EUROOPAN
KOMISSIO

Bryssel 4.10.2017
COM(2017) 476 final

ANNEX 1

NOTE
This language version reflects the corrections done to the original EN version transmitted under COM(2017) 476 final of 13.9.2017 and retransmitted (with corrections) under COM(2017) 476 final/2 of 4.10.2017

LIITE

asiakirjaan

KOMISSION TIEDONANTO EUROOPAN PARLAMENTILLE JA NEUVOSTOLLE

Suurin hyöty verkko- ja tietoturvadirektiivistä – toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa annetun direktiivin (EU) 2016/1148 tehokas täytäntöönpano

SISÄLLYSLUETTELO

LIITE 4

1. Johdanto 4

2. Verkko- ja tietojärjestelmien turvallisuutta koskeva kansallinen strategia 5

2.1 Kansallisen strategian soveltamisala 5

2.2 Kansallisten strategioiden sisältö ja hyväksymismenettely 6

2.3 Prosessi ja käsiteltävät kysymykset 6

2.4 Konkreettiset toimet, jotka jäsenvaltioiden on toteutettava ennen kansallisen lainsäädännön osaksi saattamisen määräaikaa 9

3. Verkko- ja tietoturva-direktiivi: kansalliset toimivaltaiset viranomaiset, keskitetyt yhteyspisteet ja tietoturvaloukkauksiin reagoivat ja niitä tutkivat yksiköt (CSIRT-toimijat) 10

3.1 Viranomaistyyppi 11

3.2 Julkisuus ja muut merkitykselliset näkökohdat 12

3.3 Verkko- ja tietoturvadirektiivin 9 artikla: tietoturvaloukkauksiin reagoivat ja niitä tutkivat yksiköt (CSIRT-toimijat) 17

3.4 Tehtävät ja vaatimukset 17

3.5 Avunanto CSIRT-toimijoiden kehittämisessä 18

3.6 Keskitetyn yhteyspisteen rooli 19

3.7 Seuraamukset 20

4. Toimijat, joita koskevat turvallisuusvaatimuksia ja poikkeamista ilmoittamista koskevat velvollisuudet 20

4.1 Keskeisten palvelujen tarjoajat 21

4.1.1 Verkko- ja tietoturvadirektiivin liitteessä II luetellut toimijoiden tyypit 21

4.1.2 Keskeisten palvelujen tarjoajien määrittäminen 23

4.1.3 Vaatimusten soveltaminen muihin toimialoihin 23

4.1.4 Lainkäyttövalta 24

4.1.5 Komissiolle toimitettavat tiedot 25

4.1.6 Kuinka määritysprosessi toteutetaan? 25

4.1.7 Rajat ylittävä kuulemisprosessi 31

4.2. Turvallisuusvaatimukset 31

4.3 Ilmoitusvaatimukset 32

4.4 Verkko- ja tietoturvadirektiivin liite III: digitaalisen palvelun tarjoajat 32

4.4.1 Digitaalisen palvelun tarjoajien tyypit 33

4.4.2 Turvallisuusvaatimukset 35

4.4.3 Ilmoitusvaatimukset 36
4.4.4 Riskiperusteinen lähestymistapa sääntelyyn 36
4.4.5 Lainkäyttövalta 37
4.4.6 Pienten digitaalisen palvelun tarjoajien vapauttaminen turvallisuus- ja ilmoitusvaatimusten noudattamisesta 37
5. Verkko- ja tietoturvadirektiivin suhde muuhun lainsäädäntöön 37
5.1 Verkko- ja tietoturvadirektiivin 1 artiklan 7 kohta: alakohtaisia säädöksiä koskeva säännös 37
5.2 Verkko- ja tietoturvadirektiivin 1 artiklan 3 kohta: televiestintäpalvelujen tarjoajat ja luottamuspalvelun tarjoajat 41
6. Julkaistut kansalliset kyberturvallisuusstrategia-asiakirjat 43
7. ENISAn julkaisemat hyvät käytännöt ja suositukset 46

LIITE

1. Johdanto

Tällä liitteellä pyritään edistämään verkko- ja tietojärjestelmien turvallisuudesta unionissa annetun direktiivin (EU) 2016/1148[1] (jäljempänä ’verkko- ja tietoturvadirektiivi’ tai ’direktiivi’) tehokasta soveltamista, täytäntöönpanoa ja täytäntöönpanon valvontaa ja auttamaan jäsenvaltioita varmistamaan, että EU:n lainsäädäntöä sovelletaan tosiasiallisesti. Sillä on erityisesti kolme tavoitetta: a) selventää kansallisille viranomaisille direktiiviin sisältyviä näihin viranomaisiin sovellettavia velvollisuuksia, b) varmistaa niiden direktiivin velvollisuuksien täytäntöönpanon tehokas valvonta, joita sovelletaan toimijoihin, joita koskevat turvallisuusvaatimuksia ja poikkeamista ilmoittamista koskevat velvollisuudet, ja c) edistää yleisesti oikeusvarmuutta kaikkien asianomaisten toimijoiden kannalta.

Tätä varten tässä liitteessä annetaan ohjeita seuraavista näkökohdista, jotka ovat keskeisiä, jotta voidaan saavuttaa verkko- ja tietoturvadirektiivin tavoite eli varmistaa yhteiskunnan ja talouden toimintaa tukevien verkko- ja tietojärjestelmien yhteinen korkea turvallisuustaso unionissa:

- jäsenvaltioiden velvollisuus hyväksyä verkko- ja tietojärjestelmien turvallisuutta koskeva kansallinen strategia (2 jakso);
- kansallisten toimivaltaisten viranomaisten, keskitettyjen yhteyspisteiden ja tietoturvaloukkauksiin reagoivien ja niitä tutkivien yksiköiden perustaminen (3 jakso);
- keskeisten palvelujen tarjoajia ja digitaalisen palvelun tarjoajia koskevat turvallisuus- ja ilmoitusvaatimukset (4 jakso); ja
- verkko- ja tietoturvadirektiivin suhde muuhun lainsäädäntöön (5 jakso).

Komissio on hyödyntänyt näiden ohjeiden laadinnassa direktiivin valmistelun aikana kerättyjä tietoja ja analyyseja sekä Euroopan verkko- ja tietoturvaviraston (ENISA) ja yhteistyöryhmän panosta. Lisäksi se on hyödyntänyt tiettyjen jäsenvaltioiden kokemuksia. Komissio on tarvittaessa ottanut huomioon EU:n lainsäädännön tulkinnan perusperiaatteet eli verkko- ja tietoturvadirektiivin sanamuodon, asiayhteyden ja tavoitteet. Koska direktiiviä ei ole vielä saatettu osaksi kansallista lainsäädäntöä, siitä ei ole myöskään annettu Euroopan unionin tuomioistuimen tai kansallisten tuomioistuinten ratkaisuja. Oikeuskäytäntöä ei siis voida käyttää ohjeistuksena.

Näiden tietojen kokoaminen yhdeksi asiakirjaksi antaa jäsenvaltiolle hyvän yleiskuvan direktiivistä, ja ne voivat ottaa nämä tiedot huomioon kansallista lainsäädäntöä laatiessaan. Samalla komissio korostaa, että tämä liite ei ole sitova eikä sillä ole tarkoitus luoda uusia sääntöjä. Unionin tuomioistuimella on lopullinen toimivalta tulkita EU:n lainsäädäntöä.

[1] Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/1148, annettu 6 päivänä heinäkuuta 2016, toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa. Direktiivi tuli voimaan 8. elokuuta 2016.

2. Verkko- ja tietojärjestelmien turvallisuutta koskeva kansallinen strategia

Verkko- ja tietoturvadirektiivin 7 artiklan mukaan jäsenvaltioiden on hyväksyttävä verkko- ja tietojärjestelmien turvallisuutta koskeva kansallinen strategia. Tätä voidaan kutsua myös nimellä kansallinen kyberturvallisuusstrategia. Kansallisessa strategiassa on tarkoitus määritellä kyberturvallisuuteen liittyvät strategiset tavoitteet sekä asianmukaiset toimintapoliittiset toimenpiteet ja sääntelytoimenpiteet. Kansallisen kyberturvallisuusstrategian käsitettä käytetään yleisesti kansainvälisesti ja Euroopassa. Näin on ollut etenkin ENISAn yhdessä jäsenvaltioiden kanssa toteuttamassa kansallisia strategioita koskevassa työssä, jonka pohjalta on hiljattain julkaistu ajan tasalle saatettu kansallisia kyberturvallisuusstrategioita koskeva hyvien käytäntöjen opas[2].

Komissio kuvaa tässä jaksossa, kuinka verkko- ja tietoturvadirektiivi parantaa jäsenvaltioiden varautumista, kun siinä edellytetään, että jäsenvaltioilla on käytössä verkko- ja tietojärjestelmien turvallisuutta koskevat vankat kansalliset strategiat (7 artikla). Tässä jaksossa käsitellään seuraavia näkökohtia: a) strategian soveltamisala ja b) strategian sisältö ja hyväksymismenettely.

Kuten jäljempänä kuvataan, verkko- ja tietoturvadirektiivin 7 artiklan moitteeton saattaminen osaksi kansallista lainsäädäntöä on olennaisen tärkeää, jotta direktiivin tavoitteet voidaan saavuttaa, ja se edellyttää riittävien taloudellisten ja henkilöstöresurssien osoittamista tähän tarkoitukseen.

2.1 Kansallisen strategian soveltamisala

Direktiivin 7 artiklan sanamuodon mukaan velvollisuus hyväksyä kansallinen kyberturvallisuusstrategia koskee ainoastaan direktiivin liitteessä II tarkoitettuja toimialoja (eli energia, liikenne, pankkiala, finanssimarkkinat, terveydenhuolto, juomaveden toimittaminen ja jakelu sekä digitaalinen infrastruktuuri) ja liitteessä III tarkoitettuja palveluja (verkossa toimivat markkinapaikat, verkossa toimivat hakukoneet ja pilvipalvelut).

Direktiivin 3 artiklassa esitetään nimenomaisesti vähimmäistason yhdenmukaistamisen periaate, jonka mukaan jäsenvaltiot voivat hyväksyä tai pitää voimassa säännöksiä, joiden tarkoituksena on saavuttaa korkeatasoisempi verkko- ja tietojärjestelmien turvallisuus. Tämän periaatteen soveltaminen kansallisen kyberturvallisuusstrategian hyväksymisvelvollisuuteen antaa jäsenvaltioille mahdollisuuden sisällyttää strategiaan muita toimialoja ja palveluja direktiivin liitteissä II ja III mainittujen lisäksi.

Kun otetaan huomioon verkko- ja tietoturvadirektiivin tavoite eli yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden saavuttaminen unionissa[3], komission mielestä olisi suositeltavaa laatia kansallinen strategia, joka kattaa kaikki yhteiskunnan ja talouden merkitykselliset osa-alueet eikä ainoastaan direktiivin liitteessä II mainittuja toimialoja ja liitteessä III mainittuja digitaalisia palveluja. Tämä on kansainvälisten parhaiden käytäntöjen

[2] ENISA, *National Cyber-Security Strategy Good Practice* (2016). Saatavilla osoitteessa https://www.enisa.europa.eu/publications/ncss-good-practice-guide

[3] Ks. 1 artiklan 1 kohta.

(ks. jäljempänä mainitut ITUn ohjeet ja OECD:n analyysi) ja verkko- ja tietoturvadirektiivin mukaista.

Kuten jäljempänä selitetään tarkemmin, tämä koskee erityisesti julkishallintoja, jotka vastaavat muista kuin direktiivin liitteissä II ja III luetelluista toimialoista ja palveluista. Julkishallinnot voivat käsitellä arkaluonteisia tietoja, mikä oikeuttaa niiden sisällyttämisen kansalliseen kyberturvallisuusstrategiaan ja hallintasuunnitelmiin, joilla estetään vuodot ja varmistetaan näiden tietojen riittävä suoja.

2.2 Kansallisten strategioiden sisältö ja hyväksymismenettely

Verkko- ja tietoturvadirektiivin 7 artiklan mukaan kansallisessa kyberturvallisuusstrategiassa on käsiteltävä ainakin seuraavia kysymyksiä:

i) verkko- ja tietojärjestelmien turvallisuutta koskevan kansallisen strategian tavoitteet ja painopisteet;
ii) ohjauskehys kansallisen strategian tavoitteiden ja painopisteiden saavuttamiseksi;
iii) varautumiskykyyn, reagointiin ja toimintakunnon palauttamiseen liittyvien toimenpiteiden yksilöinti, mukaan lukien julkisen ja yksityisen sektorin välinen yhteistyö;
iv) tiedot asiaan liittyvistä opetus-, valistus- ja koulutusohjelmista;
v) tiedot tutkimus- ja kehityssuunnitelmista;
vi) riskinarviointisuunnitelma riskien yksilöimiseksi; ja
vii) luettelo strategian täytäntöönpanoon osallistuvista toimijoista.

Direktiivin 7 artiklassa tai siihen liittyvässä johdanto-osan 29 kappaleessa ei tarkenneta kansallisen kyberturvallisuusstrategian hyväksymistä koskevia vaatimuksia tai määritellä tarkemmin strategian sisältöä. Itse prosessin ja strategian sisältöön liittyvien lisätekijöiden osalta komissio katsoo, että jäljempänä esitelty lähestymistapa on yksi sopiva tapa hyväksyä kansallinen kyberturvallisuusstrategia. Tämä perustuu analyysiin niistä kokemuksista, joita jäsenvaltiot ja kolmannet maat ovat saaneet omien strategioidensa laatimisesta. Yksi tietolähde on kansallisia kyberturvallisuusstrategioita koskeva ENISAn koulutusväline, joka on saatavilla videoina ja ladattavana mediana ENISAn verkkosivuilla[4].

2.3 Prosessi ja käsiteltävät kysymykset

Kansallisen strategian laatimis- ja hyväksymisprosessi on monimutkainen ja monitahoinen, ja sen tehokkuus ja onnistuminen edellyttää kyberturvallisuusasiantuntijoiden, kansalaisyhteiskunnan ja kansallisen poliittisen prosessin kestävää sitoutumista. Sen välttämätön edellytys on vähintään valtiosihteeri- tai vastaavan tason korkea hallinnollinen tuki asiasta vastaavassa ministeriössä. Prosessi vaatii myös poliittista tukea. Kansallisen kyberturvallisuusstrategian hyväksymisessä voidaan soveltaa seuraavaa viisivaiheista prosessia (ks. kuva 1).

[4] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-training-tool

Ensimmäinen vaihe - **Strategiaan liittyvien ohjaavien periaatteiden ja strategisen tavoitteiden määrittely**

Kansallisten toimivaltaisten viranomaisten olisi ensin määriteltävä joitain kansalliseen kyberturvallisuusstrategiaan sisällytettäviä keskeisiä osatekijöitä, kuten mitkä ovat halutut tulokset, eli direktiivin sanamuodon (7 artiklan 1 kohdan a alakohta) mukaan ’*tavoitteet ja painopisteet*’, kuinka nämä tulokset täydentävät kansallista sosiaali- ja talouspolitiikkaa sekä se, sopivatko ne yhteen Euroopan unionin jäsenyydestä seuraavien oikeuksien ja velvollisuuksien kanssa. Tavoitteiden olisi oltava täsmällisiä, mitattavia, saavutettavia, realistisia ja aikasidonnaisia (SMART). Tätä voidaan havainnollistaa seuraavalla esimerkillä: ”*Varmistamme, että tämä [aikasidonnainen] strategia perustuu tarkkaan ja kattavaan mittausjärjestelmään, jonka avulla seurataan edistymistä kohti haluttuja tuloksia*.”[5]

Edellä mainittuun sisältyy myös poliittinen arviointi siitä, voidaanko strategian toteuttamiseksi saada käyttöön riittävä budjetti. Siihen sisältyy kuvaus strategian suunnitellusta soveltamisalasta ja niistä julkisen ja yksityisen sektorin sidosryhmistä, joiden pitäisi osallistua eri tavoitteiden ja toimenpiteiden luonnosteluun.

Ensimmäinen vaihe voitaisiin toteuttaa ministeriöiden johtavien virkamiesten ja poliitikkojen aihekohtaisissa työpajoissa, joita vetävät kyberalan ammattilaiset, joilla on ammatilliset viestintätaidot ja jotka voivat tuoda esiin puuttuvan tai heikon kyberturvallisuuden seuraukset nykyaikaiselle digitaaliselle taloudelle ja yhteiskunnalle.

Toinen vaihe - **Strategian sisällön laatiminen**

Strategiaan olisi sisällyttävä mahdollistavia toimenpiteitä, aikasidonnaisia toimia ja keskeisiä suorituskykyindikaattoreita, jotta sitä voidaan arvioida, tarkentaa ja parantaa määritellyn täytäntöönpanoajan jälkeen. Näillä toimenpiteillä olisi tuettava ohjaavissa periaatteissa esitettyjä tavoitteita, prioriteetteja ja tuloksia. Mahdollistavien toimenpiteiden tarve esitetään direktiivin 7 artiklan 1 kohdan c alakohdassa.

Olisi suositeltavaa perustaa asiasta vastaavan ministeriön johtama ohjausryhmä hallinnoimaan laatimisprosessia ja helpottamaan panoksen antamista siihen. Tämä voitaisiin toteuttaa perustamalla joukko asiaa käsittelevistä virkamiehistä ja asiantuntijoista koostuvia valmisteluryhmiä tarkastelemaan keskeisiä yleisiä teemoja, kuten riskinarviointia, valmiussuunnittelua, poikkeamien hallintaa, osaamisen kehittämistä, tiedottamista, tutkimusta ja teollisuuden kehittämistä jne. Kutakin toimialaa (esim. energia, liikenne jne.) pyydettäisiin myös arvioimaan erikseen, mitä seurauksia olisi niiden sisällyttämisellä strategiaan, myös resurssien kannalta, ja ottamaan nimetyt keskeisten palvelujen tarjoajat ja digitaalisen palvelun tarjoajat mukaan prioriteettien määrittelemiseen ja ehdotusten esittämiseen laatimisprosessiin. Eri alojen sidosryhmien osallistuminen on olennaisen tärkeää myös kun pidetään mielessä tarve varmistaa direktiivin yhdenmukainen täytäntöönpano eri toimialoilla ottaen kuitenkin samalla huomioon alakohtaiset erityispiirteet.

[5] Lainaus Yhdistyneen kuningaskunnan kansallisesta kyberturvallisuusstrategiasta, 2016–2021, sivu 67.

Kolmas vaihe - **Ohjauskehyksen luominen**

Jotta ohjauskehys olisi tehokas ja toimiva, sen olisi perustuttava keskeisiin sidosryhmiin, laatimisprosessissa määriteltyihin prioriteetteihin sekä kansallisten hallinnollisten ja poliittisten rakenteiden luomiin rajoitteisiin ja toimintaympäristöön. Olisi suotavaa, että poliittiselle tasolle voitaisiin raportoida suoraan kehyksessä, jolla on kyky tehdä päätöksiä ja jakaa resursseja ja joka on yhteydessä kyberturvallisuusasiantuntijoihin ja teollisuuden sidosryhmiin. Direktiivin 7 artiklan 1 kohdan b alakohdassa viitataan ohjauskehykseen ja mainitaan erityisesti ”*valtion elinten ja muiden asiaankuuluvien toimijoiden tehtävät ja vastuut*”.

Neljäs vaihe - **Strategialuonnoksen kokoaminen ja uudelleentarkastelu**

Tässä vaiheessa strategialuonnos olisi koottava ja sitä olisi tarkasteltava uudelleen käyttäen vahvuuksia, heikkouksia, mahdollisuuksia ja uhkia mittaavaa analyysia (SWOT-analyysia). Analyysin perusteella voidaan määrittää, onko sisältöä tarpeellista tarkistaa. Sisäisen uudelleentarkastelun jälkeen olisi järjestettävä sidosryhmien kuuleminen. Olisi myös tärkeää järjestää julkinen kuuleminen, jotta ehdotetun strategian merkitystä voidaan korostaa suurelle yleisölle, siihen voidaan saada kaikkien mahdollisten lähteiden panos ja voidaan hakea tukea strategian toteuttamiseksi tarvittavien resurssien osoittamiselle.

Viides vaihe – **Virallinen hyväksyminen**

Viimeisessä vaiheessa strategia hyväksytään virallisesti poliittisella tasolla ja sille osoitetaan riittävä budjetti, joka heijastaa sitä, kuinka vakavasti jäsenvaltio suhtautuu kyberturvallisuuteen. Verkko- ja tietoturvadirektiivin tavoitteiden saavuttamiseksi komissio kannustaa jäsenvaltioita antamaan tietoja myös budjetista, kun ne toimittavat kansallisen strategiansa komissiolle 7 artiklan 3 kohdan mukaisesti. Budjettia ja tarvittavia henkilöstöresursseja koskevat sitoumukset ovat aivan välttämättömiä strategian ja direktiivin tehokkaan täytäntöönpanon kannalta. Koska kyberturvallisuus on edelleen suhteellisen uusi ja nopeasti kasvava julkisen politiikan ala, useimmissa tapauksissa tarvitaan uusia investointeja, vaikka julkisen talouden yleinen tilanne edellyttääkin leikkauksia ja säästöjä.

Kansallisten strategioiden laatimisprosessia ja sisältöä koskevia neuvoja on saatavilla eri julkisista ja akateemisista lähteistä, joista voidaan mainita ENISA[6], ITU[7], OECD[8], Global Forum for Cyber Expertise ja Oxfordin yliopisto[9].

---

[6] ENISA, *National Cyber-Security Strategy Good Practice* (2016). Saatavilla osoitteessa https://www.enisa.europa.eu/publications/ncss-good-practice-guide

[7] ITU, *National Cybersecurity Strategy Guide* (2011). Saatavilla osoitteessa http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf
ITU julkaisee myös oppaan ’National Cyber Security Strategy Toolkit’ vuonna 2017 (ks. esittely osoitteessa http://www.itu.int/en/ITU-D/Cybersecurity/Documents/National%20Strategy%20Toolkit%20introduction.pdf).

[8] OECD, *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies* (2012). Saatavilla osoitteessa http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

[9] Global Cyber Security Capacity Centre and University of Oxford, Global Cyber *Cybersecurity Capacity Maturity Model for Nations (CMM) - Revised Edition* (2016). Saatavilla osoitteessa

2.4 Konkreettiset toimet, jotka jäsenvaltioiden on toteutettava ennen kansallisen lainsäädännön osaksi saattamisen määräaikaa

Lähes kaikki jäsenvaltiot[10] olivat jo julkaisset kansalliseksi kyberturvallisuusstrategiaksi kutsutun asiakirjan ennen direktiivin hyväksymistä. Tämän liitteen jaksossa 6 luetellaan jäsenvaltioiden nykyisin voimassa olevat strategiat[11]. Ne sisältävät yleensä strategisia periaatteita, suuntaviivoja ja tavoitteita ja joissain tapauksissa erityisiä toimenpiteitä kyberturvallisuuteen liittyvien riskien vähentämiseksi.

Koska osa näistä strategioista oli hyväksytty ennen verkko- ja tietoturvadirektiivin hyväksymistä, ne eivät välttämättä sisällä kaikkia 7 artiklassa lueteltuja osatekijöitä. Jotta voidaan varmistaa direktiivin moitteeton saattaminen osaksi kansallista lainsäädäntöä, jäsenvaltioiden on analysoitava mahdollisia puutteita vertaamalla kansallisten kyberturvallisuusstrategioidensa sisältöä suhteessa seitsemään 7 artiklassa lueteltuun erilliseen vaatimukseen kaikilla direktiivin liitteessä II luetelluilla toimialoilla ja kaikissa liitteessä III luetelluissa palveluissa. Havaitut puutteet voidaan tämän jälkeen täyttää tarkistamalla olemassa olevaa kansallista kyberturvallisuusstrategiaa tai päättämällä kansallisen verkko- ja tietoturvastrategian periaatteiden perinpohjaisesta uudistamisesta. Edellä esitettyjä kansallisen kyberturvallisuusstrategian hyväksymisprosessia koskevia suuntaviivoja voidaan soveltaa myös olemassa olevien strategioiden tarkistamiseen tai päivittämiseen.

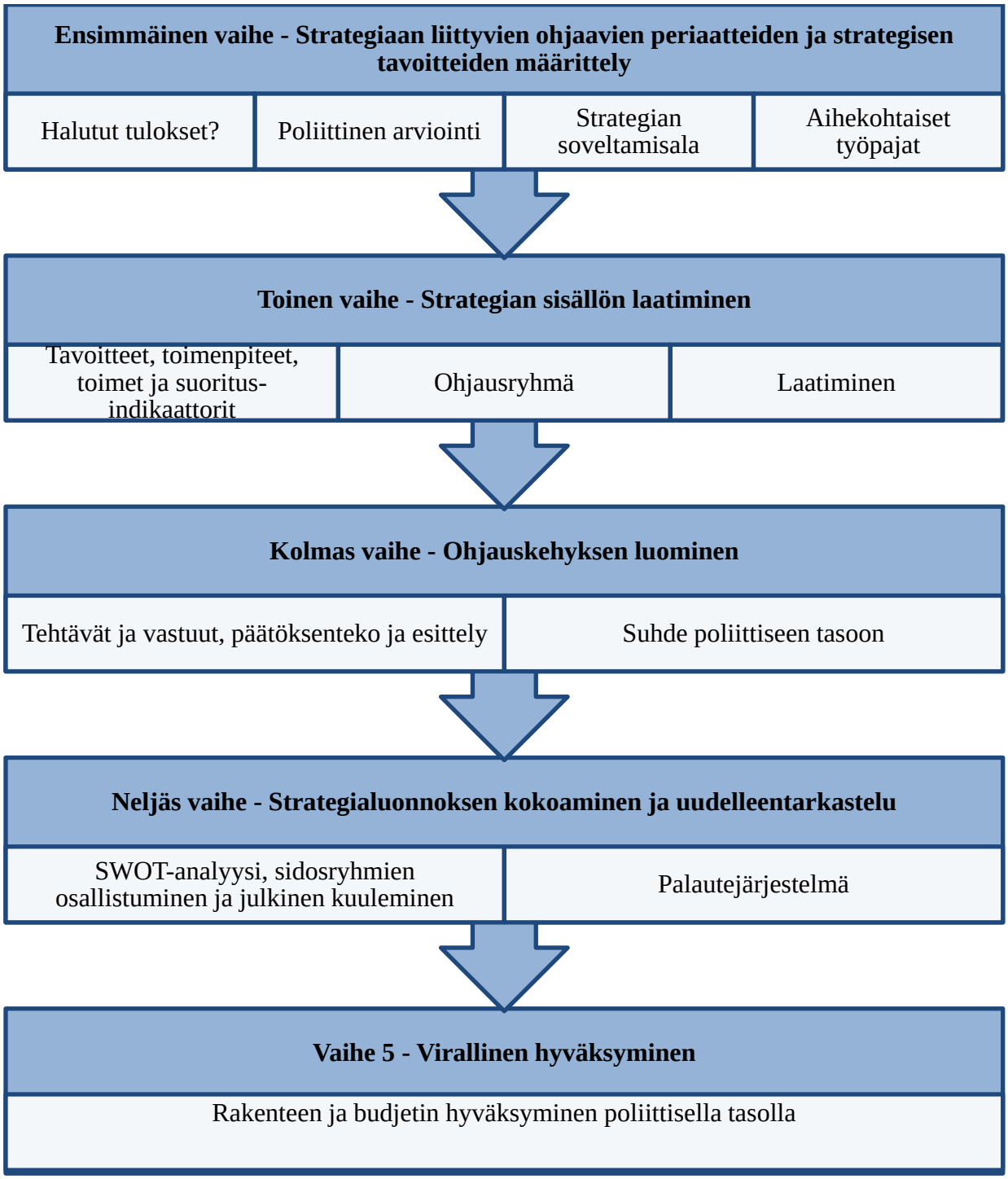
---

https://www.thegfce.com/binaries/gfce/documents/publications/2017/02/13/cybersecurity-cmm-for-nations/CMM+revised+edition.pdf

[10] Lukuun ottamatta Kreikkaa, jonka kansallinen kyberturvallisuusstrategia on ollut valmisteilla vuodesta 2014 (ks. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/national-cyber-security-strategy-greece/view).

[11] Nämä tiedot perustuvat ENISAn laatimaan yleiskatsaukseen kansallisista kyberturvallisuusstrategioista https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map

Kuva 1: Kansallisen kyberturvallisuusstrategian viisivaiheinen hyväksymisprosessi



3. Verkko- ja tietoturva-direktiivi: kansalliset toimivaltaiset viranomaiset, keskitetyt yhteyspisteet ja tietoturvaloukkauksiin reagoivat ja niitä tutkivat yksiköt (CSIRT-toimijat)

Direktiivin 8 artiklan 1 kohdan mukaan jäsenvaltioiden on nimettävä yksi tai useampi kansallinen toimivaltainen viranomainen, jonka toiminta kattaa ainakin liitteessä II tarkoitetut toimialat ja liitteessä III tarkoitetut palvelut ja jonka tehtävänä on seurata tämän direktiivin

soveltamista. Jäsenvaltiot voivat antaa tämän tehtävän olemassa olevalle viranomaiselle tai olemassa oleville viranomaisille.

Tässä jaksossa keskitytään siihen, kuinka verkko- ja tietoturvadirektiivi parantaa jäsenvaltioiden varautumista edellyttämällä, että jäsenvaltioilla on tehokkaat kansalliset toimivaltaiset viranomaiset ja tietoturvaloukkauksiin reagoivat ja niitä tutkivat yksiköt (CSIRT-toimijat). Tässä jaksossa käsitellään erityisesti velvollisuutta nimetä kansallinen toimivaltainen viranomainen sekä keskitetyn yhteyspisteen roolia. Siinä käsitellään tarkemmin kolmea aihetta: a) mahdolliset kansalliset hallintorakenteet (esim. keskitetyt ja hajautetut mallit) ja muut vaatimukset, b) keskitetyn yhteyspisteen rooli ja c) tietoturvaloukkauksiin reagoivat ja niitä tutkivat yksiköt.

3.1 Viranomaistyyppi

Verkko- ja tietoturvadirektiivin 8 artiklassa edellytetään, että jäsenvaltiot nimeävät verkko- ja tietojärjestelmien turvallisuudesta vastaavat kansalliset toimivaltaiset viranomaiset, ja siinä mainitaan nimenomaisesti mahdollisuus nimetä ’*yksi tai useampi ... kansallinen toimivaltainen viranomainen*’. Direktiivin johdanto-osan 30 kappaleessa tätä mahdollisuutta perustellaan seuraavasti: ”*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*.”

Jäsenvaltiot voivat siis valintansa mukaan nimetä joko yhden keskitetyn viranomaisen, joka käsittelee kaikkia direktiivin soveltamisalaan kuuluvia toimialoja ja palveluja, tai useita viranomaisia esimerkiksi toimialan tyypistä riippuen.

Jäsenvaltiot voivat toimintatapaansa valitessaan hyödyntää kokemuksia, joita on saatu kriittisen tietoteknisen infrastruktuurin suojaamista (CIIP) koskevan lainsäädännön yhteydessä käytetyistä kansallisista toimintamalleista. Kuten taulukossa 1 kuvataan, CIIP:n tapauksessa jäsenvaltiot ovat päättäneet omaksua joko keskitetyn tai hajautetun lähestymistavan, kun ne ovat jakaneet toimivaltaa kansallisella tasolla. Kansallisia esimerkkejä käytetään tässä ainoastaan eri vaihtoehtojen havainnollistamiseen ja olemassa olevien organisaatiokehysten tuomiseen jäsenvaltioiden tietoon. Komission tarkoituksena ei siis ole esittää, että kyseisissä maissa CIIP:n yhteydessä käytettyä mallia olisi välttämättä käytettävä verkko- ja tietoturvadirektiivin täytäntöönpanossa.

Jäsenvaltiot voivat myös valita erilaisia hybridijärjestelyjä, joihin sisältyy elementtejä sekä keskitetyistä että hajautetuista toimintamalleista. Järjestelyt voidaan sovittaa yhteen direktiivin soveltamisalaan kuuluvilla toimialoilla ja palveluissa jo käytössä olevien kansallisten hallintojärjestelyjen kanssa, tai asianomaiset viranomaiset ja keskeisten palvelujen tarjoajiksi ja digitaalisen palvelun tarjoajiksi määritellyt sidosryhmät voivat määritellä uudenlaisia järjestelyjä. Jäsenvaltioiden valintoihin voivat vaikuttaa myös kyberturvallisuuteen liittyvän erityisasiantuntemuksen olemassaolo, resurssikysymykset,

sidosryhmien väliset suhteet ja kansalliset edut (esimerkiksi talouskehitys, yleinen turvallisuus jne.).

3.2 Julkisuus ja muut merkitykselliset näkökohdat

Verkko- ja tietoturvadirektiivin 8 artiklan 7 kohdan mukaan jäsenvaltioiden on ilmoitettava komissiolle kansallisen toimivaltaisen viranomaisen ja keskitetyn yhteyspisteen nimeämisestä ja niiden tehtävistä. Tämä on tehtävä ennen direktiivin saattamiselle osaksi kansallista lainsäädäntöä asetettua määräaikaa.

Direktiivin 15 ja 17 artiklan mukaan jäsenvaltioiden on varmistettava, että toimivaltaisilla viranomaisilla on tarvittavat valtuudet ja keinot toteuttaa mainituissa artikloissa säädetyt tehtävät.

Myös tiettyjen toimijoiden nimeäminen kansallisiksi toimivaltaisiksi viranomaisiksi on julkistettava. Direktiivissä ei säädetä, kuinka tämä julkistaminen on tehtävä. Koska tämän vaatimuksen tavoitteena on saada asia hyvin verkko- ja tietoturvadirektiivin soveltamisalaan kuuluvien toimijoiden ja suuren yleisön tietoon, ja kun otetaan huomioon muilla aloilla (televiestintä, pankkiala, lääkkeet) saadut kokemukset, komissio katsoo, että tämä vaatimus voitaisiin täyttää esimerkiksi portaalilla, josta tiedotetaan laajasti.

Direktiivin 8 artiklan 5 kohdassa edellytetään, että tällaisilla viranomaisilla on ’riittävät voimavarat’ toteuttaa direktiivissä asetetut tehtävät.

Taulukko 1: Kriittisen tietoteknisen infrastruktuurin suojaamista (CIIP) koskevia kansallisia toimintamalleja

ENISA julkaisi vuonna 2016 tutkimuksen[12] eri toimintamalleista, joita jäsenvaltiot noudattavat kriittisen tietoteknisen infrastruktuurin suojaamisessa. Jäsenvaltioiden CIIP:n hallinnoinnin osalta kuvataan kaksi profiilia, joita voidaan soveltaa verkko- ja tietoturvadirektiivin täytäntöönpanossa.

Profiili 1: Hajautettu toimintamalli – useita alakohtaisia viranomaisia, joilla on toimivalta tiettyjen direktiivin liitteissä II ja III mainittujen toimialojen ja palvelujen osalta

Hajautetulle toimintamallille on luonteenomaista

(i) toissijaisuusperiaate
(ii) julkishallinnon elinten tiivis yhteistyö
(iii)alakohtainen lainsäädäntö

Toissijaisuusperiaate

Sen sijaan että perustettaisiin tai nimettäisiin yksi viranomainen, jolla on yleinen vastuu, hajautetussa toimintamallissa noudatetaan toissijaisuusperiaatetta. Tämä tarkoittaa sitä, että vastuu täytäntöönpanosta on alakohtaisella viranomaisella, joka ymmärtää parhaiten paikallista toimialaa ja jolla on jo vakiintuneet suhteet sidosryhmiin. Tämän periaatteen mukaisesti päätöksiä tekevät ne, jotka ovat lähimpänä niitä tahoja, joihin päätökset vaikuttavat.

Julkishallinnon elinten tiivis yhteistyö

Koska CIIP:n täytäntöönpanoon osallistuu useita erilaisia julkishallinnon elimiä, monet jäsenvaltiot ovat kehittäneet yhteistyöjärjestelyjä eri viranomaisten työn ja toimien koordinoimiseksi. Nämä yhteistyöjärjestelyt voivat olla muodoltaan epävirallisia verkostoja tai järjestyneempiä foorumeita tai järjestelyjä. Yhteistyöjärjestelyt on kuitenkin luotu ainoastaan eri julkishallinnon elinten välistä tietojenvaihtoa ja koordinointia varten, eikä niillä ole mitään toimivaltaa näihin elimiin nähden.

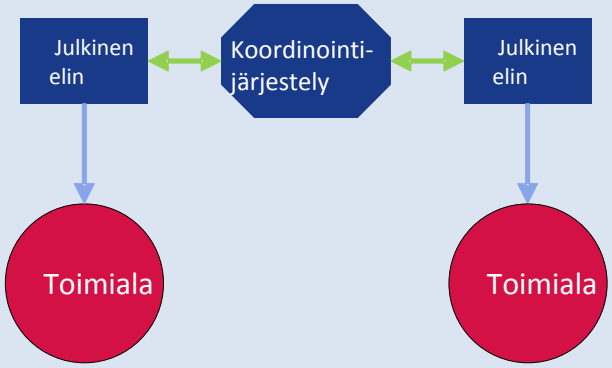
Alakohtainen lainsäädäntö

Maat, joissa sovelletaan hajautettua toimintamallia kriittisillä toimialoilla, eivät usein anna lainsäädäntöä CIIP:tä varten. Sen sijaan lait ja määräykset ovat edelleen alakohtaisia, ja siksi ne voivat vaihdella suuresti eri toimialoilla. Tällä toimintamallilla olisi se etu, että verkko- ja tietoturvaan liittyvät toimenpiteet olisivat linjassa olemassa olevien alakohtaisten määräysten kanssa, mikä parantaisi niiden hyväksyttävyyttä kyseisellä alalla samoin kuin viranomaisten harjoittaman täytäntöönpanon valvonnan tehokkuutta.

[12] ENISA, *Stocktaking, Analysis and Recommendations on the protection of CIIs* (2016). Saatavilla osoitteessa https://www.enisa.europa.eu/publications/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis

Puhtaasti hajautettuun toimintamalliin liittyy merkittävä riski siitä, että direktiivin soveltamisen yhdenmukaisuus heikkenee eri aloilla ja palveluissa. Direktiivissä säädetään keskitetystä kansallisesta yhteyspisteestä, joka vastaa yhteydenpidosta rajat ylittävissä asioissa. Hajautettua toimintamallia soveltava jäsenvaltio voisi antaa yhteyspisteelle tehtäväksi myös sisäisen koordinoinnin ja yhteistyön erilaisten kansallisten toimivaltaisten viranomaisten välillä direktiivin 10 artiklan mukaisesti.

Kuva 2 – Hajautettu toimintamalli



Esimerkkejä hajautetusta toimintamallista

Ruotsi on hyvä esimerkki maasta, jossa CIIP:hen sovelletaan hajautettua toimintamallia. Maassa käytetään ”järjestelmänäkökulmaa”, mikä tarkoittaa sitä, että CIIP:n tärkeimmät tehtävät, kuten elintärkeiden palvelujen ja kriittisten infrastruktuurien määrittely, operaattoreiden koordinointi ja tukeminen, sääntelytehtävät sekä hätätilavalmiuteen liittyvät toimenpiteet, kuuluvat eri virastojen ja kuntien vastuulle. Näihin virastoihin lukeutuvat Ruotsin yhteiskuntasuojan ja valmiuden virasto (Myndigheten för samhällsskydd och beredskap, MSB), posti- ja telehallitus (Post- och telestyrelsen, PTS) ja useita puolustus-, sotilas- ja lainvalvontavirastoja.

Ruotsin hallitus on kehittänyt eri virastojen ja julkisten elinten toimien koordinointia varten yhteistyöverkoston. Se koostuu viranomaisista, joilla on erityisiä yhteiskunnallisia tietoturvaan liittyviä vastuita. Tämä tietoturva-alan yhteistyöryhmä (SAMFI) koostuu eri viranomaisten edustajista, ja se kokoontuu useita kertoja vuodessa keskustelemaan kansalliseen tietoturvaan liittyvistä kysymyksistä. SAMFI käsittelee pääasiassa poliittis-strategisten alojen aiheita, ja sen puitteissa keskustellaan muun muassa teknisistä kysymyksistä ja standardoinnista, tietoturva-alan kansallisesta ja kansainvälisestä kehityksestä ja tietoteknisten poikkeamien hallinnasta ja ehkäisystä (Ruotsin yhteiskuntasuojan ja valmiuden virasto (MSB) 2015).

Ruotsissa ei ole annettu yhtä CIIP:tä koskevaa lakia, jota sovellettaisiin kaikkiin kriittisen tietoteknisen infrastruktuurin käyttäjiin kaikilla aloilla. Sen sijaan kunkin kansallisen viranomaisen vastuulla on antaa määräyksiä, joissa asetetaan velvollisuuksia tietyn toimialan

yrityksille. Esimerkiksi MSB:llä on oikeus antaa valtion viranomaisille tietoturvaan liittyviä määräyksiä, kun taas PTS voi vaatia operaattoreita toteuttamaan tiettyjä sekundaarilainsäädäntöön perustuvia teknisiä tai organisatorisia turvatoimenpiteitä.

Toinen esimerkki tähän profiiliin sopivasta maasta on Irlanti. Irlanti noudattaa ”toissijaisuusdoktriinia”, jonka mukaan kukin ministeriö vastaa kriittisen tietoteknisen infrastruktuurin määrittelystä ja riskinarvioinnista omalla toimialallaan. Kansallisella tasolla ei ole myöskään annettu mitään erityisiä CIIP:tä koskevia määräyksiä. Lainsäädäntö on alakohtaista, ja sitä on annettu lähinnä energia- ja televiestintäsektoreilla (2015). Muita esimerkkejä ovat Itävalta, Kypros ja Suomi.

Profiili 2: Keskitetty toimintamalli – yksi keskusviranomainen, jolla on toimivalta kaikkien direktiivin liitteissä II ja III mainittujen toimialojen ja palvelujen osalta

Keskitetylle toimintamallille on luonteenomaista

i) kaikista toimialoista vastaava keskusviranomainen
ii) kattava lainsäädäntö

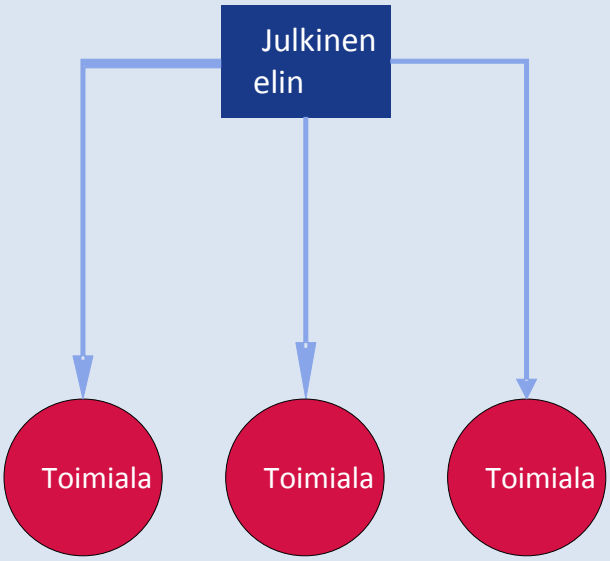
Kaikista toimialoista vastaava keskusviranomainen

Keskitettyä toimintamallia soveltavat jäsenvaltiot ovat perustaneet viranomaisia, joilla on vastuita ja laajat toimivaltuudet useilla tai kaikilla kriittisillä toimialoilla, tai ne ovat laajentaneet olemassa olevien viranomaisten toimivaltaa. CIIP:stä vastaavat keskusviranomaiset huolehtivat monista tehtävistä, kuten valmiussuunnittelusta, hätätilanteiden hallinnasta, sääntelytehtävistä ja yksityisten operaattoreiden tukemisesta. Monissa tapauksissa valtion tai hallituksen CSIRT-toimija on osa keskeistä CIIP-viranomaista. Keskusviranomaisella on todennäköisesti enemmän asiantuntemusta kyberturvallisuudesta kuin useilla alakohtaisilla viranomaisilla, kun otetaan huomioon kyberturvallisuustaitojen yleinen puute.

Kattava lainsäädäntö

Kattavassa lainsäädännössä asetetaan velvollisuuksia ja vaatimuksia kaikille kriittisen tietoteknisen infrastruktuurin operaattoreille kaikilla aloilla. Tämä voidaan toteuttaa antamalla uutta kattavaa lainsäädäntöä tai täydentämällä voimassa olevia alakohtaisia määräyksiä. Tämä toimintamalli helpottaisi verkko- ja tietoturvadirektiivin yhdenmukaista soveltamista kaikkien sen soveltamisalaan kuuluvien toimialojen ja palvelujen osalta. Sillä vältettäisiin puutteellisen täytäntöönpanon riski, joka voisi aiheutua tapauksessa, jossa täytäntöönpanosta ovat vastuussa useat viranomaiset, joilla on rajatut toimivaltuudet.

Kuva 3 – Keskitetty toimintamalli



Esimerkkejä keskitetystä toimintamallista

Ranska on hyvä esimerkki EU:n jäsenvaltiosta, jossa sovelletaan keskitettyä toimintamallia. Ranskan Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) nimettiin keskeiseksi tietojärjestelmien suojaamisesta vastaavaksi kansalliseksi viranomaiseksi vuonna 2011. ANSSIlla on vahva valvontarooli ”olennaisen tärkeiden operaattoreiden” (OIV) suhteen: virasto voi määrätä tällaisen operaattorin toteuttamaan turvallisuustoimenpiteitä, ja sillä on valtuudet tehdä tällaisten operaattoreiden turvallisuustarkastuksia. Se on myös pääasiallinen yhteyspiste olennaisen tärkeille operaattoreille, joilla on velvollisuus ilmoittaa turvallisuuspoikkeamista virastolle.

Turvallisuuspoikkeamien esiintyessä ANSSI toimii CIIP:n valmiusvirastona ja päättää toimenpiteistä, joita operaattoreiden on toteutettava kriisiin vastaamiseksi. Hallituksen toimia koordinoidaan ANSSIn operaatiokeskuksessa. Uhkien havaitsemisesta ja poikkeamiin reagoinnista vastaa operatiivisella tasolla CERT-FR, joka on osa ANSSIa.

Ranska on vahvistanut CIIP:lle kattavan lainsäädäntökehyksen. Pääministeri määräsi vuonna 2016 laadittavaksi luettelon kriittiseen infrastruktuuriin sisältyvistä toimialoista. Luettelossa yksilöitiin 12 olennaista toimialaa, ja hallitus on se perusteella määritellyt noin 250 olennaisen tärkeää operaattoria. Vuonna 2013 annettiin sotilasalan ohjelmasuunnittelua koskeva laki[13]. Siinä asetetaan olennaisen tärkeille operaattoreille erilaisia velvollisuuksia, kuten poikkeamista ilmoittaminen ja turvallisuustoimenpiteiden toteuttaminen. Nämä vaatimukset ovat pakollisia kaikille olennaisen tärkeille operaattoreille kaikilla toimialoilla (Ranskan senaatti 2013).

[13] La loi de programmation militaire.

3.3 Verkko- ja tietoturvadirektiivin 9 artikla: tietoturvaloukkauksiin reagoivat ja niitä tutkivat yksiköt (CSIRT-toimijat)

Verkko- ja tietoturvadirektiivi 9 artiklan mukaan jäsenvaltioiden on nimettävä yksi tai useampi CSIRT-toimija, joka vastaa riskien ja poikkeamien käsittelystä direktiivin liitteessä II luetelluilla toimialoilla ja liitteessä III luetelluissa palveluissa. Jäsenvaltiot voivat käyttää CSIRT-toimijoita myös direktiivin soveltamisalaan kuulumattomilla aloilla, kuten julkishallinnossa, ottaen huomioon direktiivin 3 artiklassa esitetty vähimmäistason yhdenmukaistamista koskeva vaatimus.

Jäsenvaltiot voivat perustaa CSIRT-toimijan kansallisen toimivaltaisen viranomaisen yhteyteen[14].

3.4 Tehtävät ja vaatimukset

Nimettyjen CSIRT-toimijoiden tehtävät esitetään verkko- ja tietoturvadirektiivin liitteessä I, ja niihin sisältyvät seuraavat:

- poikkeamien seuranta kansallisella tasolla
- ennakkovaroitusten, varoitusten ja tiedotusten antaminen sekä tiedon levittäminen riskeistä ja poikkeamista asiaankuuluville sidosryhmille
- poikkeamiin reagointi
- dynaamisen riskin ja poikkeamien analysointi sekä tilannetietoisuus ja
- osallistuminen 12 artiklan mukaisesti perustettuun kansallisten CSIRT-toimijoiden verkostoon (CSIRT-verkostoon).

Direktiivin 14 artiklan 3, 5 ja 6 kohdassa ja 16 artiklan 3, 6 ja 7 kohdassa asetetaan poikkeamien ilmoittamiseen liittyviä erityisiä lisätehtäviä, jos jäsenvaltio päättää, että CSIRT-toimija voi toteuttaa tällaisia tehtäviä kansallisten toimivaltaisten viranomaisten lisäksi tai niiden sijaan.

Saattaessaan direktiiviä osaksi kansallista lainsäädäntöä jäsenvaltioilla on poikkeamista ilmoittamista koskevien vaatimusten osalta vaihtoehtoja sen suhteen, mikä on CSIRT-toimijoiden rooli. Jäsenvaltiot voivat valita pakollisen suoran ilmoittamisen CSIRT-toimijoille, mistä on hyötynä hallinnollinen tehokkuus, tai ne voivat valita suoran ilmoittamisen kansallisille toimivaltaisille viranomaisille, jolloin CSIRT-toimijoilla olisi oikeus saada käyttöönsä ilmoitetut tiedot. CSIRT-toimijat ovat viime kädessä kiinnostuneita kyberturvallisuuspoikkeamien (myös sellaisten, joiden osalta pakollinen ilmoittaminen ei ole kriittistä) ehkäisyyn, havaitsemiseen, niihin reagointiin ja niiden vaikutusten lieventämiseen

[14] Ks. 9 artiklan 1 kohdan viimeinen virke.

liittyvien ongelmien ratkaisemisesta sidosryhmiensä kanssa, kun taas säännösten noudattamisen seuranta kuuluu kansallisille toimivaltaisille viranomaisille.

Direktiivin 9 artiklan 3 kohdan mukaan jäsenvaltioiden on myös varmistettava, että CSIRT-toimijoilla on pääsy suojattuun ja sietokykyiseen viestintä- ja tietoinfrastruktuuriin.

Direktiivin 9 artiklan 4 kohdan mukaan jäsenvaltioiden on annettava komissiolle tiedot nimettyjen CSIRT-toimijoiden poikkeamien käsittelyprosessiin kuuluvien tehtävien laajuudesta sekä poikkeamien käsittelyprosessin tärkeimmistä osista.

Jäsenvaltioiden nimeämiä CSIRT-toimijoita koskevat vaatimukset esitetään direktiivin liitteessä I. CSIRT-toimijan on varmistettava viestintäpalvelujensa kattava saatavuus. Sen toimitilat ja niitä tukevat tietojärjestelmät on sijoitettava suojattuihin paikkoihin ja sen on voitava varmistaa toiminnan jatkuvuus. CSIRT-toimijalla on myös oltava mahdollisuus osallistua kansainvälisiin yhteistyöverkostoihin.

3.5 Avunanto CSIRT-toimijoiden kehittämisessä

Verkkojen Eurooppa -välineestä rahoitettavasta kyberturvallisuutta koskevasta digitaalipalvelujen infrastruktuuriohjelmasta voidaan antaa merkittävää EU-rahoitusta, jolla jäsenvaltioiden CSIRT-toimijoita autetaan parantamaan valmiuksiaan ja tekemään keskinäistä yhteistyötä tietojenvaihtoon perustuvan yhteistyömekanismin kautta. SMART 2015/1089 -hankkeessa parhaillaan kehitettävän yhteistyömekanismin tarkoituksena on helpottaa vapaaehtoisuuteen perustuvaa ripeää ja tehokasta operatiivista yhteistyötä jäsenvaltioiden CSIRT-toimijoiden välillä erityisesti CSIRT-verkostolle direktiivin 12 artiklassa annettujen tehtävien tukemiseksi.

Yksityiskohtaiset tiedot jäsenvaltioiden CSIRT-toimijoiden valmiuksien parantamista koskevista ehdotuspyynnöistä ovat saatavilla Euroopan komission innovoinnin ja verkkojen toimeenpanoviraston (INEA) verkkosivustolla[15].

Verkkojen Eurooppa -välineestä rahoitettavan kyberturvallisuutta koskevan digitaalipalvelujen infrastruktuuriohjelman hallintoneuvosto muodostaa epävirallisen rakenteen poliittisen tason ohjeistukselle ja avulle, jota jäsenvaltioiden CSIRT-toimijoille annetaan niiden valmiuksien parantamiseksi, sekä vapaaehtoisen yhteistyömekanismin toteuttamiselle.

Vasta perustettu uusi CSIRT-toimija tai CSIRT-toimija, joka on nimetty toteuttamaan verkko- ja tietoturvadirektiivin liitteessä I luetellut tehtävät, voi saada ENISAlta apua ja hyödyntää sen asiantuntemusta oman suorituskykynsä parantamiseksi ja toteuttaakseen tehtävänsä tehokkaasti[16]. Tässä yhteydessä on syytä huomata, että jäsenvaltioiden CSIRT-toimijat voisivat käyttää vertailukohtana joitain ENISAn hiljattain toteuttamia töitä. Virasto on erityisesti julkaissut CSIRT-toimijoiden erilaisista valmiuksista ja palveluista lukuisia asiakirjoja ja tutkimuksia, joissa kuvataan hyviä käytäntöjä, ja antanut teknisen tason

[15] Saatavilla osoitteessa https://ec.europa.eu/inea/en/connecting-europe-facility
[16] Ks. verkko- ja tietoturvadirektiivin 9 artiklan 5 kohta.

suosituksia, joissa käsitellään CSIRT-toimijoiden kypsyysasteen arviointia. Nämä asiakirjat luetellaan tämän liitteen jaksossa 7. Ohjeita ja parhaita käytäntöjä on jaettu myös CSIRT-toimijoiden verkostoissa sekä maailmanlaajuisesti (FIRST[17]) että Euroopan tasolla (Trusted Introducer, TI[18]).

3.6 Keskitetyn yhteyspisteen rooli

Verkko- ja tietoturvadirektiivin 8 artiklan 3 kohdan mukaan kunkin jäsenvaltion on nimettävä keskitetty kansallinen yhteyspiste, jonka tehtävänä on yhteydenpito, jotta voidaan varmistaa rajat ylittävä yhteistyö muiden jäsenvaltioiden asiaankuuluvien viranomaisten kanssa sekä direktiivillä perustettujen yhteistyöryhmän ja CSIRT-verkoston[19] kanssa. Johdanto-osan 31 kappaleessa ja 8 artiklan 4 kohdassa selitetään tämän vaatimuksen tarkoitusta, eli sillä pyritään helpottamaan rajat ylittävää yhteistyötä ja viestintää. Tämä on tarpeellista erityisesti siksi, että jäsenvaltiot voivat päättää nimetä useamman kuin yhden kansallisen viranomaisen. Keskitetty yhteyspiste helpottaisi siten eri jäsenvaltioiden viranomaisten löytämistä ja niiden välistä yhteistyötä.

Keskitetyn yhteyspisteen yhteydenpitotehtävään sisältyy todennäköisesti vuorovaikutus yhteistyöryhmän ja CSIRT-verkoston sihteeristöjen kanssa niissä tapauksissa, joissa kansallinen keskitetty yhteyspiste ei ole CSIRT-toimija eikä yhteistyöryhmän jäsen. Jäsenvaltioiden on lisäksi varmistettava, että keskitetylle yhteyspisteelle tiedotetaan keskeisten palvelujen tarjoajilta ja digitaalisen palvelun tarjoajilta saaduista ilmoituksista[20].

Direktiivin 8 artiklan 3 kohdassa tarkennetaan, että jos jäsenvaltio soveltaa keskitettyä toimintamallia eli nimeää vain yhden toimivaltaisen viranomaisen, kyseinen viranomainen toimii myös keskitettynä yhteyspisteenä. Jos jäsenvaltio soveltaa hajautettua toimintamallia, se voi valita yhden toimivaltaisista viranomaista toimimaan keskitettynä yhteyspisteenä. Valitusta institutionaalisesta mallista riippumatta jäsenvaltioilla on aina, kun toimivaltainen viranomainen, CSIRT-toimija ja keskitetty yhteyspiste ovat erillisiä elimiä, velvollisuus varmistaa niiden välinen tehokas yhteistyö direktiivissä säädettyjen velvollisuuksien täyttämiseksi[21].

Keskitetyn yhteyspisteen on viimeistään 9. elokuuta 2018 ja sen jälkeen kerran vuodessa toimitettava yhteistyöryhmälle tiivistelmäraportti saaduista ilmoituksista, mukaan lukien ilmoitusten lukumäärä, ilmoitettujen poikkeamien luonne ja viranomaisten toteuttamat toimenpiteet, kuten poikkeamasta ilmoittaminen muille jäsenvaltioille, joihin se vaikuttaa, tai asiaankuuluvien tietojen antaminen ilmoituksen tehneelle yritykselle poikkeaman käsittelemiseksi[22]. Keskitetyn yhteyspisteen on toimivaltaisen viranomaisen tai CSIRT-

[17] Forum of Incident Response and Security Teams (https://www.first.org/).
[18] https://www.trusted-introducer.org/
[19] Direktiivin 12 artiklan mukainen jäsenvaltioiden operatiivista yhteistyötä edistävä kansallisten CSIRT-toimijoiden verkosto.
[20] Ks. 10 artiklan 3 kohta.
[21] Ks. 10 artiklan 1 kohta.
[22] Sama kuin edellä.

toimijan pyynnöstä toimitettava keskeisten palvelujen tarjoajien tekemät ilmoitukset muiden asiaan liittyvien jäsenvaltioiden keskitetyille yhteyspisteille[23].

Jäsenvaltioiden on ilmoitettava keskitetyn yhteyspisteen nimeämisestä ja sen tehtävistä komissiolle kansallisen lainsäädännön osaksi saattamisen määräaikaan mennessä. Keskitetyn yhteyspisteen nimeäminen on julkistettava samalla tavoin kuin kansallisten toimivaltaisten viranomaisten nimeäminen. Komissio julkaisee nimettyjen keskitettyjen yhteyspisteiden luettelon.

3.7 Seuraamukset

Direktiivin 21 artiklassa jäsenvaltioille jätetään harkintavaltaa päättää sovellettavien seuraamusten tyypistä ja luonteesta, kunhan ne ovat tehokkaita, oikeasuhteisia ja varoittavia. Toisin sanoen jäsenvaltiot voivat periaatteessa vapaasti päättää niiden kansallisessa lainsäädännössä säädettävästä seuraamusten enimmäismäärästä, mutta valitun määrän tai prosenttiosuuden olisi annettava kansallisille viranomaisille mahdollisuus määrätä jokaisessa konkreettisessa tapauksessa tehokkaita, oikeasuhteisia ja varoittavia seuraamuksia ottaen huomioon eri tekijät, kuten rikkomuksen vakavuus tai toistuvuus.

4. Toimijat, joita koskevat turvallisuusvaatimuksia ja poikkeamista ilmoittamista koskevat velvollisuudet

Toimijoiden, joilla on suuri merkitys yhteiskunnan ja talouden kannalta ja joihin viitataan direktiivin 4 artiklan 4 ja 5 kohdassa nimillä keskeisten palvelujen tarjoajat ja digitaalisen palvelun tarjoajat, on toteutettava asianmukaiset turvallisuustoimenpiteet ja ilmoitettava vakavista poikkeamista asianomaisille kansallisille viranomaisille. Tähän on syynä se, että turvallisuuspoikkeamien vaikutukset tällaisiin palveluihin voivat muodostaa merkittävän uhan niiden toiminnalle, mikä voi puolestaan aiheuttaa vakavaa haittaa taloudellisen toiminnan harjoittamiselle ja yhteiskunnalle yleensä ja mahdollisesti heikentää käyttäjien luottamusta ja aiheuttaa merkittävää vahinkoa unionin taloudelle[24].

Tässä jaksossa annetaan yleiskuva verkko- ja tietoturvadirektiivin liitteiden II ja III soveltamisalaan kuuluvista toimijoista ja luetellaan niiden velvollisuudet. Keskeisten palvelujen tarjoajien määrittämistä käsitellään laajasti, sillä tämä prosessi on erityisen tärkeä verkko- ja tietoturvadirektiivin yhdenmukaisessa täytäntöönpanossa koko unionin alueella. Siinä selitetään myös laajasti digitaalisten infrastruktuurien ja digitaalisen palvelun tarjoajien määritelmiä. Lisäksi siinä tarkastellaan muiden toimialojen mahdollista sisällyttämistä direktiivin soveltamisalaan ja selitetään tarkemmin digitaalisen palvelun tarjoajien suhteen omaksuttua lähestymistapaa.

[23] Ks. 14 artiklan 5 kohta.
[24] Ks. johdanto-osan 2 kappale.

4.1 Keskeisten palvelujen tarjoajat

Verkko- ja tietoturvadirektiivissä ei määritellä, mitkä nimenomaiset toimijat katsotaan sen soveltamisalan kuuluviksi keskeisten palvelujen tarjoajiksi. Sen sijaan siinä vahvistetaan kriteerit, joita jäsenvaltioiden on sovellettava toteuttaakseen määritysprosessin, jossa viime kädessä määritellään, mitkä liitteessä II lueteltuihin toimijoiden tyyppeihin lukeutuvat yksittäiset yritykset katsotaan keskeisten palvelujen tarjoajiksi ja mitä yrityksiä direktiivin mukaiset velvollisuudet siten koskevat.

4.1.1 Verkko- ja tietoturvadirektiivin liitteessä II luetellut toimijoiden tyypit

Direktiivin 4 artikla 4 kohdan mukaan keskeisten palvelujen tarjoajat ovat julkisia tai yksityisiä toimijoita, jotka ovat direktiivin liitteessä II tarkoitettua tyyppiä ja täyttävät 5 artiklan 2 kohdassa vahvistetut vaatimukset. Liitteessä II luetellaan toimialat, osa-alueet ja toimijoiden tyypit, joiden osalta kunkin jäsenvaltion toteutettava 5 artikla 2 kohdan mukainen määritysprosessi[25]. Toimialoihin lukeutuvat energia, liikenne, pankkiala, finanssimarkkinoiden infrastruktuurit, terveydenhuolto, vesihuolto ja digitaalinen infrastruktuuri.

Useimpien ’perinteisiin toimialoihin’ kuuluvien toimijoiden osalta EU:n lainsäädäntöön sisältyy jo vakiintuneita määritelmiä, joihin viitataan liitteessä II. Näin ei ole kuitenkaan liitteessä II olevassa 7 kohdassa mainitun digitaalisen infrastruktuurin osalta; tähän infrastruktuuriin sisältyvät internetin yhdysliikennepisteet, nimipalvelut ja aluetunnusrekisterit. Näitä määritelmiä selitetään tarkemmin seuraavassa.

1) Internetin yhdysliikennepiste (IXP)

Internetin yhdysliikennepiste määritellään 14 artiklan 3 kohdassa ja sitä selitetään edelleen johdanto-osan 18 kappaleessa. Sillä tarkoitetaan verkkoinfrastruktuurin osaa, joka mahdollistaa useamman kuin kahden riippumattoman teknisesti erillisen järjestelmän liittämisen yhteen pääasiassa internetliikenteen välittämisen helpottamiseksi. Internetin yhdysliikennepistettä voidaan myös kuvailla fyysiseksi paikaksi, jossa useat verkot voivat välittää internetliikennettä toisilleen vaihteen kautta. Yhdysliikennepisteen päätarkoituksena on mahdollistaa verkkojen yhteenliittäminen suoraan yhdysliikennepisteen kautta ilman, että liikenteen tarvitsee kulkea yhden tai useamman kolmannen osapuolen verkon kautta. IXP-palvelun tarjoaja ei tavallisesti vastaa internetliikenteen reitittämisestä, vaan siitä huolehtivat verkkopalvelujen tarjoajat. Suoralla yhteenliittämisellä on monia etuja, mutta tärkeimmät syyt ovat kustannukset, latenssi ja kaistaleveys. Mikään osapuoli ei tyypillisesti laskuta vaihteen läpi kulkevasta liikenteestä, kun taas upstream-internetpalveluntarjoajalle suuntautuvasta liikenteestä laskutetaan. Suoralla yhteenliitännällä, joka usein sijaitsee samassa kaupungissa kuin molemmat verkot, vältetään tarve siirtää dataa pitkiä matkoja sen välittämiseksi yhdestä verkosta toiseen, mikä pienentää latenssia.

[25] Ks. tarkempia tietoja määritysprosessista jäljempänä 4.1.6 kohdassa.

On syytä huomata, että internetin yhdysliikennepisteen määritelmä ei kata fyysisiä pisteitä, joissa ainoastaan kaksi fyysistä verkkoa on liitetty toisiinsa (eli verkkopalvelujen tarjoajat kuten BASE ja Proximus). Jäsenvaltioiden on siten saattaessaan direktiivin osaksi kansallista lainsäädäntöä erotettava toisistaan operaattorit, jotka helpottavat kootun internetliikenteen välittämistä useiden verkko-operaattoreiden kesken, ja yksittäiset verkko-operaattorit, jotka liittävät verkkonsa fyysisesti yhteen yhteenliittämissopimuksen perusteella. Viimeksi mainitussa tapauksessa verkkopalvelujen tarjoajat eivät kuulu 4 artiklan 13 kohdassa annetun määritelmän soveltamisalaan. Asiaa selvennetään johdanto-osan 18 kappaleessa, jossa todetaan, ettei yhdysliikennepiste anna pääsyä verkkoon eikä toimi transit-yhteyksien tarjoajana tai välittäjänä. Viimeinen tarjoajien luokka ovat yritykset, jotka tarjoavat sellaisia yleisiä viestintäverkkoja ja/tai -palveluja, joihin sovelletaan direktiivin 2002/21/EY 13 a ja 13 b artiklan mukaisia turvallisuus- ja ilmoitusvelvollisuuksia. Ne on jätetty verkko- ja tietoturvadirektiivin soveltamisalan ulkopuolelle[26].

2) Nimipalvelu (DNS)

Direktiivin 4 artiklan 14 kohdan mukaan nimipalvelulla tarkoitetaan ”*hajautettua hierarkkista verkon nimijärjestelmää, joka käsittelee nimipalvelukyselyjä*”. Tarkemmin sanottuna nimipalvelua voidaan kuvata tietokoneiden, palvelujen tai muiden internetiin liitettyjen resurssien hierarkkiseksi hajautetuksi nimijärjestelmäksi, joka mahdollistaa verkkotunnusten koodaamisen IP-osoitteiksi (yhteyskäytäntöosoitteiksi). Järjestelmän päätehtävä on annettujen verkkotunnusten muuttaminen IP-osoitteiksi. Tätä varten nimipalvelu käyttää tietokantaa sekä nimipalvelimia ja resolveria, joilla mahdollistetaan tällainen verkkotunnusten ”kääntäminen” operatiivisiksi IP-osoitteiksi. Vaikka verkkotunnusten koodaaminen ei olekaan nimipalvelun ainoa tarkoitus, se on kuitenkin järjestelmän päätehtävä. Direktiivin 4 artiklan 14 kohdassa annetussa oikeudellisessa määritelmässä keskitytään järjestelmän päätehtävään käyttäjän näkökulmasta menemättä teknisiin yksityiskohtiin, kuten nimiavaruuden, nimipalvelimien tai resolverien toimintaan. 4 artiklan 15 kohdassa selvennetään, kuka on katsottava nimipalvelujen tarjoajaksi.

3) Aluetunnusrekisteri

Direktiivin 4 artiklan 16 kohdan mukaan aluetunnusrekisterillä tarkoitetaan toimijaa, joka hallinnoi ja hoitaa internetin verkkotunnusten rekisteröintiä tietyn aluetunnuksen puitteissa. Tällaiseen verkkotunnusten hallinnointiin sisältyy aluetunnusten muuttaminen IP-osoitteiksi.

IANA (Internet Assigned Numbers Authority) vastaa DNS-juuripalvelimen, IP-osoitteiden jakamisen ja muiden internet-protokollan resurssien maailmanlaajuisesta koordinoinnista. IANA vastaa erityisesti yleisten aluetunnusten, kuten .com, ja maantieteellisen aluetunnusten, kuten .be, jakamisesta operaattoreille (rekistereille) ja niiden teknisten ja hallinnollisten tietojen ylläpitämisestä. IANA ylläpitää maailmanlaajuista rekisteriä jaetuista aluetunnuksista ja se osallistuu tämän luettelon julkaisemiseen internetin käyttäjille kaikkialla maailmassa sekä uusien aluetunnusten käyttöönottoon.

[26] Ks. lisätietoja verkko- ja tietoturvadirektiivin ja direktiivin 2002/21/EY välisestä suhteesta 5.2 kohdassa.

Yksi rekisterien tärkeä tehtävä on toisen tason verkkotunnusten jakaminen niin sanotuille rekisteröijille niiden oman aluetunnuksen puitteissa. Rekisteröijät voivat myös halutessaan itse jakaa kolmannen tason verkkotunnuksia. Maantieteelliset aluetunnukset on suunniteltu edustamaan maata tai aluetta standardin ISO 3166-1 perusteella. Yleisillä aluetunnuksilla ei yleensä ole maantieteellistä tai maatunnusta.

Aluetunnusrekisterin ylläpitoon voi sisältyä myös nimipalvelun tarjoaminen. Esimerkiksi IANAn valtuutussääntöjen mukaan maantieteellisiä aluetunnuksia käsittelevän nimetyn elimen on muun muassa valvottava verkkotunnuksia ja ylläpidettävä kyseisen maan nimipalvelua[27]. Jäsenvaltioiden on otettava nämä näkökohdat huomioon, kun ne määrittävät keskeisten palvelujen tarjoajia 5 artiklan 2 kohdan mukaisesti.

4.1.2 Keskeisten palvelujen tarjoajien määrittäminen

Direktiivin 5 artiklan vaatimusten mukaan kunkin jäsenvaltion on toteutettava määritysprosessi kaikkien alueelleen sijoittautuneiden liitteessä II lueteltujen toimijoiden tyyppien osalta. Tämän arvioinnin perusteella kaikki toimijat, jotka täyttävät 5 artiklan 2 kohdassa vahvistetut kriteerit, on määritettävä keskeisten palvelujen tarjoajiksi ja niihin on sovellettava 14 artiklassa säädettyjä turvallisuus- ja ilmoitusvaatimuksia.

Jäsenvaltioilla on 9. marraskuuta 2018 saakka aikaa määrittää toimijat kullakin toimialalla ja toimialan osa-alueella. Jäsenvaltioiden tukemiseksi tässä prosessissa yhteistyöryhmä laatii parhaillaan ohjeasiakirjaa, jossa annetaan tietoja keskeisten palvelujen tarjoajien määrittämiseen liittyvistä tarvittavista vaiheista ja parhaista käytännöistä.

Lisäksi yhteistyöryhmä keskustelee 24 artiklan 2 kohdan mukaisesti niiden kansallisten toimenpiteiden etenemisestä, sisällöstä ja tyypistä, joiden avulla voidaan määrittää tietyn toimialan keskeisten palvelujen tarjoajat. Jäsenvaltio voi ennen 9. päivää marraskuuta 2018 pyytää yhteistyöryhmää keskustelemaan kyseisen jäsenvaltion ehdotuksista kansallisiksi toimenpiteiksi, joiden avulla voidaan määrittää keskeisten palvelujen tarjoajat.

4.1.3 Vaatimusten soveltaminen muihin toimialoihin

Verkko- ja tietoturvadirektiivin 3 artiklassa esitetyn vähimmäistason yhdenmukaistamista koskevan vaatimuksen mukaisesti jäsenvaltiot voivat hyväksyä tai pitää voimassa säännöksiä, joiden tarkoituksena on saavuttaa korkeatasoisempi verkko- ja tietojärjestelmien turvallisuus. Jäsenvaltiot voivat yleisesti ottaen vapaasti laajentaa 14 artiklan mukaiset turvallisuus- ja ilmoitusvaatimukset koskemaan myös toimijoita, jotka kuuluvat muihin kuin direktiivin liitteessä II lueteltuihin toimialoihin ja osa-alueisiin. Eri jäsenvaltiot ovat päättäneet ottaa huomioon seuraavat toimialat tai harkitsevat parhaillaan tällaista päätöstä:

i) Julkishallinnot

Julkishallinnot voivat tarjota direktiivin liitteen II mukaisia keskeisiä palveluja, jotka täyttävät 5 artiklan 2 kohdan vaatimukset. Tällaisissa tapauksissa tällaisia palveluja tarjoavat julkishallinnot kuuluisivat asiaan liittyvien turvallisuus- ja ilmoitusvaatimusten

[27] Tietoja on saatavilla osoitteessa https://www.icann.org/resources/pages/delegation-2012-02-25-en

soveltamisalaan. Jos julkishallinnot sen sijaan tarjoavat palveluja, jotka eivät kuulu liitteen II soveltamisalaan, tällaiset palvelut eivät kuulu vaatimusten piiriin.

Julkishallinnot vastaavat valtion elinten, alue- ja paikallisviranomaisten, virastojen ja niiden sidosyritysten tarjoamien julkisten palvelujen moitteettomasta toimittamisesta. Nämä palvelut edellyttävät usein yksityishenkilöitä ja organisaatiota koskevien henkilö- ja yritystietojen luomista ja hallintaa. Näitä tietoja voidaan jakaa useiden julkisten elinten kanssa ja ne voidaan asettaa näiden elinten saataville. Laajemmin ottaen julkishallintojen käyttämien verkko- ja tietojärjestelmien korkea turvallisuustaso on koko yhteiskunnan ja talouden etujen mukaista. Siksi komissio katsoo, että jäsenvaltioiden olisi järkevää harkita julkishallinnon sisällyttämistä niiden säännösten soveltamisalaan, joilla direktiivi saatetaan osaksi kansallista lainsäädäntöä, liitteessä II ja 5 artiklan 2 kohdassa säädetyn keskeisten palvelujen tarjoamisen lisäksi.

ii) Postiala

Postialaan sisältyy postipalvelujen tarjonta, kuten postilähetysten kerääminen, lajittelu, kuljetus ja jakelu.

iii) Elintarvikeala

Elintarvikeala kattaa maataloustuotteiden ja muiden elintarvikkeiden tuotannon, ja siihen voi sisältyä keskeisiä palveluja, kuten elintarviketurvan varmistaminen ja elintarvikkeiden laadun ja turvallisuuden takaaminen.

iv) Kemian teollisuus ja ydinvoimateollisuus

Kemian teollisuuteen ja ydinvoimateollisuuteen sisältyy erityisesti kemikaalien, petrokemian tuotteiden ja ydinmateriaalien varastointi, tuotanto ja käsittely.

v) Ympäristöala

Ympäristöalan toimiin sisältyy ympäristön suojelussa ja luonnonvarojen hallinnassa tarvittavien tavaroiden ja palvelujen tarjonta. Toimilla pyritään siten ehkäisemään, vähentämään ja poistamaan saastumista ja säilyttämään saatavilla olevat luonnonvarat. Tämän alan keskeisiä palveluja voisivat olla saastumisen (esim. ilman ja veden) ja sääilmiöiden seuranta ja valvonta.

vi) Pelastuspalvelu

Pelastuspalvelualan tavoitteena on luonnon ja ihmisen aiheuttamien katastrofien ehkäiseminen sekä niihin varautuminen ja reagointi. Tässä tarkoituksessa tarjottuja palveluja voivat olla hätänumeroiden käyttöönotto sekä hätätilanteista tiedottamista, niiden rajoittamista ja niihin vastaamista koskevien toimien toteuttaminen.

4.1.4 Lainkäyttövalta

Direktiivin 5 artiklan 1 kohdan mukaan kunkin jäsenvaltion on määritettävä keskeisten palvelujen tarjoajat, jotka ovat sijoittautuneet sen alueelle. Säännöksessä ei tarkenneta laillisen sijoittautumisen tyyppiä, mutta johdanto-osan 21 kappaleessa selvennetään, että sijoittautuminen edellyttää tosiasiallista toimintaa ja kiinteää toimipaikkaa, kun taas sijoittautumisen oikeudellisella muodolla ei pitäisi olla ratkaisevaa merkitystä. Tämä

tarkoittaa, että sellaisten tapausten lisäksi, joissa toimijan päätoimipaikka on jäsenvaltion alueella, jäsenvaltiolla voi olla lainkäyttövalta keskeisten palvelujen tarjoajaan myös tapauksissa, joissa toimijalla on esimerkiksi sivuliike tai muun tyyppinen oikeudellinen sijoittautuminen.

Tästä seuraa, että useilla jäsenvaltioilla rinnakkain voi olla lainkäyttövaltaa samaan toimijaan.

4.1.5 Komissiolle toimitettavat tiedot

Komission on tarkasteltava verkko- ja tietoturvadirektiiviä uudelleen 23 artiklan 1 kohdan mukaisesti, ja tätä varten jäsenvaltioiden on toimitettava komissiolle viimeistään 9. marraskuuta 2018 ja sen jälkeen kahden vuoden välein seuraavat tiedot:

- kansalliset toimenpiteet, joiden avulla keskeisten palvelujen tarjoajat voidaan määrittää;
- luettelo keskeisistä palveluista;
- kunkin liitteessä II tarkoitetun toimialan osalta määritettyjen keskeisten palvelujen tarjoajien lukumäärä ja tiedot niiden merkityksestä kyseessä olevan alan osalta; ja
- kynnysarvot, jos sellaisia on olemassa, joita on käytetty toimitustason määrittämiseksi 6 artiklan 1 kohdan a alakohdassa tarkoitetun kyseisestä palvelusta riippuvaisten käyttäjien lukumäärän perusteella tai 6 artiklan 1 kohdan f alakohdassa tarkoitetun toimijan merkityksen perusteella.

Direktiivin 23 artiklan 1 kohdassa säädetty uudelleentarkastelu, joka edeltää direktiivin perinpohjaista uudelleentarkastelua, on osoitus siitä, kuinka tärkeänä lainsäädäntövallan käyttäjät pitävät direktiivin moitteetonta saattamista osaksi kansallista lainsäädäntöä keskeisten palvelujen tarjoajien määrittämisen osalta, jotta vältetään markkinoiden pirstaloituminen.

Jotta tämä prosessi voitaisiin toteuttaa parhaalla mahdollisella tavalla, komissio kehottaa jäsenvaltioita keskustelemaan tästä aiheesta ja vaihtamaan siihen liittyviä kokemuksia yhteistyöryhmässä. Lisäksi komissio kehottaa jäsenvaltioita toimittamaan komissiolle – tarvittaessa luottamuksellisesti – luettelot määritetyistä keskeisten palvelujen tarjoajista (jotka on viime kädessä valittu) kaikkien niiden tietojen lisäksi, jotka jäsenvaltioiden on direktiivin mukaan toimitettava komissiolle. Jos tällaiset luettelot olisivat komission käytettävissä, komission olisi helpompi arvioida määritysprosessin yhdenmukaisuutta, ja se parantaisi myös arvioinnin laatua. Komissio voisi myös näiden luettelojen pohjalta vertailla jäsenvaltioiden toimintamalleja, mikä helpottaisi direktiivin tavoitteiden saavuttamista.

4.1.6 Kuinka määritysprosessi toteutetaan?

Kuten kuvassa 4 esitetään, kansallisen viranomaisen olisi tiettyä toimijaa koskevassa määritysprosessissa tarkasteltava kuutta keskeistä kysymystä. Seuraavassa kukin kysymys vastaa yhtä vaihetta, joka on toteutettava 5 artiklan mukaisesti, yhdessä 6 artiklan kanssa ja ottaen huomioon myös 1 artiklan 7 kohdan mahdollinen soveltaminen.

Vaihe 1 – **Kuuluko toimija direktiivin liitteessä II tarkoitettuun toimialaan/osa-alueeseen ja vastaa siinä tarkoitettua toimijan tyyppiä?**

Kansallisen viranomaisen olisi arvioitava, kuuluuko kyseisen jäsenvaltion alueelle sijoittautunut toimija direktiivin liitteessä II lueteltuihin toimialoihin ja toimialojen osa-alueisiin. Liite II kattaa talouden alat, joita pidetään olennaisen tärkeinä sisämarkkinoiden moitteettoman toiminnan kannalta. Liitteessä II viitataan erityisesti seuraaviin toimialoihin ja niiden osa-alueisiin:

- Energia: sähkö, öljy ja kaasu
- Liikenne: lentoliikenne, rautatieliikenne, vesiliikenne ja tieliikenne
- Pankkiala: luottolaitokset
- Finanssimarkkinoiden infrastruktuurit: kauppapaikat, keskusvastapuolet
- Terveydenhuoltoala: terveydenhuoltolaitokset (mukaan lukien sairaalat ja yksityisklinikat)
- Vesihuolto: juomaveden toimittaminen ja jakelu
- Digitaalinen infrastruktuuri: internetin yhdysliikennepisteet, nimipalvelujen tarjoajat ja aluetunnusrekisterit[28].

Vaihe 2 – **Sovelletaanko alakohtaista säädöstä?**

Seuraavassa vaiheessa kansallisen viranomaisen on arvioitava, sovelletaanko jotain alakohtaista säädöstä 1 artiklan 7 kohdan mukaisesti. Mainitussa kohdassa säädetään, että jos jossain EU:n säädöksessä asetetaan keskeisten palvelujen tarjoajille tai digitaalisen palvelujen tarjoajille turvallisuus- ja/tai ilmoitusvaatimuksia, jotka ovat vähintään vastaavia kuin verkko- ja tietoturvadirektiivissä säädetyt vaatimukset, sovelletaan kyseisen alakohtaisen säädöksen mukaisia velvollisuuksia. Johdanto-osan 9 kappaleessa tarkennetaan, että jos 1 artiklan 7 kohdassa vahvistetut vaatimukset täyttyvät, jäsenvaltioiden olisi sovellettava alakohtaisten EU:n säädösten säännöksiä, myös tuomioistuimen toimivaltaan liittyviä säännöksiä. Verkko- ja tietoturvadirektiivin asiaa koskevia säännöksiä ei tällöin sovellettaisi. Tällaisessa tapauksessa toimivaltaisen viranomaisen olisi lopetettava 5 artiklan 2 kohdan mukainen määritysprosessi[29].

Vaihe 3 – **Tarjoaako toimija direktiivissä tarkoitettua keskeistä palvelua?**

Direktiivin 5 artiklan 2 kohdan a alakohdan mukaan määritettävän toimijan on tarjottava palvelua, joka on keskeinen yhteiskunnan ja/tai talouden kriittisten toimintojen ylläpitämiseksi. Jäsenvaltioiden on otettava tässä arvioinnissa huomioon se, että yksi toimija voi tarjota sekä keskeisiä että muita kuin keskeisiä palveluja. Tämä tarkoittaa, että verkko- ja tietoturvadirektiivin turvallisuus- ja ilmoitusvaatimuksia sovelletaan tiettyyn toimijaan ainoastaan siltä osin kuin se tarjoaa keskeisiä palveluja.

Direktiivin 5 artiklan 3 kohdan mukaan jäsenvaltion olisi laadittava luettelo kaikista keskeisistä palveluista, joita keskeisten palvelujen tarjoaja tarjoaa jäsenvaltion alueella. Tämä

[28] Näitä toimijoita selitetään tarkemmin 4.1.1 kohdassa.
[29] Lisätietoja alakohtaisten säädösten soveltamisesta annetaan 5.1 kohdassa.

luettelo on toimitettava komissiolle viimeistään 9. marraskuuta 2018 ja sen jälkeen kahden vuoden välein[30].

Vaihe 4 - **Onko palvelu riippuvainen verkko- ja tietojärjestelmästä?**

Seuraavaksi on selvitettävä, täyttääkö palvelu 5 artiklan 2 kohdan b alakohdassa esitetyn kriteerin eli se, onko keskeisen palvelun tarjoaminen riippuvainen 4 artiklan 1 kohdassa määritellyistä verkko- ja tietojärjestelmistä.

Vaihe 5 – **Olisiko turvallisuuspoikkeamalla merkittävä haitallinen vaikutus?**

Direktiivin 5 artiklan 2 kohdan c alakohdan mukaan kansallisen viranomaisen on arvioitava, olisiko poikkeamalla merkittävää haitallista vaikutusta palvelun tarjoamiseen. Tähän liittyen 6 artiklan 1 kohdassa esitetään joukko toimialojen välisiä tekijöitä, jotka on otettava huomioon tässä arvioinnissa. Lisäksi 6 artiklan 2 kohdassa säädetään, että arvioinnissa olisi tarvittaessa otettava huomioon myös toimialakohtaiset tekijät.

Direktiivin 6 artiklan 1 kohdassa luetellut **toimialojen väliset tekijät** ovat seuraavat:

- asianomaisen toimijan tarjoamasta palvelusta riippuvaisten käyttäjien lukumäärä;
- muiden liitteessä II tarkoitettujen toimialojen riippuvaisuus kyseisen toimijan tarjoamasta palvelusta;
- vaikutus, joka poikkeamilla voisi olla vakavuutensa ja kestonsa perusteella talouden ja yhteiskunnan toimintoihin tai yleiseen turvallisuuteen;
- kyseisen toimijan markkinaosuus;
- maantieteellinen levinneisyys alueella, johon poikkeama saattaa vaikuttaa;
- toimijan merkitys palvelun riittävän tason ylläpitämisessä ottaen huomioon kyseisen palvelun tarjoamista koskevien vaihtoehtoisten keinojen saatavuus.

Johdanto-osan 28 kappaleessa annetaan joitain esimerkkejä **toimialakohtaisista tekijöistä** (ks. taulukko 4). Tämä voi tarjota kansallisille viranomaisille hyödyllistä ohjeistusta.

[30] Ks. 5 artiklan 7 kohdan b alakohta.

Taulukko 4: Esimerkkejä toimialakohtaisista tekijöistä, jotka olisi otettava huomioon määritettäessä, olisiko poikkeamalla merkittävä haitallinen vaikutus

Toimiala	Esimerkkejä toimialakohtaisista tekijöistä
Energiantoimittajat	tuotetun kansallisen energian määrä tai osuus siitä
Öljyntoimittajat	toimitetun öljyn päiväkohtainen määrä;
Lentoliikenne (mukaan lukien lentoasemat ja lentoliikenteen harjoittajat) **Rautatieliikenne** **Meriliikenne**	osuus kansallisesta liikennemäärästä; matkustajien tai rahtikuljetusten lukumäärä vuodessa
Pankkiala tai finanssimarkkinoiden infrastruktuurit	järjestelmäkohtainen merkitys kokonaisvarojen perusteella; kokonaisvarojen ja bruttokansantuotteen suhde
Terveydenhuoltoala	palvelun tarjoajan hoidossa olevien potilaiden lukumäärä vuodessa
Veden tuotanto, käsittely ja toimittaminen	vesimäärä sekä käyttäjien lukumäärä ja tyypit (mukaan lukien esimerkiksi sairaalat, julkiset palveluorganisaatiot tai henkilöt); vaihtoehtoisten veden lähteiden olemassaolo saman maantieteellisen alueen kattamiseksi

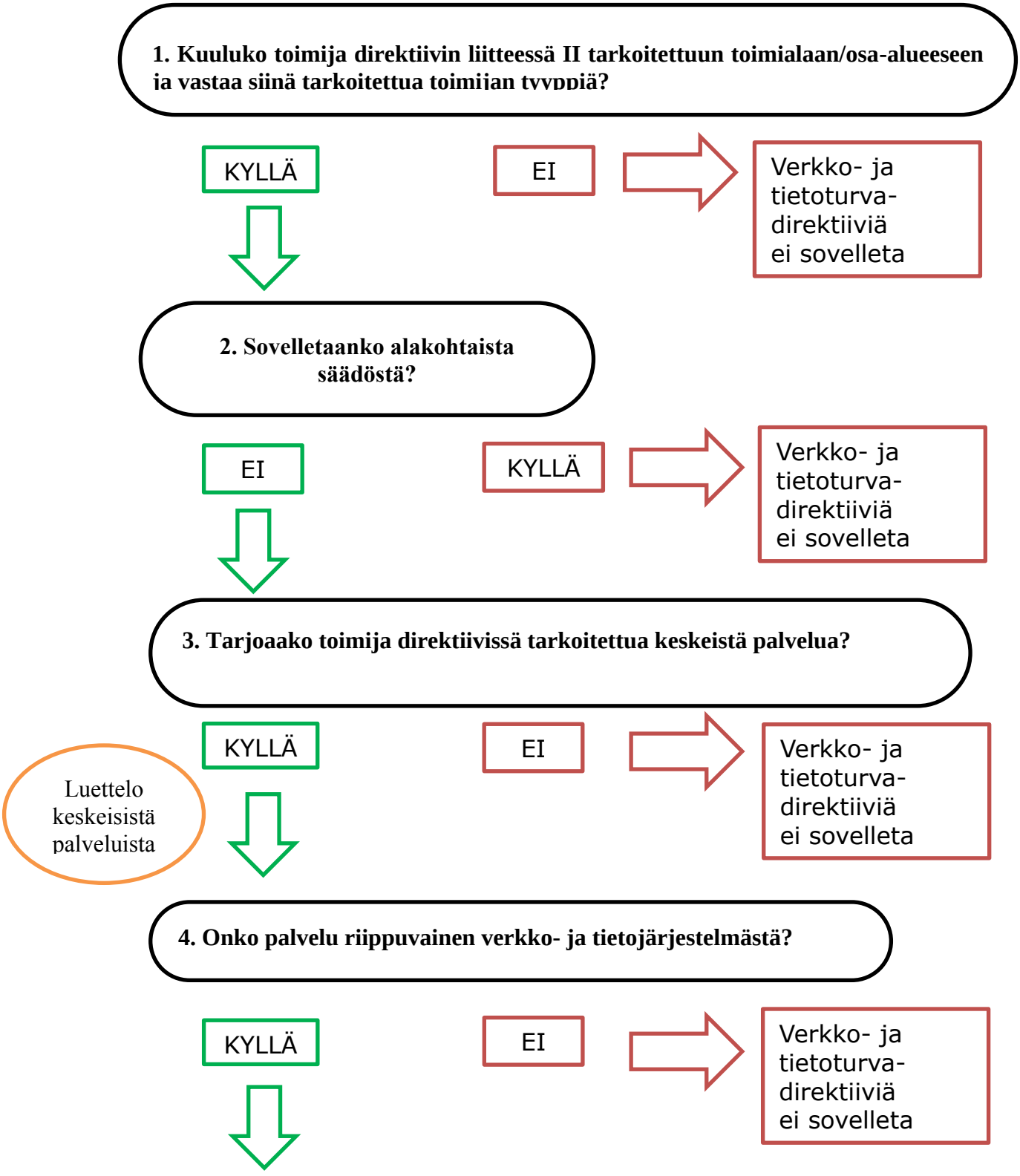
On syytä korostaa, että jäsenvaltioiden ei pitäisi 5 artiklan 2 kohdan mukaista arviointia tehdessään käyttää muita kriteerejä mainitussa kohdassa lueteltujen kriteerien lisäksi, koska tämä voisi rajoittaa määritettyjen keskeisten palvelujen tarjoajien määrää ja vaarantaa 3 artiklassa säädetyn keskeisten palvelujen tarjoajien vähimmäistason yhdenmukaistamisen.

Vaihe 6 **- Tarjoaako kyseisen toimija keskeisiä palveluja muissa jäsenvaltioissa?**

Vaihe 6 koskee tapauksia, joissa toimija tarjoaa keskeisiä palveluja kahdessa tai useammassa jäsenvaltiossa. Direktiivin 5 artiklan mukaan kyseisten jäsenvaltioiden on kuultava toisiaan ennen määritysprosessin loppuunsaattamista[31].

[31] Ks. lisätietoja kuulemisprosessista 4.1.7 kohdassa.

Kuva 4: Kuusivaiheinen määritysprosessi



5. Olisiko turvallisuuspoikkeamalla merkittävä haitallinen vaikutus?

Toimialojen väliset tekijät (6 artiklan 1 kohta)

- Palvelusta riippuvaisten **käyttäjien lukumäärä**
- Muiden toimialojen **riippuvaisuus** palvelusta
- Vaikutus, joka poikkeamilla voisi olla **talouden ja yhteiskunnan toimintoihin** tai **yleiseen turvallisuuteen**
- Mahdollinen **maantieteellinen levinneisyys**
- Toimijan merkitys **palvelun riittävän tason** ylläpitämisessä

Toimialakohtaiset tekijät (johdanto-osan 28 kappaleen esimerkit)

- **Energia**: tuotetun kansallisen energian määrä tai osuus siitä
- **Liikenne**: osuus kansallisesta liikennemäärästä ja kuljetusten lukumäärä vuodessa
- **Terveydenhuolto**: palvelun tarjoajan hoidossa olevien potilaiden lukumäärä vuodessa

KYLLÄ

EI → Verkko- ja tietoturva-direktiiviä ei sovelleta

6. Tarjoaako kyseisen toimija keskeisiä palveluja muissa jäsenvaltioissa?

KYLLÄ

EI → Verkko- ja tietoturva-direktiiviä ei sovelleta

Asianomaisten jäsenvaltioiden pakollinen kuuleminen

Kansallisten toimenpiteiden hyväksyminen (esim. keskeisten palvelujen tarjoajien luettelo, politiikkatoimet ja lainsäädäntötoimet)

4.1.7 Rajat ylittävä kuulemisprosessi

Kun toimija tarjoaa keskeisiä palveluja kahdessa tai useammassa jäsenvaltiossa, direktiivin 5 artiklan 4 kohdassa edellytetään, että asianomaiset jäsenvaltiot kuulevat toisiaan ennen määritysprosessin loppuunsaattamista. Kuulemisen tarkoituksena on helpottaa sen arviointia, onko palvelujen tarjoaja kriittisessä asemassa rajat ylittävien vaikutusten suhteen.

Kuulemisen haluttaisiin etenevän niin, että asianomaiset kansalliset viranomaiset keskustelevat asiasta ja esittävät omat näkökantansa ja parhaassa tapauksessa tulevat samaan lopputulokseen kyseisen toimijan määrityksen suhteen. Verkko- ja tietoturvadirektiivissä ei kuitenkaan suljeta pois mahdollisuutta, että jäsenvaltiot tekevät toisistaan poikkeavat päätelmät siitä, määritetäänkö tietty toimija keskeisten palvelujen tarjoajaksi. Johdanto-osan 24 kappaleessa mainitaan mahdollisuus, että jäsenvaltiot voivat pyytää asiassa yhteistyöryhmän apua.

Komissio katsoo, että jäsenvaltioiden tulisi pyrkiä saavuttamaan yksimielisyys näissä kysymyksissä sellaisen tilanteen välttämiseksi, että yhdellä yrityksellä on erilainen oikeudellinen asema eri jäsenvaltioissa. Poikkeavan kohtelun tulisi olla todella poikkeuksellista, esimerkiksi kun toimijalla, joka on määritetty keskeisten palvelujen tarjoajaksi yhdessä jäsenvaltiossa, on vain marginaalista ja vähämerkityksellistä toimintaa toisessa jäsenvaltiossa.

4.2. Turvallisuusvaatimukset

Verkko- ja tietoturvadirektiivin 14 artiklan 1 kohdan mukaan jäsenvaltioiden on varmistettava, että keskeisten palvelujen tarjoajat toteuttavat asianmukaiset ja oikeasuhteiset tekniset ja organisatoriset toimenpiteet, ottaen huomioon uusimman tekniikan, hallitakseen riskejä, joita kohdistuu niiden verkko- ja tietojärjestelmien turvallisuuteen, joita nämä organisaatiot käyttävät palvelujensa tarjonnassa. Direktiivin 14 artiklan 2 kohdan mukaan asianmukaisilla toimenpiteillä on ehkäistävä ja minimoitava poikkeamien vaikutus.

Yhteistyöryhmän puitteissa toimiva erityinen toimintalinja laatii parhaillaan keskeisten palvelujen tarjoajien turvallisuustoimenpiteitä koskevia ei-sitovia ohjeita[32]. Ryhmän on tarkoitus saada ohjeasiakirja valmiiksi vuoden 2017 viimeisellä neljänneksellä. Komissio kehottaa jäsenvaltioita noudattamaan tiiviisti yhteistyöryhmän laatimaa ohjeasiakirjaa, jotta turvallisuusvaatimuksia koskevat kansalliset säännökset voidaan yhdenmukaistaa niin pitkälle kuin mahdollista. Näiden vaatimusten yhdenmukaistaminen tekisi niiden noudattamisen huomattavasti helpommaksi keskeisten palvelujen tarjoajille, jotka usein tarjoavat keskeisiä palveluja useammassa kuin yhdessä jäsenvaltiossa. Se helpottaisi myös kansallisten toimivaltaisten viranomaisten ja CSIRT-toimijoiden valvontatehtäviä.

[32] Tätä toimintalinjaa varten kierrätettiin luetteloa kansainvälisistä standardeista, parhaista käytännöistä ja riskinarviointi ja -hallintamenetelmistä kaikilta verkko- ja tietoturvadirektiivin soveltamisalaan kuuluvilta toimialoilta, ja niitä käytettiin taustatietoina ehdotetuille turvallisuusaloille ja turvallisuustoimenpiteille.

4.3 Ilmoitusvaatimukset

Direktiivin 14 artiklan 3 kohdan mukaan jäsenvaltioiden on varmistettava, että keskeisten palvelujen tarjoajat ilmoittavat ”*poikkeamista, joilla on merkittävä vaikutus niiden tarjoamien keskeisten palvelujen jatkuvuuteen*”. Keskeisten palvelujen tarjoajien ei siten tarvitse ilmoittaa vähäisistä poikkeamista vaan ainoastaan vakavista poikkeamista, jotka vaikuttavat keskeisen palvelun jatkuvuuteen. Direktiivin 4 artiklan 7 kohdan määritelmän mukaan ’poikkeamalla’ tarkoitetaan ”*mitä tahansa tapahtumaa, joka tosiasiassa vaikuttaa haitallisesti verkko- ja tietojärjestelmien turvallisuuteen*”. ’Verkko- ja tietojärjestelmien turvallisuus’ puolestaan määritellään 4 artiklan 2 kohdassa siten, että sillä tarkoitetaan ”*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*”, Näin ollen mikä tahansa tapahtuma, jolla on haitallinen vaikutus palvelun jatkuvuuden lisäksi myös tietojen ja niihin liittyvien palvelujen aitouteen, eheyteen tai luottamuksellisuuteen, voi mahdollisesti kuulua ilmoitusvelvollisuuden piiriin. Itse asiassa 14 artiklan 3 kohdassa tarkoitetun palvelun jatkuvuuden voi vaarantaa niiden tapausten lisäksi, joissa on kyse fyysisestä saatavuudesta, mikä tahansa muu turvallisuuspoikkeama, joka vaikuttaa palvelun asianmukaiseen tarjontaan[33].

Yhteistyöryhmän puitteissa toimiva erityinen toimintalinja laatii parhaillaan ilmoittamista koskevia ei-sitovia ohjeita niistä olosuhteista, joissa keskeisten palvelujen tarjoajien edellytetään ilmoittavan poikkeamista 14 artiklan 7 kohdan mukaisesti, sekä tällaisten ilmoitusten muodosta ja ilmoitusmenettelystä. Ohjeet on tarkoitus saada valmiiksi vuoden 2017 viimeisellä neljänneksellä.

Toisistaan poikkeavat kansalliset ilmoitusvaatimukset voivat johtaa oikeudelliseen epävarmuuteen, tehdä menettelyistä monimutkaisempia ja raskaampia ja aiheuttaa huomattavia hallinnollisia kustannuksia rajojen yli toimiville palveluntarjoajille. Siksi komissio pitää yhteistyöryhmän työtä tervetulleena. Samoin kuin turvallisuusvaatimusten tapauksessa, komissio kehottaa jäsenvaltioita noudattamaan tiiviisti yhteistyöryhmän laatimaa ohjeasiakirjaa, jotta poikkeamista ilmoittamista koskevat kansalliset säännökset voidaan yhdenmukaistaa niin pitkälle kuin mahdollista.

4.4 Verkko- ja tietoturvadirektiivin liite III: digitaalisen palvelun tarjoajat

Digitaalisen palvelun tarjoajat ovat toinen verkko- ja tietoturvadirektiivin soveltamisalaan kuuluva toimijatyyppi. Niitä pidetään tärkeinä talouden toimijoina, koska monet yritykset käyttävät niitä omien palvelujensa tarjonnassa, ja digitaalisen palvelun häiriö voi vaikuttaa keskeisiin talouden ja yhteiskunnan toimintoihin.

[33] Sama koskee digitaalisen palvelun tarjoajia.

4.4.1 Digitaalisen palvelun tarjoajien tyypit

Digitaalinen palvelu määritellään direktiivin 4 artiklan 5 kohdassa. Siinä viitataan direktiivin (EU) 2015/1535 1 artiklan 1 kohdan b alakohdassa annettuun oikeudelliseen määritelmään ja rajoitetaan määritelmän soveltamisala verkko- ja tietoturvadirektiivin liitteessä III lueteltuihin palvelujen tyyppeihin. Direktiivin (EU) 2015/1535 1 artiklan 1 kohdan b alakohdan määritelmän mukaan näillä palveluilla tarkoitetaan ”*kaikkia etäpalveluina sähköisessä muodossa palvelun vastaanottajan henkilökohtaisesta pyynnöstä toimitettavia palveluja, joista tavallisesti maksetaan korvaus*”. Verkko- ja tietoturvadirektiivin liitteessä III puolestaan luetellaan seuraavat kolme palvelutyyppiä: verkossa toimiva markkinapaikka, verkossa toimiva hakukone ja pilvipalvelu. Toisin kuin keskeisten palvelujen tarjoajien tapauksessa direktiivissä ei edellytetä, että jäsenvaltiot määrittävät digitaalisen palvelun tarjoajat, joihin sitten sovellettaisiin asiaan kuuluvia velvollisuuksia. Näin ollen direktiivin asiaan kuuluvia velvollisuuksia, eli 16 artiklassa vahvistettuja turvallisuus- ja ilmoitusvaatimuksia, sovelletaan kaikkiin direktiivin soveltamisalaan kuuluviin digitaalisen palvelun tarjoajiin.

Seuraavassa selitetään tarkemmin direktiivin soveltamisalaa kuuluvia kolmea digitaalisten palvelujen tyyppiä.

1. Verkossa toimivan markkinapaikan tarjoaja

Verkossa toimivalla markkinapaikalla suuri määrä erilaisia yrityksiä voi käydä kauppaa kuluttajien kanssa ja luoda yritysten välisiä suhteita. Se tarjoaa yrityksille perusinfrastruktuurin verkossa ja rajojen yli käytävään kauppaan. Näillä markkinapaikoilla on huomattava merkitys taloudessa erityisesti siksi, että ne tarjoavat pk-yrityksille pääsyn laajemmille EU:n digitaalisille sisämarkkinoille. Asiakkaan taloudellista toimintaa helpottavien etäkäyttöpalvelujen tarjonta, kuten maksutapahtumien käsittely ja ostajia, toimittajia ja tuotteita koskevien tietojen yhdistäminen, voi myös kuulua verkossa toimivan markkinapaikan tarjoajan toimintoihin, samoin kuin sopivien tuotteiden etsinnän helpottaminen, tuotteiden tarjonta, maksutapahtumia koskeva asiantuntemus sekä ostajien ja myyjien yhteensaattaminen.

Verkossa toimiva markkinapaikka on määritelty 4 artiklan 17 kohdassa, ja sitä selitetään tarkemmin johdanto-osan 15 kappaleessa. Verkossa toimiva markkinapaikka kuvaillaan palveluksi, jonka avulla kuluttajat ja elinkeinonharjoittajat voivat tehdä verkossa kauppa- tai palvelusopimuksia elinkeinonharjoittajien kanssa, ja sen todetaan olevan lopullinen määräpaikka tällaisten sopimusten tekemiseksi. Esimerkiksi *E-bayn* kaltaista palveluntarjoajaa voidaan pitää verkossa toimivana markkinapaikkana, koska se antaa muille toimijoille mahdollisuuden perustaa kauppapaikka sen alustalle, jotta niiden tuotteet ja palvelut ovat verkossa kuluttajien tai yritysten saatavilla. Myös sovellusten ja ohjelmien jakamiseen käytettävien verkon sovelluskauppojen katsotaan kuuluvan verkossa toimivan markkinapaikan määritelmään, koska niiden avulla sovellusten kehittäjät voivat myydä tai jaella palvelujaan kuluttajille tai toisille yrityksille. Direktiivin 4 artiklan 17 kohdassa annetun määritelmän soveltamisalaan eivät toisaalta kuulu palvelut, joita käytetään välittäjinä kolmannen osapuolen palveluihin, kuten *Skyscanner*, eivätkä hintavertailupalvelut, jotka

ohjaavat käyttäjän elinkeinonharjoittajan verkkosivustolle, jossa tosiasiallinen sopimus palvelusta tai tuotteesta tehdään.

2. Verkossa toimivan hakukoneen tarjoaja

Verkossa toimiva hakukone on määritelty 4 artiklan 18 kohdassa, ja sitä selitetään tarkemmin johdanto-osan 16 kappaleessa. Se kuvaillaan digitaaliseksi palveluksi, joka antaa käyttäjille mahdollisuuden tehdä hakuja periaatteessa kaikilta verkkosivustoilta tai tietynkielisiltä verkkosivustoilta mitä tahansa aihetta koskevan hakukriteerin perusteella. Määritelmä ei kata tietyn verkkosivuston sisäisiä hakutoimintoja eikä hintavertailusivustoja. Esimerkiksi EUR-Lexin[34] tarjoamaa hakukonetta ei voida pitää direktiivissä tarkoitettuna hakukoneena, koska sen hakutoiminto rajoittuu kyseisen verkkosivuston sisältöön.

3. Pilvipalvelun tarjoaja

Direktiivin 4 artiklan 19 kohdassa pilvipalvelu määritellään ”*digitaaliseksi palveluksi, joka mahdollistaa pääsyn skaalautuvaan ja mukautuvaan joukkoon jaettavissa olevia tietoteknisiä resursseja*”, ja johdanto-osan 17 kappaleessa selitetään tarkemmin käsitteitä ’tietotekniset resurssit’, ’skaalautuva’ ja’ mukautuva joukko’.

Pilvipalvelua voidaan lyhyesti kuvata erityiseksi tietojenkäsittelypalvelujen tyypiksi, jossa käytetään jaettuja resursseja tilauksesta tapahtuvaan tietojenkäsittelyyn. Jaetuilla resursseilla tarkoitetaan minkälaisia tahansa laitteisto- tai ohjelmistokomponentteja (esim. verkot, palvelimet tai muu infrastruktuuri, tallentaminen, sovellukset ja palvelut), jotka annetaan tilauksesta käyttäjien käyttöön tietojenkäsittelyä varten. Käsite ’jaettavissa oleva’ viittaa tietoteknisiin resursseihin, joissa useat käyttäjät käyttävät samaa fyysistä infrastruktuuria tietojenkäsittelyyn. Tietoteknisiä resursseja voidaan pitää jaettavissa olevina, jos palveluntarjoajan käyttämien resurssien joukkoa voidaan laajentaa tai supistaa milloin tahansa käyttäjien vaatimuksista riippuen. Datakeskuksia tai datakeskuksen yksittäisiä komponentteja voidaan siis lisätä tai poistaa, jos laskentatehon tai tallennustilan kokonaismäärää on muutettava. Käsitettä ’mukautuva joukko’ voidaan kuvata kuormituksen mukauttamisena antamalla resursseja käyttöön ja poistamalla niitä käytöstä automaattisesti siten, että kullakin hetkellä käytettävissä olevat resurssit vastaavat mahdollisimman tarkasti kulloistakin kysyntää[35].

Palveluntarjoajat voivat nykyisin tarjota kolmea pilvipalvelumallien päätyyppiä:

- Infrastruktuuri palveluna (Infrastructure as a Service, IaaS): Pilvipalveluluokka, jossa asiakkaalle tarjottava pilviresurssityyppi on infrastruktuuri. Siihen sisältyy laskentaresurssien virtuaalinen tarjoaminen laitteistojen, verkkoyhteyksien ja tallennuspalvelujen muodossa. IaaS-palvelu käyttää palvelimia, tallennustilaa,

[34] Saatavilla osoitteessa http://eur-lex.europa.eu/homepage.html

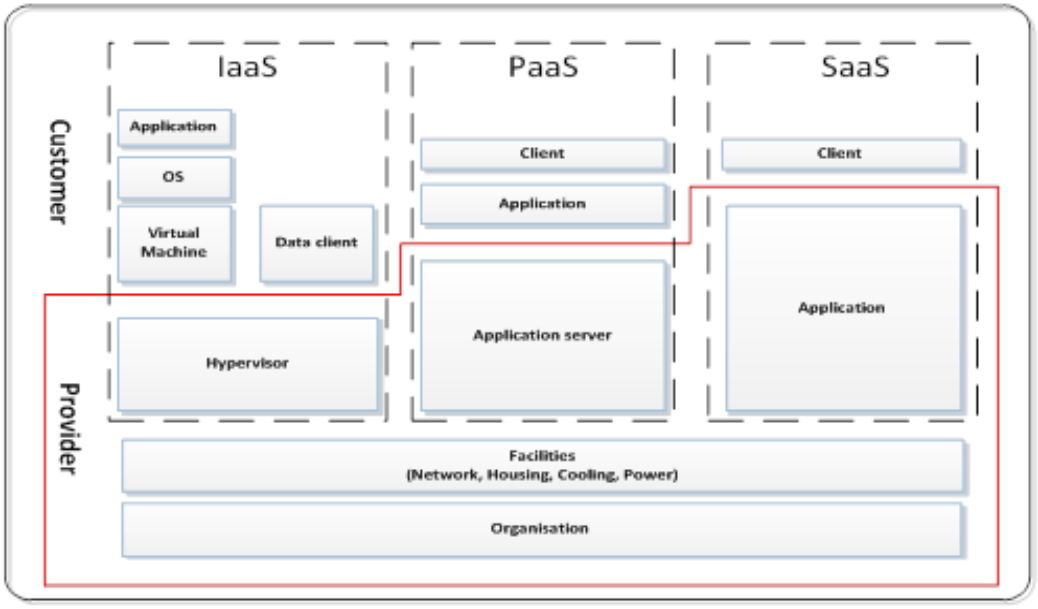
[35] Nikolas Roman Herbst, Samuel Kounev, Ralf Reussner, Karlsruhe Institute of Technology, ”Elasticity in Cloud Computing: What It Is, and What It Is Not”, saatavilla osoitteessa: https://sdqweb.ipd.kit.edu/publications/pdfs/HeKoRe2013-ICAC-Elasticity.pdf. Ks. myös asiakirjan COM(2012) 529 sivut 2–5.

verkkoyhteyksiä ja käyttöjärjestelmiä. Se tarjoaa yritysinfrastruktuurin, jossa yritys voi tallentaa datansa ja käyttää päivittäisessä toiminnassaan tarvittavia sovelluksia.

- Alusta palveluna (Platform as a Service, PaaS): Pilvipalveluluokka, jossa asiakkaalle tarjottava pilviresurssityyppi on palvelualusta. Siihen sisältyvät verkkoalustat, joiden avulla yritykset voivat käyttää olemassa olevia sovelluksia tai kehittää ja testata uusia.

- Ohjelmisto palveluna (Software as a service, SaaS): Pilvipalveluluokka, jossa asiakkaalle tarjottava pilviresurssityyppi on internetin kautta käytettävä sovellus tai ohjelmisto. Tämän pilvipalvelutyypin ansiosta loppukäyttäjän ei enää tarvitse ostaa, asentaa ja hallita ohjelmistoa, ja sillä on se etu, että ohjelmisto on käytettävissä kaikkialla, missä on internetyhteys.

Kuva 5: Pilvilaskennan palvelumallit ja hyödykkeet



ENISA on julkaissut kattavat ohjeet pilvipalvelualan erityiskysymyksistä[36] ja ohjeasiakirjan pilvilaskennan perusteista[37].

4.4.2 Turvallisuusvaatimukset

Verkko- ja tietoturvadirektiivin 16 artiklan 1 kohdan mukaan jäsenvaltioiden on varmistettava, että digitaalisen palvelun tarjoajat toteuttavat asianmukaiset ja oikeasuhteiset tekniset ja organisatoriset toimenpiteet hallitakseen riskejä, joita kohdistuu niiden verkko- ja tietojärjestelmien turvallisuuteen, joita nämä yritykset käyttävät palvelujensa tarjonnassa. Näissä turvallisuustoimenpiteissä olisi otettava huomioon uusin tekniikka ja seuraavat viisi

[36] Saatavilla osoitteessa https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security
[37] ENISA, *Cloud Security Guide for SMEs* (2015). Saatavilla osoitteessa https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes

osatekijää: i) järjestelmien ja tilojen turvallisuus; ii) poikkeamien käsittely; iii) liiketoiminnan jatkuvuuden hallinta; iv) seuranta, tarkastukset ja testaukset; v) kansainvälisten standardien noudattaminen.

Komissiolla on 16 artiklan 8 kohdan nojalla valtuudet hyväksyä täytäntöönpanosäädöksiä näiden osatekijöiden täsmentämiseksi edelleen ja näiden palveluntarjoajien korkean yhdenmukaistamisen tason varmistamiseksi. Komission on tarkoitus hyväksyä täytäntöönpanosäädös syksyllä 2017. Jäsenvaltioiden on lisäksi varmistettava, että digitaalisen palvelun tarjoajat toteuttavat toimenpiteitä poikkeamien vaikutuksen ehkäisemiseksi ja minimoimiseksi, jotta niiden palvelujen jatkuvuus voidaan taata.

4.4.3 Ilmoitusvaatimukset

Jäsenvaltioiden on varmistettava, että digitaalisen palvelun tarjoajat ilmoittavat vakavista poikkeamista toimivaltaiselle viranomaiselle tai CSIRT-toimijalle. Verkko- ja tietoturvadirektiivin 16 artiklan 3 kohdan mukaan digitaalisen palvelun tarjoajilla on ilmoitusvelvollisuus tapauksissa, joissa turvallisuuspoikkeamalla on merkittävä vaikutus palvelun tarjoamiseen. Vaikutuksen merkittävyyden määrittämiseksi 16 artiklan 4 kohdassa luetellaan viisi parametria, jotka digitaalisen palvelun tarjoajien on otettava huomioon. Komissiolla on 16 artiklan 8 kohdan nojalla valtuudet hyväksyä täytäntöönpanosäädöksiä, joissa nämä parametrit määritellään tarkemmin. Nämä parametrit määritellään tarkemmin täytäntöönpanosäädöksessä, jossa täsmennetään 4.4.2 kohdassa tarkoitetut turvallisuusnäkökohdat ja jonka komission aikoo hyväksyä syksyllä 2017.

4.4.4 Riskiperusteinen lähestymistapa sääntelyyn

Verkko- ja tietoturvadirektiivin 17 artiklan mukaan kansallisten toimivaltaisten viranomaisten on kohdistettava digitaalisen palvelun tarjoajiin jälkivalvontatoimia. Jäsenvaltioiden on varmistettava, että toimivaltaiset viranomaiset ryhtyvät toimiin, kun niille esitetään näyttöä siitä, että digitaalisen palvelun tarjoaja ei täytä direktiivin 16 artiklassa säädettyjä vaatimuksia

Lisäksi komissiolla on 16 artiklan 8 ja 9 kohdan nojalla valtuudet hyväksyä turvallisuus- ja ilmoitusvaatimuksiin liittyviä täytäntöönpanosäädöksiä, jotka parantavat yhdenmukaistamisen tasoa digitaalisen palvelun tarjoajien osalta. Direktiivin 16 artiklan 10 kohdan mukaan jäsenvaltiot eivät saa asettaa digitaalisen palvelun tarjoajille muita turvallisuus- tai ilmoitusvaatimuksia direktiivissä säädettyjen vaatimusten lisäksi lukuun ottamatta tapauksia, joissa tällaiset toimenpiteet ovat välttämättömiä keskeisten valtiolle kuuluvien tehtäviensä suojaamiseksi, erityisesti kansallisen turvallisuuden suojaamiseksi ja rikosten tutkimisen, selvittämisen ja syytteeseenpanon mahdollistamiseksi.

Digitaalisen palvelun tarjoajien rajat ylittävän luonteen vuoksi direktiivissä ei noudateta useiden rinnakkaisten lainkäyttövaltojen mallia vaan lähestymistapaa, joka perustuu yrityksen pääasialliseen toimipaikkaan EU:ssa[38]. Tämä lähestymistapa mahdollistaa sen, että digitaalisen palvelun tarjoajiin sovelletaan yksiä sääntöjä, joiden noudattamista valvoo yksi toimivaltainen viranomainen. Tämä on erityisen tärkeää siksi, että monet digitaalisen palvelun

[38] Ks. erityisesti direktiivin 18 artikla

tarjoajat tarjoavat palvelujaan useissa jäsenvaltioissa samanaikaisesti. Tämän lähestymistavan soveltaminen minimoi vaatimusten noudattamisesta digitaalisen palvelun tarjoajille aiheutuvan taakan ja varmistaa digitaalisten sisämarkkinoiden sujuvan toiminnan.

4.4.5 Lainkäyttövalta

Verkko- ja tietoturvadirektiivin 18 artiklan 1 kohdan mukaan digitaalisen palvelun tarjoajan katsotaan kuuluvan sen jäsenvaltion lainkäyttövallan piiriin, jossa sen pääasiallinen toimipaikka sijaitsee. Tapauksissa, joissa digitaalisen palvelun tarjoaja tarjoaa palveluja EU:ssa, mutta ei ole sijoittautunut EU:n alueelle, 18 artiklan 2 kohdassa digitaalisen palvelun tarjoaja velvoitetaan nimeämään edustajan unionin aluetta varten. Tässä tapauksessa digitaalisen palvelun tarjoajan katsotaan kuuluvan sen jäsenvaltion lainkäyttövallan piiriin, johon edustaja on sijoittautunut. Tapauksissa, joissa digitaalisen palvelun tarjoaja tarjoaa palveluja jäsenvaltiossa mutta ei ole nimennyt edustajaa EU:ssa, jäsenvaltio voi periaatteessa panna vireille oikeustoimia digitaalisen palvelun tarjoajaa vastaan, koska digitaalisen palvelun tarjoaja rikkoo direktiivistä johtuvia velvollisuuksiaan.

4.4.6 Pienten digitaalisen palvelun tarjoajien vapauttaminen turvallisuus- ja ilmoitusvaatimusten noudattamisesta

Verkko- ja tietoturvadirektiivin 16 artiklan 11 kohdan mukaan 16 artiklassa säädettyjä turvallisuus- ja ilmoitusvaatimuksia ei sovelleta komission suosituksessa 2003/361/EY[39] tarkoitettuihin mikroyrityksiin ja pieniin yrityksiin. Tämä tarkoittaa, että vaatimukset eivät koske yrityksiä, joiden palveluksessa on vähemmän kuin 50 työntekijää ja joiden vuosiliikevaihto ja/tai taseen loppusumma on enintään 10 miljoonaa euroa. Sillä, tarjoaako yritys ainoastaan verkko- ja tietoturvadirektiivissä tarkoitettuja digitaalisia palveluja vai myös muita palveluja, ei ole merkitystä yrityksen kokoa määritettäessä.

5. Verkko- ja tietoturvadirektiivin suhde muuhun lainsäädäntöön

Tässä jaksossa keskitytään verkko- ja tietoturvadirektiivin 1 artiklan 7 kohdassa annettuihin alakohtaisten säädösten soveltamista koskeviin säännöksiin. Siinä esitetään kolme esimerkkiä alakohtaisista säädöksistä, jotka komissio on arvioinut tähän mennessä, ja selvennetään televiestintäpalvelujen tarjoajiin ja luottamuspalvelun tarjoajiin sovellettavia turvallisuus- ja ilmoitusvaatimuksia.

5.1 Verkko- ja tietoturvadirektiivin 1 artiklan 7 kohta: alakohtaisia säädöksiä koskeva säännös

Verkko- ja tietoturvadirektiivin 1 artiklan 7 kohdan mukaan direktiivin säännöksiä, jotka koskevat keskeisten palvelujen tarjoajille tai digitaalisen palvelujen tarjoajille asetettuja turvallisuus- ja/tai ilmoitusvaatimuksia, ei sovelleta, jos alakohtaisessa EU:n säädöksessä säädetään turvallisuus- ja/tai -ilmoitusvaatimuksista, jotka ovat vaikutukseltaan vähintään vastaavia kuin verkko- ja tietoturvadirektiivissä säädetyt velvollisuudet. Jäsenvaltioiden on

[39] EUVL L 24, 20.5.2003, s. 36.

otettava 1 artiklan 7 kohta huomioon saattaessaan direktiivin osaksi kansallista lainsäädäntöä ja ilmoitettava komissiolle alakohtaisia säädöksiä koskevan säännöksen soveltamisesta.

Menetelmä

Kun arvioidaan alakohtaisen EU:n säädöksen säännösten vastaavuutta verkko- ja tietoturvadirektiivin asiaa koskevien säännösten kanssa, erityistä huomiota olisi kiinnitettävä siihen, sisältyykö alakohtaisessa säädöksessä säädettyihin turvallisuusvelvollisuuksiin toimenpiteitä, joilla varmistetaan verkko- ja tietoturvadirektiivin 4 artiklan 2 kohdassa määritelty verkko- ja tietojärjestelmien turvallisuus.

Ilmoitusvaatimusten osalta verkko- ja tietoturvadirektiivin 14 artiklan 3 kohdassa ja 16 artiklan 3 kohdassa säädetään, että keskeisten palvelujen tarjoajien ja digitaalisen palvelun tarjoajien on ilmoitettava toimivaltaiselle viranomaiselle tai CSIRT-toimijalle viipymättä kaikista poikkeamista, joilla on merkittävä vaikutus palvelun tarjoamiseen. Tältä osin on kiinnitettävä erityistä huomiota keskeisten palvelujen tarjoajan ja digitaalisen palvelun tarjoajan velvollisuuteen sisällyttää ilmoitukseen tiedot, joiden perusteella toimivaltainen viranomainen tai CSIRT-toimija voi määrittää, onko poikkeamalla mahdollisia rajat ylittäviä vaikutuksia.

Tällä hetkellä ei ole olemassa sellaisia digitaalisen palvelun tarjoajia koskevia alakohtaisia säädöksiä, joissa säädettäisiin verkko- ja tietoturvadirektiivin 16 artiklassa säädettyjä vaatimuksia vastaavista turvallisuus- ja ilmoitusvaatimuksista ja jotka voitaisiin ottaa huomioon verkko- ja tietoturvadirektiivin 1 artiklan 7 kohtaa sovellettaessa[40].

Keskeisten palvelujen tarjoajien osalta rahoitusalaan ja erityisesti liitteessä II olevassa 3 ja 4 kohdassa mainittuihin pankkialaan ja finanssimarkkinoiden infrastruktuurien alaan sovelletaan nykyisin alakohtaisista EU:n säädöksistä johtuvia turvallisuus- ja/tai ilmoitusvelvollisuuksia. Tämä johtuu siitä, että finanssilaitosten käyttämien verkko- ja tietojärjestelmien turvallisuus ja vakaus on olennainen osa finanssilaitoksille EU:n säädöksissä asetettuja operatiiviseen riskiin liittyviä vaatimuksia.

Esimerkkejä

i) Toinen maksupalveludirektiivi

Pankkialan ja erityisesti asetuksen (EU) N:o 575/2013 4 artiklan 1 kohdassa määriteltyjen luottolaitosten harjoittaman maksupalvelujen tarjonnan osalta niin kutsutussa toisessa maksupalveludirektiivissä[41] säädetään turvallisuus- ja ilmoitusvaatimuksista, jotka sisältyvät mainitun direktiivin 95 ja 96 artiklaan.

[40] Tämä ei rajoita henkilötietoja koskevasta tietoturvaloukkauksesta ilmoittamista Euroopan tietosuojavaltuutetulle, mistä säädetään yleisen tietosuoja-asetuksen 33 artiklassa.
[41] Direktiivi (EU) 2015/2366, EUVL L 337, 23.12.2015, s. 35.

Tarkemmin sanottuna 95 artiklan 1 kohdassa edellytetään, että maksupalvelutarjoajat ottavat käyttöön asianmukaiset riskinhallintatoimenpiteet ja valvontamekanismit, joiden avulla voidaan hallita niiden tarjoamiin maksupalveluihin liittyviä operatiivisia ja turvallisuusriskejä. Näiden toimenpiteiden osana olisi luotava ja pidettävä yllä tehokkaita poikkeamien hallintamenettelyjä, joihin sisältyy myös merkittävien operatiivisten ja turvapoikkeamien havaitseminen ja luokittelu. Maksupalveludirektiivin johdanto-osan 95 ja 96 kappaleessa selvennetään tällaisten turvallisuustoimenpiteiden luonnetta. Näiden säännösten perusteella on selvää, että säädetyillä toimenpiteillä pyritään hallitsemaan maksupalvelujen tarjoamiseen käytettäviin verkko- ja tietojärjestelmiin liittyviä turvallisuusriskejä. Näiden turvallisuustoimenpiteiden voidaan siis katsoa olevan vaikutukseltaan vähintään vastaavia kuin verkko- ja tietoturvadirektiivin 14 artiklan 1 ja 2 kohdan vastaavat säännökset.

Ilmoitusvaatimusten osalta maksupalveludirektiivin 96 artiklan 1 kohdassa säädetään maksupalveluntarjoajien velvollisuudesta ilmoittaa vakavista turvallisuuspoikkeamista viipymättä toimivaltaiselle viranomaiselle. Lisäksi samoin kuin verkko- ja tietoturvadirektiivin 14 artiklan 5 kohdassa, maksupalveludirektiivin 96 artiklan 2 kohdassa edellytetään, että toimivaltainen viranomainen ilmoittaa poikkeamasta muiden jäsenvaltioiden toimivaltaisille viranomaisille, jos sillä on merkitystä niiden kannalta. Tämä velvollisuus tarkoittaa myös sitä, että turvallisuuspoikkeamia koskeviin ilmoituksiin on sisällyttävä tiedot, joiden perusteella viranomaiset voivat arvioida poikkeaman rajat ylittävää merkitystä. Maksupalveludirektiivin 96 artiklan 3 kohdan a alakohdassa Euroopan pankkiviranomainen valtuutetaan laatimaan yhteistyössä Euroopan keskuspankin kanssa ilmoitusten tarkkaa sisältöä ja muotoa koskevat ohjeet.

Näin ollen voidaan päätellä, että luottolaitosten harjoittamaan maksupalvelujen tarjontaan olisi sovellettava verkko- ja tietoturvadirektiivin 1 artiklan 7 kohdan mukaisesti toisen maksupalveludirektiivin 95 ja 96 artiklassa säädettyjä turvallisuus- ja ilmoitusvaatimuksia verkko- ja tietoturvadirektiivin 14 artiklan vastaavien säännösten sijaan.

ii) Euroopan parlamentin ja neuvoston asetus (EU) N:o 648/2012, annettu 4 päivänä heinäkuuta 2012, OTC-johdannaisista, keskusvastapuolista ja kauppatietorekistereistä

Finanssimarkkinoiden infrastruktuurin osalta asetukseen (EU) 648/2012 yhdessä komission delegoidun asetuksen (EU) 153/2013 kanssa sisältyy keskusvastapuolten turvallisuusvaatimuksia koskevia säännöksiä, joita voidaan pitää alakohtaisina erityissäännöksinä. Näissä säädöksissä säädetään erityisesti verkko- ja tietojärjestelmien turvallisuuteen liittyvistä teknisistä ja organisatorisista toimenpiteistä, jotka menevät yksityiskohtaisuudessaan jopa pidemmälle kuin verkko- ja tietoturvadirektiivin 14 artiklan 1 ja 2 kohta, ja siksi niiden voidaan katsoa täyttävän verkko- ja tietoturvadirektiivin 1 artiklan 7 kohdan vaatimukset turvallisuusvaatimusten osalta.

Tarkemmin sanottuna asetuksen (EU) 648/2012 26 artiklan 1 kohdassa säädetään, että toimijalla on oltava ”*vahvat päätöksenteko-, ohjaus- ja valvontajärjestelyt, joihin sisältyvät selkeä organisaatiorakenne, jossa vastuualueet on määritelty yksityiskohtaisesti, avoimesti ja kattavasti, sekä tehokkaat menettelyt sellaisten riskien tunnistamista, hallitsemista, valvomista ja raportointia varten, joille se on tai saattaa olla alttiina, ja riittävät sisäisen valvonnan*

menetelmät, mukaan luettuina luotettavat hallinto- ja laskentamenetelmät.” Asetuksen 26 artiklan 3 kohdassa vaaditaan, että organisaatiorakenteen on varmistettava palvelujen tarjoamisen ja toiminnan harjoittamisen jatkuvuus ja säännönmukaisuus tarkoituksenmukaisia ja oikeasuhteisia järjestelmiä, voimavaroja ja menettelyjä käyttäen.

Asetuksen 26 artiklan 6 kohdassa tarkennetaan, että keskusvastapuolen on pidettävä yllä ”*tietotekniikkajärjestelmiä, jotka ovat tarjottavien palvelujen ja harjoitettavan toiminnan monimutkaisuuden, moninaisuuden ja tyypin kannalta tarkoituksenmukaisia, jotta varmistetaan korkea turvallisuustaso sekä säilytettävien tietojen eheys ja luottamuksellisuus*.” Lisäksi 34 artiklan 1 kohdan mukaan keskusvastapuolen on otettava käyttöön ja pantava täytäntöön asianmukaiset liiketoiminnan jatkuvuutta koskevat toimintaperiaatteet ja palautumissuunnitelma, joilla olisi varmistettava toiminnan nopea palautuminen, sekä ylläpidettävä niitä.

Näitä velvollisuuksia on tarkennettu Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 648/2012 täydentämisestä keskusvastapuoliin liittyviä vaatimuksia koskevien teknisten sääntelystandardien osalta 19 päivänä joulukuuta 2012 annetussa komission delegoidussa asetuksessa (EU) N:o 153/201[42]. Erityisesti sen 4 artiklassa keskusvastapuoli velvoitetaan kehittämään asianmukaiset riskinhallintavälineet, jotta se voi hallita kaikkia merkityksellisiä riskejä ja raportoida niistä, ja määritellään tarkemmin toimenpiteiden tyyppi (esim. vahvojen tiedotus- ja riskienvalvontajärjestelmien käyttö, riskienhallintatoiminnon riittävät voimavarat ja asiantuntemus ja pääsy kaikkiin merkityksellisiin tietoihin, riittävät sisäisen valvonnan menetelmät, kuten luotettavat hallinto- ja laskentamenetelmät, joiden avulla keskusvastapuolen hallitus voi seurata ja arvioida keskusvastapuolen riskienhallintaperiaatteiden, -menetelmien ja -järjestelmien riittävyyttä ja tehokkuutta).

Lisäksi delegoidun asetuksen 9 artiklassa viitataan nimenomaisesti tietotekniikkajärjestelmien turvallisuuteen ja säädetään konkreettisista teknisistä ja organisatorisista toimenpiteistä, jotka liittyvät vahvan tietoturvakehyksen ylläpitämiseen tietoturvariskin hallitsemiseksi. Näihin toimenpiteisiin olisi sisällyttävä mekanismeja ja menettelyjä, joilla varmistetaan palvelujen saatavuus sekä tietojen oikeellisuus, eheys ja luottamuksellisuus.

iii) 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[43].

Kauppapaikkojen osalta direktiivin 2014/65/EU 48 artiklan 1 kohdassa edellytetään, että markkinoiden ylläpitäjä varmistaa palvelujen jatkuvuuden kaupankäyntijärjestelmässään esiintyvien häiriöiden varalta. Tätä yleistä velvollisuutta on hiljattain tarkennettu ja täydennetty 14 päivänä heinäkuuta 2016 annetulla komission delegoidulla asetuksella (EU) 2017/584[44] Euroopan parlamentin ja neuvoston direktiivin 2014/65/EU täydentämisestä

[42] EUVL L 52, 23.2.2013, s. 41.
[43] EUVL L 173, 12.6.2014, s. 349.
[44] EUVL L 87, 31.3.2017, s. 350.

kauppapaikkojen toiminnan järjestämistä koskevia vaatimuksia täsmentävillä teknisillä sääntelystandardeilla[45]. Etenkin delegoidun asetuksen 23 artiklan 1 kohdassa säädetään, että kauppapaikoilla on oltava käytössään fyysistä ja sähköistä turvallisuutta koskevat menettelyt ja järjestelyt, joiden tarkoituksena on suojata niiden järjestelmiä väärinkäytöltä ja luvattomalta pääsyltä sekä varmistaa tietojen eheys. Näillä toimenpiteiden avulla pitäisi voida estää tai minimoida tietojärjestelmiin kohdistuvien hyökkäysten riskit.

Delegoidun asetuksen 23 artiklan 2 kohdassa vaaditaan edelleen, että markkinoiden ylläpitäjien toteuttamien menettelyjen ja järjestelyjen on mahdollistettava sellaisten riskien nopea tunnistaminen ja hallinta, jotka liittyvät luvattomaan pääsyyn, järjestelmähäiriöihin, jotka haittaavat vakavasti tietojärjestelmien toimintaa tai keskeyttävät sen, ja tietohäiriöihin, jotka vaarantavat tietojen saatavuuden, eheyden tai aitouden. Lisäksi 15 artiklassa asetetaan velvoite, joka mukaan kauppapaikoilla on oltava käytössä liiketoiminnan jatkuvuutta koskevat järjestelyt, joiden avulla voidaan varmistaa järjestelmän riittävä vakaus ja käsitellä häiriötilanteita. Näillä toimenpiteillä on erityisesti varmistettava, että kaupankäyntiä voidaan jatkaa kahden tunnin kuluessa tai pienellä viipeellä kahden tunnin kuluttua häiriötilanteesta ja että menetettyjen tietojen määrä on lähellä nollaa.

Delegoidun asetuksen 16 artiklassa tarkennetaan, että häiriötilanteiden käsittelyä ja hallintaa varten määriteltyjen toimenpiteiden olisi oltava osa kauppapaikkojen liiketoiminnan jatkuvuussuunnitelmaa, ja siinä luetellaan tekijät, jotka markkinoiden ylläpitäjän on otettava huomioon liiketoiminnan jatkuvuussuunnitelmaa laatiessaan (esim. turvallisuustoimiin tarkoitetun erityisryhmän perustaminen ja vaikutusten arvioinnin toteuttaminen riskien yksilöimiseksi ja sen tarkistaminen määräajoin).

Näiden turvallisuustoimenpiteiden sisällön perusteella vaikuttaa siltä, että niillä on tarkoitus hallita ja käsitellä tietojen tai tarjottujen palvelujen saatavuuteen, aitouteen, eheyteen ja luottamuksellisuuteen liittyvää riskiä, ja näin ollen voidaan päätellä, että edellä mainittuihin EU:n alakohtaisin säädöksiin sisältyy turvallisuusvaatimuksia, jotka ovat vaikutukseltaan vähintään vastaavia kuin verkko- ja tietoturvadirektiivin 14 artiklan 1 ja 2 kohdan vastaavat velvollisuudet.

5.2 Verkko- ja tietoturvadirektiivin 1 artiklan 3 kohta: televiestintäpalvelujen tarjoajat ja luottamuspalvelun tarjoajat

Verkko- ja tietoturvadirektiivin 1 artiklan 3 kohdan mukaan direktiivissä säädettyjä turvallisuus- ja ilmoitusvaatimuksia ei sovelleta palveluntarjoajiin, joihin sovelletaan direktiivin 2002/21/EY 13 a ja 13 b artiklan vaatimuksia. Direktiivin 2002/21/EY 13 a ja 13 b artiklaa sovelletaan yleisiä viestintäverkkoja tai yleisesti saatavilla olevia sähköisiä viestintäpalveluja tarjoaviin yrityksiin. Yrityksen on siten yleisten viestintäverkkojen tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjonnan osalta sovellettava direktiivin 2002/21/EY turvallisuus- ja ilmoitusvaatimuksia.

[45] http://ec.europa.eu/finance/securities/docs/isd/mifid/rts/160714-rts-7_en.pdf

Jos sama yritys kuitenkin tarjoaa myös muita palveluja kuten verkko- ja tietoturvadirektiivin liitteessä III lueteltuja digitaalisia palveluja (esim. pilvipalvelu tai verkossa toimiva markkinapaikka) tai direktiivin liitteessä II olevassa 7 kohdassa tarkoitettua nimipalvelua tai IXP-palvelua, yritykseen sovelletaan verkko- ja tietoturvadirektiivin mukaisia turvallisuus- ja ilmoitusvaatimuksia näiden nimenomaisten palvelujen tarjonnan osalta. On syytä huomata, että koska liitteessä II olevassa 7 kohdassa lueteltujen palvelujen tarjoajat kuuluvat keskeisten palvelujen tarjoajien luokkaan, jäsenvaltioiden on toteutettava 5 artiklan 2 kohdan mukainen määritysprosessi ja määritettävä, minkä yksittäisten nimipalvelun, IXP-palvelun tai aluetunnuspalvelun tarjoajien olisi noudatettava verkko- ja tietoturvadirektiivin vaatimuksia. Tämä tarkoittaa, että tällaisen arvioinnin jälkeen ainoastaan niillä nimipalvelun, IXP-palvelun tai aluetunnuspalvelun tarjoajilla, jotka täyttävät verkko- ja tietoturvadirektiivin 5 artiklan 2 kohdan kriteerit, on velvollisuus noudattaa verkko- ja tietoturvadirektiivin vaatimuksia.

Verkko- ja tietoturvadirektiivin 1 artiklan 3 kohdassa tarkennetaan vielä, ettei direktiivissä säädettyjä turvallisuus- ja ilmoitusvaatimuksia sovelleta myöskään luottamuspalvelun tarjoajiin, joihin sovelletaan asetuksen (EU) N:o 910/2014 19 artiklan vastaavia vaatimuksia.

6. Julkaistut kansalliset kyberturvallisuusstrategia-asiakirjat

	Jäsenvaltio	Strategian nimi ja käytettävissä olevat linkit
1	Itävalta	*Austrian Cybersecurity Strategy* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/AT_NCSS.pdf (EN)
2	Belgia	*Securing Cyberspace* (2012) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/ncss-be-fr (FR)
3	Bulgaria	*Cyber Resilient Bulgaria 2020* (2016) http://www.cyberbg.eu/ (BG)
4	Kroatia	*The national cyber security strategy of the republic of Croatia* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CRNCSSEN.pdf (EN)
5	Tšekki	*National cyber security strategy of the Czech Republic for the period from 2015 to 2020* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf (EN)
6	Kypros	*Cybersecurity Strategy of the Republic of Cyprus* (2012) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CybersecurityStrategyoftheRepublicofCyprusv10_English.pdf (EN)
7	Tanska	*The Danish Cyber and Information Security Strategy* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/DK_NCSS.pdf (EN)
8	Viro	*Cyber Security Strategy* (2014) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Estonia_Cyber_security_Strategy.pdf (EN)
9	Suomi	*Finland´s Cyber security Strategy* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/FinlandsCyberSecurityStrategy.pdf (EN)
10	Ranska	*French national digital security strategy* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf (EN)
11	Irlanti	*National Cyber Security Strategy 2015-2017* (2015)

		https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_IE.pdf (EN)
12	Italia	*National Strategic Framework for Cyberspace Security* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/IT_NCSS.pdf (EN)
13	Saksa	*Cyber-security Strategy for Germany* (2016) http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/ModerneVerwaltung-OeffentlicherDienst/Informationsgesellschaft/cybersicherheitsstrategie-2016.pdf?__blob=publicationFile (DE)
14	Unkari	*National Cyber Security Strategy of Hungary* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/HU_NCSS.pdf (EN)
15	Latvia	*Cyber Security Strategy of Latvia 2014–2018* (2014) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss (EN)
16	Liettua	*The programme for the development of electronic information security (cyber-security) for 2011–2019* (2011) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Lithuania_Cyber_Security_Strategy.pdf (EN)
17	Luxemburg	*National Cybersecurity Strategy II (2015)* https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Luxembourg_Cyber_Security_strategy.pdf (EN)
18	Malta	*National Cyber Security Strategy Green Paper* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSSGreenPaper.pdf (EN)
19	Alankomaat	*National Cyber Security Strategy 2* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS2Engelseversie.pdf (EN)
20	Puola	*Cyberspace Protection Policy of the Republic of Poland* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/copy_of_PO_NCSS.pdf (EN)
21	Romania	*Cybersecurity Strategy of Romania* (2011) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/StrategiaDeSecuritateCiberneticaARomaniei.pdf (RO)
22	Portugali	*National Cyberspace Security Strategy* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/portuguese-national-cyber-security-strategy/view

		(EN)
23	Slovakia	*Cyber Security Concept of the Slovak Republic for 2015 – 2020* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/cyber-security-concept-of-the-slovak-republic-1 (EN)
24	Slovenia	*Cyber Security Strategy establishing a system to ensure a high level of cyber security* (2016) http://www.uvtp.gov.si/fileadmin/uvtp.gov.si/pageuploads/Cyber_Security_Strategy_Slovenia.pdf (EN)
25	Espanja	*National Cyber Security Strategy* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_ESen.pdf (EN)
26	Ruotsi	*The Swedish National Cybersecurity Strategy* (2017) http://www.government.se/49edf4/contentassets/b5f956be6c50412188fb4e1d72a5e501/fact-sheet-a-national-cyber-security-strategy.pdf (EN)
27	Yhdistynyt kuningaskunta	*National Cyber Security Strategy (2016-2021)* (2016) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national_cyber_security_strategy_2016.pdf (EN)

7. ENISAn julkaisemat hyvät käytännöt ja suositukset

Poikkeamiin reagointi

- ✓ Poikkeamiin reagoinnin ja kyberkriisiyhteistyön strategiat[46]

Poikkeamien käsittely

- ✓ Poikkeamien käsittelyn automatisointihanke[47]
- ✓ Poikkeamien hallinnan hyvien käytäntöjen opas[48]

Poikkeamien luokittelu ja kuvaus

- ✓ Yleiskatsaus olemassa olevista luokituksista[49]
- ✓ Hyvien käytäntöjen opas luokitusten käyttöön poikkeamien ehkäisyssä ja havaitsemisessa[50]

CSIRT-toimijoiden kypsyys

- ✓ Euroopan kansallisten CSIRT-toimijoiden haasteet vuonna 2016: tutkimus CSIRT-toimijoiden kypsyydestä[51]
- ✓ Tutkimus CSIRT-toimijoiden kypsyydestä – Arviointiprosessi[52]
- ✓ Kypsyyden arviointi koskevat ohjeet kansallisille ja valtiollisille CSIRT-toimijoille[53]

CSIRT-toimijoiden valmiuksien rakentaminen ja koulutus

- ✓ Koulutusmenetelmien hyvien käytäntöjen opas[54]

Tietoja Euroopan nykyisistä CSIRT-toimijoista –Yleiskatsaus CSIRT-toimijoista maittain[55]

[46] ENISA, *Strategies for incident response and cyber crisis cooperation* (2016). Saatavilla osoitteessa https://www.enisa.europa.eu/publications/strategies-for-incident-response-and-cyber-crisis-cooperation
[47] Lisätietoja: https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/incident-handling-automation
[48] ENISA, *Good Practice Guide for Incident Management* (2010). Saatavilla osoitteessa https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management
[49] Lisätietoja: https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/existing-taxonomies
[50] ENISA, *A good practice guide of using taxonomies in incident prevention and detection* (2017). Saatavilla osoitteessa https://www.enisa.europa.eu/publications/using-taxonomies-in-incident-prevention-detection
[51] ENISA, *Challenges for National CSIRTs in Europe in 2016: Study on CSIRT Maturity* (2017). Saatavilla osoitteessa https://www.enisa.europa.eu/publications/study-on-csirt-maturity
[52] ENISA, *Study on CSIRT Maturity – Evaluation Process* (2017). Saatavilla osoitteessa https://www.enisa.europa.eu/publications/study-on-csirt-maturity-evaluation-process
[53] ENISA, CSIRT Capabilities. *How to assess maturity? Guidelines for national and governmental CSIRTs* (2016). Saatavilla osoitteessa https://www.enisa.europa.eu/publications/csirt-capabilities
[54] ENISA, *Good Practice Guide on Training Methodologies* (2014). Saatavilla osoitteessa https://www.enisa.europa.eu/publications/good-practice-guide-on-training-methodologies
[55] Lisätietoja: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map