisena ennen asianomaisten turvallisuuspäivitysten julkistamista.

(29) Toimivaltaisilla viranomaisilla olisi oltava tarvittavat keinot tehtäviensä suorittamiseen, mukaan lukien valtuudet saada riittävät tiedot markkinatoimijoilta ja julkishallinnoilta verkko- ja tietojärjestelmien turvatason arvioimiseksi sekä luotettavat ja kattavat tiedot verkko- ja tietojärjestelmien toimintaan vaikuttaneista tosiasiallisista turvapoikkeamista.

(30) Turvapoikkeaman taustalla on usein rikollinen toiminta. Turvapoikkeamien rikollista luonnetta voidaan epäillä, vaikka sitä tukeva näyttö ei olisi riittävän selvä alusta alkaen. Toimivaltaisten viranomaisten ja lainvalvontaviranomaisten välisen yhteistyön olisi tällöin oltava osa tehokasta ja kokonaisvaltaista reagointia turvapoikkeamien uhkaan. Turvallisen, varman ja kestävämmän ympäristön kehittäminen edellyttää erityisesti, että turvapoikkeamista, joihin epäillään liittyvän vakavaa rikollisuutta, raportoidaan järjestelmällisesti lainvalvontaviranomaisille. Se, liittyykö turvapoikkeamiin vakavaa rikollisuutta, olisi arvioitava tietoverkkorikollisuutta koskevan EU:n lainsäädännön perusteella.

(31) Turvapoikkeamat vaarantavat monissa tapauksissa henkilötiedot. Toimivaltaisten viranomaisten ja tietosuojaviranomaisten olisi tässä yhteydessä tehtävä yhteistyötä ja vaihdettava tietoa kaikista asiaankuuluvista seikoista, jotta voidaan puuttua turvapoikkeamista johtuviin henkilötietojen tietoturvaloukkauksiin. Jäsenvaltioiden on pantava täytäntöön velvollisuus ilmoittaa turvapoikkeamista tavalla, joka minimoi hallinnollisen rasitteen tapauksissa, joissa turvapoikkeama on myös yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta

annetussa Euroopan parlamentin ja neuvoston asetuksessa[5] tarkoitettu henkilötietojen tietoturvaloukkaus. ENISA voisi tällöin toimia toimivaltaisten viranomaisten ja tietosuojaviranomaisten kanssa yhteistyössä kehittämällä tiedonvaihtomekanismeja ja -malleja, joiden avulla vältetään tarve kahdelle ilmoitusmallille. Yksi yhteinen ilmoitusmalli helpottaisi henkilötiedot vaarantaneista turvapoikkeamista raportoimista ja keventäisi yrityksille ja julkishallinnoille koituvaa hallinnollista taakkaa.

(32) Turvallisuusvaatimusten standardointi tapahtuu markkinavetoisesti. Turvastandardien johdonmukaisen soveltamisen varmistamiseksi jäsenvaltioiden olisi edistettävä tiettyjen standardien noudattamista tai mukaisuutta, jotta voidaan varmistaa turvallisuuden korkea taso unionissa. Tätä varten voi olla tarpeen laatia yhdenmukaistettuja standardeja, jolloin olisi noudatettava 25 päivänä lokakuuta 2012 annettua Euroopan parlamentin ja neuvoston asetusta (EU) N:o 1025/2012 eurooppalaisesta standardoinnista, neuvoston direktiivien 89/686/ETY ja 93/15/ETY sekä Euroopan parlamentin ja neuvoston direktiivien 94/9/EY, 94/25/EY, 95/16/EY, 97/23/EY, 98/34/EY, 2004/22/EY, 2007/23/EY, 2009/23/EY ja 2009/105/EY muuttamisesta ja neuvoston päätöksen 87/95/ETY ja Euroopan parlamentin ja neuvoston päätöksen N:o 1673/2006/EY kumoamisesta[6].

(33) Komission olisi tarkasteltava tätä direktiiviä säännöllisin väliajoin uudelleen erityisesti tekniikan ja markkinaolojen kehitykseen perustuvien muutostarpeiden selvittämiseksi.

(34) Yhteistyöverkoston moitteettoman toiminnan mahdollistamiseksi olisi komissiolle siirrettävä valta hyväksyä Euroopan unionin toiminnasta tehdyn sopimuksen 290 artiklan mukaisesti säädösvallan siirron nojalla annettavia delegoituja säädöksiä, joilla määritellään perusteet, jotka jäsenvaltion on täytettävä voidakseen osallistua suojattuun tiedonjakojärjestelmään, täsmennetään tarkemmin varhaisvaroituksen käynnistävät tapahtumat ja määritellään olosuhteet, joissa markkinatoimijoiden ja julkishallintojen on ilmoitettava turvapoikkeamista.

(35) On erityisen tärkeää, että komissio toteuttaa asiaa valmistellessaan asianmukaiset kuulemiset, myös asiantuntijatasolla. Komission olisi delegoituja säädöksiä valmistellessaan ja laatiessaan varmistettava, että asianomaiset asiakirjat toimitetaan Euroopan parlamentille ja neuvostolle yhtäaikaisesti, hyvissä ajoin ja asianmukaisesti.

(36) Jotta voidaan varmistaa yhdenmukaiset edellytykset tämän direktiivin täytäntöönpanolle komissiolle olisi siirrettävä täytäntöönpanovaltaa siltä osin kuin on kyse toimivaltaisten viranomaisten ja komission välisestä yhteistyöstä yhteistyöverkostossa, pääsystä suojattuun tiedonjakoinfrastruktuuriin, unionin verkko- ja tietoturvan yhteistyösuunnitelmasta, turvapoikkeamia koskevan julkisen tiedotuksen muodoista ja menettelyistä sekä verkko- ja tietoturvan kannalta merkityksellisistä standardeista ja/tai teknisistä eritelmistä. Tätä valtaa olisi käytettävä yleisistä säännöistä ja periaatteista, joiden mukaisesti jäsenvaltiot valvovat komission täytäntöönpanovallan käyttöä, 16 päivänä helmikuuta 2011 annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 182/2011[7] mukaisesti.

(37) Komission olisi tämän direktiivin täytäntöönpanossa toimittava tarpeen mukaan yhteistyössä asiaankuuluvien alakohtaisten komiteoiden ja EU:n tasolla erityisesti energian, liikenteen ja terveyden alalla perustettujen elinten kanssa.

---

5 SEC(2012) 72 final.

6 EUVL L 316, 14.11.2012, s. 12.

7 EUVL L 55, 28.2.2011, s. 13.

(38) Tietoja, jotka toimivaltainen viranomainen katsoo liikesalaisuuksia koskevien unionin ja kansallisten sääntöjen mukaisesti luottamuksellisiksi, olisi vaihdettava komission ja muiden toimivaltaisten viranomaisten kanssa vain silloin kun se on ehdottoman välttämätöntä tämän direktiivin soveltamiseksi. Tällöin olisi toimitettava vain ne tiedot, jotka ovat merkityksellisiä ja laajuudeltaan oikein suhteutettuja kulloisenkin tiedonvaihdon tarkoituksen kannalta.

(39) Turvariskejä ja -poikkeamia koskevien tietojen jakaminen yhteistyöverkostossa ja turvapoikkeamista kansallisille viranomaisille ilmoittamista koskevien vaatimusten noudattaminen voivat edellyttää henkilötietojen käsittelyä. Tällainen henkilötietojen käsittely on tarpeen, jotta voidaan saavuttaa tämän direktiivin tavoitteet, jotka liittyvät yleiseen etuun ja jotka ovat näin ollen perusteltuja direktiivin 95/46/EY 7 artiklan nojalla. Se ei näiden oikeutettujen tavoitteiden kannalta merkitse perusoikeuskirjan 8 artiklalla taattuun henkilötietojen suojaan puuttumista suhteettomalla ja kohtuuttomalla tavalla, joka loukkaisi tämän oikeuden keskeistä sisältöä. Tämän direktiivin soveltamiseksi olisi soveltuvin osin sovellettava Euroopan parlamentin, neuvoston ja komission asiakirjojen saamisesta yleisön tutustuttavaksi 30 päivänä toukokuuta 2001 annettua Euroopan parlamentin ja neuvoston asetusta (EY) N:o 1049/2001[8]. Kun tietoja käsittelevät unionin toimielimet ja muut elimet, kyseisessä tämän direktiivin täytäntöönpanemiseksi suoritettavassa tietojen käsittelyssä olisi noudatettava yksilöiden suojelusta yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta 18 päivänä joulukuuta 2000 annettua Euroopan parlamentin ja neuvoston asetusta (EY) N:o 45/2001.

(40) Koska jäsenvaltiot eivät voi yksinään riittävällä tavalla saavuttaa tämän direktiivin tavoitetta, joka on verkko- ja tietoturvan korkean tason varmistaminen unionissa, vaan se voidaan toimien vaikutusten vuoksi saavuttaa paremmin unionin tasolla, unioni voi toteuttaa toimenpiteitä Euroopan unionista tehdyn sopimuksen 5 artiklassa vahvistetun toissijaisuusperiaatteen mukaisesti. Mainitussa artiklassa vahvistetun suhteellisuusperiaatteen mukaisesti tässä direktiivissä ei ylitetä sitä, mikä on näiden tavoitteiden saavuttamiseksi tarpeen.

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

OVAT HYVÄKSYNEET TÄMÄN DIREKTIIVIN:

I LUKU

YLEISET SÄÄNNÖKSET

1 artikla

Kohde ja soveltamisala

1. Tässä direktiivissä säädetään toimenpiteistä verkko- ja tietoturvan yhteisen korkean tason varmistamiseksi unionissa.

[8] EYVL L 145, 31.05.2001, s. 43.

2. Tätä varten tässä direktiivissä

(a) vahvistetaan kaikille jäsenvaltioille velvoitteet, jotka koskevat verkko- ja tietojärjestelmiin vaikuttavien turvariskien ja -poikkeamien ennaltaehkäisyä ja käsittelyä ja niihin reagoimista;

(b) luodaan jäsenvaltioiden välinen yhteistyömekanismi, jotta voidaan varmistaa tämän direktiivin yhtenäinen soveltaminen unionissa ja tarvittaessa verkko- ja tietojärjestelmiin vaikuttavien turvariskien ja -poikkeamien koordinoitu ja tehokas käsittely ja niihin reagoiminen;

(c) vahvistetaan turvavaatimukset markkinatoimijoille ja julkishallinnoille.

3. Jäljempänä 14 artiklassa vahvistettuja turvavaatimuksia ei sovelleta yrityksiin, jotka tarjoavat käyttöön direktiivissä 2002/21/EY tarkoitettuja yleisiä viestintäverkkoja tai yleisesti saatavilla olevia sähköisiä viestintäpalveluja, joihin sovelletaan mainitun direktiivin 13 a ja 13 b artiklassa vahvistettuja erityisiä turvallisuutta ja eheyttä koskevia vaatimuksia, eikä luottamuspalvelun tarjoajiin.

4. Tämä direktiivi ei rajoita tietoverkkorikollisuutta koskevan EU:n lainsäädännön soveltamista eikä Euroopan elintärkeän infrastruktuurin määrittämisestä ja nimeämisestä sekä arvioinnista, joka koskee tarvetta parantaa sen suojaamista, annetun neuvoston direktiivin 2008/114/EY[9] soveltamista.

5. Tämä direktiivi ei myöskään rajoita yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta 24 päivänä lokakuuta 1995 annetun Euroopan parlamentin ja neuvoston direktiivin 95/46/EY[10], henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla 12 päivänä heinäkuuta 2002 annetun Euroopan parlamentin ja neuvoston direktiivin 2002/58/EY eikä yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta annetun Euroopan parlamentin ja neuvoston asetuksen[11] soveltamista.

6. Tiedon jakaminen yhteistyöverkostossa III luvun mukaisesti ja verkko- ja tietoturvapoikkeamista 14 artiklan mukaisesti tehtävät ilmoitukset voivat edellyttää henkilötietojen käsittelyä. Jäsenvaltion on hyväksyttävä tällainen käsittely, joka on välttämätöntä yleiseen etuun liittyvien tämän direktiivin tavoitteiden kannalta, direktiivin 95/46/EY 7 artiklan ja direktiivin 2002/58/EY, sellaisina kuin ne on pantu täytäntöön kansallisessa lainsäädännössä, mukaisesti.

2 artikla

Vähimmäistason yhdenmukaistaminen

Jäsenvaltioita ei estetä hyväksymästä tai pitämästä voimassa säännöksiä, joilla varmistetaan korkeampi turvataso, sanotun kuitenkaan rajoittamatta niille unionin lainsäädännön nojalla kuuluvia velvoitteita.

3 artikla

Määritelmät

Tässä direktiivissä tarkoitetaan

---

9 EUVL L 345, 23.12.2008, s. 75.
10 EYVL L 281, 23.11.1995, s. 31.
11 SEC(2012) 72 final.

(1) ’verkko- ja tietojärjestelmällä’

(a) direktiivissä 2002/21/EY tarkoitettua sähköistä viestintäverkkoa ja

(b) yhtä tai useampaa laitetta tai yhteen kytkettyjen tai toisiinsa yhteydessä olevien laitteiden ryhmää, joka ohjelman avulla suorittaa automaattista tietojenkäsittelyä sekä

(c) sähköisiä tietoja, joita a ja b alakohdassa mainituissa järjestelmissä varastoidaan, käsitellään, hankitaan tai välitetään niiden toimintaa, käyttöä, suojausta tai ylläpitoa varten.

(2) ’turvallisuudella’ verkko- tai tietojärjestelmän kykyä suojautua tietyllä varmuudella onnettomuuksilta tai tahallisilta toimilta, jotka vaarantavat tallennettujen tai siirrettyjen tietojen ja muiden kyseisessä verkko- ja tietojärjestelmässä tai sen välityksellä tarjottujen tai välitettävien palvelujen saatavuuden, aitouden, eheyden ja luottamuksellisuuden;

(3) ’turvariskillä’ mitä tahansa tilannetta tai tapahtumaa, joka saattaa vaikuttaa kielteisesti turvallisuuteen;

(4) ’turvapoikkeamalla’ mitä tahansa tilannetta tai tapahtumaa, joka tosiasiassa vaikuttaa kielteisesti turvallisuuteen;

(5) ’tietoyhteiskunnan palvelulla’ direktiivin 98/34/EY 1 artiklan 2 alakohdassa tarkoitettua palvelua;

(6) ’verkko- ja tietoturvan yhteistyösuunnitelmalla’ suunnitelmaa, jossa vahvistetaan puitteet organisatorisille tehtäville, vastuille ja menettelyille verkkojen ja tietojärjestelmien toiminnan ylläpitämiseksi tai palauttamiseksi niihin vaikuttavan turvariskin tai turvapoikkeaman tapauksessa;

(7) ’turvapoikkeamien käsittelyllä’ kaikkia menettelyjä, jotka tukevat turvapoikkeaman analyysia, sen vaikutusten rajoittamista ja siihen reagointia;

(8) ’markkinatoimijalla’

(a) sellaisten tietoyhteiskunnan palvelujen tarjoajaa, jotka mahdollistavat muiden tietoyhteiskunnan palvelujen tarjoamisen; näistä palveluntarjoajista on ei-tyhjentävä luettelo liitteessä II;

(b) sellaisten elintärkeiden infrastruktuurien ylläpitäjää, jotka ovat olennaisia elintärkeiden talouden ja yhteiskunnan toimintojen ylläpitämiselle energiahuollon, liikenteen, pankkitoimen, pörssitoimen ja terveydenhuollon aloilla; näistä operaattoreista on ei-tyhjentävä luettelo liitteessä II;

(9) ’standardilla’ asetuksessa (EU) N:o 1025/2012 tarkoitettua standardia;

(10) ’eritelmällä’ asetuksessa (EU) N:o 1025/2012 tarkoitettua eritelmää;

(11) ‘luottamuspalvelun tarjoajalla’ luonnollista tai oikeushenkilöä, joka tarjoaa sähköistä palvelua, joka koostuu sähköisten allekirjoitusten, sähköisten sinettien, sähköisten aikaleimojen, sähköisten asiakirjojen, sähköisten jakelupalvelujen, verkkosivustojen todentamisen ja sähköisten varmenteiden, mukaan luettuina sähköisten allekirjoitusten ja sähköisten sinettien varmenteet, luomisesta, tarkastamisesta, todentamisesta, käsittelystä ja säilyttämisestä.

II LUKU

KANSALLISET VERKKO- JA TIETOTURVAPUITTEET

4 artikla

Periaate

Jäsenvaltioiden on varmistettava verkko- ja tietojärjestelmien korkea turvataso alueellaan tämän direktiivin mukaisesti.

5 artikla

Kansallinen verkko- ja tietoturvastrategia ja kansallinen verkko- ja tietoturvan yhteistyösuunnitelma

1. Jokaisen jäsenvaltion on vahvistettava kansallinen verkko- ja tietoturvastrategia, jossa määritellään strategiset tavoitteet ja konkreettiset poliittiset ja sääntelylliset toimenpiteet verkko- ja tietoturvan korkean tason saavuttamiseksi ja ylläpitämiseksi. Kansallisen verkko- ja tietoturvastrategian on sisällettävä erityisesti seuraavat seikat:

(a) strategian tavoitteiden ja painopisteiden määrittely turvariskien ja -poikkeamien ajantasaisen analyysin perusteella,

(b) ohjauskehys strategian tavoitteiden ja painopisteiden saavuttamiseksi, mukaan lukien valtion elinten ja muiden asiaankuuluvien toimijoiden tehtävien ja vastuiden selkeä määrittely,

(c) varautumiseen, reagointiin ja toimintakunnon palauttamiseen liittyvien yleisten toimenpiteiden, myös julkisen ja yksityisen sektorin välisten yhteistyömekanismien, yksilöinti,

(d) tiedot opetus-, valistus- ja koulutusohjelmista,

(e) tutkimus- ja kehittämissuunnitelmat ja kuvaus siitä, miten niissä otetaan huomioon yksilöidyt painopisteet.

2. Kansallisen verkko- ja tietoturvastrategian on sisällettävä kansallinen verkko- ja tietoturvan yhteistyösuunnitelma, joka täyttää ainakin seuraavat vaatimukset:

(a) riskinhallintasuunnitelma riskien yksilöimiseksi ja mahdollisten turvapoikkeamien vaikutusten arvioimiseksi,

(b) suunnitelman täytäntöönpanoon osallistuvien eri toimijoiden tehtävien ja vastuiden määrittely,

(c) ennaltaehkäisyn, havaitsemisen, reagoinnin, korjauksen ja toimintakunnon palauttamisen takaavien yhteistyö- ja viestintäprosessien määrittely varoitustason mukaan,

(d) etenemissuunnitelma verkko- ja tietoturvaharjoituksia ja -koulutusta varten verkko- ja tietoturvan yhteistyösuunnitelman lujittamiseksi, validoimiseksi ja testaamiseksi. Saadut kokemukset dokumentoidaan ja otetaan huomioon yhteistyösuunnitelmassa sen tarkistusten yhteydessä.

3. Kansallinen verkko- ja tietoturvastrategia ja kansallinen verkko- ja tietoturvan yhteistyösuunnitelma on toimitettava komissiolle kuukauden kuluessa niiden hyväksymisestä.

6 artikla

Verkko- ja tietojärjestelmien turvallisuudesta vastaava kansallinen toimivaltainen viranomainen

1. Jokaisen jäsenvaltion on nimettävä verkko- ja tietojärjestelmien turvallisuudesta vastaava kansallinen toimivaltainen viranomainen, jäljempänä ’toimivaltainen viranomainen’.

2. Toimivaltaisten viranomaisten on seurattava tämän direktiivin soveltamista kansallisella tasolla ja edistettävä sen johdonmukaista soveltamista kaikkialla unionissa.

3. Jäsenvaltioiden on varmistettava, että toimivaltaisilla viranomaisilla on riittävät tekniset, taloudelliset ja henkilöstön voimavarat, jotta ne voivat suorittaa tehokkaasti ja tuloksekkaasti niille osoitetut tehtävät ja siten täyttää tämän direktiivin tavoitteet. Jäsenvaltioiden on varmistettava toimivaltaisten viranomaisten tuloksellinen, tehokas ja suojattu yhteistyö 8 artiklassa tarkoitetussa verkostossa.

4. Jäsenvaltioiden on varmistettava, että toimivaltaiset viranomaiset saavat turvapoikkeamista ilmoitukset julkishallinnoilta ja markkinatoimijoilta siten kuin 14 artiklan 2 kohdassa säädetään sekä 15 artiklassa tarkoitetut täytäntöönpanovaltuudet ja täytäntöönpanon valvontavaltuudet.

5. Toimivaltaisten viranomaisten on tarvittaessa kuultava asiaankuuluvia kansallisia lainvalvontaviranomaisia ja tietosuojaviranomaisia ja tehtävä yhteistyötä niiden kanssa.

6. Jokaisen jäsenvaltion on ilmoitettava komissiolle viipymättä toimivaltaisen viranomaisen nimeämisestä ja tehtävistä sekä mahdollisista myöhemmistä muutoksista näissä tiedoissa. Jokaisen jäsenvaltion on julkistettava toimivaltaisen viranomaisen nimeäminen.

7 artikla

Tietotekniikan kriisiryhmä

1. Jokaisen jäsenvaltion on perustettava tietotekniikan kriisiryhmä, jäljempänä ’CERT-ryhmä’ (Computer Emergency Response Team), joka vastaa turvapoikkeamien ja -riskien käsittelystä hyvin määritellyn prosessin mukaisesti ja täyttää liitteessä I olevassa 1 kohdassa esitetyt vaatimukset. CERT-ryhmä voidaan perustaa toimivaltaisen viranomaisen yhteyteen.

2. Jäsenvaltioiden on varmistettava, että CERT-ryhmillä on riittävät tekniset, taloudelliset ja henkilöstön voimavarat voidakseen suorittaa tuloksekkaasti liitteessä I olevassa 2 kohdassa mainitut tehtävänsä.

3. Jäsenvaltioiden on varmistettava, että CERT-ryhmien toiminta tukeutuu kansallisella tasolla suojattuun ja vakaaseen viestintä- ja tietoinfrastruktuuriin, joka on yhteensopiva ja yhteentoimiva 9 artiklassa tarkoitetun suojatun tiedonjakojärjestelmän kanssa.

4. Jäsenvaltioiden on annettava komissiolle tiedot CERT-ryhmien voimavaroista ja toimeksiannosta sekä turvapoikkeamien käsittelyprosessista.

5. CERT-ryhmän on toimittava toimivaltaisen viranomaisen valvonnassa, ja toimivaltaisen viranomaisen on säännöllisesti tarkasteltava uudelleen sen voimavarojen riittävyyttä, toimeksiantoa ja turvapoikkeamien käsittelyprosessin tuloksekkuutta.

III LUKU

TOIMIVALTAISTEN VIRANOMAISTEN VÄLINEN YHTEISTYÖ

8 artikla

Yhteistyöverkosto

1. Toimivaltaiset viranomaiset ja komissio muodostavat verkoston, jäljempänä ’yhteistyöverkosto’, jotta voidaan tehdä yhteistyötä verkko- ja tietojärjestelmiin vaikuttavien turvariskien ja -poikkeamien torjumiseksi.

2. Komissio ja toimivaltaiset viranomaiset ovat yhteistyöverkostossa pysyvästi yhteydessä toisiinsa. Euroopan verkko- ja tietoturvavirasto, jäljempänä ’ENISA’, avustaa pyynnöstä yhteistyöverkostoa antamalla asiantuntemusta ja neuvontaa.

3. Yhteistyöverkostossa toimivaltaisten viranomaisten on

   (a) annettava varhaisvaroituksia turvariskeistä ja -poikkeamista 10 artiklan mukaisesti,

   (b) varmistettava koordinoitu reagointi 11 artiklan mukaisesti,

   (c) julkaistava yhteisellä verkkosivustolla säännöllisesti ei-luottamukselliset tiedot voimassa olevista varhaisvaroituksista ja meneillään olevasta koordinoidusta reagoinnista,

   (d) jäsenvaltion tai komission pyynnöstä yhdessä keskusteltava ja tehtävä arviointi yhdestä tai useammasta 5 artiklassa tarkoitetusta kansallisesta verkko- ja tietoturvastrategiasta ja kansallisesta verkko- ja tietoturvan yhteistyösuunnitelmasta tämän direktiivin soveltamisalan rajoissa,

   (e) jäsenvaltion tai komission pyynnöstä yhdessä keskusteltava ja tehtävä arviointi CERT-ryhmien tuloksellisuudesta erityisesti tehtäessä verkko- ja tietoturvaharjoituksia unionin tasolla,

   (f) tehtävä yhteistyötä ja vaihdettava tietoa kaikista asiaankuuluvista seikoista Europolin yhteydessä toimivan Euroopan verkkorikostorjuntakeskuksen kanssa ja muiden asianomaisten, erityisesti tietosuojan, energiahuollon, liikenteen, pankkitoimen, pörssitoimen ja terveydenhuollon alan eurooppalaisten elinten kanssa,

   (g) vaihdettava tietoa ja parhaita toimintatapoja keskenään ja komission kanssa sekä avustettava toisiaan verkko- ja tietoturvavalmiuksien kehittämisessä,

   (h) järjestettävä säännöllisiä vertaisarviointeja valmiuksista ja varautumistasosta,

   (i) järjestettävä verkko- ja tietoturvaharjoituksia unionin tasolla ja tarvittaessa osallistuttava kansainvälisiin verkko- ja tietoturvaharjoituksiin.

4. Komissio vahvistaa täytäntöönpanosäädöksissä tarvittavat säännöt 2 ja 3 kohdassa tarkoitetun toimivaltaisten viranomaisten ja komission välisen yhteistyön helpottamiseksi. Nämä täytäntöönpanosäädökset hyväksytään 19 artiklan 2 kohdassa tarkoitettua kuulemismenettelyä noudattaen.

9 artikla

Suojattu tiedonjakojärjestelmä

1. Arkaluonteisten ja luottamuksellisten tietojen vaihto yhteistyöverkostossa on toteutettava suojatun infrastruktuurin kautta.

2. Siirretään komissiolle 18 artiklan mukaisesti valta antaa delegoituja säädöksiä, joissa määritellään seuraaviin näkökohtiin liittyvät perusteet, jotka jäsenvaltion on täytettävä voidakseen osallistua suojattuun tiedonjakojärjestelmään:

   (a) se, onko kansallisella tasolla käytettävissä suojattu ja vakaa viestintä- ja tietoinfrastruktuuri, joka on yhteensopiva ja yhteentoimiva yhteistyöverkoston suojatun infrastruktuurin kanssa 7 artiklan 3 kohdan mukaisesti, ja

   (b) se, onko niiden toimivaltaisella viranomaisella ja CERT-ryhmällä riittävät tekniset, taloudelliset ja inhimilliset voimavarat ja prosessit, joiden avulla suojattuun tiedonjakojärjestelmään voidaan osallistua tuloksellisesti, tehokkaasti ja turvallisesti 6 artiklan 3 kohdan ja 7 artiklan 2 ja 3 kohdan mukaisesti.

3. Komissio hyväksyy täytäntöönpanosäädöksillä 2 ja 3 kohdassa tarkoitettujen perusteiden nojalla päätökset jäsenvaltioiden pääsystä tähän suojattuun infrastruktuuriin. Nämä täytäntöönpanosäädökset hyväksytään 19 artiklan 3 kohdassa tarkoitettua sääntelymenettelyä noudattaen.

10 artikla
Varhaisvaroitukset

1. Toimivaltaisten viranomaisten ja komission on annettava yhteistyöverkostossa varhaisvaroitukset turvariskeistä ja -poikkeamista, jotka täyttävät ainakin yhden seuraavista edellytyksistä:

   (a) ne leviävät tai voivat levitä nopeasti,

   (b) ne ylittävät tai voivat ylittää kansalliset reagointivalmiudet,

   (c) ne vaikuttavat tai voivat vaikuttaa useampaan kuin yhteen jäsenvaltioon.

2. Toimivaltaisten viranomaisten ja komission on varhaisvaroituksissa annettava kaikki asiaankuuluvat hallussaan olevat tiedot, joista voi olla hyötyä turvariskin tai -poikkeaman arvioinnissa.

3. Komissio voi jäsenvaltion pyynnöstä tai omasta aloitteestaan pyytää jäsenvaltiota antamaan kaikki tarvittavat tiedot tietystä turvariskistä tai -poikkeamasta.

4. Jos turvariskiin tai -poikkeamaan, josta on tehty varhaisvaroitus, epäillään liittyvän rikollisuutta, toimivaltaisten viranomaisten tai komission on ilmoitettava tästä Europolin yhteydessä toimivalle Euroopan verkkorikostorjuntakeskukselle.

5. Siirretään komissiolle 18 artiklan mukaisesti valta antaa delegoituja säädöksiä, joissa määritellään tarkemmin 1 kohdassa tarkoitetut varhaisvaroituksen käynnistävät turvariskit ja -poikkeamat.

11 artikla
Koordinoitu reagointi

1. Edellä 10 artiklassa tarkoitetun varhaisvaroituksen jälkeen toimivaltaisten viranomaisten on asiaankuuluvat tiedot arvioituaan sovittava koordinoidusta reagoinnista 12 artiklassa tarkoitetun unionin verkko- ja tietoturvan yhteistyösuunnitelman mukaisesti.

2. Koordinoidun reagoinnin seurauksena kansallisella tasolla toteutetuista eri toimenpiteistä on ilmoitettava yhteistyöverkostolle.

12 artikla

Unionin verkko- ja tietoturvan yhteistyösuunnitelma

1. Siirretään komissiolle valta hyväksyä täytäntöönpanosäädöksillä unionin verkko- ja tietoturvan yhteistyösuunnitelma. Nämä täytäntöönpanosäädökset hyväksytään 19 artiklan 3 kohdassa tarkoitettua sääntelymenettelyä noudattaen.

2. Unionin verkko- ja tietoturvan yhteistyösuunnitelmassa on määriteltävä

   (a) 10 artiklan soveltamiseksi

   – muoto ja menettelyt sille, miten toimivaltaiset viranomaiset keräävät ja jakavat yhteensopivaa ja vertailukelpoista tietoa turvariskeistä ja -poikkeamista,

   – menettelyt ja perusteet yhteistyöverkoston suorittamalle turvariskien ja -poikkeamien arvioinnille;

   (b) koordinoidussa reagoinnissa 11 artiklan mukaisesti noudatettavat prosessit, mukaan lukien tehtävät ja vastuut sekä yhteistyömenettelyt,

   (c) etenemissuunnitelma verkko- ja tietoturvaharjoituksia ja -koulutusta varten verkko- ja tietoturvan yhteistyösuunnitelman lujittamiseksi, validoimiseksi ja testaamiseksi,

   (d) ohjelma osaamisen siirtämiseksi jäsenvaltioiden välillä valmiuksien kehittämistä ja vertaisoppimista varten,

   (e) ohjelma jäsenvaltioiden välistä tietoisuuden lisäämistä ja koulutusta varten.

3. Unionin verkko- ja tietoturvan yhteistyösuunnitelma on vahvistettava vuoden kuluessa tämän direktiivin voimaantulosta, ja sitä on tarkistettava säännöllisesti.

13 artikla

Kansainvälinen yhteistyö

Rajoittamatta yhteistyöverkoston mahdollisuutta epäviralliseen kansainväliseen yhteistyöhön unioni voi tehdä kolmansien maiden tai kansainvälisten järjestöjen kanssa kansainvälisiä sopimuksia, joissa sallitaan ja organisoidaan niiden osallistuminen joihinkin yhteistyöverkoston toimiin. Tällaisissa sopimuksissa on otettava huomioon tarve taata yhteistyöverkostossa levitettävien henkilötietojen riittävä suoja.

IV LUKU

JULKISHALLINTOJEN JA MARKKINATOIMIJOIDEN VERKKO- JA TIETOJÄRJESTELMIEN TURVALLISUUS

14 artikla

Turvallisuusvaatimukset ja turvapoikkeamien ilmoittaminen

1. Jäsenvaltioiden on varmistettava, että julkishallinnot ja markkinatoimijat toteuttavat tarkoituksenmukaiset tekniset ja organisatoriset toimenpiteet valvonnassaan olevien ja toiminnoissaan käyttämiensä verkko- ja tietojärjestelmien turvallisuuteen kohdistuvien riskien hallitsemiseksi. Näillä toimenpiteillä on voitava varmistaa riskiin suhteutettu turvallisuustaso ottaen huomioon uusin tekniikka. Erityisesti on toteutettava toimenpiteet, joilla ehkäistään ja minimoidaan niiden verkko- ja tietojärjestelmään niiden tarjoamissa keskeisissä palveluissa vaikuttavien

turvapoikkeamien vaikutukset ja näin taataan näiden verkko- ja tietojärjestelmien tukemien palvelujen jatkuvuus.

2. Jäsenvaltioiden on varmistettava, että julkishallinnot ja markkinatoimijat ilmoittavat toimivaltaiselle viranomaiselle turvapoikkeamista, jotka vaikuttavat merkittävästi niiden tarjoamien keskeisten palvelujen turvallisuuteen.

3. Edellä olevien 1 ja 2 kohdan vaatimuksia sovelletaan kaikkiin Euroopan unionissa palveluja tarjoaviin markkinatoimijoihin.

4. Toimivaltainen viranomainen voi tiedottaa yleisölle tai vaatia julkishallintoja ja markkinatoimijoita tiedottamaan yleisölle, jos se katsoo turvapoikkeaman julkistamisen olevan yleisen edun mukaista. Toimivaltaisen viranomaisen on toimitettava yhteistyöverkostolle vuosittain tiivistelmäraportti vastaanotetuista ilmoituksista ja tämän kohdan mukaisesti toteutetuista toimista.

5. Siirretään komissiolle 18 artiklan mukaisesti valta antaa delegoituja säädöksiä, joissa määritellään olosuhteet, joissa julkishallintojen ja markkinatoimijoiden edellytetään ilmoittavan turvapoikkeamista.

6. Jollei 5 kohdan mukaisesti hyväksytyistä delegoiduista säädöksistä muuta johdu, toimivaltaiset viranomaiset voivat hyväksyä suuntaviivoja ja tarvittaessa antaa ohjeita liittyen olosuhteisiin, joissa julkishallintojen ja markkinatoimijoiden edellytetään ilmoittavan turvapoikkeamista.

7. Siirretään komissiolle valta määritellä täytäntöönpanosäädöksillä muodot ja menettelyt 2 kohdan soveltamiseksi. Nämä täytäntöönpanosäädökset hyväksytään 19 artiklan 3 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

8. Edellä olevia 1 ja 2 kohtaa ei sovelleta mikroyritysten sekä pienten ja keskisuurten yritysten määritelmästä 6 päivänä toukokuuta 2003 annetussa komission suosituksessa 2003/361/EY[12] määriteltyihin mikroyrityksiin.

15 artikla

Täytäntöönpano ja sen valvonta

1. Jäsenvaltioiden on varmistettava, että toimivaltaisilla viranomaisilla on kaikki tarvittavat valtuudet tutkia tapaukset, joissa julkishallinnot tai markkinatoimijat eivät ole noudattaneet 14 artiklan mukaisia velvoitteitaan, sekä näiden tapausten vaikutukset verkko- ja tietojärjestelmien turvallisuuteen.

2. Jäsenvaltioiden on varmistettava, että toimivaltaisilla viranomaisilla on valtuudet vaatia markkinatoimijoita ja julkishallintoja

   (a) antamaan tiedot, jotka tarvitaan niiden verkko- ja tietojärjestelmien turvallisuuden arvioimiseksi, mukaan lukien dokumentoidut turvallisuusohjeet,

   (b) läpikäymään turvallisuustarkastuksen, jonka suorittaa pätevä ulkopuolinen elin tai kansallinen viranomainen, ja toimittamaan sen tulokset toimivaltaiselle viranomaiselle.

3. Jäsenvaltioiden on varmistettava, että toimivaltaisilla viranomaisilla on valtuudet antaa sitovia ohjeita markkinatoimijoille ja julkishallinnoille.

[12] EUVL L 124, 20.5.2003, s. 36.

4. Toimivaltaisten viranomaisten on ilmoitettava turvapoikkeamista, joihin epäillään liittyvän vakavaa rikollisuutta, lainvalvontaviranomaisille.

5. Toimivaltaisten viranomaisten on työskenneltävä tiiviisti yhteistyössä tietosuojaviranomaisten kanssa, kun ne käsittelevät henkilötietojen tietoturvaloukkauksiin johtaneita turvapoikkeamia.

6. Jäsenvaltioiden on varmistettava, että kaikkiin tämän luvun nojalla julkishallinnoille ja markkinatoimijoille määrättäviin velvoitteisiin voidaan hakea muutosta tuomioistuimessa.

16 artikla

Standardointi

1. Jäsenvaltioiden on 14 artiklan 1 kohdan johdonmukaisen täytäntöönpanon varmistamiseksi edistettävä verkko- ja tietoturvan kannalta merkityksellisten standardien ja/tai eritelmien käyttöä.

2. Komissio laatii täytäntöönpanosäädöksillä luettelon 1 kohdassa tarkoitetuista standardeista. Luettelo julkaistaan *Euroopan unionin virallisessa lehdessä*.

V LUKU

LOPPUSÄÄNNÖKSET

17 artikla

Seuraamukset

1. Jäsenvaltioiden on säädettävä seuraamusjärjestelmästä, jota sovelletaan tämän direktiivin täytäntöönpanemiseksi annettujen kansallisten säännösten rikkomiseen, ja toteutettava kaikki tarvittavat toimenpiteet seuraamusten täytäntöönpanon varmistamiseksi. Seuraamusten on oltava tehokkaita, oikeasuhteisia ja varoittavia. Jäsenvaltioiden on annettava nämä säännökset tiedoksi komissiolle viimeistään päivänä, jona tämä direktiivi on saatettava osaksi kansallista lainsäädäntöä, ja kaikki niihin myöhemmin tehtävät muutokset viipymättä.

2. Jäsenvaltioiden on varmistettava, että jos turvapoikkeama koskee henkilötietoja, säädetyt seuraamukset ovat sopusoinnussa yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta annetussa Euroopan parlamentin ja neuvoston asetuksessa[13] säädettyjen seuraamusten kanssa.

18 artikla

Siirretyn säädösvallan käyttäminen

1. Siirretään komissiolle valta antaa delegoituja säädöksiä tässä artiklassa säädetyin edellytyksin.

2. Siirretään komissiolle valta antaa 9 artiklan 2 kohdassa, 10 artiklan 5 kohdassa ja 14 artiklan 5 kohdassa tarkoitettuja delegoituja säädöksiä. Komissio laatii siirrettyä säädösvaltaa koskevan kertomuksen viimeistään yhdeksän kuukautta ennen viiden vuoden pituisen kauden päättymistä. Säädösvallan siirtoa jatketaan ilman eri toimenpiteitä samanpituisiksi kausiksi, jollei Euroopan parlamentti tai neuvosto

[13] SEC(2012) 72 final.

vastusta tällaista jatkamista viimeistään kolme kuukautta ennen kunkin kauden päättymistä.

3. Euroopan parlamentti tai neuvosto voi milloin tahansa peruuttaa 9 artiklan 2 kohdassa, 10 artiklan 5 kohdassa ja 14 artiklan 5 kohdassa tarkoitetun säädösvallan siirron. Peruuttamispäätöksellä lopetetaan tuossa päätöksessä mainittu säädösvallan siirto. Päätös tulee voimaan sitä päivää seuraavana päivänä, jona se julkaistaan *Euroopan unionin virallisessa lehdessä*, tai jonakin myöhempänä, päätöksessä mainittuna päivänä. Päätös ei vaikuta jo voimassa olevien delegoitujen säädösten pätevyyteen.

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

5. Edellä olevien 9 artiklan 2 kohdan, 10 artiklan 5 kohdan ja 14 artiklan 5 kohdan nojalla annettu delegoitu säädös tulee voimaan ainoastaan, jos Euroopan parlamentti tai neuvosto ei ole kahden kuukauden kuluessa siitä, kun asianomainen säädös on annettu tiedoksi Euroopan parlamentille ja neuvostolle, ilmaissut vastustavansa sitä tai jos sekä Euroopan parlamentti että neuvosto ovat ennen mainitun määräajan päättymistä ilmoittaneet komissiolle, että ne eivät vastusta säädöstä. Euroopan parlamentin tai neuvoston aloitteesta tätä määräaikaa jatketaan kahdella kuukaudella.

19 artikla

Komiteamenettely

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

2. Kun viitataan tähän kohtaan, sovelletaan asetuksen (EU) N:o 182/2011 4 artiklaa.

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

20 artikla

Uudelleentarkastelu

Komissio tarkastelee määräajoin uudelleen tämän direktiivin toimintaa ja laatii kertomuksen Euroopan parlamentille ja neuvostolle. Ensimmäinen kertomus annetaan kolmen vuoden kuluessa 21 artiklassa tarkoitetusta osaksi kansallista lainsäädäntöä saattamiselle asetetusta määräpäivästä. Komissio voi tätä varten pyytää jäsenvaltioita antamaan tietoja ilman aiheetonta viivytystä.

21 artikla

Saattaminen osaksi kansallista lainsäädäntöä

1. Jäsenvaltioiden on annettava ja julkaistava tämän direktiivin noudattamisen edellyttämät lait, asetukset ja hallinnolliset määräykset viimeistään [18 kuukauden kuluttua sen hyväksymisestä]. Niiden on viipymättä toimitettava komissiolle kirjallisina nämä säännökset.

Jäsenvaltioiden on sovellettava näitä säännöksiä [18 kuukauden kuluttua tämän direktiivin hyväksymisestä]

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

2. Jäsenvaltioiden on toimitettava tässä direktiivissä tarkoitetuista kysymyksistä antamansa keskeiset kansalliset säännökset kirjallisina komissiolle.

22 artikla

Voimaantulo

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

23 artikla

Osoitus

Tämä direktiivi on osoitettu kaikille jäsenvaltioille.

Tehty Brysselissä

Euroopan parlamentin puolesta	*Neuvoston puolesta*
Puhemies	*Puheenjohtaja*

LIITE I

Tietotekniikan kriisiryhmän (CERT) vaatimukset ja tehtävät

CERT-ryhmän vaatimukset ja tehtävät on määriteltävä riittävästi ja selkeästi ja niiden on perustuttava kansalliseen politiikkaan ja/tai lainsäädäntöön. Niihin on sisällyttävä seuraavat:

(1) CERT-ryhmän vaatimukset

(a) CERT-ryhmän on varmistettava viestintäpalvelujensa korkea käytettävyys välttämällä yksittäisiä pisteitä, joiden toimintahäiriö keskeyttäisi koko palvelun, ja pitämällä käytössä useita kanavia, joiden kautta siihen voidaan ottaa yhteyttä ja joiden kautta se itse voi ottaa yhteyttä muualle. Viestintäkanavat on määriteltävä selkeästi, ja niiden on oltava hyvin käyttäjien ja yhteistyökumppanien tiedossa.

(b) CERT-ryhmän on toteutettava ja hallinnoitava turvallisuustoimenpiteitä, joilla voidaan varmistaa sen vastaanottamien ja käsittelemien tietojen luottamuksellisuus, eheys, käytettävyys ja aitous.

(c) CERT-ryhmän toimipaikka ja sitä tukevat tietojärjestelmät on sijoitettava suojattuihin paikkoihin.

(d) Käyttöön on otettava palvelun laadunhallintajärjestelmä, joka seuraa CERT-ryhmän suorituskykyä ja varmistaa jatkuvat parannukset. Sen on perustuttava selkeästi määriteltyihin mittareihin, joihin sisältyvät viralliset palvelutasot ja keskeiset suoritusindikaattorit.

(e) Toiminnan jatkuvuus:

– CERT-ryhmässä on oltava tarkoituksenmukainen järjestelmä pyyntöjen käsittelyä ja reititystä varten tapauksen edelleenohjauksen helpottamiseksi;

– CERT-ryhmällä on oltava riittävä henkilöstö, jotta se voi olla käytettävissä jatkuvasti;

– CERT-ryhmällä on oltava tukenaan infrastruktuuri, jonka jatkuvuus on varmistettu. Tätä varten CERT-ryhmää varten on oltava redundantit järjestelmät ja varatyöskentelytilat, jotta voidaan varmistaa viestintävälineiden jatkuva käytettävyys.

(2) CERT-ryhmän tehtävät

(a) CERT-ryhmän tehtäviin on sisällyttävä vähintään seuraavat:

– turvapoikkeamien seuranta kansallisella tasolla,

– varhaisvaroitusten, varoitusten ja tiedotusten antaminen sekä tiedon levittäminen turvariskeistä ja -poikkeamista asianosaisille,

– turvapoikkeamiin reagointi,

– dynaaminen riski- ja poikkeama-analyysi ja tilannetietoisuus,

– laajan yleisen tietoisuuden lisääminen verkkotoimintoihin liittyvistä riskeistä,

– verkko- ja tietoturvakampanjoiden järjestäminen.

(b) CERT-ryhmän ja luotava yhteistyösuhteita yksityiseen sektoriin.

(c) Yhteistyön helpottamiseksi CERT-ryhmän on edistettävä yhteisten tai standardoitujen toimintatapojen omaksumista ja käyttöä

– turvapoikkeamien ja riskien käsittelymenettelyissä,

– turvapoikkeamien, turvariskien ja informaation luokittelujärjestelmissä,

– mittareiden luokittelutavoissa,

– turvariskejä ja poikkeamia koskevan tiedonvaihdon muodoissa ja järjestelmien nimeämiskäytännöissä.

LIITE II

Markkinatoimijoiden luettelo

Markkinatoimijat, joita tarkoitetaan 3 artiklan 8 kohdan a alakohdassa:

1. Sähköisen kaupankäynnin alustat
2. Internet-välitteiset maksupalvelut
3. Verkkoyhteisöpalvelut
4. Hakukoneet
5. Pilvipalvelut
6. Sovelluskaupat

3 artiklan 8 kohdan b alakohdassa tarkoitetut markkinatoimijat:

1. Energia
   - Sähkön- ja kaasuntoimittajat
   - Sähkön ja/tai kaasun jakeluverkot ja vähittäiskaupan toimittajat
   - Maakaasun siirtoverkot ja varastointi sekä nesteytetyn maakaasun operaattorit
   - Sähkön siirtoverkot
   - Öljysiirtoputkistot ja öljyvarastot
   - Sähkö- ja kaasumarkkinatoimijat
   - Öljyn ja maakaasun tuotanto-, jalostus- ja käsittelylaitteistojen operaattorit
2. Liikenne
   - Lentoliikenteen (rahti- ja matkustajaliikenteen) harjoittajat
   - Merenkulun (meri- ja rannikkoliikenteen matkustaja- ja rahtiliikenteen) harjoittajat
   - Rautatiet (infrastruktuurin ylläpitäjät, integroituneet yritykset ja rautatieliikenteen harjoittajat)
   - Lentoasemat
   - Satamat
   - Liikenteenhallinnan ja -ohjauksen ylläpitäjät
   - Liitännäiset logistiikkapalvelut a) varastot ja varastointi, b) rahdinkäsittely ja c) muut liikenteen tukitoiminnot.
3. Pankkitoimi: direktiivin 2006/48/EY 4 artiklan 1 kohdassa tarkoitetut luottolaitokset.
4. Finanssimarkkinoiden infrastruktuurit: pörssit ja keskusvastapuoliyhteisöt.
5. Terveydenhuolto: terveydenhuoltolaitokset (kuten sairaalat ja yksityisklinikat) sekä muut terveydenhuollon tarjoamiseen osallistuvat laitokset.

SÄÄDÖKSEEN LIITTYVÄ RAHOITUSSELVITYS

1. PERUSTIEDOT EHDOTUKSESTA/ALOITTEESTA

1.1. Ehdotuksen/aloitteen nimi

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

1.3. Ehdotuksen/aloitteen luonne

1.4. Tavoitteet

1.5. Ehdotuksen/aloitteen perustelut

1.6. Toiminnan ja sen rahoitusvaikutusten kesto

1.7. Hallinnointitapa (hallinnointitavat)

2. HALLINNOINTI

2.1. Seuranta- ja raportointisäännöt

2.2. Hallinnointi- ja valvontajärjestelmä

2.3. Toimenpiteet petosten ja sääntöjenvastaisuuksien ehkäisemiseksi

3. EHDOTUKSEN/ALOITTEEN ARVIOIDUT RAHOITUSVAIKUTUKSET

3.1. Kyseeseen tulevat monivuotisen rahoituskehyksen otsakkeet ja menopuolen budjettikohdat

3.2. Arvioidut vaikutukset menoihin

3.2.1. Yhteenveto arvioiduista vaikutuksista menoihin

3.2.2. Arvioidut vaikutukset toimintamäärärahoihin

3.2.3. Arvioidut vaikutukset hallintomäärärahoihin

3.2.4. Yhteensopivuus nykyisen monivuotisen rahoituskehyksen kanssa

3.2.5. Ulkopuolisten tahojen osallistuminen rahoitukseen

3.3. Arvioidut vaikutukset tuloihin

SÄÄDÖKSEEN LIITTYVÄ RAHOITUSSELVITYS

1. PERUSTIEDOT EHDOTUKSESTA/ALOITTEESTA

1.1. Ehdotuksen/aloitteen nimi

Ehdotus Euroopan parlamentin ja neuvoston direktiiviksi toimenpiteistä yhteisen korkeatasoisen verkko- ja tietoturvan varmistamiseksi koko unionissa

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

– 09 – Viestintäverkot, sisällöt ja teknologia

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

Ehdotetun direktiivin tavoitteena on varmistaa verkko- ja tietoturvan yhteinen korkea taso koko EU:ssa.

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

Ehdotuksessa säädetään toimenpiteistä verkko- ja tietojärjestelmien yhteisen korkean turvatason varmistamiseksi koko unionissa.

Erityistavoitteina on:

1. Siirtyä verkko- ja tietoturvan yhteiseen vähimmäistasoon jäsenvaltioissa ja siten lisätä yleistä varautumistasoa ja reagointikykyä.

2. Parantaa verkko- ja tietoturvaan liittyvää yhteistyötä EU:n tasolla rajat ylittävien turvapoikkeamien ja -uhkien torjumiseksi tehokkaasti. Verkostossa otetaan käyttöön suojattu tiedonvaihtoinfrastruktuuri, jossa toimivaltaiset viranomaiset voivat vaihtaa arkaluonteisia ja luottamuksellisia tietoja.

3. Luoda riskinhallintakulttuuri ja parantaa tietojen vaihtoa yksityisen ja julkisen sektorin välillä.

Toiminto (toiminnot) toimintoperusteisessa johtamis- ja budjetointijärjestelmässä

Direktiivi koskee toimijoita (yrityksiä ja organisaatioita, myös pk-yrityksiä) eri aloilla (energia, liikenne, luottolaitokset, pörssit, terveydenhuolto ja keskeisten internet-palvelujen infrastruktuurit) sekä julkishallintoja. Se kattaa myös yhteydet lainvalvontaan ja tietosuojaan sekä ulkosuhteiden verkko- ja tietoturvanäkökohdat.

– 09 – Viestintäverkot, sisällöt ja teknologia

[37] ABM: toimintoperusteinen johtaminen; ABB: toimintoperusteinen budjetointi.

[38] Sellaisina kuin nämä on määritelty varainhoitoasetuksen 49 artiklan 6 kohdan a tai b alakohdassa.

– 02 – Yritystoiminta

– 32 – Energia

– 06 – Liikkuvuus ja liikenne

– 17 – Terveys- ja kuluttaja-asiat

– 18 – Sisäasiat

– 19 – Ulkosuhteet

– 33 – Oikeusasiat

– 12 – Sisämarkkinat

1.4.3. Odotettavissa olevat tulokset ja vaikutukset

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

EU:n kuluttajien, yritysten ja julkishallintojen suojelu verkko- ja tietoturvapoikkeamilta, -uhilta ja -riskeiltä paranisi huomattavasti.

Lisätietoja on tähän säädösehdotukseen liittyvän vaikutusarvioinnin kohdassa 8.2 (Vaihtoehdon 2 vaikutukset – Sääntelyyn perustuva lähestymistapa).

1.4.4. Tulos- ja vaikutusindikaattorit

Selvitys siitä, millaisin indikaattorein ehdotuksen/aloitteen toteuttamista seurataan

Seurannassa ja arvioinnissa käytettävät indikaattorit selostetaan vaikutusarvioinnin kohdassa 10.

1.5. Ehdotuksen/aloitteen perustelut

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

Kullakin jäsenvaltiolla edellytetään olevan

– kansallinen verkko- ja tietoturvastrategia,

– verkko- ja tietoturvan yhteistyösuunnitelma,

– toimivaltainen kansallinen verkko- ja tietoturvaviranomainen sekä

– tietotekniikan kriisiryhmä (CERT).

EU:n tasolla jäsenvaltioiden edellytetään tekevän yhteistyötä verkostossa.

Julkishallinnot ja keskeiset yksityissektorin toimijat velvoitetaan verkko- ja tietoturvan riskinhallintaan ja raportoimaan vaikutuksiltaan merkittävistä verkko- ja tietoturvapoikkeamista toimivaltaisille viranomaisille.

1.5.2. EU:n osallistumisesta saatava lisäarvo

Verkko- ja tietoturvan rajatylittävät luonteen vuoksi erot lainsäädännössä ja politiikassa muodostavat esteen yrityksille, jotka toimivat useissa maissa, ja kokonaisvaltaisten mittakaavaetujen saavuttamiselle. Toiminnan puute EU:n tasolla johtaisi tilanteeseen, jossa kukin jäsenvaltio toimisi yksinään ottamatta huomioon verkko- ja tietojärjestelmien keskinäisiä riippuvuussuhteita.

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

1.5.3. Vastaavista toimista saadut kokemukset

Ehdotusta edeltäneen analyysin mukaan tarvitaan sääntelyllisiä velvoitteita, jotta voidaan luoda tasapuoliset toimintaedellytykset ja paikata lainsäädännön porsaanreikiä. Täysin vapaaehtoinen lähestymistapa on tällä alalla johtanut yhteistyöhön vain sellaisissa vähemmistönä olevissa jäsenvaltioissa, joiden valmiudet ovat korkealla tasolla.

1.5.4. Yhteensopivuus muiden kyseeseen tulevien välineiden kanssa ja mahdolliset synergiaedut

Tämä ehdotus on täysin Euroopan digitaalistrategian ja näin ollen EU 2020 -strategian mukainen. Se vastaa ja täydentää EU:n sähköisen viestinnän sääntelyjärjestelmää, Euroopan elintärkeän infrastruktuurin määrittämisestä annettua EU:n direktiiviä ja EU:n tietosuojadirektiiviä.

Ehdotus esitetään yhdessä komission ja unionin ulkoasioiden ja turvallisuuspolitiikan korkean edustajan yhteisen eurooppalaisen kyberturvallisuusstrategian kanssa, josta se muodostaan olennaisen osan.

1.6. Toiminnan ja sen rahoitusvaikutusten kesto

– ☐ Ehdotuksen/aloitteen mukaisen toiminnan kesto on rajattu.

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

– ☐ Rahoitusvaikutukset alkavat vuonna VVVV ja päättyvät vuonna VVVV.

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

– Määräaika direktiivi saattamiselle osaksi kansallista lainsäädäntö alkaa välittömästi sen hyväksymisen jälkeen (ennakkoarvion mukaan vuonna 2015) ja kestää 18 kuukautta. Direktiivin täytäntöönpano käynnistyy kuitenkin heti sen hyväksymisestä muun muassa perustamalla suojattu infrastruktuuri jäsenvaltioiden yhteistyön tueksi.

– minkä jälkeen toteutus täydessä laajuudessa.

1.7. Hallinnointitapa (hallinnointitavat)[39]

– ☒ Komissio hallinnoi suoraan keskitetysti

– ☒ Välillinen keskitetty hallinnointi, jossa täytäntöönpanotehtäviä on siirretty

– ☐toimeenpanovirastoille

– ☒ yhteisöjen perustamille elimille[40]

– ☐ kansallisille julkisoikeudellisille elimille tai julkisen palvelun tehtäviä hoitaville elimille

– ☐ 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, mukaan lukien Euroopan avaruusjärjestö

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

[40] Sellaisina kuin nämä määritellään varainhoitoasetuksen 185 artiklassa.

Jos käytetään useampaa kuin yhtä hallinnointitapaa, huomautuksille varatussa kohdassa olisi annettava lisätietoja.

Huomautukset:
ENISA voi yhteisöjen perustamana erillisvirastona avustaa jäsenvaltioita ja komissiota direktiivin täytäntöönpanossa toimeksiantonsa mukaisesti ja kohdentamalla uudelleen virastolle monivuotisessa rahoituskehyksessä 2014–2020 osoitettuja resursseja.

2. HALLINNOINTI

2.1. Seuranta- ja raportointisäännöt

Ilmoitetaan sovellettavat aikavälit ja edellytykset

Komissio tarkastelee määräajoin uudelleen tämän direktiivin toimintaa ja laatii kertomuksen Euroopan parlamentille ja neuvostolle.

Komissio arvioi myös direktiivin täytäntöönpanotoimet jäsenvaltioissa.

Verkkojen Eurooppa -välinettä koskevan asetuksen mukaan voidaan myös tehdä arviointi hankkeiden toteuttamisen menetelmistä ja niiden vaikutuksista määritettäessä, onko asetetut tavoitteet saavutettu muun muassa ympäristönsuojelun alalla.

2.2. Hallinnointi- ja valvontajärjestelmä

2.2.1. Todetut riskit

– viiveet suojatun infrastruktuurin kehittämiseen liittyvien hankkeiden toteutuksessa

2.2.2. Valvontamenetelmät

Verkkojen Eurooppa -välineen mukaisten toimien täytäntöönpanoa koskevissa sopimuksissa ja päätöksissä määrätään komission tai minkä tahansa komission valtuuttaman edustajan tekemästä seurannasta ja rahoitusvalvonnasta sekä tilintarkastustuomioistuimen tarkastuksista ja Euroopan petostentorjuntaviraston (OLAF) paikalla tekemistä tarkastuksista.

2.2.3. Valvonnan kustannukset ja hyödyt ja todennäköinen vaatimustenvastaisuusaste

Riskiin perustuvat ennakko- ja jälkeistarkastukset sekä mahdollisuus paikan päällä tehtäviin tarkastuksiin varmistavat sen, että valvontakustannukset ovat kohtuulliset.

2.3. Toimenpiteet petosten ja sääntöjenvastaisuuksien ehkäisemiseksi

Ilmoitetaan käytössä olevat ja suunnitellut torjunta- ja suojatoimenpiteet

Komissio varmistaa asianmukaisin toimenpitein, että tämän direktiivin mukaisesti rahoitettavia toimia toteutettaessa unionin taloudellisia etuja suojataan petoksia, lahjontaa ja muuta laitonta toimintaa ehkäisevillä toimenpiteillä, tehokkailla tarkastuksilla ja, jos sääntöjenvastaisuuksia havaitaan, perimällä aiheettomasti maksetut määrät takaisin sekä soveltuvin osin käyttämällä tehokkaita, oikeasuhteisia ja ennalta ehkäiseviä seuraamuksia.

Komissiolla ja sen edustajilla sekä tilintarkastustuomioistuimella on valtuudet tehdä kaikkien unionilta tämän ohjelman mukaisesti rahoitusta saaneiden avustuksensaajien, toimeksisaajien ja alihankkijoiden osalta asiakirjoihin perustuvia ja paikalla suoritettavia tarkastuksia.

Euroopan petostentorjuntavirasto, jäljempänä ’OLAF’, voi asetuksessa (Euratom, EY) N:o 2185/96 säädettyjen menettelyjen mukaisesti tehdä niihin talouden toimijoihin kohdistuvia paikalla suoritettavia todentamisia ja tarkastuksia, joille on suoraan tai välillisesti myönnetty asianomaista rahoitusta, selvittääkseen, onko avustussopimukseen tai -päätökseen taikka unionin rahoitusta koskevaan sopimukseen liittynyt unionin taloudellisia etuja vahingoittavia petoksia, korruptiota tai muuta laitonta toimintaa.

Kolmansien maiden ja kansainvälisten järjestöjen kanssa tehdyissä yhteistyösopimuksissa, avustussopimuksissa, avustuspäätöksissä ja sopimuksissa, kun nämä ovat seurausta tämän asetuksen täytäntöönpanosta, on nimenomaisesti annettava komissiolle, tilintarkastustuomioistuimelle ja OLAFille valtuudet tehdä tällaisia tarkastuksia sekä paikalla suoritettavia todentamisia ja tarkastuksia, sanotun kuitenkaan rajoittamatta edellisten kohtien soveltamista.

Verkkojen Eurooppa -välineen sääntöjen mukaan avustus- ja hankintasopimukset perustuvat vakiomalleihin, joissa esitetään yleisesti sovellettavat petostentorjuntatoimenpiteet.

3. EHDOTUKSEN/ALOITTEEN ARVIOIDUT RAHOITUSVAIKUTUKSET

3.1. Kyseeseen tulevat monivuotisen rahoituskehyksen otsakkeet ja menopuolen budjettikohdat

- Talousarviossa jo olevat budjettikohdat

Monivuotisen rahoituskehyksen otsakkeiden ja budjettikohtien mukaisessa järjestyksessä.

Moniv. rahoituskehyksen otsake	Budjettikohta	Menolaji	Rahoitusosuudet			
	Numero [Nimi……...…….]	JM/EI-JM (41)	EFTA-mailta[42]	ehdokasmailta[43]	kolmansilta mailta	varainhoitoasetuksen 18 artiklan 1 kohdan aa alakohdassa tarkoitetut rahoitusosuudet
	09 03 02 kansallisten julkisten palvelujen verkkoon liittäminen ja yhteentoimivuus sekä pääsy tällaisiin verkkoihin	JM	EI	EI	EI	EI

- Uudet perustettaviksi esitetyt budjettikohdat (Ei koske tätä ehdotusta)

Monivuotisen rahoituskehyksen otsakkeiden ja budjettikohtien mukaisessa järjestyksessä.

Moniv. rahoituskehyksen otsake	Budjettikohta	Menolaji	Rahoitusosuudet			
	Numero [Nimi……..]	JM/EI-JM	EFTA-mailta	ehdokasmailta	kolmansilta mailta	varainhoitoasetuksen 18 artiklan 1 kohdan aa alakohdassa tarkoitetut rahoitusosuudet
	[XX.YY.YY.YY]		KYLLÄ/EI	KYLLÄ/EI	KYLLÄ/EI	KYLLÄ/EI

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

42 EFTA: Euroopan vapaakauppaliitto.

43 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	Älykäs ja osallistava kasvu

PO: <…….>			2015* [44]	vuosi **2016**	vuosi **2017**	vuosi **2018**	2019–2021 ja myöh. vuodet			**YHTEENSÄ**
• Toimintamäärärahat										
09 03 02	Sitoumukset	(1)	1,250**	0,000						**1,250**
	Maksut	(2)	0,750	0,250	0,250					**1,250**
Tiettyjen ohjelmien määrärahoista katettavat hallintomäärärahat[45]			**0,000**							**0,000**
Budjettikohdan numero		(3)	**0,000**							**0,000**
<….> PO:n määrärahat YHTEENSÄ	Sitoumukset	=1+1a +3	1,250	0,000						**1,250**
	Maksut	=2+2a +3	0,750	0,250	0,250					**1,250**

• Toimintamäärärahat YHTEENSÄ	Sitoumukset	(4)	1,250	0,000						**1,250**
	Maksut	(5)	0,750	0,250	0,250					**1,250**
• Tiettyjen ohjelmien määrärahoista katettavat hallintomäärärahat YHTEENSÄ		(6)	**0,000**							

[44] Vuosi N on ehdotuksen/aloitteen toteutuksen aloitusvuosi.

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

Monivuotisen rahoituskehyksen **OTSAKKEESEEN 1 kuuluvat määrärahat YHTEENSÄ**	Sitoumukset	=4+ 6	1,250	0,000						**1,250**
	Maksut	=5+ 6	0,750	0,250	0,250					**1,250**

* Tarkka ajankohta riippuu siitä, milloin lainsäädäntävallan käyttäjä hyväksyy ehdotuksen (jos direktiivi hyväksytään vuoden 2014 kuluessa, nykyisen infrastruktuurin mukauttaminen käynnistyisi 2015, muussa tapauksessa vuotta myöhemmin).

** Jos jäsenvaltiot päättävät käyttää olemassa olevaa infrastruktuuria ja kattaa sen mukauttamiseen liittyvät kertaluonteiset kustannukset EU:n talousarviosta, kuten kohdissa 1.4.3 ja 1.7 selitetään, direktiivin III luvun mukaista jäsenvaltioiden välistä yhteistyötä (varhaisvaroitukset, koordinoitu reagointi jne.) tukevan verkon mukauttamisesta aiheutuu arviolta 1 250 000 euron kustannukset. Tämä määrä on vaikutusarvioinnissa mainittua kustannusarviota (”noin 1 miljoonaa euroa”) suurempi, koska se perustuu täsmällisempään arviointiin tällaisen infrastruktuurin välttämättömistä rakennetekijöistä. Rakennetekijöiden kustannusarvio perustuu arviointiin, jonka JRC on tehnyt vastaavien järjestelmien kehittämisestä muilla, esim. kansanterveyden, aloilla saadun kokemuksen pohjalta. Kustannusarvio kattaa seuraavat: verkko- ja tietoturvan nopea varoitus- ja ilmoitusjärjestelmä (275 000 euroa), tiedonvaihtoalusta (400 000 euroa), varhaisvaroitus- ja reagointijärjestelmä (275 000 euroa) ja tilannekeskus (300 000 euroa), yhteensä 1 250 000 euroa. Yksityiskohtaisempi täytäntöönpanosuunnitelma on määrä tehdä osana toteutettavuustutkimusta pohjautuen erillissopimukseen SMART 2012/0010: *Feasibility study and preparatory activities for the implementation of a European early warning and response system against cyber-attacks and disruptions*.

Jos ehdotuksella/aloitteella on vaikutuksia useampaan otsakkeeseen:

• Toimintamäärärahat YHTEENSÄ	Sitoumukset	(4)	0,000	0,000						
	Maksut	(5)	0,000	0,000						
• Tiettyjen ohjelmien määrärahoista katettavat hallintomäärärahat YHTEENSÄ		(6)	**0,000**	**0,000**						
Monivuotisen rahoituskehyksen **OTSAKKEISIIN 1–4 kuuluvat määrärahat YHTEENSÄ** (viitemäärä)	Sitoumukset	=4+ 6	1,250	0,000						1,250
	Maksut	=5+ 6	0,750	0,250	0,250					1,250

Moniv. rahoituskehyksen otsake	**5**	”Hallintomenot”

milj. euroa (kolmen desimaalin tarkkuudella)

		vuosi **2015**	vuosi **2016**	vuosi **2017**	vuosi **2018**	2019–2021 ja myöh. vuodet			**YHTEENSÄ**
PO:CNECT									
• Henkilöresurssit		0,572	0,572	0,572	0,572	0,572	0,572	**0,572**	**4,004**
• Muut hallintomenot		0,318	0,118	0,318	0,118	0,318	0,118	**0,118**	**1,426**
PO CNECT **YHTEENSÄ**	Määrärahat	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

Monivuotisen rahoituskehyksen **OTSAKKEESEEN 5 kuuluvat määrärahat YHTEENSÄ**	(Sitoumukset yhteensä = maksut yhteensä)	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

milj. euroa (kolmen desimaalin tarkkuudella)

		vuosi **2015**[46]	vuosi **2016**	vuosi **2017**	vuosi **2018**	2019–2021 ja myöh. vuodet			**YHTEENSÄ**
Monivuotisen rahoituskehyksen **OTSAKKEISIIN 1–5 kuuluvat määrärahat YHTEENSÄ**	Sitoumukset	2,140	0,690	0,890	0,690	0,890	0,690	0,690	**6,680**
	Maksut	1,640	0,940	1,140	0,690	0,890	0,690	0,690	**6,680**

[46] Vuosi N on ehdotuksen/aloitteen toteutuksen aloitusvuosi.

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 ⇩			vuosi **2015***		vuosi **2016**		vuosi **2017**		vuosi **2018**		2019–2021 ja myöh. vuodet						**YHTEENSÄ**	
			TUOTOKSET															
	Tyyppi[47]	Keski-määr. kustannukset	Lukumäärä	Kustannus	Lukumäärä	Kustannus	Lukumäärä	Kustannus	Lukumäärä	Kustannus	Lukumäärä	Kustannus	Lukumäärä	Kustannus	Lukumäärä	Kustannus	Lukumäärä yhteensä	Kustannukset yhteensä
ERITYISTAVOITE 2[48] Suojattu tiedonjakoinfrastruktuuri																		
– Tuotos	Infrastruktuurin mukauttaminen																	
Välisumma erityistavoite 2			1	1,250**													1	1,250
KUSTANNUKSET YHTEENSÄ				1,250														1,250

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

48 Kuten kuvattu kohdassa 1.4.2 ”Erityistavoitteet”.

* Tarkka ajankohta riippuu siitä, milloin lainsäädäntävallan käyttäjä hyväksyy ehdotuksen (jos direktiivi hyväksytään vuoden 2014 kuluessa, nykyisen infrastruktuurin mukauttaminen käynnistyisi 2015, muussa tapauksessa vuotta myöhemmin).

**Ks. kohta 3.2.1

3.2.3. Arvioidut vaikutukset hallintomäärärahoihin

3.2.3.1. Yhteenveto

– ☐ Ehdotus/aloite ei edellytä hallintomäärärahoja.

– ☑ Ehdotus/aloite edellyttää hallintomäärärahoja seuraavasti:

milj. euroa (kolmen desimaalin tarkkuudella)

	vuosi **2015**[49]	vuosi **2016**	vuosi **2017**	vuosi **2018**	2019–2021 ja myöh. vuodet			**YHTEENSÄ**
Monivuotisen rahoituskehyksen OTSAKE 5								
Henkilöresurssit	0,572	0,572	0,572	0,572	0,572	0,572	0,572	**4,004**
Muut hallintomenot	0,318	0,118	0,318	0,118	0,318	0,118	0,118	**1,426**
Monivuotisen rahoituskehyksen OTSAKE 5, välisumma	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

Monivuotisen rahoituskehyksen OTSAKKEESEEN 5 sisältymättömät[50]								
Henkilöresurssit	0,000	0,000						**0,000**
Muut hallintomenot								
Monivuotisen rahoituskehyksen OTSAKKEESEEN 5 sisältymättömät, välisumma	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

YHTEENSÄ	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

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

Euroopan verkko- ja tietoturvavirasto ENISA voi avustaa jäsenvaltioita ja komissiota direktiivin täytäntöönpanossa toimeksiantonsa mukaisesti ja kohdentamalla uudelleen

49 Vuosi N on ehdotuksen/aloitteen toteutuksen aloitusvuosi.

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

virastolle monivuotisessa rahoituskehyksessä 2014–2020 osoitettuja resursseja ilman lisämäärärahoja tai -henkilöstöä.

3.2.3.2. Henkilöresurssien arvioitu tarve

– ☐ Ehdotus/aloite ei edellytä henkilöresursseja.

– ☑ Ehdotus/aloite edellyttää komission henkilöresursseja seuraavasti:

Periaatteessa lisähenkilöstöä ei tarvita. Henkilöresursseja tarvitaan vain rajoitetusti, ja ne voidaan kattaa toimen hallinnointiin pääosastossa jo osoitetusta henkilöstöstä.

Arvio kokonaislukuina (tai enintään yhden desimaalin tarkkuudella)

		vuosi **2015**	vuosi **2016**	vuosi **2017**	vuosi **2018**	2019–2021 ja myöh. vuodet		
• Henkilöstötaulukkoon sisältyvät virat/toimet (virkamiehet ja väliaikaiset toimihenkilöt)								
09 01 01 01 (päätoimipaikka ja komission edustustot EU:ssa)		4	4	4	4	4	4	4
XX 01 01 02 (edustustot EU:n ulkopuolella)								
XX 01 05 01 (epäsuora tutkimustoiminta)								
10 01 05 01 (suora tutkimustoiminta)								
• Ulkopuolinen henkilöstö (kokoaikaiseksi muutettuna)[51]								
XX 01 02 01 (CA, INT, SNE – katetaan kokonaismäärärahoista)		1	1	1	1	1	1	1
XX 01 02 02 (CA, INT, JED, LA ja SNE EU:n ulkopuolisissa edustustoissa)								
XX 01 04 ***yy***[52]	– päätoimipaikassa[53]							
	– EU:n ulkopuolisissa edustustoissa							
XX 01 05 02 (CA, INT, SNE – epäsuora tutkimustoiminta)								
10 01 05 02 (CA, INT, SNE – suora tutkimustoiminta)								
Muu budjettikohta (mikä?)								
YHTEENSÄ		**5**	**5**	**5**	**5**	**5**	**5**	**5**

XX viittaa kyseessä olevaan toimintalohkoon eli talousarvion osastoon.

51 CA = sopimussuhteiset toimihenkilöt; INT= vuokrahenkilöstö (”Intérimaire”); JED = ”Jeune Expert en Délégation” (nuoremmat asiantuntijat EU:n ulkopuolisissa edustustoissa); LA = paikalliset toimihenkilöt; SNE = kansalliset asiantuntijat.

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

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

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

Euroopan verkko- ja tietoturvavirasto ENISA voi avustaa jäsenvaltioita ja komissiota direktiivin täytäntöönpanossa nykyisen toimeksiantonsa mukaisesti ja kohdentamalla uudelleen virastolle monivuotisessa rahoituskehyksessä 2014–2020 osoitettuja resursseja ilman lisämäärärahoja tai -henkilöstöä.

Kuvaus henkilöstön tehtävistä:

Virkamiehet ja väliaikaiset toimihenkilöt	– Delegoitujen säännösten valmistelu (14 artiklan 3 kohta) – Täytäntöönpanosäädösten valmistelu (8 artikla, 9 artiklan 2 kohta, 12 artikla, 14 artiklan 5 kohta ja 16 artikla) – Osallistuminen verkossa tehtävään yhteistyöhön sekä poliittisella että operatiivisella tasolla – Osallistuminen kansainväliseen keskusteluihin ja mahdollisten kansainvälisten sopimusten tekemiseen
Ulkopuolinen henkilöstö	Tuki kaikille edellä mainituille toimille tarpeen mukaan

3.2.4. Yhteensopivuus nykyisen monivuotisen rahoituskehyksen kanssa

– ☑ Ehdotus/aloite on nykyisen monivuotisen rahoituskehyksen mukainen.

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

Ehdotuksella on arvioitu vaikutus toimintamenoihin, jos jäsenvaltiot päättävät mukauttaa olemassa olevaa infrastruktuuria ja antavat komissiolle tehtäväksi panna tämä täytäntöön monivuotisessa rahoituskehyksessä 2014–2020. Tähän liittyvät kertaluonteiset kustannukset katettaisiin Verkkojen Eurooppa -välineestä sillä ehdolla, tarjolla on riittävästi varoja. Vaihtoehtoisesti jäsenvaltiot voivat joko jakaa infrastruktuurin mukauttamisesta aiheutuvat kustannukset tai uuden infrastruktuurin luomisesta aiheutuvat kustannukset.

– ☐ Ehdotus/aloite edellyttää joustovälineen varojen käyttöön ottamista tai monivuotisen rahoituskehyksen tarkistamista[54].

Ei sovelleta.

3.2.5. Ulkopuolisten tahojen osallistuminen rahoitukseen

– Ehdotuksen/aloitteen rahoittamiseen ei osallistu ulkopuolisia tahoja.

3.3. Arvioidut vaikutukset tuloihin

– ☑ Ehdotuksella/aloitteella ei ole vaikutuksia tuloihin.

[54] Katso toimielinten sopimuksen 19 ja 24 kohta.