Euroopan unionin
virallinen lehti

L 194

59. vuosikerta

Suomenkielinen laitos **Lainsäädäntö**

19. heinäkuuta 2016

Sisältö

FI

Säädökset, joiden otsikot on painettu laihalla kirjasintyypillä, ovat maatalouspolitiikan alaan kuuluvia juoksevien asioiden hoitoon liittyviä säädöksiä, joiden voimassaoloaika on yleensä rajoitettu.

Kaikkien muiden säädösten otsikot on painettu lihavalla kirjasintyypillä ja merkitty tähdellä.

I

(Lainsäätämisjärjestyksessä hyväksyttävät säädökset)

DIREKTIIVIT

EUROOPAN PARLAMENTIN JA NEUVOSTON DIREKTIIVI (EU) 2016/1148,

annettu 6 päivänä heinäkuuta 2016,

toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa

EUROOPAN PARLAMENTTI JA EUROOPAN UNIONIN NEUVOSTO, jotka

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

ottavat huomioon Euroopan komission ehdotuksen,

sen jälkeen kun esitys 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 talouden ja yhteiskunnan toiminnoille ja erityisesti sisämarkkinoiden toiminnalle.

(2) Turvapoikkeamien laajuus, esiintymistiheys ja vaikutukset kasvavat ja muodostavat merkittävän uhan verkko- ja tietojärjestelmien toiminnalle. Nämä järjestelmät voivat myös joutua sellaisten tahallisten haitallisten toimien kohteeksi, joiden tarkoituksena on vahingoittaa tai häiritä järjestelmien toimintaa. Tällaiset poikkeamat voivat haitata taloudellisen toiminnan harjoittamista, aiheuttaa huomattavia taloudellisia tappioita, heikentää käyttäjien luottamusta ja aiheuttaa merkittävää vahinkoa unionin taloudelle.

(3) Verkko- ja tietojärjestelmät, ja ensisijaisesti internet, helpottavat olennaisesti tavaroiden, palvelujen ja ihmisten liikkumista rajojen yli. Tämän ylikansallisen luonteen vuoksi näiden järjestelmien merkittävät häiriöt, olivatpa ne tahallisia tai tahattomia ja riippumatta siitä, missä ne tapahtuvat, voivat vaikuttaa yksittäisiin jäsenvaltioihin ja koko unioniin. Verkko- ja tietojärjestelmien turvallisuus on sen vuoksi olennaisen tärkeää sisämarkkinoiden moitteettomalle toiminnalle.

(4) Euroopan jäsenvaltiofoorumilla on viety merkittävästi eteenpäin keskustelua ja tiedonvaihtoa hyvistä toimintapoliittisista käytännöistä, mukaan lukien periaatteiden kehittäminen eurooppalaiselle kyberkriisejä koskevalle yhteistyölle; tämän pohjalta olisi perustettava jäsenvaltioiden edustajista, komissiosta ja Euroopan unionin verkko- ja tietoturvavirastosta (ENISA) muodostuva yhteistyöryhmä tukemaan ja helpottamaan jäsenvaltioiden välistä

([1]) EUVL C 271, 19.9.2013, s. 133.

([2]) Euroopan parlamentin kanta, vahvistettu 13. maaliskuuta 2014 (ei vielä julkaistu virallisessa lehdessä), ja neuvoston ensimmäisen käsittelyn kanta, vahvistettu 17. toukokuuta 2016 (ei vielä julkaistu virallisessa lehdessä). Euroopan parlamentin kanta, vahvistettu 6. heinäkuuta 2016 (ei vielä julkaistu virallisessa lehdessä).

strategista yhteistyötä verkko- ja tietojärjestelmien turvallisuuden alalla. Jotta tämä ryhmä olisi tehokas ja kaikkien jäsenvaltioiden käytettävissä, on olennaisen tärkeää, että kaikilla jäsenvaltioilla on vähimmäisvalmiudet ja strategia, joilla varmistetaan korkeatasoinen verkko- ja tietojärjestelmien turvallisuus niiden alueella. Lisäksi turvallisuus- ja ilmoitusvaatimuksia olisi sovellettava keskeisten palvelujen tarjoajiin ja digitaalisen palvelun tarjoajiin, jotta voidaan edistää riskinhallintakulttuuria ja varmistaa raportointi vakavimmista poikkeamista.

(5) Nykyiset valmiudet eivät riitä varmistamaan korkeatasoista verkko- ja tietojärjestelmien turvallisuutta unionissa. Jäsenvaltioiden varautumisen tasot ovat hyvin erilaisia, mikä on johtanut hajanaisiin lähestymistapoihin eri puolilla unionia. Tämä johtaa kuluttajien ja yritysten epätasaiseen suojaan sekä heikentää yleistä verkko- ja tietojärjestelmien turvallisuuden tasoa unionissa. Keskeisten palvelujen tarjoajia ja digitaalisen palvelun tarjoajia koskevien yhteisten vaatimusten puuttuminen puolestaan merkitsee sitä, ettei unionin tasolla ole mahdollista luoda kokonaisvaltaista ja tuloksellista yhteistyömekanismia. Yliopistoilla ja tutkimuskeskuksilla on ratkaiseva rooli tutkimuksen, kehityksen ja innovoinnin vauhdittamisessa näillä aloilla.

(6) Tehokas reagointi verkko- ja tietojärjestelmien turvallisuuden asettamiin haasteisiin edellyttää sen vuoksi unionin tason kokonaisvaltaista lähestymistapaa, joka kattaa valmiuksien luomista ja suunnittelua koskevat yhteiset vähimmäisvaatimukset, tiedonvaihdon, yhteistyön sekä yhteiset turvallisuusvaatimukset keskeisten palvelujen tarjoajille ja digitaalisen palvelun tarjoajille. Keskeisten palvelujen tarjoajia ja digitaalisen palvelun tarjoajia ei kuitenkaan estetä panemasta täytäntöön turvallisuustoimenpiteitä, jotka ovat tiukempia kuin tässä direktiivissä säädetyt.

(7) Jotta tämä direktiivi kattaisi kaikki merkitykselliset poikkeamat ja riskit, sitä olisi sovellettava sekä keskeisten palvelujen tarjoajiin että digitaalisen palvelun tarjoajiin. Keskeisten palvelujen tarjoajia ja digitaalisen palvelun tarjoajia koskevia velvollisuuksia ei kuitenkaan olisi sovellettava Euroopan parlamentin ja neuvoston direktiivissä 2002/21/EY ([1]) tarkoitettuihin yleisiä viestintäverkkoja tai yleisesti saatavilla olevia sähköisiä viestintäpalveluja tarjoaviin yrityksiin, joihin sovelletaan mainitussa direktiivissä vahvistettuja erityisiä turvallisuutta ja eheyttä koskevia vaatimuksia, eikä niitä olisi sovellettava Euroopan parlamentin ja neuvoston asetuksessa (EU) N:o 910/2014 ([2]) tarkoitettuihin luottamuspalvelun tarjoajiin, joihin sovelletaan mainitussa asetuksessa vahvistettuja turvallisuusvaatimuksia.

(8) Tämä direktiivi ei saisi rajoittaa kunkin jäsenvaltion mahdollisuutta toteuttaa tarvittavat toimenpiteet, joilla varmistetaan sen keskeisten turvallisuusetujen suojelu, taataan yleinen järjestys ja turvallisuus sekä mahdollistetaan rikosten tutkiminen, selvittäminen ja syytteeseenpano. Euroopan unionin toiminnasta tehdyn sopimuksen 346 artiklan mukaisesti mitään jäsenvaltiota ei ole velvoitettava antamaan tietoja, joiden ilmaisemisen se katsoo olevan keskeisten turvallisuusetujensa vastaista. Tässä yhteydessä ovat merkityksellisiä neuvoston päätös 2013/488/EU ([3]) sekä salassapitosopimukset tai epäviralliset salassapitosopimukset, kuten Traffic Light Protocol -käsittelyluokitus.

(9) Tiettyjä talouden aloja säännellään jo tai voidaan säännellä tulevaisuudessa alakohtaisilla unionin säädöksillä, joihin sisältyy verkko- ja tietojärjestelmien turvallisuuteen liittyviä sääntöjä. Kun tällaisiin unionin säädöksiin sisältyy säännöksiä, joilla asetetaan verkko- ja tietojärjestelmien turvallisuutta tai poikkeamien ilmoittamisia koskevia vaatimuksia, näitä säännöksiä olisi sovellettava, jos ne sisältävät vaatimuksia, jotka ovat vaikutukseltaan vähintään vastaavia kuin tähän direktiiviin sisältyvät velvollisuudet. Jäsenvaltioiden olisi sitten sovellettava tällaisten alakohtaisten unionin säädösten säännöksiä, myös tuomioistuimen toimivaltaan liittyviä säännöksiä, eikä niiden olisi suoritettava tässä direktiivissä määriteltyjen keskeisten palvelujen tarjoajien määrittämisprosessia. Jäsenvaltioiden olisi annettava tässä yhteydessä tietoja komissiolle tällaisten erityissäännösten (*lex specialis*) soveltamisesta. Määritettäessä, vastaavatko alakohtaisiin unionin säädöksiin sisältyvät verkko- ja tietojärjestelmien turvallisuutta ja poikkeamien ilmoittamista koskevat vaatimukset tähän direktiiviin sisältyviä vaatimuksia, olisi otettava huomioon ainoastaan asiaankuuluvien unionin säädösten säännökset ja niiden soveltaminen jäsenvaltioissa.

(10) Vesiliikenteen alalla yhtiöitä, aluksia, satamarakenteita, satamia ja alusliikennepalveluja koskevat unionin säädösten mukaiset turvallisuusvaatimukset koskevat kaikkea toimintaa, mukaan lukien radio- ja televiestintäjärjestelmät, tietokonejärjestelmät ja verkot. Osaan noudatettavista pakollisista menettelyistä sisältyy kaikkien poikkeamien raportointi, joten niiden olisi katsottava olevan erityissäännöksiä (*lex specialis*), siltä osin kuin kyseiset vaatimukset ovat vähintään vastaavia kuin tämän direktiivin vastaavat säännökset.

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

([3]) Neuvoston päätös 2013/488/EU, annettu 23 päivänä syyskuuta 2013, EU:n turvallisuusluokiteltujen tietojen suojaamista koskevista turvallisuussäännöistä (EUVL L 274, 15.10.2013, s. 1).

(11) Määrittäessään vesiliikenteen alan palvelujen tarjoajia jäsenvaltioiden olisi otettava huomioon erityisesti Kansainvälisen merenkulkujärjestön kehittämät olemassa olevat ja tulevat kansainväliset säännöstöt ja suuntaviivat, jotta yksittäisiin meriliikenteen palvelujen tarjoajiin voidaan soveltaa johdonmukaista lähestymistapaa.

(12) Pankkialan ja finanssimarkkinoiden infrastruktuurien alan sääntely ja valvonta on erittäin yhdenmukaistettua unionin tasolla unionin primaari- ja sekundaarioikeuden soveltamisen sekä yhdessä Euroopan valvontaviranomaisten kanssa kehitettyjen standardien käyttämisen myötä. Näiden vaatimusten soveltaminen ja valvonta varmistetaan pankkiunionissa yhteisellä valvontamekanismilla. Niissä jäsenvaltioissa, jotka eivät ole osa pankkiunionia, tämä varmistetaan jäsenvaltioiden asiaankuuluvien pankkialan sääntelyviranomaisten avulla. Rahoitusalan sääntelyn muilla aloilla myös Euroopan finanssivalvojien järjestelmä varmistaa valvontakäytäntöjen yhdenmukaisuuden ja yhtenäisyyden korkean tason. Myös Euroopan arvopaperimarkkinaviranomaisella on suora valvontarooli tiettyjen toimijoiden eli luottoluokituslaitosten ja kauppatietorekisterien osalta.

(13) Operatiivinen riski on keskeinen osa vakavaraisuussääntelyä ja -valvontaa pankkialalla ja finanssimarkkinoiden infrastruktuurien alalla. Se kattaa kaikki toiminnot, mukaan lukien verkko- ja tietojärjestelmien turvallisuuden, eheyden ja häiriönsietokyvyn. Näitä järjestelmiä koskevat vaatimukset, jotka ovat usein tiukempia kuin tämän direktiivin nojalla säädetyt vaatimukset, on vahvistettu useissa unionin säädöksissä, mukaan lukien: säännöt oikeudesta harjoittaa luottolaitostoimintaa sekä luottolaitosten ja sijoituspalveluyritysten vakavaraisuusvalvonnasta ja säännöt luottolaitosten ja sijoituspalveluyritysten vakavaraisuusvaatimuksista, joihin sisältyy operatiivista riskiä koskevia vaatimuksia; säännöt rahoitusvälineiden markkinoista, joihin sisältyy sijoituspalveluyritysten ja säänneltyjen markkinoiden riskinarviointia koskevia vaatimuksia; säännöt OTC-johdannaisista, keskusvastapuolista ja kauppatietorekistereistä, joihin sisältyy keskusvastapuolten ja kauppatietorekisterien operatiivista riskiä koskevia vaatimuksia; ja säännöt arvopaperikaupan selvitysjärjestelmän parantamisesta unionissa sekä arvopaperikeskuksista, joihin sisältyy operatiivista riskiä koskevia vaatimuksia. Lisäksi poikkeamien ilmoittamista koskevat vaatimukset ovat osa rahoitusalan tavanomaista valvontakäytäntöä, ja ne sisältyvät usein valvontaohjeisiin. Jäsenvaltioiden olisi otettava nämä säännöt ja vaatimukset huomioon soveltaessaan erityissäännöksiä (*lex specialis*).

(14) Kuten Euroopan keskuspankki totesi 25 päivänä heinäkuuta 2014 antamassaan lausunnossa ([1]), tämä direktiivi ei vaikuta unionin oikeuden mukaiseen eurojärjestelmän harjoittamaan maksu- ja selvitysjärjestelmien yleisvalvontaan. Tällaisesta yleisvalvonnasta vastaavien viranomaisten olisi aiheellista vaihtaa kokemuksia verkko- ja tietojärjestelmien turvallisuuteen liittyvistä asioista tämän direktiivin mukaisten toimivaltaisten viranomaisten kanssa. Tämä pätee myös Euroopan keskuspankkijärjestelmän euroalueen ulkopuolisiin jäseniin, jotka harjoittavat tällaista maksu- ja selvitysjärjestelmien yleisvalvontaa kansallisten lakien ja asetusten nojalla.

(15) Verkossa toimiva markkinapaikka mahdollistaa sen, että kuluttajat ja elinkeinonharjoittajat voivat tehdä verkossa kauppa- tai palvelusopimuksia elinkeinonharjoittajien kanssa, ja se on lopullinen määräpaikka tällaisten sopimusten tekemiseksi. Sen ei pitäisi kattaa verkkopalveluja, joita käytetään vain välittäjänä kolmannen osapuolen palveluihin, joiden kautta sopimus voidaan lopulta tehdä. Sen ei pitäisi näin ollen kattaa verkkopalveluja, joissa vertaillaan eri elinkeinonharjoittajien tiettyjen tuotteiden tai palvelujen hintoja ja sen jälkeen ohjataan käyttäjä valitun elinkeinonharjoittajan palveluun tuotteen ostamiseksi. Verkossa toimivan markkinapaikan tarjoamiin tietojenkäsittelypalveluihin voivat sisältyä maksutapahtumien käsittely, tietojen yhdistäminen tai käyttäjien profilointi. Sovelluskauppojen, jotka toimivat kolmansien osapuolien tarjoamien sovellusten tai ohjelmistojen digitaalisen jakelun mahdollistavina verkkokauppoina, on katsottava olevan yhdentyyppisiä verkossa toimivia markkinapaikkoja.

(16) Verkossa toimiva hakukone antaa käyttäjälle mahdollisuuden tehdä hakuja periaatteessa kaikilta verkkosivustoilta mitä tahansa aihetta koskevan kyselyn perusteella. Se voidaan vaihtoehtoisesti kohdistaa tietynkielisille verkkosivustoille. Verkossa toimivaa hakukonetta koskevan, tässä direktiivissä säädetyn määritelmän ei olisi katettava hakutoimintoja, jotka rajoittuvat tietyn verkkosivuston sisältöön, riippumatta siitä, tarjoaako hakutoiminnon ulkoinen hakukone. Sen ei olisi liioin katettava verkkopalveluja, joissa vertaillaan eri elinkeinonharjoittajien tiettyjen tuotteiden tai palvelujen hintoja ja sen jälkeen ohjataan käyttäjä valitun elinkeinonharjoittajan palveluun tuotteen ostamiseksi.

(17) Pilvipalvelut kattavat laajan kirjon toimintoja, joita voidaan tarjota erilaisten mallien mukaisesti. Tätä direktiiviä sovellettaessa ilmaisu ”pilvipalvelut” kattaa palvelut, jotka mahdollistavat pääsyn skaalautuvaan ja mukautuvaan joukkoon jaettavissa olevia tietoteknisiä resursseja. Näihin tietoteknisiin resursseihin sisältyy verkkojen, palvelinten tai muun infrastruktuurin, tallentamisen, sovellusten ja palvelujen kaltaisia resursseja. Termi ”skaalautuva” viittaa tietoteknisiin resursseihin, joita pilvipalvelujen tarjoaja jakaa joustavasti resurssien maantieteellisestä sijainnista riippumatta kysynnän vaihtelujen käsittelemiseksi. Termiä ”mukautuva joukko” käytetään kuvailemaan niitä tietoteknisiä resursseja, joita tarjotaan ja annetaan käyttöön kysynnän mukaan, jotta käytettävissä olevia resursseja

([1]) EUVL C 352, 7.10.2014, s. 4.

voidaan lisätä ja vähentää nopeasti työtaakan mukaan. Termiä ”jaettavissa oleva” käytetään kuvailemaan niitä tietoteknisiä resursseja, joita tarjotaan useille käyttäjille, joilla on yhteinen pääsy palveluun, mutta jossa käsittely kuitenkin tapahtuu erikseen kunkin käyttäjän osalta, vaikka palvelua tarjotaan samasta sähköisestä laitteistosta.

(18) Internetin yhdysliikennepisteen (internet exchange point, IXP) tehtävänä on yhdistää verkkoja toisiinsa. IXP ei anna pääsyä verkkoon eikä toimi transit-yhteyksien tarjoajana tai välittäjänä. IXP ei liioin tarjoa muita, yhteenliittämiseen liittymättömiä palveluja, vaikka tämä ei estä sitä, että IXP tarjoaa siihen liittymättömiä palveluja. IXP:n tarkoituksena on yhdistää toisiinsa verkkoja, jotka ovat teknisesti ja organisatorisesti erillisiä. Termiä ”autonominen järjestelmä” käytetään kuvaamaan teknisesti erillistä verkkoa.

(19) Jäsenvaltioiden olisi vastattava sen määrittämisestä, mitkä toimijat täyttävät keskeisten palvelujen tarjoajan määritelmän kriteerit. Johdonmukaisen lähestymistavan varmistamiseksi kaikkien jäsenvaltioiden olisi sovellettava yhdenmukaisesti keskeisten palvelujen tarjoajan määritelmää. Tätä varten tässä direktiivissä säädetään tiettyjen toimialojen ja niiden osa-alueiden toimijoiden arvioimisesta, keskeisten palvelujen luettelon laatimisesta, toimialojen välisiä tekijöitä koskevan yhteisen luettelon tarkastelusta sen määrittämiseksi, olisiko mahdollisella poikkeamalla merkittävää haitallista vaikutusta, asiaankuuluvat jäsenvaltiot osallistavasta kuulemisprosessista tapauksissa, joissa toimijat tarjoavat palveluja useammassa kuin yhdessä jäsenvaltiossa, sekä yhteistyöryhmän tuesta määritysprosessissa. Jotta voidaan varmistaa markkinoiden mahdollisten muutosten asianmukainen huomioon ottaminen, jäsenvaltioiden olisi säännöllisesti tarkistettava määritettyjen palveluntarjoajien luettelo ja tarvittaessa saatettava se ajan tasalle. Lopuksi jäsenvaltioiden olisi toimitettava komissiolle tiedot, jotka tarvitaan sen arvioimiseksi, missä määrin tämä yhteinen menettelytapa on mahdollistanut määritelmän yhdenmukaisen soveltamisen jäsenvaltioissa.

(20) Määritettäessä keskeisten palvelujen tarjoajia jäsenvaltioiden olisi arvioitava vähintään kunkin tässä direktiivissä tarkoitetun toimialan osa-alueen osalta, mitä palveluja on pidettävä keskeisinä yhteiskunnan ja talouden kriittisten toimintojen ylläpitämiseksi ja täyttävätkö tässä direktiivissä tarkoitetuilla toimialoilla ja toimialojen osa-alueilla luetellut ja noita palveluja tarjoavat toimijat palveluntarjoajien määrittämisen kriteerit. Arvioitaessa sitä, tarjoaako toimija yhteiskunnan tai talouden kriittisten toimintojen ylläpitämisen kannalta keskeistä palvelua, on riittävää tarkastella, tarjoaako kyseinen toimija palvelua, joka sisältyy keskeisten palvelujen luetteloon. Lisäksi olisi osoitettava, että keskeisen palvelun tarjoaminen on riippuvaista verkko- ja tietojärjestelmistä. Lopuksi arvioitaessa sitä, olisiko poikkeamalla merkittävää haitallista vaikutusta palvelun tarjoamiseen, jäsenvaltioiden olisi otettava huomioon useita toimialojen välisiä tekijöitä ja tarvittaessa myös toimialakohtaisia tekijöitä.

(21) Keskeisten palvelujen tarjoajia määritettäessä sijoittautuminen jäsenvaltioon edellyttää tosiasiallista toimintaa ja kiinteää toimipaikkaa. Sijoittautumisen oikeudellisella muodolla eli sillä, onko kyseessä sivuliike tai tytäryhtiö, jolla on oikeushenkilöys, ei ole tältä osin ratkaisevaa merkitystä.

(22) On mahdollista, että tässä direktiivissä tarkoitettujen toimialojen ja niiden osa-alueiden toimijat tarjoavat sekä keskeisiä että muita kuin keskeisiä palveluja. Esimerkiksi lentoliikenteen alalla lentoasemat tarjoavat palveluja, joiden jäsenvaltio voi katsoa olevan keskeisiä, kuten kiitoratojen hallinnointia, mutta myös useita palveluja, joiden voidaan katsoa olevan muita kuin keskeisiä, kuten ostostilojen tarjoamista. Keskeisten palvelujen tarjoajiin olisi sovellettava erityisiä turvallisuusvaatimuksia ainoastaan keskeisiksi katsottujen palvelujen osalta. Palvelujen tarjoajien määrittämiseksi jäsenvaltioiden olisi näin ollen laadittava luettelo palveluista, joiden katsotaan olevan keskeisiä.

(23) Palvelujen luettelon olisi sisällettävä kaikki tietyn jäsenvaltion alueella tarjottavat palvelut, jotka täyttävät tämän direktiivin mukaiset vaatimukset. Jäsenvaltioiden olisi voitava täydentää olemassa olevaa luetteloa sisällyttämällä siihen uusia palveluja. Jäsenvaltioiden olisi käytettävä palvelujen luetteloa viitekohtana määritettäessä keskeisten palvelujen tarjoajia. Luettelon tarkoituksena on määrittää tässä direktiivissä tarkoitettujen toimialojen keskeisten palvelujen tyypit erottaen ne näin muista kuin keskeisistä toiminnoista, joista tietyn toimialan toimija saattaa olla vastuussa. Kunkin jäsenvaltion laatimaa palvelujen luetteloa käytettäisiin yhtenä keinona arvioitaessa kunkin jäsenvaltion sääntelykäytäntöä, jotta voidaan varmistaa määrittämisprosessin yleinen yhdenmukaisuustaso jäsenvaltioiden kesken.

(24) Kun toimija tarjoaa keskeistä palvelua kahdessa tai useammassa jäsenvaltiossa, näiden jäsenvaltioiden olisi käytävä keskenään kahden- tai monenvälisiä keskusteluja. Tämän kuulemisprosessin tarkoituksena on auttaa niitä arvioimaan, onko palvelujen tarjoaja kriittisessä asemassa rajat ylittävien vaikutusten suhteen, jolloin kullakin asianomaisella jäsenvaltiolla on mahdollisuus esittää näkemyksensä tarjottuihin palveluihin liittyvistä riskeistä. Asianomaisten jäsenvaltioiden olisi otettava tässä prosessissa huomioon toistensa näkemykset, ja niiden olisi voitava pyytää yhteistyöryhmän apua tältä osin.

(25) Määrittämisprosessin tuloksena jäsenvaltioiden olisi hyväksyttävä kansallisia toimenpiteitä sen määrittämiseksi, mihin toimijoihin sovelletaan verkko- ja tietojärjestelmien turvallisuutta koskevia velvollisuuksia. Tämä tulos voitaisiin saavuttaa hyväksymällä luettelo, jossa luetellaan kaikki keskeisten palvelujen tarjoajat, tai hyväksymällä kansallisia toimenpiteitä, mukaan lukien objektiiviset määrällisesti ilmaistavat kriteerit, kuten palvelujen tarjoajan tuotantomäärä tai käyttäjien määrä, joiden avulla voidaan määrittää, mihin toimijoihin sovelletaan verkko- ja tietojärjestelmien turvallisuutta koskevia velvollisuuksia. Kansallisten toimenpiteiden, riippumatta siitä, ovatko ne jo olemassa vai hyväksytäänkö ne tämän direktiivin puitteissa, olisi sisällettävä kaikki oikeudelliset toimenpiteet, hallinnolliset toimenpiteet ja toimintapolitiikat, joiden avulla voidaan määrittää keskeisten palvelujen tarjoajat tämän direktiivin mukaisesti.

(26) Osoittaakseen keskeisten palvelujen määritettyjen tarjoajien merkityksen kyseessä olevalla toimialalla jäsenvaltioiden olisi otettava huomioon näiden palveluntarjoajien lukumäärä ja koko, esimerkiksi markkinaosuuden taikka tuotettujen tai välitettyjen määrien suhteen, ilman että niille asetetaan velvollisuutta paljastaa tietoja, joista ilmenisi, mitkä ovat määritettyjä palveluntarjoajia.

(27) Sen määrittämiseksi, olisiko poikkeamalla merkittävä haitallinen vaikutus keskeisen palvelun tarjoamiseen, jäsenvaltioiden olisi otettava huomioon useita eri tekijöitä, kuten niiden käyttäjien lukumäärä, jotka ovat riippuvaisia kyseisestä palvelusta henkilökohtaisten tai ammatillisten tarkoitusten vuoksi. Kyseisen palvelun käyttö voi olla suoraa, epäsuoraa tai välityksen kautta tapahtuvaa. Arvioidessaan vaikutusta, joka poikkeamalla voisi vakavuutensa ja kestonsa perusteella olla talouden ja yhteiskunnan toimintoihin tai yleiseen turvallisuuteen, jäsenvaltioiden olisi arvioitava myös aika, joka todennäköisesti kuluu, ennen kuin palvelun keskeytymisellä alkaisi olla kielteinen vaikutus.

(28) Toimialojen välisten tekijöiden lisäksi olisi otettava huomioon myös toimialakohtaisia tekijöitä määritettäessä sitä, olisiko poikkeamalla merkittävä haitallinen vaikutus keskeisen palvelun tarjoamiseen. Energiantoimittajien osalta tällaisiin tekijöihin voisi sisältyä tuotetun kansallisen energian määrä tai osuus siitä; öljyntoimittajien osalta päiväkohtainen määrä; lentoliikenteen, mukaan lukien lentoasemat ja lentoliikenteen harjoittajat, sekä rautatieliikenteen ja merisatamien osalta osuus kansallisesta liikennemäärästä ja matkustajien tai rahtikuljetusten lukumäärä vuodessa; pankkialan tai finanssimarkkinoiden infrastruktuurien osalta niiden järjestelmäkohtainen merkitys perustuen kokonaisvaroihin tai näiden kokonaisvarojen ja bruttokansantuotteen suhteeseen; terveydenhuoltoalan osalta palvelun tarjoajan hoidossa olevien potilaiden lukumäärä vuodessa; veden tuotannon, käsittelyn ja toimittamisen osalta vesimäärä sekä käyttäjien lukumäärä ja tyypit, mukaan lukien esimerkiksi sairaalat, julkiset palveluorganisaatiot tai henkilöt, sekä vaihtoehtoisten veden lähteiden olemassaolo saman maantieteellisen alueen kattamiseksi.

(29) Korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden saavuttamiseksi ja ylläpitämiseksi kullakin jäsenvaltiolla olisi oltava verkko- ja tietojärjestelmien turvallisuutta koskeva kansallinen strategia, jossa määritellään strategiset tavoitteet ja toteutettavat konkreettiset politiikkatoimet.

(30) Koska kansallisissa hallintorakenteissa on eroja ja jotta taataan jo olemassa olevien toimialakohtaisten järjestelyjen tai unionin valvonta- ja sääntelyelinten säilyttäminen ja vältetään päällekkäisyyksiä, jäsenvaltioiden olisi voitava nimetä useampi kuin yksi kansallinen toimivaltainen viranomainen, joka vastaa keskeisten palvelujen tarjoajien ja digitaalisen palvelun tarjoajien verkko- ja tietojärjestelmien turvallisuuteen liittyvien tehtävien hoitamisesta tämän direktiivin mukaisesti.

(31) Rajat ylittävän yhteistyön ja viestinnän helpottamiseksi ja jotta tämä direktiivi voitaisiin panna tehokkaasti täytäntöön, on välttämätöntä, että kukin jäsenvaltio nimeää kansallisen keskitetyn yhteyspisteen, joka vastaa verkko- ja tietojärjestelmien turvallisuuteen liittyvien asioiden koordinoinnista sekä rajat ylittävästä yhteistyöstä unionin tasolla, sanotun kuitenkaan vaikuttamatta toimialakohtaisiin sääntelyjärjestelyihin. Toimivaltaisilla viranomaisilla ja keskitetyillä yhteyspisteillä olisi oltava riittävät tekniset ja taloudelliset resurssit sekä henkilöresurssit, jotta ne voivat toteuttaa niille osoitetut tehtävät tehokkaasti ja tuloksekkaasti ja siten saavuttaa tämän direktiivin tavoitteet. Koska tällä direktiivillä pyritään parantamaan sisämarkkinoiden toimintaa luomalla luottamusta ja luotettavuutta, jäsenvaltioiden elinten on voitava tehdä tehokasta yhteistyötä talouden toimijoiden kanssa ja niiden rakenteen on oltava tähän soveltuva.

(32) Toimivaltaisten viranomaisten tai tietoturvaloukkauksiin reagoivien ja niitä tutkivien yksiköiden (computer security incident response teams, jäljempänä 'CSIRT-toimijat') olisi saatava ilmoitukset poikkeamista. Keskitettyjen yhteyspisteiden ei pitäisi saada suoraan ilmoituksia poikkeamista, elleivät ne toimi myös toimivaltaisena viranomaisena tai CSIRT-toimijana. Toimivaltaisen viranomaisen tai CSIRT-toimijan olisi kuitenkin voitava antaa keskitetylle yhteyspisteelle tehtäväksi toimittaa poikkeamia koskevia ilmoituksia muiden asiaan liittyvien jäsenvaltioiden keskitetyille yhteyspisteille.

(33) Jotta voidaan varmistaa toimiva tiedottaminen jäsenvaltioille ja komissiolle, keskitetyn yhteyspisteen olisi toimitettava yhteistyöryhmälle tiivistelmäraportti, joka olisi muutettava nimettömään muotoon ilmoitusten luottamuksellisuuden sekä keskeisten palvelujen tarjoajien ja digitaalisen palvelun tarjoajien identiteetin suojaamiseksi, koska ilmoittavien toimijoiden identiteettiä koskevat tiedot eivät ole tarpeen parhaiden käytäntöjen vaihtamiseksi yhteistyöryhmässä. Tiivistelmäraportin olisi sisällettävä tiedot vastaanotettujen ilmoitusten lukumäärästä sekä maininta ilmoitettujen poikkeamien luonteesta, kuten turvallisuusloukkausten tyypit, niiden vakavuus tai niiden kesto.

(34) Jäsenvaltioilla olisi oltava käytössään riittävät sekä tekniset että organisatoriset valmiudet, jotta voidaan ehkäistä ja havaita verkko- ja tietojärjestelmien poikkeamia ja riskejä, reagoida niihin ja lieventää niiden vaikutuksia. Jäsenvaltioiden olisi näin ollen varmistettava, että niillä on hyvin toimivat ja olennaiset vaatimukset täyttävät CSIRT-toimijat, toiselta nimeltään CERT-toimijat (computer emergency response teams eli tietoturvaloukkauksiin ja niiden ennaltaehkäisyyn keskittyvät ryhmät), jotta voidaan taata toimivat ja yhteensopivat valmiudet poikkeamien ja riskien varalta sekä varmistaa tehokas yhteistyö unionin tasolla. Jotta kaikentyyppiset keskeisten palvelujen tarjoajat ja digitaalisen palvelun tarjoajat voisivat hyötyä tällaisista valmiuksista ja yhteistyöstä, jäsenvaltioiden olisi varmistettava, että kaikki tyypit kuuluvat nimetyn CSIRT-toimijan piiriin. Kun otetaan huomioon kyberturvallisuutta koskevan kansainvälisen yhteistyön tärkeys, CSIRT-toimijoiden olisi voitava osallistua kansainvälisiin yhteistyöverkostoihin tällä direktiivillä perustetun CSIRT-verkoston lisäksi.

(35) Koska useimmat verkko- ja tietojärjestelmät ovat yksityisten ylläpitämiä, julkisen ja yksityisen sektorin välinen yhteistyö on olennaisen tärkeää. Keskeisten palvelujen tarjoajia ja digitaalisen palvelun tarjoajia olisi kannustettava kehittämään omia epävirallisia yhteistyömekanismejaan verkko- ja tietoturvajärjestelmien turvallisuuden varmistamiseksi. Yhteistyöryhmän olisi tarvittaessa voitava kutsua asiaankuuluvia sidosryhmiä keskusteluihin. Jotta voidaan tehokkaasti kannustaa tiedon ja parhaiden käytäntöjen jakamiseen, on välttämätöntä varmistaa, etteivät tällaisiin keskusteluihin osallistuvat keskeisten palvelujen tarjoajat ja digitaalisen palvelun tarjoajat joudu yhteistyönsä vuoksi epäsuotuisaan asemaan.

(36) ENISAn olisi avustettava jäsenvaltioita ja komissiota tarjoamalla asiantuntemusta ja neuvontaa sekä helpottamalla parhaiden käytäntöjen vaihtamista. Erityisesti tätä direktiiviä sovellettaessa komission olisi kuultava ja jäsenvaltioiden olisi voitava kuulla ENISAa. Jäsenvaltioiden valmiuksien ja tietämyksen kehittämiseksi yhteistyöryhmän olisi myös toimittava välineenä, jonka avulla vaihdetaan parhaita käytäntöjä, keskustellaan jäsenvaltioiden toiminta- ja varautumiskyvystä sekä vapaaehtoisuuteen perustuen avustetaan sen jäseniä verkko- ja tietojärjestelmien turvallisuutta koskevien kansallisten strategioiden arvioimisessa, valmiuksien kehittämisessä sekä verkko- ja tietoturvajärjestelmien turvallisuutta koskevien harjoitusten arvioinnissa.

(37) Jäsenvaltioiden olisi voitava tarvittaessa käyttää tai mukauttaa olemassa olevia organisaatiorakenteita tai strategioita tätä direktiiviä soveltaessaan.

(38) Yhteistyöryhmän tehtävät ja ENISAn tehtävät ovat toisistaan riippuvaisia ja toisiaan täydentäviä. ENISAn olisi yleisesti avustettava yhteistyöryhmää sen tehtävien suorittamisessa Euroopan parlamentin ja neuvoston asetuksessa (EU) N:o 526/2013 ([1]) säädetyn ENISAn tavoitteen mukaisesti, joka on auttaa unionin toimielimiä, elimiä, laitoksia ja virastoja sekä jäsenvaltioita panemaan täytäntöön toimintapolitiikat, joita tarvitaan nykyisissä ja tulevissa unionin säädöksissä asetettujen, verkko- ja tietojärjestelmien turvallisuuteen liittyvien lakisääteisten ja sääntelyllisten vaatimusten täyttämiseksi. ENISAn olisi erityisesti annettava apua aloilla, jotka vastaavat sen omia tehtäviä, jotka vahvistetaan asetuksessa (EU) N:o 526/2013 ja joita ovat verkko- ja tietojärjestelmien turvallisuutta koskevien strategioiden analysointi, verkko- ja tietojärjestelmien turvallisuutta koskevien unionin harjoitusten järjestämisen ja toteutuksen tukeminen sekä valistusta ja koulutusta koskevien tietojen ja parhaiden käytäntöjen vaihtaminen. ENISAn olisi osallistuttava myös niiden suuntaviivojen kehittämiseen, jotka koskevat toimiala-kohtaisia kriteerejä poikkeaman vaikutuksen merkityksen määrittämiseksi.

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

(39) Verkko- ja tietojärjestelmien korkeatasoisen turvallisuuden edistämiseksi yhteistyöryhmän olisi tarvittaessa tehtävä yhteistyötä asiaankuuluvien unionin toimielinten, elinten, laitosten ja virastojen kanssa vaihtaakseen taitotietoa ja parhaita käytäntöjä sekä antaakseen neuvoja verkko- ja tietojärjestelmien turvallisuuteen liittyvistä seikoista, joilla voi olla vaikutusta niiden työskentelyyn, noudattaen samalla jakelultaan rajoitettujen tietojen vaihtamista koskevia olemassa olevia järjestelyjä. Tehdessään lainvalvontaviranomaisten kanssa yhteistyötä verkko- ja tietojärjestelmien turvallisuuteen liittyvissä kysymyksissä, joilla voi olla vaikutusta niiden työskentelyyn, yhteistyöryhmän olisi käytettävä olemassa olevia tiedonvaihtokanavia ja vakiintuneita verkostoja.

(40) Poikkeamia koskevat tiedot ovat yhä arvokkaampia suurelle yleisölle ja yrityksille, erityisesti pienille ja keskisuurille yrityksille. Joissain tapauksissa tällaisia tietoja esitetään jo verkkosivustoilla kansallisella tasolla tietyn maan kielellä ja keskittyen pääasiassa poikkeamiin ja tapahtumiin, joilla on kansallista merkitystä. Koska yritysten toiminta on yhä useammin rajat ylittävää ja kansalaiset käyttävät verkkopalveluja, poikkeamia koskevat tiedot olisi annettava yhdistellyssä muodossa unionin tasolla. CSIRT-verkoston sihteeristöä kannustetaan ylläpitämään verkkosivustoa tai olemassa olevalla verkkosivustolla erityistä sivua, jossa yleisön käyttöön annetaan unionissa tapahtuneita merkittäviä poikkeamia koskevaa yleistä tietoa, jossa kiinnitetään erityistä huomiota yritysten etuihin ja tarpeisiin. CSIRT-verkostoon osallistuvia CSIRT-toimijoita kannustetaan tarjoamaan tietoja julkaistavaksi tällä verkkosivustolla vapaaehtoisuuteen perustuen sisällyttämättä mukaan luottamuksellisia tai arkaluonteisia tietoja.

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

(42) Harjoitukset, joissa simuloidaan reaaliaikaisia poikkeamaskenaarioita, ovat olennaisen tärkeitä jäsenvaltioiden varautumiskyvyn ja yhteistyön testaamiseksi verkko- ja tietojärjestelmien turvallisuuden osalta. CyberEurope-harjoitussykli, jota ENISA koordinoi jäsenvaltioiden kanssa, on hyödyllinen väline testaukseen ja suositusten laatimiseen siitä, miten poikkeamien käsittelyä unionin tasolla olisi ajan kuluessa parannettava. Ottaen huomioon, että jäsenvaltioilla ei ole tällä hetkellä mitään velvollisuutta suunnitella harjoituksia tai osallistua niihin, CSIRT-verkoston perustamisen tämän direktiivin nojalla olisi mahdollistettava se, että jäsenvaltiot voivat osallistua harjoituksiin täsmällisen suunnittelun ja strategisten valintojen pohjalta. Tämän direktiivin nojalla perustetun yhteistyöryhmän olisi keskusteltava harjoituksia koskevista strategisista päätöksistä, jotka koskevat erityisesti, vaikkakaan eivät yksinomaan, harjoitusten säännöllisyyttä ja skenaarioiden suunnittelua. ENISAn olisi toimeksiantonsa mukaisesti tuettava unionin laajuisten harjoitusten järjestämistä ja toteuttamista tarjoamalla asiantuntemustaan ja neuvojaan yhteistyöryhmälle ja CSIRT-verkostolle.

(43) Verkko- ja tietojärjestelmiin vaikuttavien turvallisuusongelmien maailmanlaajuisen luonteen vuoksi tarvitaan tiiviimpää kansainvälistä yhteistyötä, jolla voidaan parantaa turvallisuusstandardeja ja tiedonvaihtoa sekä edistää yhteistä maailmanlaajuista lähestymistapaa turvallisuuskysymyksiin.

(44) Vastuu verkko- ja tietojärjestelmien turvallisuuden varmistamisesta lankeaa suurelta osin keskeisten palvelujen tarjoajille ja digitaalisen palvelun tarjoajille. Riskinhallintakulttuuria, johon sisältyy riskinarviointi ja riskeihin suhteutettujen turvallisuustoimenpiteiden toteuttaminen, olisi edistettävä ja kehitettävä asianmukaisten sääntely-vaatimusten ja toimialojen vapaaehtoisten käytäntöjen kautta. Luotettavien ja tasavertaisten toimintaedellytysten luominen on myös olennaista yhteistyöryhmän ja CSIRT-verkoston tehokkaan toiminnan kannalta, jotta voidaan varmistaa tuloksellinen yhteistyö kaikkien jäsenvaltioiden taholta.

(45) Tätä direktiiviä sovelletaan ainoastaan niihin julkishallintoihin, jotka on määritetty keskeisten palvelujen tarjoajiksi. Jäsenvaltioiden tehtävänä on näin ollen varmistaa niiden julkishallintojen verkko- ja tietojärjestelmien turvallisuus, jotka eivät kuulu tämän direktiivin soveltamisalaan.

(46) Riskinhallintatoimenpiteisiin sisältyvät toimenpiteet, joilla tunnistetaan mahdolliset poikkeamien riskit, estetään, havaitaan ja käsitellään poikkeamat ja lievennetään niiden vaikutusta. Verkko- ja tietojärjestelmien turvallisuus käsittää tallennettujen, siirrettyjen ja käsiteltyjen tietojen turvallisuuden.

(47) Toimivaltaisten viranomaisten olisi edelleen voitava hyväksyä kansallisia suuntaviivoja olosuhteista, joissa keskeisten palvelujen tarjoajien edellytetään ilmoittavan poikkeamista.

(48) Monet unionin yritykset ovat riippuvaisia digitaalisen palvelun tarjoajista palvelujensa tarjoamiseksi. Koska jotkin digitaaliset palvelut voivat olla merkittävä resurssi käyttäjilleen, keskeisten palvelujen tarjoajat mukaan lukien, ja koska tällaisilla käyttäjillä ei kenties aina ole käytettävissään vaihtoehtoja, tätä direktiiviä olisi sovellettava myös tällaisten palvelujen tarjoajiin. Tässä direktiivissä tarkoitettujen digitaalisten palvelujen tyyppien turvallisuus, jatkuvuus ja luotettavuus ovat olennaisen tärkeitä useiden yritysten moitteettomalle toiminnalle. Tällaisen digitaalisen palvelun häiriö voisi estää muiden siitä riippuvaisten palvelujen tarjoamisen, ja sillä voisi näin olla vaikutus keskeisiin talouden ja yhteiskunnan toimintoihin unionissa. Tällaiset digitaaliset palvelut saattavat siis olla ratkaisevan tärkeitä niistä riippuvaisten yritysten moitteettomalle toiminnalle sekä tällaisten yritysten osallistumiselle sisämarkkinoihin ja rajat ylittävään kauppaan unionin alueella. Tämän direktiivin soveltamisalaan kuuluvia digitaalisen palvelun tarjoajia ovat ne, joiden katsotaan tarjoavan digitaalisia palveluja, joista monet unionin yritykset ovat lisääntyvässä määrin riippuvaisia.

(49) Digitaalisen palvelun tarjoajien olisi varmistettava turvallisuuden taso, joka on oikeassa suhteessa niiden tarjoamien digitaalisten palvelujen turvallisuuteen kohdistuvan riskin suuruuteen, ottaen huomioon niiden palvelujen merkitys muiden yritysten toiminnalle unionissa. Käytännössä riskin suuruus on keskeisten palvelujen tarjoajille korkeampi kuin digitaalisen palvelun tarjoajille, koska keskeiset palvelut ovat usein olennaisia yhteiskunnan ja talouden kriittisten toimintojen ylläpitämiseksi. Näin ollen digitaalisen palvelun tarjoajia koskevien turvallisuusvaatimusten olisi oltava löyhempiä. Digitaalisen palvelun tarjoajilla olisi oltava vapaus toteuttaa toimenpiteet, jotka ne katsovat aiheellisiksi verkko- ja tietojärjestelmiensä turvallisuuteen kohdistuvien riskien hallitsemiseksi. Rajat ylittävän luonteensa vuoksi digitaalisen palvelun tarjoajiin olisi sovellettava yhdenmukaistetumpaa lähestymistapaa unionin tasolla. Tällaisten toimenpiteiden määrittämistä ja täytäntöönpanoa olisi helpotettava täytäntöönpanosäädöksillä.

(50) Laitteiden valmistajat ja ohjelmistojen kehittäjät eivät ole keskeisten palvelujen tarjoajia eivätkä digitaalisen palvelun tarjoajia, mutta niiden tuotteet lisäävät verkko- ja tietojärjestelmien turvallisuutta. Niillä on tämän vuoksi merkittävä rooli sen mahdollistamisessa, että keskeisten palvelujen tarjoajat ja digitaalisen palvelun tarjoajat voivat turvata verkko- ja tietojärjestelmänsä. Tällaisiin laite- ja ohjelmistotuotteisiin sovelletaan jo tuotevastuuta koskevia olemassa olevia sääntöjä.

(51) Keskeisten palvelujen tarjoajille ja digitaalisen palvelun tarjoajille määrättävät tekniset ja organisatoriset toimenpiteet eivät saisi edellyttää jonkin tietyn kaupallisen tieto- ja viestintäteknologiatuotteen suunnittelua, kehittämistä tai valmistamista tietyllä tavalla.

(52) Keskeisten palvelujen tarjoajien ja digitaalisen palvelun tarjoajien olisi varmistettava käyttämiensä verkko- ja tietojärjestelmien turvallisuus. Näitä ovat ensisijaisesti yksityiset verkko- ja tietojärjestelmät, joita hallinnoi niiden oma tietotekninen henkilöstö tai joiden tietoturvahallinto on ulkoistettu. Turvallisuus- ja ilmoitusvaatimuksia olisi sovellettava asiaankuuluviin keskeisten palvelujen tarjoajiin ja digitaalisen palvelun tarjoajiin riippumatta siitä, huolehtivatko ne verkko- ja tietojärjestelmiensä ylläpidosta sisäisesti vai ulkoistavatko ne sen.

(53) Jotta keskeisten palvelujen tarjoajille ja digitaalisen palvelun tarjoajille ei aiheutuisi suhteetonta taloudellista ja hallinnollista rasitetta, vaatimusten olisi oltava oikeassa suhteessa kulloisenkin verkko- ja tietojärjestelmän aiheuttamaan riskiin ottaen huomioon tällaisiin toimenpiteisiin käytettävä uusin tekniikka. Kun kyse on digitaalisen palvelun tarjoajista, näitä vaatimuksia ei olisi sovellettava mikroyrityksiin ja pieniin yrityksiin.

(54) Kun jäsenvaltioiden julkishallinnot käyttävät digitaalisen palvelun tarjoajien tarjoamia palveluja, erityisesti pilvipalveluja, ne saattavat haluta edellyttää tällaisten palvelujen tarjoajilta ylimääräisiä turvallisuustoimenpiteitä niiden toimenpiteiden lisäksi, joita digitaalisen palvelun tarjoajat tavanomaisesti tarjoaisivat tämän direktiivin vaatimusten mukaisesti. Niiden olisi voitava tehdä niin sopimusvelvoitteita käyttäen.

(55) Tässä direktiivissä vahvistetut verkossa toimivien markkinapaikkojen, verkossa toimivien hakukoneiden ja pilvipalvelujen määritelmät on tarkoitettu nimenomaisesti tätä direktiiviä varten, eivätkä ne rajoita muiden välineiden soveltamista.

(56) Tämän direktiivin ei olisi estettävä jäsenvaltioita hyväksymästä kansallisia toimenpiteitä, joilla vaaditaan julkisen sektorin elimiä varmistamaan erityiset turvallisuusvaatimukset, kun ne tekevät hankintasopimuksia pilvipalveluista. Tällaisia kansallisia toimenpiteitä olisi sovellettava kyseiseen julkisen sektorin elimeen eikä pilvipalvelujen tarjoajaan.

(57) Koska keskeisten palvelujen tarjoajien ja digitaalisen palvelun tarjoajien välillä on perustavanlaatuisia eroja, kun otetaan huomioon erityisesti edellisten suora yhteys fyysiseen infrastruktuuriin ja jälkimmäisten rajat ylittävä luonne, tässä direktiivissä olisi sovellettava eriytettyä lähestymistapaa näihin kahteen toimijaryhmään liittyvään yhdenmukaistamisen tasoon. Keskeisten palvelujen tarjoajien osalta jäsenvaltioiden olisi voitava määrittää asiaankuuluvat palvelujen tarjoajat ja määrätä vaatimuksia, jotka ovat tiukempia kuin tässä direktiivissä säädetyt. Jäsenvaltioiden ei olisi määritettävä digitaalisen palvelun tarjoajia, koska tätä direktiiviä olisi sovellettava kaikkiin sen soveltamisalaan kuuluviin digitaalisen palvelun tarjoajiin. Lisäksi tällä direktiivillä ja sen nojalla hyväksytyillä täytäntöönpanosäädöksillä olisi varmistettava digitaalisen palvelun tarjoajia koskeva korkea yhdenmukaistamisen taso turvallisuus- ja ilmoitusvaatimusten osalta. Tämän olisi mahdollistettava digitaalisen palvelun tarjoajien yhdenmukainen kohtelu koko unionissa tavalla, joka on oikeasuhteinen niiden luonteeseen ja niihin mahdollisesti kohdistuvan riskin suuruuteen nähden.

(58) Tämän direktiivin ei olisi estettävä jäsenvaltioita asettamasta turvallisuus- ja ilmoitusvaatimuksia toimijoille, jotka eivät ole tämän direktiivin soveltamisalaan kuuluvia digitaalisen palvelun tarjoajia, sanotun kuitenkaan rajoittamatta unionin oikeuden mukaisia jäsenvaltioiden velvollisuuksia.

(59) Toimivaltaisten viranomaisten olisi kiinnitettävä asianmukaista huomiota epävirallisten ja luotettavien tiedonjakokanavien säilyttämiseen. Toimivaltaisille viranomaisille raportoitujen poikkeamien julkistamisessa olisi otettava asianmukaisesti ja tasapainoisesti huomioon yleisön yleinen etu saada tietoa uhista sekä toisaalta poikkeamista raportoivien keskeisten palvelujen tarjoajien ja digitaalisen palvelun tarjoajien mahdollinen maineen vahingoittuminen ja niille mahdollisesti koituva taloudellinen vahinko. Ilmoitusvelvollisuuksien täytäntöönpanossa toimivaltaisten viranomaisten ja CSIRT-toimijoiden olisi kiinnitettävä erityistä huomiota tarpeeseen pitää tuotteiden haavoittuvuutta koskevat tiedot tiukasti luottamuksellisina ennen asiaankuuluvien turvallisuuspäivitysten julkistamista.

(60) Digitaalisen palvelun tarjoajiin olisi sovellettava kevyitä ja reaktiivisia jälkikäteen toteutettavia valvontatoimia, jotka ovat perusteltavissa niiden palvelujen ja toiminnan luonteella. Asianomaisen toimivaltaisen viranomaisen olisi näin ollen ryhdyttävä toimiin ainoastaan silloin, kun sille esitetään näyttöä esimerkiksi digitaalisen palvelun tarjoajan itsensä, toisen toimivaltaisen viranomaisen, mukaan lukien toisen jäsenvaltion toimivaltainen viranomainen, tai palvelun käyttäjän toimesta siitä, että digitaalisen palvelun tarjoaja ei noudata tämän direktiivin vaatimuksia, etenkin poikkeaman jo tapahduttua. Toimivaltaisella viranomaisella ei siis pitäisi olla yleistä velvoitetta valvoa digitaalisen palvelun tarjoajia.

(61) Toimivaltaisilla viranomaisilla olisi oltava tarvittavat keinot suorittaa tehtävänsä, mukaan lukien toimivalta saada riittävät tiedot arvioidakseen verkko- ja tietojärjestelmien turvallisuuden tason.

(62) Poikkeamat saattavat olla seurausta rikollisesta toiminnasta, jonka torjumista, tutkimista ja syytteeseenpanoa tuetaan keskeisten palvelujen tarjoajien, digitaalisen palvelun tarjoajien, toimivaltaisten viranomaisten ja lainvalvontaviranomaisten välisellä koordinoinnilla ja yhteistyöllä. Jos epäillään, että poikkeama liittyy unionin tai kansallisen oikeuden mukaiseen vakavaan rikolliseen toimintaan, jäsenvaltioiden olisi kannustettava keskeisten palvelujen tarjoajia ja digitaalisen palvelun tarjoajia raportoimaan asiaankuuluville lainvalvontaviranomaisille poikkeamista, joiden epäillään olevan vakavaan rikollisuuteen liittyviä. On toivottavaa, että Euroopan verkkorikostorjuntakeskus (EC3) ja ENISA helpottavat tarvittaessa eri jäsenvaltioiden toimivaltaisten viranomaisten ja lainvalvontaviranomaisten välistä koordinointia.

(63) Poikkeamat vaarantavat monissa tapauksissa henkilötietoja. Toimivaltaisten viranomaisten ja tietosuojaviranomaisten olisi tässä yhteydessä tehtävä yhteistyötä ja vaihdettava tietoja kaikista asiaankuuluvista seikoista, jotta voidaan puuttua poikkeamista johtuviin henkilötietojen tietoturvaloukkauksiin.

(64) Digitaalisen palvelun tarjoajia koskeva lainkäyttövalta olisi annettava sille jäsenvaltiolle, jossa asianomaisella digitaalisen palvelun tarjoajalla on pääasiallinen toimipaikkansa unionissa, joka periaatteessa vastaa paikkaa, jossa palvelun tarjoajalla on kotipaikkansa unionissa. Sijoittautuminen edellyttää tosiasiallista toimintaa ja kiinteää toimipaikkaa. Sijoittautumisen oikeudellisella muodolla eli sillä, onko kyseessä sivuliike tai tytäryhtiö, jolla on oikeushenkilöys, ei ole tältä osin ratkaisevaa merkitystä. Tämän kriteerin ei pitäisi olla riippuvainen siitä,

sijaitsevatko verkko- ja tietojärjestelmät fyysisesti tietyssä paikassa; tällaisten järjestelmien olemassaolo ja käyttö eivät itsessään muodosta tällaista pääasiallista toimipaikkaa, eivätkä ne näin ollen ole kriteerejä pääasiallisen toimipaikan määrittämiseksi.

(65) Jos digitaalisen palvelun tarjoaja, joka ei ole sijoittautunut unioniin, tarjoaa palveluja unionissa, sen olisi nimettävä edustaja. Jotta voidaan määrittää, tarjoaako tällainen digitaalisen palvelun tarjoaja palveluja unionissa, olisi varmistettava, onko ilmeistä, että digitaalisen palvelun tarjoaja aikoo tarjota palveluja henkilöille yhdessä tai useammassa jäsenvaltiossa. Pelkkä digitaalisen palvelun tarjoajan tai välittäjän verkkosivuston tai sähköpostiosoitteen ja muiden yhteystietojen saatavuus unionissa taikka se, että käytetään siinä kolmannessa maassa, johon digitaalisen palvelun tarjoaja on sijoittautunut, yleisesti käytettävää kieltä, ei riitä tällaisen aikomuksen varmistamiseksi. Sellaiset seikat, kuten yhdessä tai useammassa jäsenvaltiossa yleisesti käytettävän kielen tai rahayksikön käyttö ja mahdollisuus tilata palveluja kyseisellä muulla kielellä tai maininta unionissa olevista asiakkaista tai käyttäjistä, voivat kuitenkin osoittaa olevan ilmeistä, että digitaalisen palvelun tarjoaja aikoo tarjota palveluja unionissa. Edustajan olisi toimittava digitaalisen palvelun tarjoajan puolesta, ja toimivaltaisten viranomaisten tai CSIRT-toimijoiden olisi voitava ottaa yhteyttä edustajaan. Edustaja olisi nimenomaisesti nimettävä digitaalisen palvelun tarjoajan antamalla kirjallisella valtuutuksella hoitamaan tämän puolesta tämän direktiivin mukaiset velvollisuudet, mukaan lukien poikkeamista raportointi.

(66) Turvallisuusvaatimusten standardointi tapahtuu markkinavetoisesti. Turvallisuusstandardien johdonmukaisen soveltamisen varmistamiseksi jäsenvaltioiden olisi edistettävä tiettyjen standardien noudattamista tai standardienmukaisuutta, jotta voidaan varmistaa verkko- ja tietojärjestelmien turvallisuuden korkea taso unionissa. ENISAn olisi avustettava jäsenvaltioita neuvoin ja suuntaviivoin. Tätä varten voi olla hyödyllistä laatia yhdenmukaistettuja standardeja, mikä olisi tehtävä Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 1025/2012 ([1]) mukaisesti.

(67) Tämän direktiivin soveltamisalaan kuulumattomat toimijat voivat havaita poikkeamia, joilla on merkittävä vaikutus niiden tarjoamiin palveluihin. Kun tällaiset toimijat katsovat, että on yleisen edun mukaista ilmoittaa tällaisten poikkeamien esiintymisestä, niiden olisi voitava tehdä niin vapaaehtoisesti. Toimivaltaisen viranomaisen tai CSIRT-toimijan olisi käsiteltävä tällaiset ilmoitukset, jos tällainen käsittely ei muodosta kohtuutonta tai aiheetonta rasitetta kyseessä oleville jäsenvaltioille.

(68) Jotta voidaan varmistaa tämän direktiivin yhdenmukainen täytäntöönpano, komissiolle olisi siirrettävä täytäntöönpanovaltaa vahvistaa yhteistyöryhmän toimintaa varten tarvittavat menettelytapajärjestelyt sekä digitaalisen palvelun tarjoajiin sovellettavat turvallisuus- ja ilmoitusvaatimukset. Tätä valtaa olisi käytettävä Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 182/2011 ([2]) mukaisesti. Hyväksyessään yhteistyöryhmän toimintaa varten tarvittavia menettelytapajärjestelyjä koskevia täytäntöönpanosäädöksiä komission olisi otettava mahdollisimman tarkasti huomioon ENISAn lausunto.

(69) Kun komissio hyväksyy täytäntöönpanosäädöksiä digitaalisen palvelun tarjoajia koskevista turvallisuusvaatimuksista, sen olisi otettava mahdollisimman tarkasti huomioon ENISAn lausunto sekä kuultava asianomaisia sidosryhmiä. Lisäksi komissiota kannustetaan ottamaan huomioon seuraavat esimerkit: järjestelmien ja tilojen turvallisuuden osalta: fyysinen turvallisuus ja ympäristön turvallisuus, toimitusvarmuus, verkko- ja tietojärjestelmiin pääsyn valvonta sekä verkko- ja tietojärjestelmien eheys; poikkeamien käsittelyn osalta: poikkeamien käsittelymenettelyt, poikkeamien havaitsemisvalmius, poikkeamista raportoiminen ja tiedottaminen; liiketoiminnan jatkuvuuden hallinnan osalta: palvelun jatkuvuutta koskeva strategia ja varautumissuunnitelmat, palautumisvalmiudet; ja seurannan, tarkastusten ja testausten osalta: seuranta- ja lokinpitomenettelyt, varautumissuunnitelmien läpiviennit, verkko- ja tietojärjestelmien testaus, turvallisuusarvioinnit ja vaatimustenmukaisuuden seuranta.

(70) Tätä direktiiviä täytäntöönpantaessa komission olisi pidettävä tarpeen mukaan yhteyttä asiaankuuluviin toimialakohtaisiin komiteoihin ja asiaankuuluviin elimiin, jotka on perustettu unionin tasolla tämän direktiivin soveltamisalaan kuuluvilla aloilla.

([1]) 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).

([2]) 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).

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

(72) Riskejä ja poikkeamia koskevien tietojen jakaminen yhteistyöryhmässä ja CSIRT-verkostossa sekä poikkeamista kansallisille toimivaltaisille viranomaisille tai CSIRT-toimijoille ilmoittamista koskevien vaatimusten noudattaminen saattaa edellyttää henkilötietojen käsittelyä. Tällaisessa käsittelyssä olisi noudatettava Euroopan parlamentin ja neuvoston direktiiviä 95/46/EY ([1]) sekä Euroopan parlamentin ja neuvoston asetusta (EY) N:o 45/2001 ([2]). Tätä direktiiviä sovellettaessa olisi soveltuvin osin sovellettava Euroopan parlamentin ja neuvoston asetusta (EY) N:o 1049/2001 ([3]).

(73) Euroopan tietosuojavaltuutettua kuultiin asetuksen (EY) N:o 45/2001 28 artiklan 2 kohdan mukaisesti, ja hän antoi lausunnon 14 päivänä kesäkuuta 2013 ([4]).

(74) Jäsenvaltiot eivät voi riittävällä tavalla saavuttaa tämän direktiivin tavoitetta eli yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden saavuttamista unionissa, vaan se voidaan toiminnan vaikutusten vuoksi saavuttaa paremmin unionin tasolla. Sen vuoksi unioni voi toteuttaa toimenpiteitä Euroopan unionista tehdyn sopimuksen 5 artiklassa vahvistetun toissijaisuusperiaatteen mukaisesti. Mainitussa artiklassa vahvistetun suhteellisuusperiaatteen mukaisesti tässä direktiivissä ei ylitetä sitä, mikä on tarpeen tämän tavoitteen saavuttamiseksi.

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

OVAT HYVÄKSYNEET TÄMÄN DIREKTIIVIN:

I LUKU

YLEISET SÄÄNNÖKSET

1 artikla

Kohde ja soveltamisala

1. Tässä direktiivissä säädetään toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden saavuttamiseksi unionissa sisämarkkinoiden toiminnan parantamiseksi.

2. Tätä varten tässä direktiivissä

a) säädetään kaikkien jäsenvaltioiden velvollisuuksista hyväksyä verkko- ja tietojärjestelmien turvallisuutta koskeva kansallinen strategia;

b) luodaan yhteistyöryhmä tukemaan ja helpottamaan strategista yhteistyötä ja tiedonvaihtoa jäsenvaltioiden kesken sekä kehittämään luottamusta ja luotettavuutta niiden keskuudessa;

c) luodaan tietoturvaloukkauksiin reagoivien ja niitä tutkivien yksiköiden (computer security incident response teams) verkosto, jäljempänä 'CSIRT-verkosto', edistämään luottamuksen ja luotettavuuden kehittämistä jäsenvaltioiden välillä sekä edistämään ripeää ja tehokasta operatiivista yhteistyötä;

([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 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).
([4]) EUVL C 32, 4.2.2014, s. 19.

d) otetaan käyttöön keskeisten palvelujen tarjoajia sekä digitaalisen palvelun tarjoajia koskevat turvallisuus- ja ilmoitusvaatimukset;

e) säädetään jäsenvaltioiden velvollisuuksista nimetä kansalliset toimivaltaiset viranomaiset, keskitetyt yhteyspisteet ja CSIRT-toimijat, joiden tehtävät liittyvät verkko- ja tietojärjestelmien turvallisuuteen.

3. Tässä direktiivissä säädettyjä turvallisuus- ja ilmoitusvaatimuksia ei sovelleta yrityksiin, joihin sovelletaan direktiivin 2002/21/EY 13 a ja 13 b artiklan vaatimuksia, eikä luottamuspalvelun tarjoajiin, joihin sovelletaan asetuksen (EU) N:o 910/2014 19 artiklan vaatimuksia.

4. Tämän direktiivin soveltaminen ei rajoita neuvoston direktiivin 2008/114/EY ([1]) eikä Euroopan parlamentin ja neuvoston direktiivien 2011/93/EU ([2]) ja 2013/40/EU ([3]) soveltamista.

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

6. Tämä direktiivi ei rajoita toimia, joita jäsenvaltiot toteuttavat keskeisten valtiolle kuuluvien tehtäviensä suojaamiseksi, erityisesti kansallisen turvallisuuden suojaamiseksi, mukaan lukien toimet sellaisten tietojen suojaamiseksi, joiden ilmaisemisen jäsenvaltiot katsovat keskeisten turvallisuusetujensa vastaiseksi, sekä yleisen järjestyksen ylläpitämiseksi, erityisesti rikosten tutkimisen, selvittämisen ja syytteeseenpanon mahdollistamiseksi.

7. Kun alakohtaisessa unionin säädöksessä edellytetään keskeisten palvelujen tarjoajien tai digitaalisen palvelun tarjoajien joko varmistavan verkko- ja tietojärjestelmiensä turvallisuuden tai ilmoittavan poikkeamista, sovelletaan kyseisen alakohtaisen unionin säädöksen säännöksiä, edellyttäen, että siinä säädetyt vaatimukset ovat vaikutukseltaan vähintään vastaavia kuin tässä direktiivissä säädetyt velvollisuudet.

2 artikla

Henkilötietojen käsittely

1. Tämän direktiivin mukaisessa henkilötietojen käsittelyssä on noudatettava direktiiviä 95/46/EY.

2. Tämän direktiivin mukaisessa unionin toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä on noudatettava asetusta (EY) N:o 45/2001.

3 artikla

Vähimmäistason yhdenmukaistaminen

Jäsenvaltioita voivat hyväksyä tai pitää voimassa säännöksiä, joiden tarkoituksena on saavuttaa korkeatasoisempi verkko- ja tietojärjestelmien turvallisuus, sanotun kuitenkaan rajoittamatta 16 artiklan 10 kohdan ja jäsenvaltioiden unionin oikeuden mukaisten velvollisuuksien soveltamista.

([1]) 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).

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

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

4 artikla

Määritelmät

Tässä direktiivissä tarkoitetaan

1) ’verkko- ja tietojärjestelmällä’

   a) direktiivin 2002/21/EY 2 artiklan a alakohdassa tarkoitettua sähköistä viestintäverkkoa;

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

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

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

3) ’verkko- ja tietojärjestelmien turvallisuutta koskevalla kansallisella strategialla’ kehystä, jossa esitetään verkko- ja tietojärjestelmien turvallisuutta koskevat kansallisen tason strategiset tavoitteet ja painopisteet;

4) ’keskeisten palvelujen tarjoajalla’ julkista tai yksityistä toimijaa, joka on liitteessä II tarkoitettua tyyppiä ja täyttää 5 artiklan 2 kohdassa säädetyt kriteerit;

5) ’digitaalisella palvelulla’ Euroopan parlamentin ja neuvoston direktiivin (EU) 2015/1535 ([1]) 1 artiklan 1 kohdan b alakohdassa tarkoitettua palvelua, joka on liitteessä III lueteltua tyyppiä;

6) ’digitaalisen palvelun tarjoajalla’ oikeushenkilöä, joka tarjoaa digitaalista palvelua;

7) ’poikkeamalla’ mitä tahansa tapahtumaa, joka tosiasiassa vaikuttaa haitallisesti verkko- ja tietojärjestelmien turvallisuuteen;

8) ’poikkeamien käsittelyllä’ kaikkia menettelyjä, jotka tukevat poikkeaman havaitsemista, analyysia ja sen vaikutusten rajoittamista sekä siihen reagointia;

9) ’riskillä’ mitä tahansa kohtuullisesti tunnistettavissa olevaa tilannetta tai tapahtumaa, joka saattaa vaikuttaa haitallisesti verkko- ja tietojärjestelmien turvallisuuteen;

10) ’edustajalla’ unioniin sijoittautunutta luonnollista henkilöä tai oikeushenkilöä, joka on nimenomaisesti nimetty toimimaan sellaisen digitaalisen palvelun tarjoajan puolesta, joka ei ole sijoittautunut unioniin; kansallinen toimivaltainen viranomainen tai CSIRT-toimija voi ottaa yhteyttä tällaiseen edustajaan digitaalisen palvelun tarjoajan sijasta kyseisen digitaalisen palvelun tarjoajan tämän direktiivin mukaisten velvollisuuksien osalta;

11) ’standardilla’ asetuksen (EU) N:o 1025/2012 2 artiklan 1 kohdassa tarkoitettua standardia;

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

13) ’internetin yhdysliikennepisteellä (IXP)’ verkkoinfrastruktuurin osaa, joka mahdollistaa useamman kuin kahden riippumattoman autonomisen järjestelmän yhdistämisen pääasiassa internetliikenteen välittämisen helpottamiseksi; IXP tarjoaa yhteenliittämistä ainoastaan autonomisille järjestelmille; IXP ei edellytä minkään yhteenliittämänsä kahden autonomisen järjestelmän väliseltä internetliikenteeltä kulkemista minkään kolmannen autonomisen järjestelmän kautta, eikä se muuta tällaista liikennettä tai muutoin puutu siihen;

14) ’nimipalvelulla’ hajautettua hierarkkista verkon nimijärjestelmää, joka käsittelee nimipalvelukyselyjä;

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

15) 'nimipalvelujen tarjoajalla' toimijaa, joka tarjoaa nimipalveluja internetissä;

16) 'aluetunnusrekisterillä' toimijaa, joka hallinnoi ja hoitaa internetin verkkotunnusten rekisteröintiä tietyn aluetunnuksen puitteissa;

17) 'verkossa toimivalla markkinapaikalla' digitaalista palvelua, joka antaa Euroopan parlamentin ja neuvoston direktiivin 2013/11/EU ([1]) 4 artiklan 1 kohdan a alakohdassa määritellyille kuluttajille ja/tai kyseisen direktiivin 4 artiklan 1 kohdan b alakohdassa määritellyille elinkeinonharjoittajille mahdollisuuden tehdä verkossa kauppa- tai palvelusopimuksia elinkeinonharjoittajien kanssa joko verkossa toimivan markkinapaikan verkkosivustolla tai elinkeinonharjoittajan verkkosivustolla, joka käyttää verkossa toimivan markkinapaikan tarjoamia tietojenkäsittelypalveluja;

18) 'verkossa toimivalla hakukoneella' digitaalista palvelua, joka antaa käyttäjille mahdollisuuden tehdä hakuja periaatteessa kaikilta verkkosivustoilta tai tietynkielisiltä verkkosivustoilta mitä tahansa aihetta koskevan hakusanan, lausekkeen tai muun tiedon muodossa tehdyn kyselyn perusteella ja joka antaa tulokseksi linkkejä, joista voi saada pyydettyyn sisältöön liittyvää tietoa;

19) 'pilvipalvelulla' digitaalista palvelua, joka mahdollistaa pääsyn skaalautuvaan ja mukautuvaan joukkoon jaettavissa olevia tietoteknisiä resursseja.

5 artikla

Keskeisten palvelujen tarjoajien määrittäminen

1. Jäsenvaltioiden on määritettävä viimeistään 9 päivänä marraskuuta 2018 kunkin liitteessä II tarkoitetun toimialan ja toimialan osa-alueen osalta ne keskeisten palvelujen tarjoajat, jotka ovat sijoittautuneet niiden alueelle.

2. Edellä 4 artiklan 4 kohdassa tarkoitetut kriteerit keskeisten palvelujen tarjoajien määrittämiseksi ovat seuraavat:

a) toimija tarjoaa palvelua, joka on keskeinen yhteiskunnan ja/tai talouden kriittisten toimintojen ylläpitämiseksi;

b) kyseisen palvelun tarjoaminen on riippuvainen verkko- ja tietojärjestelmistä; ja

c) poikkeamalla olisi merkittäviä haitallisia vaikutuksia kyseisen palvelun tarjoamiseen.

3. Edellä olevaa 1 kohtaa sovellettaessa kunkin jäsenvaltion on laadittava luettelo 2 kohdan a alakohdassa tarkoitetuista palveluista.

4. Jos 1 kohtaa sovellettaessa toimija tarjoaa 2 kohdan a alakohdassa tarkoitetun kaltaista palvelua kahdessa tai useammassa jäsenvaltiossa, kyseisten jäsenvaltioiden on kuultava toisiaan. Tällainen kuuleminen on toteutettava, ennen kuin määrittämistä koskeva päätös tehdään.

5. Jäsenvaltioiden on säännöllisesti ja vähintään kahden vuoden välein 9 päivästä toukokuuta 2018 tarkistettava ja tarvittaessa saatettava ajan tasalle määritettyjen keskeisten palvelujen tarjoajien luettelo.

6. Yhteistyöryhmän roolina on 11 artiklassa tarkoitettujen tehtävien mukaisesti tukea jäsenvaltioita yhdenmukaisen lähestymistavan soveltamisessa keskeisten palvelujen tarjoajien määrittämisprosessissa.

7. Jäsenvaltioiden on 23 artiklassa tarkoitettua uudelleentarkastelua varten ja viimeistään 9 päivänä marraskuuta 2018 sekä sen jälkeen kahden vuoden välein toimitettava komissiolle tiedot, jotka komissio tarvitsee tämän direktiivin täytäntöönpanon, erityisesti keskeisten palvelujen tarjoajien määrittämistä koskevien jäsenvaltioiden lähestymistapojen yhdenmukaisuuden, arvioimiseksi. Näihin tietoihin on sisällyttävä vähintään seuraavat:

a) kansalliset toimenpiteet, joiden avulla keskeisten palvelujen tarjoajat voidaan määrittää;

([1]) Euroopan parlamentin ja neuvoston direktiivi 2013/11/EU, annettu 21 päivänä toukokuuta 2013, kuluttajariitojen vaihtoehtoisesta riidanratkaisusta sekä asetuksen (EY) N:o 2006/2004 ja direktiivin 2009/22/EY muuttamisesta (vaihtoehtoista kuluttajariitojen ratkaisua koskeva direktiivi) (EUVL L 165, 18.6.2013, s. 63).

b) edellä 3 kohdassa tarkoitettu luettelo palveluista;

c) kunkin liitteessä II tarkoitetun toimialan osalta määritettyjen keskeisten palvelujen tarjoajien lukumäärä ja tiedot niiden merkityksestä kyseessä olevan alanosalta;

d) kynnysarvot, jos sellaisia on olemassa, asiaankuuluvan toimitustason määrittämiseksi 6 artiklan 1 kohdan a alakohdassa tarkoitetun kyseisestä palvelusta riippuvaisten käyttäjien lukumäärän perusteella tai 6 artiklan 1 kohdan f alakohdassa tarkoitetun kyseisen keskeisten palvelujen tarjoajan merkityksen perusteella.

Vertailukelpoisten tietojen esittämisen edistämiseksi komissio voi hyväksyä asianmukaisia teknisiä suuntaviivoja tässä kohdassa tarkoitettuja tietoja koskevista parametreista ottaen mahdollisimman tarkasti huomioon ENISAn lausunnon.

6 artikla

Merkittävä haitallinen vaikutus

1. Määrittäessään 5 artiklan 2 kohdan c alakohdassa tarkoitetun haitallisen vaikutuksen merkitystä jäsenvaltioiden on otettava huomioon vähintään seuraavat toimialojen väliset tekijät:

a) asianomaisen toimijan tarjoamasta palvelusta riippuvaisten käyttäjien lukumäärä;

b) muiden liitteessä II tarkoitettujen toimialojen riippuvaisuus kyseisen toimijan tarjoamasta palvelusta;

c) vaikutus, joka poikkeamilla voisi olla vakavuutensa ja kestonsa perusteella talouden ja yhteiskunnan toimintoihin tai yleiseen turvallisuuteen;

d) kyseisen toimijan markkinaosuus;

e) maantieteellinen levinneisyys alueella, johon poikkeama saattaa vaikuttaa;

f) toimijan merkitys palvelun riittävän tason ylläpitämisessä ottaen huomioon kyseisen palvelun tarjoamista koskevien vaihtoehtoisten keinojen saatavuus.

2. Sen määrittämiseksi, olisiko poikkeamalla merkittävä haitallinen vaikutus, jäsenvaltioiden on otettava tarvittaessa huomioon myös toimialakohtaiset tekijät.

II LUKU

VERKKO- JA TIETOJÄRJESTELMIEN TURVALLISUUTTA KOSKEVAT KANSALLISET KEHYKSET

7 artikla

Verkko- ja tietojärjestelmien turvallisuutta koskeva kansallinen strategia

1. Kunkin jäsenvaltion on hyväksyttävä verkko- ja tietojärjestelmien turvallisuutta koskeva kansallinen strategia, jossa määritellään strategiset tavoitteet sekä asianmukaiset toimintapoliittiset toimenpiteet ja sääntelytoimenpiteet korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden saavuttamiseksi ja ylläpitämiseksi ja joka kattaa vähintään liitteessä II tarkoitetut toimialat ja liitteessä III tarkoitetut palvelut. Verkko- ja tietojärjestelmien turvallisuutta koskevassa kansallisessa strategiassa on käsiteltävä erityisesti seuraavia kysymyksiä:

a) verkko- ja tietojärjestelmien turvallisuutta koskevan kansallisen strategian tavoitteet ja painopisteet;

b) ohjauskehys verkko- ja tietojärjestelmien turvallisuutta koskevan kansallisen strategian tavoitteiden ja painopisteiden saavuttamiseksi, mukaan lukien valtion elinten ja muiden asiaankuuluvien toimijoiden tehtävät ja vastuut;

c) varautumiskykyyn, reagointiin ja toimintakunnon palauttamiseen liittyvien toimenpiteiden yksilöinti, mukaan lukien julkisen ja yksityisen sektorin välinen yhteistyö;

d) tiedot verkko- ja tietojärjestelmien turvallisuutta koskevaan kansalliseen strategiaan liittyvistä opetus-, valistus- ja koulutusohjelmista;

e) tiedot verkko- ja tietojärjestelmien turvallisuutta koskevaan kansalliseen strategiaan liittyvistä tutkimus- ja kehityssuunnitelmista;

f) riskinarviointisuunnitelma riskien yksilöimiseksi;

g) luettelo verkko- ja tietojärjestelmien turvallisuutta koskevan kansallisen strategian täytäntöönpanoon osallistuvista eri toimijoista.

2. Jäsenvaltiot voivat pyytää ENISAn apua verkko- ja tietojärjestelmien turvallisuutta koskevien kansallisten strategioiden kehittämisessä.

3. Jäsenvaltioiden on toimitettava verkko- ja tietojärjestelmien turvallisuutta koskevat kansalliset strategiansa komissiolle kolmen kuukauden kuluessa niiden hyväksymisestä. Näin tehdessään jäsenvaltiot voivat jättää toimittamatta kansalliseen turvallisuuteen liittyvät strategian osat.

8 artikla

Kansalliset toimivaltaiset viranomaiset ja keskitetty yhteyspiste

1. Kunkin jäsenvaltion on nimettävä yksi tai useampi verkko- ja tietojärjestelmien turvallisuudesta vastaava kansallinen toimivaltainen viranomainen, jäljempänä 'toimivaltainen viranomainen', jonka toiminta kattaa ainakin liitteessä II tarkoitetut toimialat ja liitteessä III tarkoitetut palvelut. Jäsenvaltiot voivat antaa tämän tehtävän olemassa olevalle viranomaiselle tai olemassa oleville viranomaisille.

2. Toimivaltaisten viranomaisten on seurattava tämän direktiivin soveltamista kansallisella tasolla.

3. Kunkin jäsenvaltion on nimettävä verkko- ja tietojärjestelmien turvallisuudesta vastaava keskitetty kansallinen yhteyspiste, jäljempänä 'keskitetty yhteyspiste'. Jäsenvaltiot voivat antaa tämän tehtävän olemassa olevalle viranomaiselle. Jos jäsenvaltio nimeää vain yhden toimivaltaisen viranomaisen, kyseinen toimivaltainen viranomainen on myös keskitetty yhteyspiste.

4. Keskitetyn yhteyspisteen tehtävänä on yhteydenpito, jotta voidaan varmistaa jäsenvaltion viranomaisten rajat ylittävä yhteistyö ja rajat ylittävä yhteistyö muiden jäsenvaltioiden asiaankuuluvien viranomaisten kanssa sekä 11 artiklassa tarkoitetun yhteistyöryhmän ja 12 artiklassa tarkoitetun CSIRT-verkoston kanssa.

5. Jäsenvaltioiden on varmistettava, että toimivaltaisilla viranomaisilla ja keskitetyillä yhteyspisteillä on riittävät voimavarat, jotta ne voivat suorittaa tuloksekkaasti ja tehokkaasti niille osoitetut tehtävät ja siten täyttää tämän direktiivin tavoitteet. Jäsenvaltioiden on varmistettava nimettyjen edustajien tuloksellinen, tehokas ja suojattu yhteistyö yhteistyöryhmässä.

6. Toimivaltaisten viranomaisten ja keskitetyn yhteyspisteen on tarvittaessa ja kansallisen lainsäädännön mukaisesti kuultava asiaankuuluvia kansallisia lainvalvontaviranomaisia ja kansallisia tietosuojaviranomaisia sekä tehtävä yhteistyötä niiden kanssa.

7. Kunkin jäsenvaltion on ilmoitettava komissiolle viipymättä toimivaltaisen viranomaisen ja keskitetyn yhteyspisteen nimeämisestä, niiden tehtävistä sekä näiden tietojen mahdollisista myöhemmistä muutoksista. Kunkin jäsenvaltion on julkistettava toimivaltaisen viranomaisen ja keskitetyn yhteyspisteen nimeäminen. Komissio julkaisee nimettyjen keskitettyjen yhteyspisteiden luettelon.

9 artikla

Tietoturvaloukkauksiin reagoivat ja niitä tutkivat yksiköt (CSIRT-toimijat)

1. Kunkin jäsenvaltion on nimettävä yksi tai useampi CSIRT-toimija, joka täyttää liitteessä I olevassa 1 kohdassa vahvistetut vaatimukset ja jonka toiminta kattaa vähintään liitteessä II tarkoitetut toimialat sekä liitteessä III tarkoitetut palvelut ja joka vastaa riskien ja poikkeamien käsittelystä hyvin määritellyn prosessin mukaisesti. CSIRT-toimija voidaan perustaa toimivaltaisen viranomaisen yhteyteen.

2. Jäsenvaltioiden on varmistettava, että CSIRT-toimijoilla on riittävät resurssit voidakseen suorittaa tuloksekkaasti liitteessä I olevassa 2 kohdassa vahvistetut tehtävänsä.

Jäsenvaltioiden on varmistettava CSIRT-toimijoidensa tuloksellinen, tehokas ja suojattu yhteistyö 12 artiklassa tarkoitetussa CSIRT-verkostossa.

3. Jäsenvaltioiden on varmistettava, että niiden CSIRT-toimijoilla on pääsy asianmukaiseen, suojattuun ja kestävään viestintä- ja tietoinfrastruktuuriin kansallisella tasolla.

4. Jäsenvaltioiden on annettava komissiolle tiedot CSIRT-toimijoidensa poikkeamien käsittelyprosessiin kuuluvien tehtävien laajuudesta sekä poikkeamien käsittelyprosessin tärkeimmistä osista.

5. Jäsenvaltiot voivat pyytää ENISAn apua kansallisten CSIRT-toimijoiden kehittämisessä.

10 artikla

Yhteistyö kansallisella tasolla

1. Jos saman jäsenvaltion toimivaltainen viranomainen, keskitetty yhteyspiste ja CSIRT-toimija ovat erillisiä, niiden on tehtävä yhteistyötä tässä direktiivissä säädettyjen velvollisuuksien täyttämisen osalta.

2. Jäsenvaltioiden on varmistettava, että joko toimivaltaiset viranomaiset tai CSIRT-toimijat saavat tämän direktiivin nojalla toimitetut poikkeamia koskevat ilmoitukset. Jos jäsenvaltio päättää, että CSIRT-toimijat eivät saa ilmoituksia, CSIRT-toimijoille on, siinä määrin kuin on tarpeen niiden tehtävien täyttämiseksi, annettava pääsy tietoihin, jotka koskevat keskeisten palvelujen tarjoajien 14 artiklan 3 ja 5 kohdan nojalla tai digitaalisen palvelun tarjoajien 16 artiklan 3 ja 6 kohdan nojalla ilmoittamia poikkeamia.

3. Jäsenvaltioiden on varmistettava, että toimivaltaiset viranomaiset tai CSIRT-toimijat ilmoittavat keskitetyille yhteyspisteille tämän direktiivin nojalla toimitetuista poikkeamia koskevista ilmoituksista.

Keskitetyn yhteyspisteen on toimitettava yhteistyöryhmälle tiivistelmäraportti saaduista ilmoituksista, mukaan lukien ilmoitusten lukumäärä ja ilmoitettujen poikkeamien luonne, sekä 14 artiklan 3 ja 5 kohdan ja 16 artiklan 3 ja 6 kohdan mukaisesti toteutetuista toimista viimeistään 9 päivänä elokuuta 2018 ja sen jälkeen kerran vuodessa.

III LUKU

YHTEISTYÖ

11 artikla

Yhteistyöryhmä

1. Perustetaan yhteistyöryhmä jäsenvaltioiden keskinäisen strategisen yhteistyön ja tietojen vaihtamisen tukemiseksi ja helpottamiseksi, luottamuksen ja luotettavuuden kehittämiseksi sekä verkko- ja tietojärjestelmien korkeatasoisen ja yhtenäisen suojan varmistamiseksi unionissa.

Yhteistyöryhmä suorittaa tehtävänsä 3 kohdan toisessa alakohdassa tarkoitettujen kaksivuotisten työohjelmien pohjalta.

2. Yhteistyöryhmä muodostuu jäsenvaltioiden edustajista, komissiosta ja ENISAsta.

Yhteistyöryhmä voi tarvittaessa kutsua asiaankuuluvien sidosryhmien edustajia osallistumaan työskentelyynsä.

Komissio huolehtii sihteeristötehtävistä.

3. Yhteistyöryhmällä on seuraavat tehtävät:

a) strategisen ohjeistuksen antaminen 12 artiklan nojalla perustetun CSIRT-verkoston toimia varten;

b) parhaiden käytäntöjen vaihtaminen 14 artiklan 3 ja 5 kohdassa sekä 16 artiklan 3 ja 6 kohdassa tarkoitettuun poikkeamien ilmoittamiseen liittyvästä tiedonvaihdosta;

c) parhaiden käytäntöjen vaihtaminen jäsenvaltioiden välillä ja jäsenvaltioiden avustaminen yhteistyössä ENISAn kanssa valmiuksien kehittämisessä verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi;

d) keskusteleminen jäsenvaltioiden valmiuksista ja varautumiskyvystä sekä vapaaehtoisuuteen perustuva verkko- ja tietojärjestelmien turvallisuutta koskevien kansallisten strategioiden ja CSIRT-toimijoiden tehokkuuden arvioiminen sekä parhaiden käytäntöjen määrittäminen;

e) tietojen ja parhaiden käytäntöjen vaihtaminen valistuksesta ja koulutuksesta;

f) tietojen ja parhaiden käytäntöjen vaihtaminen verkko- ja tietojärjestelmien turvallisuutta koskevasta tutkimuksesta ja kehityksestä;

g) tarvittaessa kokemusten vaihtaminen verkko- ja tietojärjestelmien turvallisuutta koskevista kysymyksistä asiaankuuluvien unionin toimielinten, elinten, virastojen ja laitosten kanssa;

h) keskusteleminen 19 artiklassa tarkoitetuista standardeista ja eritelmistä asiaankuuluvien eurooppalaisten standardointiorganisaatioiden edustajien kanssa;

i) tiedon kerääminen riskejä ja poikkeamia koskevista parhaista käytännöistä;

j) edellä 10 artiklan 3 kohdan toisessa alakohdassa tarkoitettujen tiivistelmäraporttien tarkasteleminen vuosittain;

k) keskusteleminen toteutetuista toimista, jotka koskevat verkko- ja tietojärjestelmien turvallisuutta koskevia harjoituksia, opetusohjelmia ja koulutusta, mukaan lukien ENISAn toteuttamat toimet;

l) parhaiden käytäntöjen vaihtaminen ENISAn avustuksella jäsenvaltioiden toteuttamasta keskeisten palvelujen tarjoajien määrittämisestä, myös rajat ylittävien riippuvuussuhteiden osalta, siltä osin kuin kyse on riskeistä ja poikkeamista;

m) keskusteleminen järjestelyistä, jotka koskevat raportointia 14 ja 16 artiklassa tarkoitetuista poikkeamia koskevista ilmoituksista.

Viimeistään 9 päivänä helmikuuta 2018 ja sen jälkeen kahden vuoden välein yhteistyöryhmä laatii työohjelman toteutettavista toimista, joilla pannaan täytäntöön sen tavoitteet ja tehtävät, joiden on oltava tämän direktiivin tavoitteiden mukaisia.

4. Yhteistyöryhmän on 23 artiklassa tarkoitettua uudelleentarkastelua varten ja viimeistään 9 päivänä elokuuta 2018 sekä sen jälkeen puolentoista vuoden välein laadittava raportti, jossa arvioidaan tämän artiklan nojalla toteutetussa strategisessa yhteistyössä saatuja kokemuksia.

5. Komissio hyväksyy täytäntöönpanosäädökset, joissa vahvistetaan yhteistyöryhmän toimintaa varten tarvittavat menettelytapajärjestelyt. Nämä täytäntöönpanosäädökset hyväksytään 22 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

Ensimmäistä alakohtaa sovellettaessa komissio toimittaa ensimmäisen luonnoksen täytäntöönpanosäädökseksi 22 artiklan 1 kohdassa tarkoitetulle komitealle viimeistään 9 päivänä helmikuuta 2017.

12 artikla

CSIRT-verkosto

1. Jotta voidaan edistää luottamuksen kehittämistä jäsenvaltioiden välillä sekä edistää ripeää ja tehokasta operatiivista yhteistyötä, perustetaan kansallisten CSIRT-toimijoiden verkosto.

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

3. CSIRT-verkostolla on seuraavat tehtävät:

a) tietojen vaihtaminen CSIRT-toimijoiden palveluista, toiminnoista ja yhteistyövalmiuksista;

b) poikkeamaa ja siihen liittyviä riskejä koskevien muiden kuin kaupallisesti arkaluonteisten tietojen vaihtaminen ja niistä keskusteleminen sellaisen jäsenvaltion, johon kyseinen poikkeama mahdollisesti vaikuttaa, CSIRT-toimijan edustajan pyynnöstä; minkä tahansa jäsenvaltion CSIRT-toimija voi kuitenkin kieltäytyä osallistumasta tällaiseen keskusteluun, jos on olemassa riski siitä, että poikkeaman tutkimiselle aiheutuu haittaa;

c) yksittäisiä poikkeamia koskevien ei-luottamuksellisten tietojen vaihtaminen ja niiden saataville asettaminen vapaaehtoisuuteen perustuen;

d) jäsenvaltion lainkäyttöalueella tunnistetusta poikkeamasta keskusteleminen ja mahdollisuuksien mukaan tällaista poikkeamaa koskevan koordinoidun vastauksen määrittäminen kyseisen jäsenvaltion CSIRT-toimijan edustajan pyynnöstä;

e) jäsenvaltioiden tukeminen rajat ylittävien poikkeamien käsittelyssä niiden vapaaehtoisen keskinäisen avunannon pohjalta;

f) muista operatiivisen yhteistyön muodoista keskusteleminen sekä niiden tarkasteleminen ja määrittäminen, myös seuraavien osalta:

   i) riskien ja poikkeamien luokat;

   ii) ennakkovaroitukset;

   iii) keskinäinen avunanto;

   iv) periaatteet ja yksityiskohtaiset säännöt koordinointia varten tilanteisiin, joissa jäsenvaltiot reagoivat rajat ylittäviin riskeihin ja poikkeamiin;

g) tiedottaminen yhteistyöryhmälle CSIRT-verkoston toimista ja f alakohdan nojalla keskustelluista muista operatiivisen yhteistyön muodoista ja niitä koskevan ohjeistuksen pyytäminen;

h) keskusteleminen verkko- ja tietojärjestelmien turvallisuutta koskevista harjoituksista saaduista kokemuksista, mukaan lukien ENISAn järjestämistä tällaisista harjoituksista saadut kokemukset;

i) keskusteleminen yksittäisen CSIRT-toimijan valmiuksista ja varautumiskyvystä kyseisen CSIRT-toimijan pyynnöstä;

j) suuntaviivojen laatiminen operatiivisten käytäntöjen lähentämisen helpottamiseksi siltä osin kuin kyse on operatiivista yhteistyötä koskevien tämän artiklan säännösten soveltamisesta.

4. CSIRT-verkoston on 23 artiklassa tarkoitettua uudelleentarkastelua varten ja viimeistään 9 päivänä elokuuta 2018 sekä sen jälkeen puolentoista vuoden välein laadittava raportti, jossa arvioidaan tämän artiklan nojalla toteutetussa operatiivisessa yhteistyössä, mukaan lukien päätelmät ja suositukset, saatuja kokemuksia. Kyseinen raportti toimitetaan myös yhteistyöryhmälle.

5. CSIRT-verkosto vahvistaa työjärjestyksensä.

13 artikla

Kansainvälinen yhteistyö

Unioni voi tehdä Euroopan unionin toiminnasta tehdyn sopimuksen 218 artiklan mukaisesti kolmansien maiden tai kansainvälisten järjestöjen kanssa kansainvälisiä sopimuksia, joissa määrätään siitä, että ne voivat osallistua joihinkin yhteistyöryhmän toimiin, ja organisoidaan tämä osallistuminen. Tällaisissa sopimuksissa on otettava huomioon tarve varmistaa riittävä tietosuoja.

IV LUKU

KESKEISTEN PALVELUJEN TARJOAJIEN VERKKO- JA TIETOJÄRJESTELMIEN TURVALLISUUS

14 artikla

Turvallisuusvaatimukset ja poikkeamien ilmoittaminen

1. Jäsenvaltioiden on varmistettava, että keskeisten palvelujen tarjoajat toteuttavat asianmukaiset ja oikeasuhteiset tekniset ja organisatoriset toimenpiteet hallitakseen riskejä, joita kohdistuu niiden verkko- ja tietojärjestelmien turvallisuuteen, joita nämä keskeisten palvelujen tarjoajat käyttävät toiminnoissaan. Näillä toimenpiteillä on varmistettava riskiin suhteutettu verkko- ja tietojärjestelmien turvallisuuden taso uusin tekniikka huomioon ottaen.

2. Jäsenvaltioiden on varmistettava, että keskeisten palvelujen tarjoajat toteuttavat asianmukaiset toimenpiteet, joilla ehkäistään ja minimoidaan tällaisten keskeisten palvelujen tarjoamisessa käytettyjen verkko- ja tietojärjestelmien turvallisuuteen vaikuttavien poikkeamien vaikutus näiden palvelujen jatkuvuuden takaamiseksi.

3. Jäsenvaltioiden on varmistettava, että keskeisten palvelujen tarjoajat ilmoittavat ilman aiheetonta viivytystä toimivaltaiselle viranomaiselle tai CSIRT-toimijalle poikkeamista, joilla on merkittävä vaikutus niiden tarjoamien keskeisten palvelujen jatkuvuuteen. Ilmoituksiin on sisällytettävä tiedot, joiden perusteella toimivaltainen viranomainen tai CSIRT-toimija voi määrittää poikkeaman mahdollisen rajat ylittävän vaikutuksen. Ilmoittaminen ei lisää ilmoituksen tekevän osapuolen vastuuta.

4. Poikkeaman vaikutuksen merkittävyyden määrittämiseksi on otettava huomioon erityisesti seuraavat parametrit:

a) niiden käyttäjien lukumäärä, joihin keskeisen palvelun häiriö vaikuttaa;

b) poikkeaman kesto;

c) maantieteellinen levinneisyys alueella, johon poikkeama vaikuttaa.

5. Toimivaltaisen viranomaisen tai CSIRT-toimijan on keskeisten palvelujen tarjoajan tekemään ilmoitukseen sisältyvien tietojen perusteella ilmoitettava muille asiaan liittyville jäsenvaltioille, onko poikkeamalla merkittävä vaikutus keskeisten palvelujen jatkuvuuteen kyseisessä jäsenvaltiossa. Näin tehdessään toimivaltaisen viranomaisen tai CSIRT-toimijan on unionin oikeuden tai unionin oikeuden mukaisen kansallisen lainsäädännön mukaisesti säilytettävä keskeisten palvelujen tarjoajan turvallisuusedut ja kaupalliset edut sekä sen tekemään ilmoitukseen sisältyvien tietojen luottamuksellisuus.

Jos olosuhteet sallivat, toimivaltaisen viranomaisen tai CSIRT-toimijan on annettava ilmoituksen tehneelle keskeisten palvelujen tarjoajalle asiaankuuluvat tiedot sen tekemään ilmoitukseen liittyvistä jatkotoimista, kuten tiedot, jotka voivat tukea poikkeaman tuloksellista käsittelyä.

Keskitetyn yhteyspisteen on toimivaltaisen viranomaisen tai CSIRT-toimijan pyynnöstä toimitettava ensimmäisessä alakohdassa tarkoitetut ilmoitukset muiden asiaan liittyvien jäsenvaltioiden keskitetyille yhteyspisteille.

6. Kuultuaan ilmoituksen tehnyttä keskeisten palvelujen tarjoajaa toimivaltainen viranomainen tai CSIRT-toimija voi tiedottaa yleisölle yksittäisistä poikkeamista, jos yleinen tietoisuus on tarpeen poikkeaman estämiseksi tai käynnissä olevan poikkeaman käsittelemiseksi.

7. Toimivaltaiset viranomaiset voivat yhdessä yhteistyöryhmän kanssa toimien kehittää ja hyväksyä suuntaviivoja niistä olosuhteista, joissa keskeisten palvelujen tarjoajien edellytetään ilmoittavan poikkeamista, mukaan lukien 4 kohdassa tarkoitetut parametrit poikkeaman vaikutuksen merkittävyyden määrittämiseksi.

15 artikla

Täytäntöönpano ja sen valvonta

1. Jäsenvaltioiden on varmistettava, että toimivaltaisilla viranomaisilla on tarvittavat valtuudet ja keinot arvioida, noudattavatko keskeisten palvelujen tarjoajat 14 artiklan mukaisia velvollisuuksiaan, sekä tämän vaikutuksia verkko- ja tietojärjestelmien turvallisuuteen.

2. Jäsenvaltioiden on varmistettava, että toimivaltaisilla viranomaisilla on valtuudet ja keinot pyytää keskeisten palvelujen tarjoajia

a) antamaan tiedot, jotka tarvitaan niiden verkko- ja tietojärjestelmien turvallisuuden arvioimiseksi, mukaan lukien todennettavassa muodossa olevat turvallisuusohjeet;

b) esittämään näyttöä turvallisuusohjeiden tosiasiallisesta täytäntöönpanosta, kuten toimivaltaisen viranomaisen tai pätevän tarkastajan suorittaman turvallisuustarkastuksen tulokset, ja viimeksi mainitussa tapauksessa antamaan turvallisuustarkastuksen tulokset, mukaan lukien niitä tukeva näyttö, toimivaltaisen viranomaisen käyttöön.

Toimivaltaisen viranomaisen on tällaisia tietoja tai näyttöä pyytäessään ilmoitettava pyynnön tarkoitus ja täsmennettävä, mitä tietoja pyydetään.

3. Toimivaltainen viranomainen voi 2 kohdassa tarkoitettujen tietojen tai turvallisuustarkastusten tulosten arvioinnin jälkeen antaa keskeisten palvelujen tarjoajille sitovia ohjeita havaittujen puutteiden korjaamiseksi.

4. Toimivaltaisen viranomaisen on toimittava tiiviisti yhteistyössä tietosuojaviranomaisten kanssa käsitellessään henkilötietojen tietoturvaloukkauksiin johtaneita poikkeamia.

V LUKU

DIGITAALISEN PALVELUN TARJOAJIEN VERKKO- JA TIETOJÄRJESTELMIEN TURVALLISUUS

16 artikla

Turvallisuusvaatimukset ja poikkeamien ilmoittaminen

1. Jäsenvaltioiden on varmistettava, että digitaalisen palvelun tarjoajat määrittävät ja toteuttavat asianmukaiset ja oikeasuhteiset tekniset ja organisatoriset toimenpiteet hallitakseen riskejä, joita kohdistuu niiden verkko- ja tietojärjestelmien turvallisuuteen, joita nämä digitaalisen palvelun tarjoajat käyttävät tarjotessaan liitteessä III tarkoitettuja palveluja unionissa. Näillä toimenpiteillä on varmistettava riskiin suhteutettu verkko- ja tietojärjestelmien turvallisuuden taso uusin tekniikka huomioon ottaen, ja niissä on otettava huomioon seuraavat seikat:

a) järjestelmien ja tilojen turvallisuus;

b) poikkeamien käsittely;

c) liiketoiminnan jatkuvuuden hallinta;

d) seuranta, tarkastukset ja testaukset;

e) kansainvälisten standardien noudattaminen.

2. Jäsenvaltioiden on varmistettava, että digitaalisen palvelun tarjoajat toteuttavat toimenpiteitä, joilla ehkäistään ja minimoidaan niiden verkko- ja tietojärjestelmien turvallisuuteen vaikuttavien poikkeamien vaikutus liitteessä III tarkoitettuihin unionissa tarjottuihin palveluihin, jotta voidaan taata näiden palvelujen jatkuvuus.

3. Jäsenvaltioiden on varmistettava, että digitaalisen palvelun tarjoajat ilmoittavat toimivaltaiselle viranomaiselle tai CSIRT-toimijalle ilman aiheetonta viivytystä kaikista poikkeamista, joilla on merkittävä vaikutus sellaisen liitteessä III tarkoitetun palvelun tarjoamiseen, jota ne tarjoavat unionissa. Ilmoituksiin on sisällytettävä tiedot, joiden perusteella toimivaltainen viranomainen tai CSIRT-toimija voi määrittää mahdollisen rajat ylittävän vaikutuksen merkittävyyden. Ilmoittaminen ei lisää ilmoituksen tekevän osapuolen vastuuta.

4. Sen määrittämiseksi, onko poikkeaman vaikutus merkittävä, on otettava huomioon erityisesti seuraavat parametrit:

a) niiden käyttäjien lukumäärä, joihin poikkeama vaikuttaa, erityisesti niiden käyttäjien lukumäärä, jotka ovat riippuvaisia kyseessä olevasta palvelusta omien palvelujensa tarjoamiseksi;

b) poikkeaman kesto;

c) maantieteellinen levinneisyys alueella, johon poikkeama vaikuttaa;

d) palvelun toiminnan häiriön laajuus;

e) talouden ja yhteiskunnan toimintoihin kohdistuvan vaikutuksen laajuus.

Velvollisuutta ilmoittaa poikkeamasta sovelletaan ainoastaan, jos digitaalisen palvelun tarjoajalla on pääsy tietoihin, joita tarvitaan arvioitaessa poikkeaman vaikutusta suhteessa ensimmäisessä alakohdassa tarkoitettuihin parametreihin.

5. Jos keskeisten palvelujen tarjoaja on riippuvainen kolmantena osapuolena olevasta digitaalisen palvelun tarjoajasta sellaisen palvelun tarjoamiseksi, joka on olennainen yhteiskunnan ja talouden kriittisten toimintojen ylläpitämiseksi, keskeisten palvelujen tarjoajan on ilmoitettava sellaisista merkittävistä vaikutuksista keskeisten palvelujen jatkuvuuteen, jotka johtuvat digitaalisen palvelun tarjoajaan vaikuttavasta poikkeamasta.

6. Toimivaltaisen viranomaisen tai CSIRT-toimijan on tarvittaessa ja erityisesti silloin, kun 3 kohdassa tarkoitettu poikkeama koskee kahta tai useampaa jäsenvaltiota, tiedotettava asiasta muille asiaan liittyville jäsenvaltioille. Näin tehdessään toimivaltaisten viranomaisten, CSIRT-toimijoiden ja keskitettyjen yhteyspisteiden on unionin oikeuden tai unionin oikeuden mukaisen kansallisen lainsäädännön mukaisesti säilytettävä digitaalisen palvelun tarjoajan turvallisuusedut ja kaupalliset edut sekä annettujen tietojen luottamuksellisuus.

7. Kuultuaan kyseessä olevaa digitaalisen palvelun tarjoajaa toimivaltainen viranomainen tai CSIRT-toimija ja tarvittaessa muiden asiaankuuluvien jäsenvaltioiden viranomaiset tai CSIRT-toimijat voivat tiedottaa yleisölle yksittäisistä poikkeamista tai vaatia digitaalisen palvelun tarjoajaa tekemään niin, jos yleinen tietoisuus on tarpeen poikkeaman estämiseksi tai käynnissä olevan poikkeaman käsittelemiseksi tai jos poikkeaman ilmaiseminen on muutoin yleisen edun mukaista.

8. Komissio hyväksyy täytäntöönpanosäädöksiä 1 kohdassa tarkoitettujen seikkojen ja tämän artiklan 4 kohdassa lueteltujen parametrien täsmentämiseksi edelleen. Nämä täytäntöönpanosäädökset hyväksytään 22 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen viimeistään 9 päivänä elokuuta 2017.

9. Komissio voi hyväksyä täytäntöönpanosäädöksiä, joissa vahvistetaan ilmoitusvaatimuksiin sovellettavat muotoseikat ja menettelyt. Nämä täytäntöönpanosäädökset hyväksytään 22 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

10. Jäsenvaltiot eivät saa asettaa digitaalisen palvelun tarjoajille muita turvallisuus- tai ilmoitusvaatimuksia, sanotun kuitenkaan rajoittamatta 1 artiklan 6 kohdan soveltamista.

11. V lukua ei sovelleta mikroyrityksiin ja pieniin yrityksiin, sellaisina kuin ne määritellään komission suosituksessa 2003/361/EY ([1]).

([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).

17 artikla

Täytäntöönpano ja sen valvonta

1. Jäsenvaltioiden on varmistettava, että toimivaltaiset viranomaiset ryhtyvät tarvittaessa toimiin panemalla täytäntöön jälkikäteen toteutettavia valvontatoimenpiteitä, kun niille esitetään näyttöä siitä, että digitaalisen palvelun tarjoaja ei täytä 16 artiklassa säädettyjä vaatimuksia. Tällaisen näytön voi esittää sellaisen toisen jäsenvaltion toimivaltainen viranomainen, jossa palvelua tarjotaan.

2. Edellä olevaa 1 kohtaa sovellettaessa toimivaltaisilla viranomaisilla on oltava tarvittavat valtuudet ja keinot vaatia, että digitaalisen palvelun tarjoajat

a) antavat niiden verkko- ja tietojärjestelmien turvallisuuden arvioimiseksi tarvittavat tiedot, mukaan lukien todennettavassa muodossa olevat turvallisuusohjeet;

b) korjaavat mahdolliset puutteet 16 artiklassa säädettyjen vaatimusten täyttämisessä.

3. Jos digitaalisen palvelun tarjoajan pääasiallinen toimipaikka tai edustaja on jäsenvaltiossa mutta sen verkko- ja tietojärjestelmät sijaitsevat yhdessä tai useammassa muussa jäsenvaltiossa, pääasiallisen toimipaikan tai edustajan jäsenvaltion toimivaltaisen viranomaisen ja näiden muiden jäsenvaltioiden toimivaltaisten viranomaisten on tehtävä yhteistyötä ja avustettava toisiaan tarpeen mukaan. Tällaiseen avustamiseen ja yhteistyöhön voivat sisältyä tiedonvaihto asianomaisten toimivaltaisten viranomaisten välillä sekä pyynnöt 2 kohdassa tarkoitettujen valvontatoimenpiteiden toteuttamiseksi.

18 artikla

Lainkäyttövalta ja alueperiaate

1. Tätä direktiiviä sovellettaessa digitaalisen palvelun tarjoajan katsotaan kuuluvan sen jäsenvaltion lainkäyttövallan piiriin, jossa sen pääasiallinen toimipaikka sijaitsee. Digitaalisen palvelun tarjoajan pääasiallisen toimipaikan katsotaan olevan jäsenvaltiossa, jos sen kotipaikka on kyseisessä jäsenvaltiossa.

2. Digitaalisen palvelun tarjoajan, joka ei ole sijoittautunut unioniin mutta joka tarjoaa liitteessä III tarkoitettuja palveluja unionissa, on nimettävä edustaja unionin aluetta varten. Edustajan on oltava sijoittautunut johonkin niistä jäsenvaltioista, joissa palveluja tarjotaan. Digitaalisen palvelun tarjoajan katsotaan kuuluvan sen jäsenvaltion lainkäyttövallan piiriin, johon edustaja on sijoittautunut.

3. Se, että digitaalisen palvelun tarjoaja on nimennyt edustajan, ei rajoita oikeustoimia, joita voidaan panna vireille digitaalisen palvelun tarjoajaa itseään vastaan.

VI LUKU

STANDARDOINTI JA VAPAAEHTOINEN ILMOITTAMINEN

19 artikla

Standardointi

1. Jäsenvaltioiden on 14 artiklan 1 ja 2 kohdan sekä 16 artiklan 1 ja 2 kohdan johdonmukaisen täytäntöönpanon edistämiseksi kannustettava käyttämään verkko- ja tietojärjestelmien turvallisuuden kannalta merkityksellisiä eurooppalaisia tai kansainvälisesti hyväksyttyjä standardeja ja eritelmiä ilman, että ne määräävät käyttämään jotain tiettyä teknologiaa tai harjoittavat syrjintää jonkin tietyn teknologian käytön suosimiseksi.

2. ENISA antaa yhteistyössä jäsenvaltioiden kanssa neuvoja ja suuntaviivoja teknisistä aloista, joita on tarkasteltava 1 kohdan soveltamiseksi, sekä jo olemassa olevista standardeista, mukaan lukien jäsenvaltioiden kansalliset standardit, millä varmistetaan se, että nämä alat kuuluvat tarkastelun piiriin.

20 artikla

Vapaaehtoinen ilmoittaminen

1. Toimijat, joita ei ole määritetty keskeisten palvelujen tarjoajiksi ja jotka eivät ole digitaalisen palvelun tarjoajia, voivat vapaaehtoisuuteen perustuen ilmoittaa poikkeamista, joilla on merkittävä vaikutus niiden tarjoamien palvelujen jatkuvuuteen, sanotun kuitenkaan rajoittamatta 3 artiklan soveltamista.

2. Kun jäsenvaltiot käsittelevät ilmoituksia, niiden on noudatettava 14 artiklassa säädettyä menettelyä. Jäsenvaltiot voivat antaa etusijan pakollisten ilmoitusten käsittelylle vapaaehtoisten ilmoitusten käsittelyyn nähden. Vapaaehtoiset ilmoitukset käsitellään ainoastaan, jos tällainen käsittely ei muodosta kohtuutonta tai aiheetonta rasitusta kyseessä oleville jäsenvaltioille.

Vapaaehtoinen ilmoittaminen ei saa johtaa sellaisten velvollisuuksien asettamiseen ilmoittavalle toimijalle, joita siihen ei olisi sovellettu, jos se ei olisi antanut kyseistä ilmoitusta.

VII LUKU

LOPPUSÄÄNNÖKSET

21 artikla

Seuraamukset

Jäsenvaltioiden on säädettävä tämän direktiivin nojalla annettujen kansallisten säännösten rikkomiseen sovellettavista seuraamuksista ja toteutettava kaikki tarvittavat toimenpiteet sen varmistamiseksi, että ne pannaan täytäntöön. Säädettyjen seuraamusten on oltava tehokkaita, oikeasuhteisia ja varoittavia. Jäsenvaltioiden on annettava komissiolle tiedoksi nämä säännökset ja toimenpiteet viimeistään 9 päivänä toukokuuta 2018 ja ilmoitettava sille niihin vaikuttavista myöhemmistä muutoksista viipymättä.

22 artikla

Komiteamenettely

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

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

23 artikla

Uudelleentarkastelu

1. Komissio toimittaa Euroopan parlamentille ja neuvostolle viimeistään 9 päivänä toukokuuta 2019 kertomuksen, jossa arvioidaan jäsenvaltioiden lähestymistapojen yhdenmukaisuutta keskeisten palvelujen tarjoajien määrittämisessä.

2. Komissio tarkastelee määräajoin uudelleen tämän direktiivin toimivuutta ja laatii kertomuksen Euroopan parlamentille ja neuvostolle. Tätä tarkoitusta varten sekä strategisen ja operatiivisen yhteistyön edistämiseksi edelleen komissio ottaa huomioon yhteistyöryhmän ja CSIRT-verkoston raportit strategisella ja operatiivisella tasolla saaduista kokemuksista. Komissio arvioi uudelleentarkastelussaan myös liitteissä II ja III olevia luetteloja sekä liitteessä II tarkoitettujen toimialojen keskeisten palvelujen tarjoajien ja palvelujen määrittämisen yhdenmukaisuutta. Ensimmäinen kertomus annetaan viimeistään 9 päivänä toukokuuta 2021.

24 artikla

Siirtymätoimenpiteet

1. Jotta jäsenvaltioille annettaisiin lisämahdollisuuksia asianmukaiseen yhteistyöhön määräaikana, jonka kuluessa direktiivi on saatettava osaksi kansallista lainsäädäntöä, yhteistyöryhmän on aloitettava 11 artiklan 3 kohdassa vahvistettujen tehtävien suorittaminen ja CSIRT-verkoston on aloitettava 12 artiklan 3 kohdassa vahvistettujen tehtävien suorittaminen viimeistään 9 päivänä helmikuuta 2017, sanotun kuitenkaan rajoittamatta 25 artiklan soveltamista.

2. Jäsenvaltioiden tukemiseksi yhdenmukaisen lähestymistavan soveltamisessa keskeisten palvelujen tarjoajien määrittämisprosessissa yhteistyöryhmän on 9 päivän helmikuuta 2017 ja 9 päivän marraskuuta 2018 välisenä aikana keskusteltava niiden kansallisten toimenpiteiden etenemisestä, sisällöstä ja tyypistä, joiden avulla voidaan määrittää tietyn toimialan keskeisten palvelujen tarjoajat 5 ja 6 artiklassa vahvistettujen kriteerien mukaisesti. Yhteistyöryhmän on jäsenvaltion pyynnöstä keskusteltava myös kyseisen jäsenvaltion erityisistä ehdotuksista kansallisiksi toimenpiteiksi, joiden avulla voidaan määrittää tietyn toimialan keskeisten palvelujen tarjoajat 5 ja 6 artiklassa vahvistettujen kriteerien mukaisesti.

3. Tämän artiklan soveltamiseksi jäsenvaltioiden on varmistettava asianmukainen edustus yhteistyöryhmässä ja CSIRT-verkostossa viimeistään 9 päivänä helmikuuta 2017.

25 artikla

Saattaminen osaksi kansallista lainsäädäntöä

1. Jäsenvaltioiden on annettava ja julkaistava tämän direktiivin noudattamisen edellyttämät lait, asetukset ja hallinnolliset määräykset viimeistään 9 päivänä toukokuuta 2018. Niiden on viipymättä ilmoitettava tästä komissiolle.

Niiden on sovellettava näitä säädöksiä 10 päivästä toukokuuta 2018.

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.

26 artikla

Voimaantulo

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

27 artikla

Osoitus

Tämä direktiivi on osoitettu kaikille jäsenvaltioille.

Tehty Strasbourgissa 6 päivänä heinäkuuta 2016.

Euroopan parlamentin puolesta	*Neuvoston puolesta*
Puhemies	*Puheenjohtaja*
M. SCHULZ	I. KORČOK

LIITE I

TIETOTURVALOUKKAUKSIIN REAGOIVIA JA NIITÄ TUTKIVIA YKSIKÖITÄ (COMPUTER SECURITY INCIDENT RESPONSE TEAMS, JÄLJEMPÄNÄ 'CSIRT-TOIMIJAT') KOSKEVAT VAATIMUKSET JA TEHTÄVÄT

CSIRT-toimijoita koskevat vaatimukset ja tehtävät on määriteltävä riittävällä tavalla ja selkeästi, ja niiden on perustuttava kansalliseen politiikkaan ja/tai sääntelyyn. Niihin on sisällyttävä seuraavat:

1) CSIRT-toimijoita koskevat vaatimukset:

   a) CSIRT-toimijoiden on varmistettava viestintäpalvelujensa kattava saatavuus välttämällä yksittäisiä pisteitä, joiden toimintahäiriö keskeyttäisi koko palvelun, ja niiden on pidettävä käytössä useita kanavia, joiden kautta niihin voidaan ottaa yhteyttä ja joiden kautta ne itse voivat ottaa yhteyttä muualle milloin tahansa. Viestintäkanavat on lisäksi määritettävä selkeästi, ja niiden on oltava hyvin käyttäjien ja yhteistyökumppanien tiedossa.

   b) CSIRT-toimijoiden toimitilat ja niitä tukevat tietojärjestelmät on sijoitettava suojattuihin paikkoihin.

   c) Toiminnan jatkuvuus:

      i) CSIRT-toimijoilla on oltava tarkoituksenmukainen järjestelmä pyyntöjen käsittelyä ja reititystä varten tapauksen edelleenohjauksen helpottamiseksi.

      ii) CSIRT-toimijoilla on oltava riittävä henkilöstö, jotta ne voivat olla käytettävissä jatkuvasti.

      iii) CSIRT-toimijoilla on oltava tukenaan infrastruktuuri, jonka jatkuvuus on varmistettu. Tätä varten on oltava käytettävissä varmistetut järjestelmät ja varatyöskentelytilat.

   d) CSIRT-toimijoilla on oltava mahdollisuus halutessaan osallistua kansainvälisiin yhteistyöverkostoihin.

2) CSIRT-toimijoiden tehtävät:

   a) CSIRT-toimijoiden tehtäviin on sisällyttävä vähintään seuraavat:

      i) poikkeamien seuranta kansallisella tasolla;

      ii) ennakkovaroitusten, varoitusten ja tiedotusten antaminen sekä tiedon levittäminen riskeistä ja poikkeamista asiaankuuluville sidosryhmille;

      iii) poikkeamiin reagointi;

      iv) dynaamisen riskin ja poikkeamien analysointi sekä tilannetietoisuus;

      v) CSIRT-verkostoon osallistuminen.

   b) CSIRT-toimijoiden on luotava yhteistyösuhteita yksityiseen sektoriin.

   c) Yhteistyön helpottamiseksi CSIRT-toimijoiden on edistettävä yhteisten tai standardoitujen toimintatapojen omaksumista ja käyttöä

      i) poikkeamien ja riskien käsittelymenettelyissä;

      ii) poikkeamien, riskien ja tietojen luokittelujärjestelmissä.

LIITE II

4 ARTIKLAN 4 KOHDASSA TARKOITETTUJEN TOIMIJOIDEN TYYPIT

Toimiala	Osa-alue	Toimijan tyyppi
1. Energia	a) Sähkö	— Sähköalan yritykset, sellaisina kuin ne määritellään Euroopan parlamentin ja neuvoston direktiivin 2009/72/EY ([1]) 2 artiklan 35 kohdassa, jotka harjoittavat kyseisen direktiivin 2 artiklan 19 kohdassa määriteltyä toimitusta
		— Jakeluverkonhaltijat, sellaisina kuin ne määritellään direktiivin 2009/72/EY 2 artiklan 6 kohdassa
		— Siirtoverkonhaltijat, sellaisina kuin ne määritellään direktiivin 2009/72/EY 2 artiklan 4 kohdassa
	b) Öljy	— Öljynsiirtoputkistojen haltijat
		— Öljyn tuotanto-, jalostus- ja käsittelylaitteistojen haltijat sekä öljyn varastointia ja siirtoa hoitavat operaattorit
	c) Kaasu	— Maakaasun toimittajat, sellaisina kuin ne määritellään Euroopan parlamentin ja neuvoston direktiivin 2009/73/EY ([2]) 2 artiklan 8 kohdassa
		— Jakeluverkonhaltijat, sellaisina kuin ne määritellään direktiivin 2009/73/EY 2 artiklan 6 kohdassa
		— Siirtoverkonhaltijat, sellaisina kuin ne määritellään direktiivin 2009/73/EY 2 artiklan 4 kohdassa
		— Varastointilaitteiston haltijat, sellaisina kuin ne määritellään direktiivin 2009/73/EY 2 artiklan 10 kohdassa
		— Nesteytetyn maakaasun käsittelylaitteiston haltijat, sellaisina kuin ne määritellään direktiivin 2009/73/EY 2 artiklan 12 kohdassa
		— Maakaasualan yritykset, sellaisina kuin ne määritellään direktiivin 2009/73/EY 2 artiklan 1 kohdassa
		— Maakaasun jalostus- ja käsittelylaitteistojen haltijat
2. Liikenne	a) Lentoliikenne	— Lentoliikenteen harjoittajat, sellaisina kuin ne määritellään Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 300/2008 ([3]) 3 artiklan 4 kohdassa
		— Lentoaseman pitäjät, sellaisina kuin ne määritellään Euroopan parlamentin ja neuvoston direktiivin 2009/12/EY ([4]) 2 artiklan 2 kohdassa, lentoasemat, sellaisina kuin ne määritellään kyseisen direktiivin 2 artiklan 1 kohdassa, mukaan lukien Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 1315/2013 ([5]) liitteessä II olevassa 2 jaksossa luetellut ydinlentoasemat, sekä lentoasemilla sijaitsevia lisärakennelmia ja -laitteita hoitavat toimijat

Toimiala	Osa-alue	Toimijan tyyppi
		— Liikenteenhallinnan ylläpitäjät, jotka tarjoavat lennonjohtopalvelua, sellaisena kuin se määritellään Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 549/2004 ([6]) 2 artiklan 1 kohdassa
	b) Rautatieliikenne	— Rataverkon haltijat, sellaisina kuin ne määritellään Euroopan parlamentin ja neuvoston direktiivin 2012/34/EU ([7]) 3 artiklan 2 kohdassa
		— Rautatieyritykset, sellaisina kuin ne määritellään direktiivin 2012/34/EU 3 artiklan 1 kohdassa, mukaan lukien palvelupaikan ylläpitäjät, sellaisina kuin ne määritellään direktiivin 2012/34/EU 3 artiklan 12 kohdassa
	c) Vesiliikenne	— Sisävesillä, merillä ja rannikoilla matkustaja- ja rahtiliikennettä hoitavat yhtiöt, sellaisina kuin ne määritellään meriliikennettä varten Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 725/2004 ([8]) liitteessä I, lukuun ottamatta noiden yhtiöiden liikennöimiä yksittäisiä aluksia
		— Euroopan parlamentin ja neuvoston direktiivin 2005/65/EY ([9]) 3 artiklan 1 kohdassa määriteltyjen satamien hallinnointielimet, mukaan lukien niiden satamarakenteet, sellaisina kuin ne määritellään asetuksen (EY) N:o 725/2004 2 artiklan 11 kohdassa, sekä toimijat, jotka huolehtivat tuotantolaitoksista ja laitteista satamien alueella
		— Euroopan parlamentin ja neuvoston direktiivin 2002/59/EY ([10]) 3 artiklan o alakohdassa määriteltyjen alusliikennepalvelujen tarjoajat
	d) Tieliikenne	— Tieviranomaiset, sellaisina kuin ne määritellään komission delegoidun asetuksen (EU) 2015/962 ([11]) 2 artiklan 12 kohdassa, jotka vastaavat liikenteenhallinnasta
		— Euroopan parlamentin ja neuvoston direktiivin 2010/40/EU ([12]) 4 artiklan 1 kohdassa määriteltyjen älykkäiden liikennejärjestelmien ylläpitäjät
3. Pankkiala		Luottolaitokset, sellaisina kuin ne määritellään Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 575/2013 ([13]) 4 artiklan 1 kohdassa
4. Finanssimarkkinoiden infrastruktuurit		— Euroopan parlamentin ja neuvoston direktiivin 2014/65/EU ([14]) 4 artiklan 24 kohdassa määriteltyjen kauppapaikkojen ylläpitäjät
		— Keskusvastapuolet, sellaisina kuin ne määritellään Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 648/2012 ([15]) 2 artiklan 1 kohdassa
5. Terveydenhuoltoala	Terveydenhuoltolaitokset (mukaan lukien sairaalat ja yksityisklinikat)	Terveydenhuollon tarjoajat, sellaisina kuin ne määritellään Euroopan parlamentin ja neuvoston direktiivin 2011/24/EU ([16]) 3 artiklan g alakohdassa

Toimiala	Osa-alue	Toimijan tyyppi
6. Juomaveden toimittaminen ja jakelu		Neuvoston direktiivin 98/83/EY ([17]) 2 artiklan 1 kohdan a alakohdassa määritellyn ihmisten käyttöön tarkoitetun veden toimittajat ja jakelijat, lukuun ottamatta jakelijoita, joille ihmisten käyttöön tarkoitetun veden jakelu on ainoastaan osa niiden yleistä toimintaa, joka muodostuu sellaisten muiden hyödykkeiden ja tavaroiden jakelusta, joita ei katsota keskeisiksi palveluiksi.
7. Digitaalinen infrastruktuuri		— IXP:t
		— Nimipalvelujen tarjoajat
		— Aluetunnusrekisterit

([1]) Euroopan parlamentin ja neuvoston direktiivi 2009/72/EY, annettu 13 päivänä heinäkuuta 2009, sähkön sisämarkkinoita koskevista yhteisistä säännöistä ja direktiivin 2003/54/EY kumoamisesta (EUVL L 211, 14.8.2009, s. 55).
([2]) Euroopan parlamentin ja neuvoston direktiivi 2009/73/EY, annettu 13 päivänä heinäkuuta 2009, maakaasun sisämarkkinoita koskevista yhteisistä säännöistä ja direktiivin 2003/55/EY kumoamisesta (EUVL L 211, 14.8.2009, s. 94).
([3]) Euroopan parlamentin ja neuvoston asetus (EY) N:o 300/2008, annettu 11 päivänä maaliskuuta 2008, yhteisistä siviili-ilmailun turvaamista koskevista säännöistä ja asetuksen (EY) N:o 2320/2002 kumoamisesta (EUVL L 97, 9.4.2008, s. 72).
([4]) Euroopan parlamentin ja neuvoston direktiivi 2009/12/EY, annettu 11 päivänä maaliskuuta 2009, lentoasemamaksuista (EUVL L 70, 14.3.2009, s. 11).
([5]) Euroopan parlamentin ja neuvoston asetus (EU) N:o 1315/2013, annettu 11 päivänä joulukuuta 2013, unionin suuntaviivoista Euroopan laajuisen liikenneverkon kehittämiseksi ja päätöksen N:o 661/2010/EU kumoamisesta (EUVL L 348, 20.12.2013, s. 1).
([6]) Euroopan parlamentin ja neuvoston asetus (EY) N:o 549/2004, annettu 10 päivänä maaliskuuta 2004, yhtenäisen eurooppalaisen ilmatilan toteuttamisen puitteista (puiteasetus) (EUVL L 96, 31.3.2004, s. 1).
([7]) Euroopan parlamentin ja neuvoston direktiivi 2012/34/EU, annettu 21 päivänä marraskuuta 2012, yhtenäisestä eurooppalaisesta rautatiealueesta (EUVL L 343, 14.12.2012, s. 32).
([8]) Euroopan parlamentin ja neuvoston asetus (EY) N:o 725/2004, annettu 31 päivänä maaliskuuta 2004, alusten ja satamarakenteiden turvatoimien parantamisesta (EUVL L 129, 29.4.2004, s. 6).
([9]) Euroopan parlamentin ja neuvoston direktiivi 2005/65/EY, annettu 26 päivänä lokakuuta 2005, satamien turvallisuuden parantamisesta (EUVL L 310, 25.11.2005, s. 28).
([10]) Euroopan parlamentin ja neuvoston direktiivi 2002/59/EY, annettu 27 päivänä kesäkuuta 2002, alusliikennettä koskevan yhteisön seuranta- ja tietojärjestelmän perustamisesta sekä neuvoston direktiivin 93/75/ETY kumoamisesta (EYVL L 208, 5.8.2002, s. 10).
([11]) Komission delegoitu asetus (EU) 2015/962, annettu 18 päivänä joulukuuta 2014, Euroopan parlamentin ja neuvoston direktiivin 2010/40/EU täydentämisestä EU:n laajuisten tosiaikaisten liikennetietopalvelujen tarjoamisen osalta (EUVL L 157, 23.6.2015, s. 21).
([12]) Euroopan parlamentin ja neuvoston direktiivi 2010/40/EU, annettu 7 päivänä heinäkuuta 2010, tieliikenteen älykkäiden liikennejärjestelmien käyttöönoton sekä tieliikenteen ja muiden liikennemuotojen rajapintojen puitteista (EUVL L 207, 6.8.2010, s. 1).
([13]) Euroopan parlamentin ja neuvoston asetus (EU) N:o 575/2013, annettu 26 päivänä kesäkuuta 2013, luottolaitosten ja sijoituspalveluyritysten vakavaraisuusvaatimuksista ja asetuksen (EU) N:o 648/2012 muuttamisesta (EUVL L 176, 27.6.2013, s. 1).
([14]) Euroopan parlamentin ja neuvoston direktiivi 2014/65/EU, annettu 15 päivänä toukokuuta 2014, rahoitusvälineiden markkinoista sekä direktiivin 2002/92/EY ja direktiivin 2011/61/EU muuttamisesta (EUVL L 173, 12.6.2014, s. 349).
([15]) Euroopan parlamentin ja neuvoston asetus (EU) N:o 648/2012, annettu 4 päivänä heinäkuuta 2012, OTC-johdannaisista, keskusvastapuolista ja kauppatietorekistereistä (EUVL L 201, 27.7.2012, s. 1).
([16]) Euroopan parlamentin ja neuvoston direktiivi 2011/24/EU, annettu 9 päivänä maaliskuuta 2011, potilaiden oikeuksien soveltamisesta rajatylittävässä terveydenhuollossa (EUVL L 88, 4.4.2011, s. 45).
([17]) Neuvoston direktiivi 98/83/EY, annettu 3 päivänä marraskuuta 1998, ihmisten käyttöön tarkoitetun veden laadusta (EYVL L 330, 5.12.1998. s. 32).

LIITE III

4 ARTIKLAN 5 KOHDASSA TARKOITETTUJEN DIGITAALISTEN PALVELUJEN TYYPIT

1. Verkossa toimiva markkinapaikka.

2. Verkossa toimiva hakukone.

3. Pilvipalvelu.

ISSN 1977-0812 (sähköinen julkaisu)
ISSN 1725-261X (painettu julkaisu)

Euroopan unionin julkaisutoimisto
2985 Luxemburg
LUXEMBURG

FI