Torstai 13. maaliskuuta 2014

P7_TA(2014)0244

Yhteinen korkeatasoinen verkko- ja tietoturva ***I

Euroopan parlamentin lainsäädäntöpäätöslauselma 13. maaliskuuta 2014 ehdotuksesta Euroopan parlamentin ja neuvoston direktiiviksi toimenpiteistä yhteisen korkeatasoisen verkko- ja tietoturvan varmistamiseksi koko unionissa (COM(2013)0048 – C7-0035/2013 – 2013/0027(COD))

(Tavallinen lainsäätämisjärjestys: ensimmäinen käsittely)

(2017/C 378/74)

Euroopan parlamentti, joka

— ottaa huomioon komission ehdotuksen Euroopan parlamentille ja neuvostolle (COM(2013)0048),

— ottaa huomioon Euroopan unionin toiminnasta tehdyn sopimuksen 294 artiklan 2 kohdan ja 114 artiklan, joiden mukaisesti komissio on antanut ehdotuksen Euroopan parlamentille (C7-0035/2013),

— ottaa huomioon Euroopan unionin toiminnasta tehdyn sopimuksen 294 artiklan 3 kohdan,

— ottaa huomioon Ruotsin parlamentin toissijaisuus- ja suhteellisuusperiaatteen soveltamisesta tehdyn pöytäkirjan N:o 2 mukaisesti antaman perustellun lausunnon, jonka mukaan esitys lainsäätämisjärjestyksessä hyväksyttäväksi säädökseksi ei ole toissijaisuusperiaatteen mukainen,

— ottaa huomioon Euroopan talous- ja sosiaalikomitean 22. toukokuuta 2013 antaman lausunnon ([1]),

— ottaa huomioon 12. syyskuuta 2013 antamansa päätöslauselman ”Unionin tietoverkkoturvallisuusstrategia: Avoin, turvallinen ja vakaa verkkoympäristö” ([2]),

— ottaa huomioon työjärjestyksen 55 artiklan,

— ottaa huomioon sisämarkkina- ja kuluttajansuojavaliokunnan mietinnön sekä teollisuus-, tutkimus- ja energiavaliokunnan, kansalaisvapauksien sekä oikeus- ja sisäasioiden valiokunnan ja ulkoasiainvaliokunnan lausunnot (A7-0103/2014),

1. vahvistaa jäljempänä esitetyn ensimmäisen käsittelyn kannan;

2. pyytää komissiota antamaan asian uudelleen Euroopan parlamentin käsiteltäväksi, jos se aikoo tehdä ehdotukseensa huomattavia muutoksia tai korvata sen toisella ehdotuksella;

3. kehottaa puhemiestä välittämään parlamentin kannan neuvostolle ja komissiolle sekä kansallisille parlamenteille.

P7_TC1-COD(2013)0027

Euroopan parlamentin kanta, vahvistettu ensimmäisessä käsittelyssä 13. maaliskuuta 2014, Euroopan parlamentin ja neuvoston direktiivin 2014/…/EU antamiseksi 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,

---

([1]) EUVL C 271, 19.9.2013, s. 133.
([2]) Hyväksytyt tekstit, P7_TA(2013)0376.

ottavat huomioon Euroopan komission ehdotuksen,

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

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

noudattavat tavallista lainsäätämisjärjestystä ([2]),

sekä katsovat seuraavaa:

(1) Verkko- ja tietojärjestelmillä ja -palveluilla on elintärkeä tehtävä yhteiskunnassa. Niiden luotettavuus ja turvallisuus ovat olennaisen tärkeitä ***unionin kansalaisten vapaudelle ja kokonaisvaltaiselle turvallisuudelle sekä*** talouden toiminnalle ja sosiaaliselle hyvinvoinnille ja erityisesti sisämarkkinoiden toiminnalle. **[tark. 1]**

(2) ~~Tahallisten tai tahattomien~~ Turvapoikkeamien laajuus, esiintymistiheys ***ja vaikutukset*** kasvavat ja muodostavat merkittävän uhan verkko- ja tietojärjestelmien toiminnalle. ***Nämä järjestelmät voivat olla myös helppo kohde tahallisille haitallisille toimenpiteille, joiden tarkoituksena on vahingoittaa tai häiritä järjestelmien toimintaa.*** Tällaiset turvapoikkeamat voivat toimia esteenä taloudelliselle toiminnalle, tuottaa huomattavia taloudellisia tappioita, heikentää käyttäjien ***ja investoijien*** luottamusta ja aiheuttaa merkittävää vahinkoa unionin taloudelle. ***Lisäksi ne voivat viime kädessä vaarantaa kansalaisten hyvinvoinnin ja unionin jäsenvaltioiden kyvyn suojautua ja varmistaa elintärkeiden infrastruktuurien turvallisuus.*** **[tark. 2]**

(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.

(3 a) ***Koska järjestelmien pettäminen johtuu yleensä edelleen tahattomista syistä, kuten luonnollisista syistä tai inhimillisistä erehdyksistä, infrastruktuurien olisi oltava suojattuja tahallisia ja tahattomia toimintahäiriöitä vastaan ja elintärkeiden infrastruktuurien toimittajien olisi suunniteltava häiriönsietokykyyn perustuvia järjestelmiä.*** **[tark. 3]**

(4) Olisi otettava käyttöön unionin tason yhteistyömekanismi, joka mahdollistaa verkko- ja tietoturvaan liittyvän tiedonvaihdon sekä koordinoidun ***ennaltaehkäisyn,*** 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~~ ***ainakin tiettyihin*** tietoinfrastruktuurin ~~operaattoreihin~~ ***markkinatoimijoihin***, jotta voidaan edistää riskinhallintakulttuuria ja varmistaa raportointi vakavimmista turvapoikkeamista. ***Pörssiyhtiöitä olisi kannustettava julkistamaan turvapoikkeamat tilinpäätöksessään vapaaehtoisesti. Oikeudellisen kehyksen olisi perustuttava tarpeeseen suojata kansalaisten yksityisyyttä ja koskemattomuutta. Elintärkeiden infrastruktuurien varoitusjärjestelmää (CIWIN) olisi laajennettava kattamaan tämän direktiivin soveltamisalaan kuuluvat markkinatoimijat.*** **[tark. 4]**

(4 a) ***Julkishallintojen olisi julkisten tehtäviensä vuoksi noudatettava asianmukaista huolellisuutta verkko- ja tietojärjestelmiensä hallinnoinnissa ja suojelussa, kun taas tässä direktiivissä olisi painotettava elintärkeitä infrastruktuureja, sillä ne ovat olennaisia elintärkeiden talouden ja yhteiskunnan toimintojen ylläpitämiselle energian, liikenteen, pankkitoiminnan, finanssimarkkinoiden infrastruktuurien ja terveydenhuollon alalla. Ohjelmistojen kehittäjät ja laitevalmistajat olisi jätettävä tämän direktiivin soveltamisalan ulkopuolelle.*** **[tark. 5]**

([1]) EUVL C 271, 19.9.2013, s. 133.
([2]) Euroopan parlamentin kanta, vahvistettu 13. maaliskuuta 2014.

Torstai 13. maaliskuuta 2014

(4 b) Olisi varmistettava yhteistyö ja koordinointi asianomaisten unionin viranomaisten sekä yhteisestä ulko- ja turvallisuuspolitiikasta ja yhteisestä turvallisuus- ja puolustuspolitiikasta vastaavan korkean edustajan / komission varapuheenjohtajan välillä sekä EU:n terrorisminvastaisen toiminnan koordinaattorin välillä tapauksissa, joissa vaikutuksiltaan merkittävien turvapoikkeamien havaitaan olevan luonteeltaan ulkoisia terrorismiin liittyviä uhkia. **[tark. 6]**

(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 Euroopan parlamentin ja neuvoston direktiivissä 2002/21/EY ([1]) 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. ***Yliopistoilla ja tutkimuskeskuksilla on ratkaiseva rooli tutkimuksen, kehityksen ja innovaation vauhdittamisessa näillä aloilla, ja niille olisi varattava riittävästi määrärahoja.*** **[tark. 7]**

(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***, riittävien tietoverkkoturvaa koskevien taitojen kehittämisen***, tiedonvaihdon ja toimien koordinoinnin sekä yhteiset vähimmäisturvavaatimukset ~~kaikille kyseeseen tuleville markkinatoimijoille ja julkishallinnoille~~. ***Yhteisiä vähimmäisvaatimuksia olisi sovellettava tietoverkkoturvan koordinoinnista vastaavien ryhmien (Cyber Security Coordination Groups, CSGC) antamien asianmukaisten suositusten mukaisesti.*** **[tark. 8]**

(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. Euroopan unionin toiminnasta tehdyn sopimuksen 346 artiklan mukaisesti mitään jäsenvaltiota ei pitäisi velvoittaa antamaan tietoja, joiden ilmaisemisen se katsoo keskeisten turvallisuusetujensa vastaiseksi. ***Mitään jäsenvaltiota ei velvoiteta ilmaisemaan neuvoston päätöksen 2011/292/EU*** ([2]) ***mukaisia EU:n turvallisuusluokiteltuja tietoja tai salassapitosopimusten tai epävirallisten salassapitosopimusten kuten Traffic Light Protocol -säännöstön mukaisia tietoja.*** **[tark. 9]**

(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 ***ja tässä direktiivissä asetettuihin vähimmäisvaatimuksiin perustuvia*** verkko- ja tietoturvan yhteistyösuunnitelmia, jotta saavutetaan valmiudet ja reagointikyky sellaisella tasolla, että voidaan toimia tuloksellisesti yhteistyössä kansallisella ja unionin tasolla turvapoikkeamien sattuessa ***siten, että kunnioitetaan ja suojellaan yksityiselämää ja henkilötietoja. Kaikki jäsenvaltiot olisi siksi velvoitettava täyttämään tiedon muotoa sekä jaettavan ja arvioitavan tiedon vaihdettavuutta koskevat yhteiset standardit. Jäsenvaltioiden olisi voitava pyytää apua Euroopan unionin verkko- ja tietoturvavirastolta (ENISA) kehittäessään yhteiseen verkko- ja tietoturvastrategiaa koskevaan vähimmäistason suunnitelmaan perustuvia kansallisia verkko- ja tietoturvastrategioitaan.*** **[tark. 10]**

([1]) Euroopan parlamentin ja neuvoston direktiivi 2002/21/EY, annettu 7 päivänä maaliskuuta 2002, sähköisten viestintäverkkojen ja -palvelujen yhteisestä sääntelyjärjestelmästä (puitedirektiivi) (EYVL L 108, 24.4.2002, s. 33).

([2]) ***Neuvoston päätös 2011/292/EU, annettu 31 päivänä maaliskuuta 2011, turvallisuussäännöistä EU:n turvallisuusluokiteltujen tietojen suojaamiseksi (EUVL L 141, 27.5.2011, s. 17).***

(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.

***(10 a) Koska kansallisissa hallinnointirakenteissa on eroja ja jotta taataan jo olemassa olevien alakohtaisten järjestelyjen tai unionin valvonta- ja sääntelyelinten säilyttäminen ja vältetään päällekkäisyyksiä, jäsenvaltioiden olisi voitava nimetä useampi kuin yksi kansallinen toimivaltainen viranomainen, joka vastaa markkinatoimijoiden verkko- ja tietojärjestelmien turvallisuuteen liittyvistä tehtävistä tämän direktiivin mukaisesti. Sujuvan rajat ylittävän yhteistyön ja viestinnän varmistamiseksi on kuitenkin välttämätöntä, että kukin jäsenvaltio nimeää vain yhden kansallisen yhteyspisteen, joka vastaa rajat ylittävästä yhteistyöstä unionin tasolla, sanotun kuitenkaan vaikuttamatta alakohtaisiin sääntelyjärjestelyihin. Jäsenvaltion olisi voitava nimetä vain yksi toimivaltainen viranomainen hoitamaan toimivaltaisen viranomaisen ja yhteyspisteen tehtäviä, jos sen perustuslaillinen rakenne tai muut järjestelyt sitä edellyttävät. Toimivaltaisten viranomaisten ja yhteyspisteiden olisi oltava täysimääräisen demokraattisen valvonnan alaisia siviilielimiä, eivätkä ne saisi suorittaa mitään tiedusteluun, lainvalvontaan tai puolustukseen liittyviä tehtäviä eivätkä olla organisatorisesti millään tavalla kytköksissä näillä aloilla toimiviin elimiin.* [tark. 11]**

(11) Kaikilla jäsenvaltioilla ***ja markkinatoimijoilla*** olisi oltava käytössään riittävät sekä tekniset että organisatoriset valmiudet, jotta voidaan ***milloin tahansa*** ehkäistä ja havaita verkko- ja tietojärjestelmien turvapoikkeamia ja -riskejä, reagoida niihin ja lieventää niiden vaikutuksia. ***Julkishallintojen turvajärjestelmien olisi oltava turvallisia sekä demokraattisen valvonnan ja tarkkailun alaisia. Yleisesti edellytettyjen laitteistojen ja valmiuksien olisi täytettävä yhteisesti hyväksytyt tekniset standardit ja oltava standardinmukaisten toimintamenettelyjen mukaisia.*** Tämän vuoksi kaikkiin jäsenvaltioihin olisi perustettava hyvin toimivat ja olennaiset vaatimukset täyttävät tietotekniikan kriisiryhmät (Computer Emergency Response Teams, CERT), jotta voidaan taata toimivat ja yhteensopivat valmiudet turvapoikkeamien ja -riskien varalta ja varmistaa tehokas yhteistyö unionin tasolla. ***Näille CERT-ryhmille olisi annettava valtuudet toteuttaa vastavuoroisia toimia yhteisten teknisten standardien ja standardinmukaisten toimintamenettelyjen pohjalta. Jäsenvaltioiden olisi, ottaen huomioon nykyisten CERT-ryhmien erilaiset ominaispiirteet, jotka vastaavat eri alojen ja toimijoiden tarpeita, varmistettava, että ainakin yksi CERT-ryhmä tarjoaa palveluja kullakin tähän direktiiviin sisältyvässä markkinatoimijoiden luettelossa tarkoitetulla alalla. Jäsenvaltioiden olisi CERT-ryhmien rajat ylittävän yhteistyön kyseessä ollessa huolehdittava siitä, että ryhmillä on riittävät resurssit osallistua jo toiminnassa oleviin kansainvälisiin ja unionin yhteistyöverkostoihin.*** [tark. 12]

(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***, johon markkinatoimijat tarvittaessa osallistuvat,*** olisi mahdollistettava jäsennetty ja koordinoitu tiedonvaihto sekä tietojen havaitseminen ja reagointi unionin tasolla. [tark. 13]

(13) ~~Euroopan verkko- ja tietoturvaviraston (ENISA)~~ ***ENISAn*** olisi avustettava jäsenvaltioita ja komissiota antamalla asiantuntemusta ja neuvontaa ja helpottamalla parhaiden käytäntöjen vaihtamista. Komission ***ja jäsenvaltioiden*** 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. [tark. 14]

(13 a) Jäsenvaltioiden olisi voitava tarvittaessa käyttää tai mukauttaa olemassa olevia organisaatiorakenteita tai strategioita tämän direktiivin säännöksiä soveltaessaan. [tark. 15]

Torstai 13. maaliskuuta 2014

(14) Arkaluonteisten ja luottamuksellisten tietojen vaihtamiseksi verkostossa olisi otettava käyttöön suojattu tiedonjakoinfrastruktuuri. ***Unionin nykyisiä rakenteita olisi käytettävä täysimääräisesti tähän tarkoitukseen.*** 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 ***ja avoimia menetelmiä käyttäen***. **[tark. 16]**

(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 ***turvapoikkeamien tapauksessa keskenään*** tietoa ja parhaita toimintatapoja vastineeksi ***asiaa koskevasta tiedosta,*** operatiivisesta tuesta ~~turvapoikkeamien tapauksessa~~ ***ja strategisesti analysoiduista tiedoista. Jotta voidaan tehokkaasti kannustaa tiedon ja parhaiden toimintatapojen jakamiseen, on varmistettava, etteivät tällaiseen vaihtoon osallistuvat markkinatoimijat joudu yhteistyön vuoksi epäsuotuisaan asemaan. Tarvitaan riittäviä turvatakuita sen varmistamiseksi, ettei tällaisella yhteistyöllä altisteta kyseisiä toimijoita suuremmille säännösten laiminlyöntiin liittyville riskeille tai uusille velvoitteille muun muassa kilpailua, immateriaalioikeuksia, tietosuojaa tai tietoverkkorikollisuutta koskevan lainsäädännön nojalla eikä lisääntyneille toiminta- tai turvallisuusriskeille.*** **[tark. 17]**

(16) Avoimuuden varmistamiseksi ja ~~EU:n~~ ***unionin*** kansalaisten ja markkinatoimijoiden informoimiseksi asianmukaisesti ~~toimivaltaisten viranomaisten~~ ***yhteyspisteiden*** olisi perustettava yhteinen ***unionin laajuinen*** verkkosivusto, jolla julkaistaan ei-luottamukselliset tiedot turvapoikkeamista ja -riskeistä ***ja keinoista riskien lieventämiseksi sekä annetaan tarvittaessa asianmukaisia ylläpitotoimia koskevia neuvoja. Verkkosivuston tietoihin olisi oltava pääsy riippumatta käytetystä laitteesta. Tällä verkkosivustolla olisi julkaistava henkilötietoja ainoastaan siinä määrin kuin se on välttämätöntä ja mahdollisimman anonyymisti.*** **[tark. 18]**

(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***, parhaat toimintatavat ja toimintamallit*** turvariskien ja -poikkeamien ***ennaltaehkäisemiseksi, havaitsemiseksi,*** torjumiseksi ***ja niistä ilmoittamiseksi***. Tämä suunnitelma olisi otettava asianmukaisesti huomioon varhaisvaroitusten tekemisessä yhteistyöverkostossa. **[tark. 19]**

(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. **[tark. 20]**

(20) Saatuaan varhaisvaroituksen ja sen arvioinnin ~~toimivaltaisten viranomaisten~~ ***yhteyspisteiden*** olisi sovittava koordinoidusta reagoinnista unionin verkko- ja tietoturvan yhteistyösuunnitelman mukaisesti. Sekä ~~toimivaltaisille viranomaisille~~ ***yhteyspisteille, ENISAlle*** että komissiolle olisi ilmoitettava toimenpiteistä, jotka kansallisella tasolla on toteutettu koordinoidun reagoinnin tuloksena. **[tark. 21]**

Torstai 13. maaliskuuta 2014

(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. ***Kaikkiin tällaisen kansainvälisen yhteistyön puitteisiin olisi sovellettava Euroopan parlamentin ja neuvoston direktiiviä 95/46/EY*** ([1]) ***ja Euroopan parlamentin ja neuvoston asetusta (EY) N:o 45/2001*** ([2])**. [tark. 22]**

(22) Vastuu verkko- ja tietoturvan varmistamisesta lankeaa paljolti ~~julkishallinnoille ja~~ markkinatoimijoille. ~~Riskinhallintakulttuuria~~ ***Riskinhallinnan, tiiviin yhteistyön ja luottamuksen kulttuuria***, johon sisältyy riskinarviointi ~~ja~~ ***sekä*** riskeihin ***ja tahallisiin tai tahattomiin turvapoikkeamiin*** suhteutettujen turvatoimenpiteiden toteuttaminen, olisi edistettävä ja kehitettävä asianmukaisten sääntelyllisten vaatimusten ja toimialojen vapaaehtoisten käytäntöjen kautta. Tasavertaisten ***ja luotettavien*** toimintaedellytysten luominen on myös olennaista yhteistyöverkoston tehokkaan toiminnan kannalta, jotta voidaan varmistaa tuloksellinen yhteistyö kaikkien jäsenvaltioiden taholta. **[tark. 23]**

(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. 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 ***infrastruktuurien operaattoreihin, sillä ne ovat vahvasti riippuvaisia tieto- ja viestintäteknologiasta ja olennaisia elintärkeiden talouden ja yhteiskunnan toimintojen, kuten sähkön ja kaasun jakelun, liikenteen, luottolaitosten, rahoitusmarkkinoiden infrastruktuurien ja terveydenhuollon, ylläpitämiselle. Häiriö näissä verkko- ja tietojärjestelmissä vaikuttaisi sisämarkkinoihin. Vaikka tässä direktiivissä vahvistettuja velvoitteita ei tulisi ulottaa koskemaan*** Euroopan parlamentin ja neuvoston direktiivissä 98/34/EY ([4]) määriteltyjä sellaisten tietoyhteiskunnan palvelujen keskeisiä tarjoajia, jotka tukevat loppukäyttäjille suunnattuja tietoyhteiskunnan palveluja tai verkkotoimintoja, kuten sähköisen kaupankäynnin alustoja, internet-välitteisiä maksupalveluja, verkkoyhteisöpalveluja, hakukoneita, pilvipalveluja ***yleensä tai*** ~~ja~~ sovelluskauppoja***, nämä palvelujen tarjoajat voisivat vapaaehtoisesti ilmoittaa toimivaltaiselle viranomaiselle tai yhteyspisteelle sellaisista verkon turvapoikkeamista, joista ilmoittamista ne pitävät asianmukaisena. Toimivaltaisen viranomaisen tai yhteyspisteen olisi, mikäli mahdollista, toimitettava turvapoikkeamasta ilmoittaneille markkinatoimijoille strategisesti analysoidut tiedot, joiden avulla turvallisuusuhka voidaan torjua.*** ~~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 terveydenhuollon, ylläpitämiselle. Häiriö näissä verkko- ja tietojärjestelmissä vaikuttaisi sisämarkkinoihin.~~ **[tark. 24]**

([1]) ***Euroopan parlamentin ja neuvoston direktiivi 95/46/EY, annettu 24 päivänä lokakuuta 1995, yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta (EYVL L 281, 23.11.1995, s. 31).***

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

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

([4]) Euroopan parlamentin ja neuvoston direktiivi 98/34/EY, annettu 22 päivänä kesäkuuta 1998, teknisiä standardeja ja määräyksiä ja tietoyhteiskunnan palveluja koskevia määräyksiä koskevien tietojen toimittamisessa noudatettavasta menettelystä (EYVL L 204, 21.7.1998, s. 37).

Torstai 13. maaliskuuta 2014

(***24 a***) ***Laitteiden ja ohjelmistojen toimittajat eivät ole tämän direktiivin soveltamisalaan kuuluviin markkinatoimijoihin verrattavia toimijoita, mutta niiden tuotteet lisäävät verkko- ja tietojärjestelmien turvallisuutta. Ne tarjoavat markkinatoimijoille mahdollisuuden turvata verkko- ja tietoinfrastruktuurinsa ja niillä on siksi tärkeä tehtävä. Koska laitteisiin ja ohjelmistoihin kuuluville tuotteille on jo vahvistettu tuotevastuuta koskevia sääntöjä, jäsenvaltioiden olisi varmistettava, että kyseiset säännöt pannaan täytäntöön.*** **[tark. 25]**

(25) ~~Julkishallinnoille ja~~ Markkinatoimijoille määrättävät tekniset ja organisatoriset toimenpiteet eivät saisi edellyttää jonkin tietyn kaupallisen tieto- ja viestintäteknologiatuotteen suunnittelua, kehittämistä tai valmistamista tietyllä tavalla. **[tark. 26]**

(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. **[tark. 27]**

(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 ***ja yhteyspisteiden*** olisi kiinnitettävä asianmukaista huomiota epävirallisten ja luotettavien tiedonjakokanavien säilyttämiseen markkinatoimijoiden välillä ja julkisen ja yksityisen sektorin välillä. ***Toimivaltaisten viranomaisten ja yhteyspisteiden olisi ilmoitettava kyseisten tieto- ja viestintäteknologiatuotteiden ja -palvelujen valmistajille ja palveluntarjoajille niille ilmoitetuista turvapoikkeamista, joilla on näihin merkittävä vaikutus***. Toimivaltaisille viranomaisille ***ja yhteyspisteille*** 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 ***ja yhteyspisteiden*** olisi kiinnitettävä erityistä huomiota tarpeeseen pitää tuotteiden haavoittuvuutta koskevat tiedot tiukasti luottamuksellisena ennen asianomaisten turvallisuuspäivitysten ~~julkistamista~~ ***käyttöönottoa***. ***Yhteyspisteiden ei pääsääntöisesti tulisi luovuttaa turvapoikkeamiin osallisten henkilöiden henkilötietoja. Yhteyspisteiden olisi luovutettava henkilötietoja vain tapauksissa, joissa se on välttämätöntä ja oikeasuhteista tavoitteen saavuttamiseksi.*** **[tark. 28]**

(29) Toimivaltaisilla viranomaisilla olisi oltava tarvittavat keinot tehtäviensä suorittamiseen, mukaan lukien valtuudet saada riittävät tiedot markkinatoimijoilta ~~ja julkishallinnoilta~~ verkko- ja tietojärjestelmien turvatason arvioimiseksi ***ja turvapoikkeamien määrän, laajuuden ja kohteiden mittaamiseksi*** sekä luotettavat ja kattavat tiedot verkko- ja tietojärjestelmien toimintaan vaikuttaneista tosiasiallisista turvapoikkeamista. **[tark. 29]**

(30) Turvapoikkeaman taustalla on usein rikollinen toiminta. Turvapoikkeamien rikollista luonnetta voidaan epäillä, vaikka sitä tukeva näyttö ei olisi riittävän selvä alusta alkaen. Toimivaltaisten viranomaisten***, yhteyspisteiden*** ja lainvalvontaviranomaisten välisen yhteistyön ***sekä Euroopan verkkorikostorjuntakeskuksen (EC3) ja ENISAn kanssa tehtävän 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 unionin lainsäädännön perusteella. **[tark. 30]**

(31) Turvapoikkeamat vaarantavat monissa tapauksissa henkilötiedot. ***Jäsenvaltioiden ja markkinatoimijoiden olisi suojeltava tallennettuja, käsiteltyjä tai siirrettyjä henkilötietoja vahingossa tapahtuvalta tai laittomalta tuhoamiselta, vahingossa tapahtuvalta häviämiseltä tai muuttamiselta sekä luvattomalta tai laittomalta tallentamiselta, käytöltä tai luovuttamiselta tai levittämiseltä ja varmistettava henkilötietojen käsittelyn turvallisuus.*** Toimivaltaisten viranomaisten***, yhteyspisteiden*** ja tietosuojaviranomaisten olisi tässä yhteydessä tehtävä yhteistyötä ja vaihdettava tietoa ~~kaikista asiaankuuluvista seikoista~~ ***tarvittaessa myös markkinatoimijoiden kanssa***, jotta voidaan puuttua turvapoikkeamista johtuviin henkilötietojen tietoturvaloukkauksiin ***voimassa olevien tietosuojasääntöjen mukaisesti***. ~~Jäsenvaltioiden on pantava täytäntöön~~ Velvollisuus ilmoittaa turvapoikkeamista ***olisi täytettävä*** 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 ([1]) tarkoitettu~~ henkilötietojen tietoturvaloukkaus, ***josta on ilmoitettava unionin tietosuojalainsäädännön mukaisesti***. ~~Enisa voisi~~ ***ENISAn olisi*** tällöin ~~toimia toimivaltaisten viranomaisten~~ ***avustettava toimivaltaisia viranomaisia*** ja ~~tietosuojaviranomaisten kanssa yhteistyössä~~ ***tietosuojaviranomaisia*** kehittämällä tiedonvaihtomekanismeja ja ~~malleja, joiden avulla vältetään tarve kahdelle ilmoitusmallille.~~ yksi yhteinen ilmoitusmalli, ***joka*** helpottaisi henkilötiedot vaarantaneista turvapoikkeamista raportoimista ja keventäisi yrityksille ja julkishallinnoille koituvaa hallinnollista taakkaa. **[tark. 31]**

(32) Turvallisuusvaatimusten standardointi tapahtuu markkinavetoisesti ***vapaaehtoisuuden pohjalta siten, että markkinatoimijoiden olisi voitava käyttää vaihtoehtoisia keinoja, joilla saavutetaan vähintään samanlaisia tuloksia***. Turvastandardien johdonmukaisen soveltamisen varmistamiseksi jäsenvaltioiden olisi edistettävä tiettyjen ***yhteentoimivien*** standardien noudattamista tai mukaisuutta, jotta voidaan varmistaa turvallisuuden korkea taso unionissa. Tätä varten ***on syytä harkita verkon tietoturvaa koskevien avoimien kansainvälisten standardien soveltamista tai tällaisten välineiden kehittämistä***. Voi olla ***myös*** tarpeen laatia yhdenmukaistettuja standardeja, jolloin olisi noudatettava Euroopan parlamentin ja neuvoston asetusta (EU) N:o 1025/2012 ([2]). ***Erityisesti ETSI (eurooppalainen telealan standardointijärjestö), CEN (Euroopan standardointikomitea) ja CENELEC (Euroopan sähkötekninen standardointijärjestö) olisi valtuutettava ehdottamaan vaikuttavia ja tehokkaita unionin avoimia turvastandardeja, joissa vältetään mahdollisuuksien mukaan tiettyjen teknisten ratkaisujen suosimista ja joiden olisi oltava pienten ja keskisuurten markkinatoimijoiden helposti hallinnoitavissa. Tietoverkkoturvallisuutta koskevia kansainvälisiä standardeja olisi tarkasteltava huolellisesti sen varmistamiseksi, että ne eivät ole uhattuja ja että niillä taataan asianmukainen turvallisuus, varmistaen näin, että tietoverkkoturvallisuutta koskevia standardeja noudattamalla parannetaan unionin tietoverkkoturvallisuutta kokonaisvaltaisesti eikä päinvastoin.*** **[tark. 32]**

(33) Komission olisi tarkasteltava tätä direktiiviä säännöllisin väliajoin uudelleen***, kaikkia asianosaisia sidosryhmiä kuullen,*** erityisesti ***yhteiskunnan, politiikan,*** tekniikan ja markkinaolojen kehitykseen perustuvien muutostarpeiden selvittämiseksi. **[tark. 33]**

(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~~ ***jotka koskevat*** suojattuun ~~tiedonjakojärjestelmään,~~ ***tiedonjakoinfrastruktuuriin liittyviä yleisiä yhteenliitettävyys- ja turvastandardeja ja joilla*** täsmennetään tarkemmin varhaisvaroituksen käynnistävät tapahtumat ~~ja määritellään olosuhteet, joissa markkinatoimijoiden ja julkishallintojen on ilmoitettava turvapoikkeamista~~. **[tark. 34]**

([1]) ~~SEC(2012) 72 final.~~

([2]) Euroopan parlamentin ja neuvoston asetus (EU) N:o 1025/2012, annettu 25 päivänä lokakuuta 2012, eurooppalaisesta standardoinnista, neuvoston direktiivien 89/686/ETY ja 93/15/ETY sekä Euroopan parlamentin ja neuvoston direktiivien 94/9/EY, 94/25/EY, 95/16/EY, 97/23/EY, 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 (EUVL L 316, 14.11.2012, s. 12).

Torstai 13. maaliskuuta 2014

(35) On erityisen tärkeää, että komissio asiaa valmistellessaan toteuttaa 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~~ ***tämän direktiivin yhdenmukainen täytäntöönpano,*** komissiolle olisi siirrettävä täytäntöönpanovaltaa siltä osin kuin on kyse ~~toimivaltaisten viranomaisten~~ ***yhteyspisteiden*** ja komission välisestä yhteistyöstä yhteistyöverkostossa, ~~pääsystä suojattuun tiedonjakoinfrastruktuuriin~~ ***sanotun kuitenkaan rajoittamatta kansallisella tasolla olemassa olevien yhteistyömekanismien toimintaa***, unionin verkko- ja tietoturvan yhteistyösuunnitelmasta~~, turvapoikkeamia koskevan julkisen tiedotuksen~~ ***sekä vaikutuksiltaan merkittävistä turvapoikkeamista ilmoittamiseen käytettävistä*** muodoista ja menettelyistä ~~sekä verkko- ja tietoturvan kannalta merkityksellisistä standardeista ja/tai teknisistä eritelmistä~~. Tätä valtaa olisi käytettävä Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 182/2011 ([1]) mukaisesti. **[tark. 35]**

(37) Komission olisi tämän direktiivin täytäntöönpanossa toimittava tarpeen mukaan yhteistyössä asiaankuuluvien alakohtaisten komiteoiden ja ***unionin*** tasolla erityisesti ***sähköisten viranomaispalvelujen,*** energian, liikenteen, ~~ja~~ terveyden ***ja puolustuksen*** alalla perustettujen elinten kanssa. **[tark. 36]**

(38) Tietoja, jotka toimivaltainen viranomainen ***tai yhteyspiste*** katsoo liikesalaisuuksia koskevien unionin ja kansallisten sääntöjen mukaisesti luottamuksellisiksi, olisi vaihdettava komission***, sen asiaan liittyvien virastojen, yhteyspisteiden*** ja/***tai*** muiden ***kansallisten*** toimivaltaisten viranomaisten kanssa vain silloin kun se on ehdottoman välttämätöntä tämän direktiivin soveltamiseksi. Tällöin olisi toimitettava vain ne tiedot, jotka ovat merkityksellisiä***, tarpeellisia*** ja ~~laajuudeltaan oikein suhteutettuja~~ ***oikeasuhteisia*** kulloisenkin tiedonvaihdon tarkoituksen kannalta***, ja olisi noudatettava luottamuksellisuutta ja turvallisuutta koskevia ennalta määriteltyjä kriteerejä päätöksen 2011/292/EU mukaisesti, kun on kyse tiedoista, joihin sovelletaan salassapitosopimuksia tai epävirallisia salassapitosopimuksia, kuten Traffic Light Protocol -säännöstöä***. **[tark. 37]**

(39) Turvariskejä ja -poikkeamia koskevien tietojen jakaminen yhteistyöverkostossa ja turvapoikkeamista kansallisille viranomaisille ***tai yhteyspisteille*** 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 Euroopan unionin 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 ja neuvoston asetusta (EY) N:o 1049/2001 ([2]). Kun tietoja käsittelevät unionin toimielimet ja muut elimet, kyseisessä tämän direktiivin täytäntöönpanemiseksi suoritettavassa tietojen käsittelyssä olisi noudatettava asetusta (EY) N:o 45/2001. **[tark. 38]**

(40) Jäsenvaltiot eivät voi 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. Sen vuoksi unioni voi toteuttaa toimenpiteitä Euroopan unionista tehdyn sopimuksen 5 artiklassa vahvistetun toissijaisuusperiaatteen mukaisesti. Mainitussa artiklassa vahvistetun suhteellisuusperiaatteen mukaisesti tässä direktiivissä ei ylitetä sitä, mikä on tarpeen näiden tavoitteiden saavuttamiseksi.

(41) Tässä direktiivissä kunnioitetaan Euroopan unionin perusoikeuskirjassa tunnustettuja perusoikeuksia ja noudatetaan siinä tunnustettuja periaatteita, erityisesti 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,

---

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

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

(41 a) 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. **[tark. 39]**

(41 b) Euroopan tietosuojavaltuutettua on kuultu asetuksen (EY) N:o 45/2001 28 artiklan 2 kohdan mukaisesti, ja hän on antanut lausunnon 14 päivänä kesäkuuta 2013 ([1]),

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.

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***, johon asianomaiset sidosryhmät osallistuvat***, jotta voidaan varmistaa tämän direktiivin yhtenäinen soveltaminen unionissa ja tarvittaessa verkko- ja tietojärjestelmiin vaikuttavien turvariskien ja -poikkeamien koordinoitu, ~~ja~~ tehokas ***ja tuloksellinen*** käsittely ja niihin reagoiminen; **[tark. 40]**

c) vahvistetaan turvavaatimukset markkinatoimijoille ~~ja julkishallinnoille~~. **[tark. 41]**

3. Tämän direktiivin 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 unionin lainsäädännön soveltamista eikä neuvoston direktiivin 2008/114/EY ([2]) soveltamista.

5. Tämä direktiivi ei myöskään rajoita direktiivin 95/46/EY, direktiivin 2002/58/EY eikä asetuksen ***(EY) N:o 45/2001*** soveltamista. ***Henkilötietojen käyttö on rajoitettava siihen, mikä on ehdottomasti välttämätöntä tämän direktiivin soveltamisen kannalta, ja niiden olisi oltava mahdollisimman anonyymeja tai täysin anonyymeja.*** **[tark. 42]**

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.

([1]) EUVL C 32, 4.2.2014, s. 19.
([2]) Neuvoston direktiivi 2008/114/EY, annettu 8 päivänä joulukuuta 2008, Euroopan elintärkeän infrastruktuurin määrittämisestä ja nimeämisestä sekä arvioinnista, joka koskee tarvetta parantaa sen suojaamista (EUVL L 345, 23.12.2008, s. 75).

Torstai 13. maaliskuuta 2014

1 a artikla

Henkilötietojen suojelu ja käsittely

1. Kaikessa tämän direktiivin mukaisessa henkilötietojen käsittelyssä jäsenvaltioissa on noudatettava direktiiviä 95/46/EY ja direktiiviä 2002/58/EY.

2. Kaikessa tämän asetuksen mukaisessa henkilötietojen käsittelyssä komissiossa ja ENISAssa on noudatettava asetusta (EY) N:o 45/2001/EY.

3. Kaikessa tämän direktiivin tarkoituksiin suoritettavassa henkilötietojen käsittelyssä Europolin alaisessa verkkorikostorjuntakeskuksessa on noudatettava neuvostom päätöstä 2009/371/YOS [1].

4. Henkilötietoja on käsiteltävä oikeudenmukaisesti ja laillisesti ja käsittely on rajattava tiukasti vähimmäistietoihin, jotka ovat tarpeen niiden tarkoitusten toteuttamiseksi, joita varten niitä käsitellään. Tietoja on säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten.

5. Tämän direktiivin 14 artiklassa tarkoitetut turvapoikkeamia koskevat ilmoitukset eivät estä soveltamasta säännöksiä ja velvoitteita, jotka koskevat direktiivin 2002/58/EY 4 artiklassa ja komission asetuksessa (EU) N:o 611/2013 [2] ***tarkoitettuja ilmoituksia henkilötietojen tietoturvaloukkauksista.*** **[tark. 43]**

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

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~~ ***digitaalisten tietojen käsittelyä*** sekä **[tark. 44]**

c) ~~sähköisiä~~ ***digitaalisia*** tietoja, joita a ja b alakohdassa mainituissa järjestelmissä varastoidaan, käsitellään, hankitaan tai välitetään niiden toimintaa, käyttöä, suojausta tai ylläpitoa varten. **[tark. 45]**

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; ***”turvallisuuteen” sisältyvät asianmukaiset tekniset laitteet, ratkaisut ja toimintamenettelyt, joilla varmistetaan tässä direktiivissä vahvistettujen turvallisuusvaatimusten noudattaminen;*** **[tark. 46]**

---

[1] ***Neuvoston päätös 2009/371/YOS, tehty 6 päivänä huhtikuuta 2009, Euroopan poliisiviraston (Europol) perustamisesta (EUVL L 121, 15.5.2009, s. 37).***

[2] ***Komission asetus (EU) N:o 611/2013, annettu 24 päivänä kesäkuuta 2013, henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla annetun Euroopan parlamentin ja neuvoston direktiivin 2002/58/EY mukaisten henkilötietojen tietoturvaloukkausten ilmoittamiseen sovellettavista toimenpiteistä (EUVL L 173, 26.6.2013, s. 2).***

3) ”turvariskillä” mitä tahansa ***kohtuullisesti tunnistettavissa olevaa*** tilannetta tai tapahtumaa, joka saattaa vaikuttaa kielteisesti turvallisuuteen; **[tark. 47]**

4) ”turvapoikkeamalla” mitä tahansa ~~tilannetta tai~~ tapahtumaa, joka tosiasiassa vaikuttaa kielteisesti turvallisuuteen; **[tark. 48]**

~~5) ”tietoyhteiskunnan palvelulla” direktiivin 98/34/EY 1 artiklan 2 alakohdassa tarkoitettua palvelua;~~ **[tark. 49]**

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 ***havaitsemista, ennaltaehkäisyä,*** analyysia, sen vaikutusten rajoittamista ja siihen reagointia; **[tark. 50]**

8) ”markkinatoimijalla”

~~a) sellaisten tietoyhteiskunnan palvelujen tarjoajaa, jotka mahdollistavat muiden tietoyhteiskunnan palvelujen tarjoamisen; näistä palveluntarjoajista on ei-tyhjentävä luettelo liitteessä II;~~ **[tark. 51]**

b) sellaisten ~~elintärkeiden~~ infrastruktuurien ylläpitäjää, jotka ovat olennaisia elintärkeiden talouden ja yhteiskunnan toimintojen ylläpitämiselle energiahuollon, liikenteen, pankkitoimen, ~~pörssitoimen~~ ***finanssimarkkinoiden infrastruktuurien***, ***internetin yhdysliikennepisteiden, elintarvikkeiden toimitusketjun*** ja terveydenhuollon aloilla ***ja joiden keskeytymisellä tai tuhoutumisella olisi merkittäviä vaikutuksia jäsenvaltioon siksi, että edellä mainittuja toimintoja ei voitaisi ylläpitää***; näistä operaattoreista on ei-tyhjentävä luettelo liitteessä II***, sikäli kuin kyseiset verkko- ja tietojärjestelmät ovat merkityksellisiä niiden keskeisten palvelujen kannalta***; **[tark. 52]**

8 a) ”vaikutuksiltaan merkittävällä turvapoikkeamalla” turvapoikkeamaa, joka vaikuttaa tietoverkon tai -järjestelmän turvallisuuteen ja jatkuvuuteen siten, että se aiheuttaa vakavan häiriön elintärkeille talouden ja yhteiskunnan toiminnoille; **[tark. 53]**

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.

11 a) ”säännellyllä markkinalla” Euroopan parlamentin ja neuvoston direktiivin 2004/39/EY [1] ***4 artiklan 1 kohdan 14 alakohdassa määriteltyä säänneltyä markkinaa;*** **[tark. 54]**

11 b) ”monenkeskisellä kaupankäyntijärjestelmällä” direktiivin 2004/39/EY 4 artiklan 1 kohdan 15 alakohdassa määriteltyä monenkeskistä kaupankäyntijärjestelmää; **[tark. 55]**

11 c) ”organisoidulla kaupankäyntijärjestelmällä” monenkeskistä järjestelmää, joka ei ole sijoituspalveluyrityksen tai markkinoiden ylläpitäjän ylläpitämä säännelty markkina, monenkeskinen kaupankäyntijärjestelmä tai keskusvastapuoli ja jossa useiden kolmansien osapuolten joukkovelkakirjoja, strukturoituja rahoitustuotteita, päästöoikeuksia tai johdannaisia koskevat osto- ja myynti-intressit voivat olla keskenään vuorovaikutuksessa siten, että tuloksena on sopimus direktiivin 2004/39/EY II osaston säännösten mukaisesti. **[tark. 56]**

---

[1] ***Euroopan parlamentin ja neuvoston direktiivi 2004/39/EY, annettu 21 päivänä huhtikuuta 2004, rahoitusvälineiden markkinoista (EUVL L 45, 16.2.2005, s. 18).***

Torstai 13. maaliskuuta 2014

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,

e a) Jäsenvaltiot voivat pyytää tukea ENISAlta kehittäessään kansallisia verkko- ja tietoturvastrategioitaan ja kansallisia verkko- ja tietoturvayhteistyösuunnitelmiaan yhteisen vähimmäistason verkko- ja tietoturvastrategian pohjalta. **[tark. 57]**

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

a) ~~riskinhallintasuunnitelma~~ ***riskinhallintakehys, jossa vahvistetaan menetelmä*** riskien yksilöimiseksi, ~~ja~~ ***priorisoimiseksi, arvioimiseksi ja käsittelemiseksi,*** mahdollisten turvapoikkeamien vaikutusten ***ja ennaltaehkäisy- ja valvontamahdollisuuksien*** arvioimiseksi ***sekä mahdollisten vastatoimien valintaa koskevien kriteerien määrittelemiseksi***; **[tark. 58]**

b) ~~suunnitelman~~ ***kehyksen*** täytäntöönpanoon osallistuvien eri ***viranomaisten ja muiden*** toimijoiden tehtävien ja vastuiden määrittely, **[tark. 59]**

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 ***kolmen*** kuukauden kuluessa niiden hyväksymisestä. **[tark. 60]**

6 artikla

Verkko- ja tietojärjestelmien turvallisuudesta ~~vastaava kansallinen toimivaltainen viranomainen~~ ***vastaavat kansalliset toimivaltaiset viranomaiset ja yhteyspisteet*** **[tark. 61]**

1. Jokaisen jäsenvaltion on nimettävä ***yksi tai useampi*** verkko- ja tietojärjestelmien turvallisuudesta vastaava kansallinen toimivaltainen ~~viranomainen~~ ***siviiliviranomainen*** (jäljempänä ”toimivaltainen viranomainen” ***tai ”toimivaltaiset viranomaiset”***). **[tark. 62]**

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

2 a. Jos jäsenvaltio nimeää useampia kuin yhden toimivaltaisen viranomaisen, sen on nimettävä kansallinen siviiliviranomainen, esimerkiksi toimivaltainen viranomainen, verkko- ja tietojärjestelmien turvallisuudesta vastaavaksi kansalliseksi yhteyspisteeksi, jäljempänä ”yhteyspiste”. Jos jäsenvaltio nimeää vain yhden toimivaltaisen viranomaisen, toimivaltainen viranomainen on myös yhteyspiste. **[tark. 63]**

2 b. Jäsenvaltion toimivaltaisten viranomaisten ja yhteyspisteen on tehtävä tekevät tiivistä yhteistyötä tässä direktiivissä vahvistettujen velvoitteiden täyttämiseksi. **[tark. 64]**

2 c. Yhteyspisteen on varmistettava, että muiden yhteyspisteiden kanssa tehdään rajat ylittävää yhteistyötä. **[tark. 65]**

3. Jäsenvaltioiden on varmistettava, että toimivaltaisilla viranomaisilla ***ja yhteyspisteillä*** 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~~ ***yhteyspisteiden*** tuloksellinen, tehokas ja suojattu yhteistyö 8 artiklassa tarkoitetussa verkostossa. **[tark. 66]**

4. Jäsenvaltioiden on varmistettava, että toimivaltaiset viranomaiset ***ja yhteyspisteet*** saavat ***tarvittaessa tämän artiklan 2 a kohdan mukaisesti*** turvapoikkeamista ilmoitukset ~~julkishallinnoilta ja~~ markkinatoimijoilta siten kuin 14 artiklan 2 kohdassa säädetään sekä 15 artiklassa tarkoitetut täytäntöönpanovaltuudet ja täytäntöönpanon valvontavaltuudet. **[tark. 67]**

4 a. Jos unionin lainsäädännössä säädetään alakohtaisesta unionin valvonta- tai sääntelyelimestä, joka sääntelee muun muassa verkko- ja tietojärjestelmien turvallisuutta, tämän elimen on saatava kyseisen alan asianomaisilta markkinatoimijoilta ilmoitukset turvapoikkeamista 14 artiklan 2 kohdan mukaisesti, ja sille on annettava 15 artiklassa tarkoitetut täytäntöönpano- ja valvontavaltuudet. Tämän unionin elimen on tehtävä tiivistä yhteistyötä vastaanottavan jäsenvaltion yhteyspisteen kanssa näiden velvoitteiden täyttämiseksi. Vastaanottavan jäsenvaltion yhteyspisteen on edustettava unionin elintä luvussa III säädettyjen velvoitteiden kyseessä ollessa. **[tark. 48]**

5. Toimivaltaisten viranomaisten ***ja yhteyspisteiden*** on tarvittaessa kuultava asiaankuuluvia kansallisia lainvalvontaviranomaisia ja tietosuojaviranomaisia ja tehtävä yhteistyötä niiden kanssa. **[tark. 69]**

6. Jokaisen jäsenvaltion on ilmoitettava komissiolle viipymättä ~~toimivaltaisen viranomaisen~~ ***toimivaltaisten viranomaisten ja yhteyspisteiden*** nimeämisestä ja tehtävistä sekä mahdollisista myöhemmistä muutoksista näissä tiedoissa. Jokaisen jäsenvaltion on julkistettava ~~toimivaltaisen viranomaisen~~ ***toimivaltaisten viranomaisten*** nimeäminen. **[tark. 70]**

7 artikla

Tietotekniikan kriisiryhmä

1. Jokaisen jäsenvaltion on perustettava ***kutakin liitteessä II lueteltua alaa varten vähintään yksi*** 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. **[tark. 71]**

Torstai 13. maaliskuuta 2014

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 tiedonjako-järjestelmän kanssa.

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

5. ~~CERT-ryhmän~~ ***CERT-ryhmien*** on toimittava toimivaltaisen viranomaisen ***tai yhteyspisteen*** valvonnassa, ja toimivaltaisen viranomaisen ***tai yhteyspisteen*** on säännöllisesti tarkasteltava uudelleen ~~sen~~ ***niiden*** voimavarojen riittävyyttä, ~~toimeksiantoa~~ ***toimeksiantoja*** ja turvapoikkeamien käsittelyprosessin tuloksekkuutta. **[tark. 72]**

5 a. Jäsenvaltioiden on varmistettava, että CERT-ryhmillä on riittävät inhimilliset ja taloudelliset resurssit, jotta ne voivat osallistua aktiivisesti kansainvälisten ja erityisesti unionin tason yhteistyöverkostojen toimintaan. **[tark. 73]**

5 b. CERT-ryhmille on annettava valtuudet aloittaa yhteisiä harjoituksia ja osallistua sellaisiin muiden CERT-ryhmien, jäsenvaltioiden kaikkien CERT-ryhmien ja muiden kuin jäsenvaltioiden asianomaisten toimielinten sekä Naton ja YK:n kaltaisten monikansallisten ja kansainvälisten instituutioiden CERT-ryhmien kanssa, ja niitä on rohkaistava aloittamaan tällaisia harjoituksia ja osallistumaan niihin. **[tark. 74]**

5 c. Jäsenvaltiot voivat kansallisia CERT-ryhmiään kehittäessään pyytää apua ENISAlta tai muilta jäsenvaltioilta. **[tark. 75]**

III LUKU

TOIMIVALTAISTEN VIRANOMAISTEN VÄLINEN YHTEISTYÖ

8 artikla

Yhteistyöverkosto

1. ~~Toimivaltaiset viranomaiset ja~~ ***Yhteyspisteet,*** komissio ***ja ENISA*** muodostavat verkoston, jäljempänä ”yhteistyö-verkosto”, jotta voidaan tehdä yhteistyötä verkko- ja tietojärjestelmiin vaikuttavien turvariskien ja -poikkeamien torjumiseksi. **[tark. 76]**

2. Komissio ja ~~toimivaltaiset viranomaiset~~ ***yhteyspisteet*** ovat yhteistyöverkostossa pysyvästi yhteydessä toisiinsa. ~~Euroopan verkko- ja tietoturvavirasto, jäljempänä ”~~ENISA”, avustaa pyynnöstä yhteistyöverkostoa antamalla asiantunte-musta ja neuvontaa. ***Myös markkinatoimijoita ja verkkoturvaratkaisujen toimittajia voidaan tarvittaessa pyytää osallistumaan 3 kohdan g ja i alakohdassa tarkoitettuihin yhteistyöverkoston tehtäviin.***

Yhteistyöverkoston on tehtävä tarvittaessa yhteistyötä tietosuojaviranomaisten kanssa.

Komissio tiedottaa säännöllisesti yhteistyöverkostolle Horisontti 2020 -puiteohjelman turvallisuustutkimuksista ja muista asiaan liittyvistä ohjelmista. **[tark. 77]**

3. Yhteistyöverkostossa ~~toimivaltaisten viranomaisten~~ ***yhteyspisteden*** 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 ***asiantuntevaa*** tietoa ~~kaikista asiaankuuluvista~~ ***verkko- ja tietoturvaa koskevista merkityksellisistä*** seikoista ~~Europolin yhteydessä toimivan Euroopan verkkorikostorjuntakeskuksen kanssa ja muiden asianomaisten~~, erityisesti tietosuojan, energiahuollon, liikenteen, pankkitoimen, ~~pörssitoimen~~ ***finanssimarkkinoiden*** ja terveydenhuollon ~~alan~~ ***alalla Europolin yhteydessä toimivan Euroopan verkkorikostorjuntakeskuksen ja muiden asianomaisten*** eurooppalaisten elinten kanssa,

f a) annettava tarvittaessa selontekoja EU:n terrorisminvastaisen toiminnan koordinaattorille, jota voidaan pyytää avustamaan yhteistyöverkostoa sen tutkimuksissa, valmistelevassa työssä ja toiminnassa;

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,

i a) osallistettava ja kuultava tarvittaessa markkinatoimijoita ja vaihdettava niiden kanssa tietoja niiden verkko- ja tietojärjestelmiin vaikuttavista turvariskeistä ja -poikkeamista,

i b) kehitettävä yhteistyössä ENISAn kanssa suuntaviivoja merkittävistä turvapoikkeamista ilmoittamista koskeville alakohtaisille kriteereille 14 artiklan 2 kohdassa säädettyjen parametrien lisäksi, jotta niitä voidaan tulkita yhtenäisesti sekä soveltaa johdonmukaisesti ja jotta ne voidaan panna täytäntöön yhdenmukaisesti koko unionissa. **[tark. 78]**

3 a. Yhteistyöverkoston on julkaistava vuosittain 12 edeltävää kuukautta kattava kertomus, joka perustuu verkoston toteuttamiin toimiin ja tämän direktiivin 14 artiklan 4 kohdan mukaisesti annettuun tiivistelmäraporttiin. **[tark. 79]**

4. Komissio vahvistaa täytäntöönpanosäädöksissä tarvittavat säännöt 2 ja 3 kohdassa tarkoitetun ~~toimivaltaisten viranomaisten ja~~ ***yhteyspisteiden,*** komission ***ja ENISAn*** välisen yhteistyön helpottamiseksi. Nämä täytäntöönpanosäädökset hyväksytään 19 artiklan 2 kohdassa tarkoitettua ~~kuulemismenettelyä~~ ***tarkastelumenettelyä*** noudattaen. **[tark. 80]**

9 artikla

Suojattu tiedonjakojärjestelmä

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

1 a. Suojattuun infrastruktuuriin osallistuvien toimijoiden on noudatettava muun muassa direktiivin 95/46/EY ja asetuksen (EY) N:o 45/2001 mukaisia tarvittavia luottamuksellisuutta ja turvallisuutta koskevia toimia käsittelyn kaikissa vaiheissa. **[tark. 81]**

Torstai 13. maaliskuuta 2014

~~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.~~ **[tark. 82]**

3. Komissio hyväksyy ***18 artiklan mukaisesti*** ~~täytäntöönpanosäädöksillä 2 ja 3 kohdassa tarkoitettujen perusteiden nojalla päätökset jäsenvaltioiden pääsystä tähän suojattuun infrastruktuuriin. Nämä täytäntöönpanosäädökset hyväksytään 19 artiklan 3 kohdassa tarkoitettua sääntelymenettelyä noudattaen~~ ***delegoiduilla säädöksillä yhteiset yhteenliitettävyys- ja turvastandardit, joita yhteyspisteiden on noudatettava ennen arkaluonteisten ja luottamuksellisten tietojen vaihtoa yhteistyöverkostossa***. **[tark. 83]**

10 artikla

Varhaisvaroitukset

1. ~~Toimivaltaisten viranomaisten~~ ***yhteyspisteiden*** 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~~ ***yhteyspiste arvioi, että turvariski tai -poikkeama mahdollisesti*** ylittää kansalliset reagointivalmiudet;

c) ~~ne vaikuttavat tai voivat~~ ***yhteyspiste tai komissio arvioi, että turvariski tai -poikkeama*** vaikuttaa useampaan kuin yhteen jäsenvaltioon. **[tark. 84]**

2. ~~Toimivaltaisten viranomaisten~~ ***Yhteyspisteiden*** ja komission on varhaisvaroituksissa annettava ***viipymättä*** kaikki asiaankuuluvat hallussaan olevat tiedot, joista voi olla hyötyä turvariskin tai -poikkeaman arvioinnissa. **[tark. 85]**

~~3. Komissio voi jäsenvaltion pyynnöstä tai omasta aloitteestaan pyytää jäsenvaltiota antamaan kaikki tarvittavat tiedot tietystä turvariskistä tai -poikkeamasta.~~ **[tark. 86]**

4. Jos turvariskiin tai -poikkeamaan, josta on tehty varhaisvaroitus, epäillään liittyvän rikollisuutta~~, toimivaltaisten viranomaisten tai komission on ilmoitettava tästä~~ ***ja jos asianomainen markkinatoimija on 15 artiklan 4 kohdan mukaisesti ilmoittanut poikkeamista, joihin epäillään liittyvän vakavaa rikollisuutta, jäsenvaltioiden on varmistettava, että asiasta ilmoitetaan tarvittaessa*** Europolin yhteydessä toimivalle Euroopan verkkorikostorjuntakeskukselle. **[tark. 87]**

4 a. Yhteistyöverkoston jäsenet eivät voi julkaista 1 kohdassa tarkoitetuista turvariskeistä ja -poikkeamista saamiaan tietoja, jos ne eivät ole saaneet ennalta hyväksyntää ilmoittavalta yhteyspisteeltä.

Ilmoittavan yhteyspisteen on lisäksi ennen yhteistyöverkostossa tapahtuvaa tietojen jakamista ilmoitettava aikomuksestaan markkinatoimijalle, jota tiedot koskevat, ja, jos se pitää tätä tarpeellisena, anonymisoitava tiedot. **[tark. 88]**

4 b. Jos turvariskiin tai -poikkeamaan, josta on tehty varhaisvaroitus, epäillään liittyvän vakavia teknisiä rajatylittäviä piirteitä, yhteyspisteiden tai komission on ilmoitettava tästä ENISAlle. **[tark. 89]**

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

11 artikla

Koordinoitu reagointi

1. Edellä 10 artiklassa tarkoitetun varhaisvaroituksen jälkeen ~~toimivaltaisten viranomaisten~~ ***yhteyspisteiden*** on asiaankuuluvat tiedot arvioituaan ***viipymättä*** sovittava koordinoidusta reagoinnista 12 artiklassa tarkoitetun unionin verkko- ja tietoturvan yhteistyösuunnitelman mukaisesti. **[tark. 90]**

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~~ ***yhteyspisteet*** keräävät ja jakavat yhteensopivaa ja vertailukelpoista tietoa turvariskeistä ja -poikkeamista, **[tark. 91]**

— 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. ***Kunkin tarkistuksen tuloksista ilmoitetaan Euroopan parlamentille.*** **[tark. 92]**

3 a. Unionin verkko- ja tietoturvan yhteistyösuunnitelman ja 5 artiklassa tarkoitettujen kansallisten verkko- ja tietoturvastrategioiden ja kansallisten verkko- ja tietoturvan yhteistyösuunnitelmien välinen johdonmukaisuus on varmistettava. **[tark. 93]**

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 ***ja määrättävä valvontamenettelystä, jota on noudatettava niiden suojan takaamiseksi. Euroopan parlamentille on ilmoitettava tällaisia sopimuksia koskevista neuvotteluista. Kaikki henkilötietojen siirrot unionin ulkopuolisissa maissa oleville vastaanottajille on tehtävä direktiivin 95/46/EY 25 ja 26 artiklan sekä asetuksen (EY) N:o 45/2001 9 artiklan mukaisesti.*** **[tark. 94]**

Torstai 13. maaliskuuta 2014

13 a artikla

Markkinatoimijoiden vaatimustaso

Jäsenvaltiot voivat määritellä markkinatoimijoiden vaatimustason ottaen huomioon alojen erityispiirteet ja parametrit, joihin sisältyvät tietyn alakohtaista riittävän tasoista palvelua ylläpitävän markkinatoimijan merkitys, toimitettujen erien määrä ja ajanjakso, jonka kuluessa markkinatoimijan keskeisen palvelun keskeyttämisellä on kielteinen vaikutus elintärkeiden talouden ja yhteiskunnan toimintojen ylläpitämiseen. **[tark. 95]**

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 ***ja oikeasuhtaiset*** tekniset ja organisatoriset toimenpiteet valvonnassaan olevien ja toiminnoissaan käyttämiensä verkko- ja tietojärjestelmien turvallisuuteen kohdistuvien riskien ***havaitsemiseksi ja*** hallitsemiseksi ***tehokkaasti***. Näillä toimenpiteillä on voitava varmistaa riskiin suhteutettu turvallisuustaso ottaen huomioon uusin tekniikka. Erityisesti on toteutettava toimenpiteet, joilla ehkäistään ja minimoidaan niiden ~~verkko- ja tietojärjestelmään~~ ***verkko- ja tietojärjestelmien turvallisuuteen*** niiden tarjoamissa keskeisissä palveluissa vaikuttavien turvapoikkeamien vaikutukset ja näin taataan näiden verkko- ja tietojärjestelmien tukemien palvelujen jatkuvuus. **[tark. 96]**

2. Jäsenvaltioiden on varmistettava, että ~~julkishallinnot ja~~ markkinatoimijat ilmoittavat ***viipymättä*** toimivaltaiselle viranomaiselle ***tai yhteyspisteelle*** turvapoikkeamista, jotka vaikuttavat merkittävästi niiden tarjoamien keskeisten palvelujen ~~turvallisuuteen~~ ***jatkuvuuteen***. ***Ilmoittaminen ei lisää ilmoituksen tekevän osapuolen vastuuta***.

Turvapoikkeaman vaikutuksen merkittävyyttä arvioitaessa otetaan huomioon muun muassa seuraavat parametrit: **[tark. 97]**

a) niiden käyttäjien lukumäärä, joiden keskeisiin palveluihin turvapoikkeama vaikuttaa; **[tark. 98]**

b) turvapoikkeaman kesto; **[tark. 99]**

c) turvapoikkeaman vaikutusten maantieteellinen levinneisyys. **[tark. 100]**

Kyseisiä parametreja on edelleen tarkennettava 8 artiklan 3 kohdan i b alakohdan mukaisesti. **[tark. 101]**

2 a. Markkinatoimijoiden on ilmoitettava 1 ja 2 kohdassa tarkoitetuista turvapoikkeamista toimivaltaiselle viranomaiselle tai yhteyspisteelle siinä jäsenvaltiossa, jossa turvapoikkeama vaikuttaa keskeisiin palveluihin. Jos turvapoikkeama vaikuttaa keskeisiin palveluihin useammassa kuin yhdessä jäsenvaltiossa, ilmoituksen vastaanottaneen yhteyspisteen on varoitettava muita asianomaisia yhteyspisteitä markkinatoimijalta saamiensa tietojen perusteella. Markkinatoimijalle on ilmoitettava mahdollisimman pian muut yhteyspisteet, joille turvapoikkeamasta on ilmoitettu, sekä toteutetut toimet, tulokset tai muut turvapoikkeaman kannalta merkitykselliset tiedot. **[tark. 102]**

2 b. Jos ilmoitus sisältää henkilötietoja, sen saa luovuttaa vain sen toimivaltaisen viranomaisen tai yhteyspisteen henkilöstölle, jonka on käsiteltävä kyseisiä tietoja suorittaakseen tehtävänsä tietosuojasäännösten mukaisesti. Vain ne tiedot voidaan luovuttaa, jotka ovat välttämättömiä tehtävien suorittamiseksi. **[tark. 103]**

2 c. Liitteen II soveltamisalaan kuulumattomat markkinatoimijat voivat ilmoittaa vapaaehtoisesti 14 artiklan 2 kohdassa tarkoitetuista turvapoikkeamista. **[tark. 104]**

3. Edellä olevia 1 ja 2 kohtaa sovelletaan kaikkiin Euroopan unionissa palveluja tarjoaviin markkinatoimijoihin.

4. ~~Toimivaltainen viranomainen~~ ***Yhteyspiste*** voi ***ilmoituksen saanutta toimivaltaista viranomaista ja asianomaista markkinatoimijaa kuultuaan*** tiedottaa yleisölle ~~tai vaatia julkishallintoja ja markkinatoimijoita tiedottamaan yleisölle~~ ***yksittäisistä turvapoikkeamista***, jos se katsoo ~~turvapoikkeaman julkistamisen~~ ***suuren yleisön tietoisuuden*** olevan ~~yleisen edun mukaista~~ ***välttämätöntä turvapoikkeaman ennalta ehkäisemiseksi tai meneillään olevaan turvapoikkeamaan reagoimiseksi tai jos turvapoikkeamaan osallinen markkinatoimija on kieltäytynyt korjaamasta turvapoikkeaman aiheuttanutta vakavaa rakenteellista puutetta viipymättä***.

Ennen yleisölle tiedottamista ilmoituksen saaneen toimivaltaisen viranomaisen on varmistettava, että asianomaisella markkinatoimijalla on mahdollisuus tulla kuulluksi ja että yleisölle tiedottamista koskeva päätös on oikeassa suhteessa yleiseen etuun nähden.

Kun yksittäisiä turvapoikkeamia koskevat tiedot julkistetaan, ilmoituksen saaneen toimivaltaisen viranomaisen tai yhteyspisteen on varmistettava, että tiedot ilmoitetaan mahdollisimman anonyymisti.

Toimivaltaisen viranomaisen tai yhteyspisteen on, mikäli se on kohtuullisesti mahdollista, toimitettava asianomaiselle markkinatoimijalle tietoja, jotka edistävät tehokasta ilmoitettuun turvapoikkeamaan reagoimista.

~~Toimivaltaisen viranomaisen~~ ***Yhteyspisteen*** on toimitettava yhteistyöverkostolle vuosittain tiivistelmäraportti vastaanotetuista ilmoituksista***, mukaan luettuina ilmoitusten lukumäärä ja tämän artiklan 2 kohdassa luetellut turvapoikkeamia koskevat parametrit,*** ja tämän kohdan mukaisesti toteutetuista toimista. **[tark. 105]**

4 a. Jäsenvaltioiden on kannustettava markkinatoimijoita ilmoittamaan niiden liiketoimintaa koskevista turvapoikkeamista vapaaehtoisesti tilinpäätöksissään. **[tark. 106]**

~~5. Siirretään komissiolle 18 artiklan mukaisesti valta antaa delegoituja säädöksiä, joissa määritellään olosuhteet, joissa julkishallintojen ja markkinatoimijoiden edellytetään ilmoittavan turvapoikkeamista.~~ **[tark. 107]**

6. ~~Jollei 5 kohdan mukaisesti hyväksytyistä delegoiduista säädöksistä muuta johdu,~~ Toimivaltaiset viranomaiset ***tai yhteyspisteet*** voivat hyväksyä suuntaviivoja ~~ja tarvittaessa antaa ohjeita liittyen olosuhteisiin~~ ***olosuhteista***, joissa ~~julkishallintojen ja~~ markkinatoimijoiden edellytetään ilmoittavan turvapoikkeamista. **[tark. 108]**

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 komission suosituksessa 2003/361/EY ([1]) määriteltyihin mikroyrityksiin***, ellei mikroyritys toimi 3 artiklan 8 kohdan b alakohdassa määritellyn markkinatoimijan tytäryhtiönä***. **[tark. 109]**

8 a. Jäsenvaltiot voivat päättää soveltaa tätä artiklaa ja 15 artiklaa soveltuvin osin julkishallintoon. **[tark. 110]**

15 artikla

Täytäntöönpano ja sen valvonta

1. Jäsenvaltioiden on varmistettava, että toimivaltaisilla viranomaisilla ***ja yhteyspisteillä*** on ~~kaikki~~ tarvittavat valtuudet ~~tutkia tapaukset, joissa julkishallinnot tai~~ ***varmistaa, että*** markkinatoimijat ~~eivät ole noudattaneet~~ ***täyttävät*** 14 artiklan ~~mukaisia velvoitteitaan~~ ***mukaiset velvoitteensa***, sekä ~~näiden tapausten~~ ***tutkia velvoitteiden noudattamatta jättämisen*** vaikutukset verkko- ja tietojärjestelmien turvallisuuteen. **[tark. 111]**

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

Torstai 13. maaliskuuta 2014

2. Jäsenvaltioiden on varmistettava, että toimivaltaisilla viranomaisilla ***ja yhteyspisteillä*** on valtuudet vaatia markkinatoimijoita ~~ja julkishallintoja~~ **[tark. 112]**

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~~ ***esittämään todisteita turvatoimien tosiasiallisesta täytäntöönpanosta, kuten pätevän ulkopuolisen elimen tai kansallisen viranomaisen suorittaman turvallisuustarkastuksen tuloksia***, ja toimittamaan ~~sen tulokset~~ ***todisteet*** toimivaltaiselle viranomaiselle ***tai yhteyspisteelle***. **[tark. 113]**

Toimivaltaisten viranomaisten ja yhteyspisteiden on pyynnön esittäessään ilmoitettava, mihin tarkoitukseen ne tarvitsevat todisteita, ja täsmennettävä, mitä tietoja ne haluavat. **[tark. 114]**

3. Jäsenvaltioiden on varmistettava, että toimivaltaisilla viranomaisilla ***ja yhteyspisteillä*** on valtuudet antaa sitovia ohjeita markkinatoimijoille ~~ja julkishallinnoille~~. **[tark. 115]**

3 a. Poiketen siitä, mitä tämän artiklan 2 kohdan b alakohdassa säädetään, jäsenvaltiot voivat päättää, että toimivaltaisten viranomaisten tai tapauksen mukaan yhteyspisteiden on sovellettava eri menettelyä tiettyihin markkinatoimijoihin niiden 13 a artiklan mukaisesti määritellyn vaatimustason perusteella. Jos jäsenvaltiot näin päättävät,

a) toimivaltaisilla viranomaisilla tai tapauksen mukaan yhteyspisteillä on valtuudet esittää markkinatoimijoille asianmukaisesti eritelty pyyntö, jolla niitä edellytetään esittämään turvatoimien tehokkaasta täytäntöönpanosta todisteet, jollaisia ovat pätevän sisäisen tarkastajan suorittaman turvallisuustarkastuksen tulokset, ja toimittamaan todisteet toimivaltaiselle viranomaiselle tai yhteyspisteelle;

b) toimivaltainen viranomainen tai yhteyspiste voi a alakohdassa tarkoitetun markkinatoimijan esittämän pyynnön jälkeen tarvittaessa vaatia lisätodisteita tai pyytää pätevää ulkopuolista elintä tai kansallista viranomaista suorittamaan lisätarkastuksen.

3 b. Jäsenvaltiot voivat päättää vähentää kyseistä markkinatoimijaa koskevien tarkastusten lukumäärää ja intensiteettiä, jos sen on turvallisuustarkastuksessa todettu jatkuvasti täyttävän IV luvussa vahvistetut vaatimukset. **[tark. 116]**

4. Toimivaltaisten viranomaisten ***ja yhteyspisteiden*** on ilmoitettava ***asianomaisille markkinatoimijoille mahdollisuudesta ilmoittaa lainvalvontaviranomaisille*** turvapoikkeamista, joihin epäillään liittyvän vakavaa rikollisuutta~~, lainvalvontaviranomaisille~~. **[tark. 117]**

5. Toimivaltaisten viranomaisten ***ja yhteyspisteiden*** on työskenneltävä tiiviisti yhteistyössä tietosuojaviranomaisten kanssa, kun ne käsittelevät henkilötietojen tietoturvaloukkauksiin johtaneita turvapoikkeamia***, sanotun kuitenkaan rajoittamatta tietosuojasäännösten soveltamista. Yhteyspisteiden ja tietosuojaviranomaisten on yhteistyössä ENISAn kanssa kehitettävä tietojenvaihtomekanismeja sekä malli, jota käytetään sekä tämän direktiivin 14 artiklan 2 kohdan että unionin muun tietosuojalainsäädännön mukaisiin ilmoituksiin.*** **[tark. 118]**

6. Jäsenvaltioiden on varmistettava, että kaikkiin tämän luvun nojalla ~~julkishallinnoille ja~~ markkinatoimijoille määrättäviin velvoitteisiin voidaan hakea muutosta tuomioistuimessa. **[tark. 119]**

6 a. Jäsenvaltiot voivat päättää soveltaa 14 artiklaa ja tätä artiklaa soveltuvin osin julkishallintoihin. **[tark. 120]**

16 artikla

Standardointi

1. Jäsenvaltioiden on 14 artiklan 1 kohdan johdonmukaisen täytäntöönpanon varmistamiseksi edistettävä***, ilman, että ne määräävät käyttämään mitään tiettyä teknologiaa,*** verkko- ja tietoturvan kannalta merkityksellisten***, yhteentoimivien eurooppalaisten tai kansainvälisten*** standardien ja/tai eritelmien käyttöä. **[tark. 121]**

2. Komissio ~~laatii täytäntöönpanosäädöksillä~~ ***valtuuttaa asianomaisen eurooppalaisen standardointielimen laatimaan yhdessä asianomaisten sidosryhmien kanssa*** luettelon 1 kohdassa tarkoitetuista standardeista ***ja/tai eritelmistä***. Luettelo julkaistaan *Euroopan unionin virallisessa lehdessä*. **[tark. 122]**

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.

1 a. Jäsenvaltioiden on varmistettava, että tämän artiklan 1 kohdassa tarkoitettuja seuraamuksia sovelletaan vain, jos markkinatoimija on jättänyt täyttämättä IV luvussa tarkoitetut velvoitteet tahallisesti tai törkeästä huolimattomuudesta. **[tark. 123]**

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 ([1]) säädettyjen seuraamusten kanssa.

18 artikla

Siirretyn säädösvallan käyttäminen

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

2. Siirretään komissiolle valta antaa 9 artiklan 3 kohdassa ja 10 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 vastusta tällaista jatkamista viimeistään kolme kuukautta ennen kunkin kauden päättymistä.

3. Euroopan parlamentti tai neuvosto voi milloin tahansa peruuttaa 9 artiklan 3 kohdassa, ***ja*** 10 artiklan 5 kohdassa ~~ja 14 artiklan 5 kohdassa~~ tarkoitetun säädösvallan siirron. Peruuttamispäätöksellä lopetetaan tuossa päätöksessä mainittu säädösvallan siirto. ~~Päätös~~ ***Peruuttaminen*** tulee voimaan sitä päivää seuraavana päivänä, jona ***sitä koskeva päätös*** julkaistaan *Euroopan unionin virallisessa lehdessä*, tai jonakin myöhempänä, ***kyseisessä*** päätöksessä mainittuna päivänä. ~~Päätös~~ ***Peruuttamispäätös*** ei vaikuta jo voimassa olevien delegoitujen säädösten pätevyyteen. **[tark. 124]**

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

([1]) SEC(2012) 72 final.

Torstai 13. maaliskuuta 2014

5. Edellä ~~olevien~~ ***olevan*** 9 artiklan 3 kohdan, ***ja*** 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. **[tark. 125]**

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***, erityisesti liitteessä II olevaa luetteloa,*** 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. **[tark. 126]**

21 artikla

Saattaminen osaksi kansallista lainsäädäntöä

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

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

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

2. Jäsenvaltioiden on toimitettava tässä direktiivissä säännellyistä 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

Euroopan parlamentin puolesta	*Neuvoston puolesta*
Puhemies	*Puheenjohtaja*

Torstai 13. maaliskuuta 2014

LIITE I

Tietotekniikan ~~kriisiryhmän (CERT)~~ ***kriisiryhmien (CERT-ryhmät)*** vaatimukset ja tehtävät **[tark. 127]**

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~~ ***CERT-ryhmien*** 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 ***milloin tahansa***. Viestintäkanavat on määriteltävä selkeästi, ja niiden on oltava hyvin käyttäjien ja yhteistyökumppanien tiedossa. **[tark. 128]**

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

c) ~~CERT-ryhmän~~ ***CERT-ryhmien*** toimipaikka ja sitä tukevat tietojärjestelmät on sijoitettava suojattuihin paikkoihin***, joissa on suojatut verkkotietojärjestelmät***. **[tark. 129]**

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 ***havaitseminen ja*** seuranta kansallisella tasolla, **[tark. 130]**

— 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,

— ***aktiivinen osallistuminen unionin tason ja kansainvälisiin CERT-ryhmien yhteistyöverkostoihin,*** *[tark. 131]*

— 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.

Torstai 13. maaliskuuta 2014

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:~~ **[tark. 132]**

1. Energia

a) Sähkö

— ~~Sähkön- ja kaasuntoimittajat~~ ***Toimittajat***

— ~~Sähkön ja/tai kaasun~~ Jakeluverkot ja vähittäiskaupan toimittajat

— ~~Maakaasun siirtoverkot ja varastointi sekä nesteytetyn maakaasun operaattorit~~

— Sähkön siirtoverkot

b) Öljy

— Öljysiirtoputkistot ja öljyvarastot

— ***Öljyn tuotanto-, jalostus- ja käsittelylaitteistojen operaattorit, varastointi ja siirto***

c) Kaasu

— ~~Sähkö- ja kaasumarkkinatoimijat~~

— ***Toimittajat***

— ***Jakeluverkot ja vähittäiskaupan toimittajat***

— ***Maakaasun siirtoverkon haltijat, maakaasun varastointilaitoksen haltijat sekä nesteytetyn maakaasun käsittelylaitoksen haltijat***

— ~~Öljyn ja~~ Maakaasun tuotanto-, jalostus- ja käsittelylaitteistojen operaattorit***, varastointilaitokset ja siirto***

— ***Kaasumarkkinatoimijat*** *[tark. 133]*

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.~~

a) Maantieliikenne

i) Liikenteenhallinnan ja -ohjauksen ylläpitäjät

ii) Liitännäiset logistiikkapalvelut:

— varastot ja varastointi

— rahdinkäsittely ja

— muut liikenteen tukitoiminnot

b) Rautatieliikenne

i) Rautatiet (rataverkon haltijat, integroituneet yritykset ja rautatieliikenteen harjoittajat)

ii) Liikenteenhallinnan ja -ohjauksen ylläpitäjät

iii) Liitännäiset logistiikkapalvelut:

— varastot ja varastointi

— rahdinkäsittely ja

— muut liikenteen tukitoiminnot

c) Lentoliikenne

i) Lentoliikenteen (rahti- ja matkustajaliikenteen) harjoittajat

ii) Lentoasemat

iii) Liikenteenhallinnan ja -ohjauksen ylläpitäjät

iv) Liitännäiset logistiikkapalvelut:

— varastointi

— rahdinkäsittely ja

— muut liikenteen tukitoiminnot

d) Meriliikenne

i) Merenkulun (sisävesien sekä meri- ja rannikkoliikenteen matkustaja- ja rahtiliikenteen) harjoittajat *[tark. 134]*

3. Pankkitoimi: Euroopan parlamentin ja neuvoston direktiivin 2006/48/EY ([1]) 4 artiklan 1 kohdassa tarkoitetut luottolaitokset

([1]) Euroopan parlamentin ja neuvoston direktiivi 2006/48/EY, annettu 14 päivänä kesäkuuta 2006, luottolaitosten liiketoiminnan aloittamisesta ja harjoittamisesta (EUVL L 177, 30.6.2006, s. 1).

Torstai 13. maaliskuuta 2014

4. Finanssimarkkinoiden infrastruktuurit: ~~pörssit~~ ***säännellyt markkinat, monenkeskiset kaupankäyntijärjestelmät, organisoidut kaupankäyntijärjestelmät*** ja keskusvastapuoliyhteisöt **[tark. 135]**

5. Terveydenhuolto: terveydenhuoltolaitokset (kuten sairaalat ja yksityisklinikat) sekä muut terveydenhuollon tarjoamiseen osallistuvat laitokset

5 a. Veden tuotanto ja toimitus **[tark. 136]**

5 b. Elintarvikeketju **[tark. 137]**

5 c. Internetin yhdysliikennepisteet **[tark. 138]**