JULKAISUJA 9/2017

Verkko- ja tietoturvadirektiivi
Kansallista täytäntöönpanoa tukevan työryhmän loppuraportti

LIIKENNE- JA VIESTINTÄMINISTERIÖ

LVM 1892–2017

Suomi Finland 100

Liikenne- ja viestintäministeriön

visio
Hyvinvointia ja kilpailukykyä hyvillä yhteyksillä

toiminta-ajatus
Liikenne- ja viestintäministeriö edistää väestön hyvinvointia ja elinkeinoelämän kilpailukykyä.
Huolehdimme toimivista, turvallisista ja edullisista yhteyksistä.

arvot
Rohkeus
Oikeudenmukaisuus
Yhteistyö

LIIKENNE- JA VIESTINTÄMINISTERIÖ

Julkaisun päivämäärä
20.4.2017

Julkaisun nimi
Verkko- ja tietoturvadirektiivi. Kansallista täytäntöönpanoa tukevan työryhmän loppuraportti

Tekijät
Verkko- ja tietoturvadirektiivin täytäntöönpanoa tukeva työryhmä

Toimeksiantaja ja asettamispäivämäärä
Liikenne- ja viestintäministeriö, 4.10.2016

Julkaisusarjan nimi ja numero
Liikenne- ja viestintäministeriön julkaisuja 9/2017

ISSN (verkkojulkaisu) 1795-4045
ISBN (verkkojulkaisu) 978-952-243-505-7
URN http://urn.fi/URN:ISBN:978-952-243-505-7

Asiasanat
Tietoturva, verkko- ja tietoturvadirektiivi, riskienhallinta

Yhteyshenkilö
Timo Kievari, Maija Rönkä

Tiivistelmä
Pääministeri Juha Sipilän hallituksen kärkihankkeena Suomeen rakennetaan digitaalisen liiketoiminnan kasvuympäristö ja sujuvoitetaan säädöksiä. Yhtenä digitaalisen liiketoiminnan kasvuympäristön rakentamisen kärkihankkeen keskeisenä toimenpiteenä liikenne- ja viestintäministeriö on hyväksynyt luottamusta internetiin sekä digitaalisiin toimintatapoihin lisäävän kansallisen tietoturvastrategian. Verkko- ja tietoturvadirektiivin kansallisen täytäntöönpanon keskeiset tavoitteet on määritelty tietoturvastrategiassa. Strategian mukaan direktiivin täytäntöönpanon yhteydessä turvataan yritysten mahdollisuudet sovittaa tietoturvariskien hallintaan liittyvät uudet velvoitteet osaksi muiden liiketoiminnan riskiensä hallintaa.

Täytäntöönpanolle asetettujen tavoitteiden varmistamiseksi liikenne- ja viestintäministeriö asetti verkko- ja tietoturvadirektiivin täytäntöönpanoa tukevan työryhmän 4.10.2016. Työryhmän tehtävänä oli tukea liikenne- ja viestintäministeriötä direktiivin voimaansaattamisen valmistelussa, arvioida vaihtoehtoisia sääntelytapoja ja edistää direktiivin edellyttämää yhteistyötä soveltamisalaan kuuluvien toimialojen välillä.

Verkko- ja tietoturvadirektiivillä jäsenvaltiot velvoitetaan järjestämään tietoturvallisuuteen liittyvää viranomaistoimintaa. Direktiivi velvoittaa myös yhteiskunnan toiminnan kannalta keskeisten palveluiden tarjoajat ja digitaalisten palveluiden tarjoajat huolehtimaan tietoturvariskien hallinnasta ja raportoimaan poikkeamista valvontaviranomaisille.

Työryhmä ehdottaa direktiivin kansallisen täytäntöönpanon lähtökohdaksi otettavan, että direktiivin mukaiset velvoitteet tulisi saattaa osaksi kansallisia relevantteja toimialakohtaisia säädöksiä. Täytäntöönpanossa tulee erityisesti kiinnittää huomiota siihen, ettei päällekkäisiä velvoitteita muusta voimassaolevasta lainsäädännöstä johtuvien velvoitteiden kanssa tarpeettomasti syntyisi. Työryhmän katsoo, että direktiivin mukaisina verkko- ja tietojärjestelmien turvallisuudesta vastaavina viranomaisina tulisi direktiivin eri toimialoilla toimia ne viranomaiset, jotka vastaavat jo nykytilassa toimialan turvallisuusvelvoitteiden valvonnasta eli nk. sektorikohtaiset valvontaviranomaiset. Lisäksi työryhmän näkemyksen mukaan Viestintäviraston tulisi toimia direktiivin tarkoittamana tietoturvaloukkauksiin reagoivana ja niitä tutkivana yksikkönä (CSIRT-toimija) sekä kansallisena yhteyspisteenä.

KOMMUNIKATIONS-
MINISTERIET

Publikationsdatum
20.4.2017

Publikation
Direktivet om nät- och informationssäkerhet
Slutrapport av den arbetsgrupp som stöder det nationella genomförandet

Författare
Arbetsgrupp som stöder genomförandet av direktivet om nät- och informationssäkerhet

Tillsatt av och datum
Kommunikationsministeriet, 4.10.2016

Publikationsseriens namn och nummer
Kommunikationsministeriets publikationer 9/2017

ISSN (webbpublikation) 1795-4045
ISBN (webbpublikation) 978-952-243-505-7
URN http://urn.fi/URN:ISBN:978-952-243-505-7

Ämnesord
Informationssäkerhet, direktivet om nät- och informationssäkerhet, riskhantering

Kontaktperson
Timo Kievari, Maija Rönkä

Rapportens språk
Finska

Sammandrag
Ett av spetsprojekten i statsminister Juha Sipiläs regering är att skapa en tillväxtmiljö för digital affärsverksamhet och att göra lagstiftningen smidigare. Som en central åtgärd i spetsprojektet har kommunikationsministeriet godkänt en informationssäkerhetsstrategi för att stärka förtroendet för internet och digitala verksamhetssätt. I informationssäkerhetsstrategin fastställs dessutom de viktigaste målen för det nationella genomförandet av direktivet om nät- och informationssäkerhet. Enligt strategin tryggas i samband med genomförandet av direktivet företagens möjligheter att samordna de nya förpliktelser som gäller hanteringen av informationssäkerhetsrisker till en del av hanteringen av övriga risker för affärsverksamheten.

För att säkerställa att de mål som ställts för genomförandet uppnås tillsatte kommunikationsministeriet den 4 oktober 2016 en arbetsgrupp som stöd för genomförandet av direktivet om nät- och informationssäkerhet. Arbetsgruppen hade till uppgift att stödja kommunikationsministeriet i beredningen av ikraftsättandet av direktivet, bedöma alternativa regleringssätt och främja det samarbete som direktivet förutsätter mellan de sektorer som omfattas av dess tillämpningsområde.

Genom direktivet om nät- och informationssäkerhet förpliktas medlemsstaterna att ordna myndighetsverksamhet som hänför sig till informationssäkerhet. Dessutom ska medlemsstaterna förplikta vissa leverantörer av tjänster som är viktiga med tanke på ett fungerande samhälle och leverantörerna av digitala tjänster att sörja för hanteringen av informationssäkerhetsrisker och att rapportera avvikelser till tillsynsmyndigheterna.

Arbetsgruppen föreslår att utgångspunkten för det nationella genomförandet av direktivet ska vara att förpliktelserna i direktivet införlivas med den relevanta, nationella sektorsspecifika lagstiftningen. Vid genomförandet ska det fästas särskilt avseende vid att det inte i onödan uppstår förpliktelser som är överlappande med förpliktelserna i någon annan gällande lagstiftning. Arbetsgruppen anser att sådana i direktivet avsedda myndigheter som ansvarar för säkerheten i nätverks- och informationssystem ska inom de olika sektorer som omfattas av direktivet vara de myndigheter som redan för närvarande ansvarar för tillsynen av säkerhetsförpliktelser inom en sektor, alltså de så kallade sektorspecifika tillsynsmyndigheterna. Dessutom anser arbetsgruppen att Kommunikationsverket ska vara en sådan behörig enhet för hantering av it-säkerhetsincidenter (CSIRT-enhet) och en sådan nationell kontaktpunkt som avses i direktivet.

MINISTRY OF TRANSPORT AND COMMUNICATIONS

Date
20.4.2017

Title of publication

Network and information security directive
Working group's final report to support national implementation

Author(s)
Working group supporting implementation of the network and information security directive

Commissioned by, date
Ministry of Transport and Communications, 04/10/2016

Publication series and number
Publications of the Ministry of Transport and Communications 9/2017

ISSN (online) 1795-4045
ISBN (online) 978-952-243-505-7
URN http://urn.fi/URN:ISBN:978-952-243-505-7

Keywords
Information security, Directive on security of network and information systems (NIS Directive), risk management

Contact person
Timo Kievari, Maija Rönkä

Language of the report
Finnish

Abstract

One of the key projects of Prime Minister Juha Sipilä's government is the construction of an environment for the growth of digital business in Finland and the streamlining of regulations. As one of the pivotal measures of the key project to construct an environment for the growth of digital business, the Ministry of Transport and Communications has approved a national information security strategy to increase confidence in the Internet as well as in digital operations. The pivotal goals of national implementation of the Directive on security of network and information systems (NIS Directive) are specified in the information security strategy. Implementation of the directive in accordance with the strategy includes securing opportunities for businesses to include the new obligations related to the management of information security as part of their management of other business risks.

In order to ensure the implementation of these objectives, the Ministry of Transport and Communications established a working group to support implementation of the NIS Directive on 4 October 2016. The task of the working group was to support the Ministry of Transport and Communications in preparing the inception of the directive, assessing alternative regulation modes, and promoting the cooperation required by the directive between the sectors covered by the scope of application.

The NIS Directive requires member states to organise official functions related to information security and also to oblige both the providers of a service which is essential for the maintenance of critical societal activities, and the providers of digital services, to take care of their information security management in addition to reporting on incidents to the supervisory authorities.

The working group proposes that the starting point of the national implementation of the directive is to assume that the obligations under the directive be established as part of the relevant national sector-specific regulations. Special attention should be given in implementation to ensuring that no duplication of obligations due to the requirements of any other current legislation are generated unnecessarily. The working group is of the view that the authorities responsible for the security of network and information systems in the various fields in accordance with the directive, should be the authorities that are already responsible for the supervision of security obligations in those sectors: i.e. the sector-specific supervisory authorities. In addition, according to the view of the working group, the Finnish Communications Regulatory Authority should function as the computer security incident response team (CSIRT) referred to in the directive, as well as the single point of contact.

Sisällysluettelo

Liikenne- ja viestintäministeriölle

Liikenne- ja viestintäministeriö asetti verkko- ja tietoturvadirektiivin täytäntöönpanoa tukevan työryhmän 4.10.2016. Työryhmän tehtävänä oli tukea liikenne ja viestintäministeriötä direktiivin voimaansaattamisen valmistelussa, arvioida vaihtoehtoisia sääntelytapoja sekä edistää direktiivin edellyttämää yhteistyötä soveltamisalaan kuuluvien toimialojen välillä.

Työryhmän puheenjohtajana toimi Timo Kievari sekä sihteereinä Maija Rönkä ja Johanna Tuohino liikenne- ja viestintäministeriöstä. Työryhmän jäsenet olivat seuraavat:

työ- ja elinkeinoministeriö, Heikki Haukirauma, kehitysjohtaja
(varajäsen Johanna Ylitepsa, hallitussihteeri

valtiovarainministeriö, Jaakko Weuro, neuvotteleva virkamies
(varajäsen Tuija Kuusisto, erityisasiantuntija)

sosiaali- ja terveysministeriö, Teemupekka Virtanen, erityisasiantuntija
(varajäsen Maarit Puhto, tietohallintopäällikkö)

Viestintävirasto: Anne Lohtander, lakimies
(varajäsen Hanna Heiskanen, lakimies)

Liikenteen turvallisuusvirasto Trafi, Maija Mansikkaniemi, lakimies

Liikennevirasto, Paul Kinnunen, tietoturvapäällikkö
(varajäsen Maija Turunen, lakimies)

Huoltovarmuuskeskus, Sauli Savisalo, johtaja
(varajäsen Erkki Räsänen, varautumispäällikkö)

Finanssivalvonta, Anne Nisén, riskiasiantuntija
(varajäsen Markku Koponen, toimistopäällikkö)

Energiavirasto, Tarvo Siukola, johtava asiantuntija
(varajäsen Sari Broman, lakimies)

Sosiaali- ja terveysalan lupa- ja valvontavirasto Valvira, Antti Härkönen, yli-insinööri (varajäsen Jari Knuuttila, ylitarkastaja)

FiCom ry, Petri Aaltonen, toimitusjohtaja
(varajäsen Jussi Mäkinen, lakimies)

Elinkeinoelämän keskusliitto EK, Mika Susi, johtava yritysturvallisuusasiantuntija (varajäsen Veli Sinda, asiantuntija)

Teknologiateollisuus ry, Marja Hamilo, asiantuntija
(varajäsen Ville Peltola, toimialajohtaja)

Energiateollisuus ry, Kenneth Hänninen, johtaja
(varajäsen Esa Niemelä, asiantuntija)

Finanssialan keskusliitto FK, Mika Linna, johtava asiantuntija
(varajäsen Peter Jansson, asiantuntija)

Ympäristöministeriö ei nimennyt jäsentä työryhmään, mutta erityisasiantuntija Riitta Autere toimi ministeriön yhdyshenkilönä.

Työryhmä kokoontui yhdeksän kertaa, joista viisi kertaa oli jaettu sektorikohtaisesti seuraavasti: liikennesektori, finanssisektori, terveydenhuoltosektori, energiasektori ja digisektori. Sektorikohtaisissa kokouksissa keskityttiin arvioimaan kunkin sektorin voimassa olevaa turvallisuusriskienhallinta lainsäädäntöä sekä verkko- ja tietoturvadirektiivin vaihtoehtoisia täytäntöönpanomalleja.

Työryhmä ehdottaa tämän loppuraportin otettavan direktiivin kansallisen täytäntöönpanon lähtökohdaksi.

Saatuaan loppuraportin valmiiksi työryhmä luovuttaa sen kunnioittavasti liikenne- ja viestintäministeriölle

Helsingissä 20.4.2017

Timo Kievari	Heikki Haukirauma	Jaakko Weuro
Teemupekka Virtanen	Anne Lohtander	Paul Kinnunen
Maija Mansikkaniemi	Sauli Savisalo	Anne Nisén
Tarvo Siukola	Antti Härkönen	Petri Aaltonen
Mika Susi	Marja Hamilo	Mika Linna
Kenneth Hänninen		
	Maija Rönkä	Johanna Tuohino

1. Johdanto

Euroopan parlamentti ja neuvosto antoivat direktiivin toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa ((EU) 2016/1148) 6.7.2016. Direktiivi on tullut voimaan 8.8.2016 ja jäsenvaltioiden on annettava ja julkaistava direktiivin noudattamisen edellyttämät lait, asetukset ja hallinnolliset määräykset viimeistään 9.5.2018.

Direktiivin yleisenä tavoitteena on kasvattaa suojan tasoa verkko- ja tietoturvaloukkauksia, -riskejä ja -uhkia vastaan. Tarkoituksena on saavuttaa korkeatasoinen verkko- ja tietojärjestelmien turvallisuus EU:n alueella parantamalla varautumista kansallisella tasolla, lisäämällä EU-tason yhteistyötä sekä säätämällä riskienhallinta- ja raportointivelvoitteita keskeisille palveluntarjoajille sekä tietyille digitaalisten palveluiden tarjoajille.

Direktiiviehdotus annettiin osana komission vuonna 2013 antaman EU:n kyberturvallisuusstrategian toimeenpanoa. Strategian yhtenä tavoitteena on kehittää tietoyhteiskunnan vankkarakenteisuutta parantamalla varautuneisuutta, yhteistyötä, osaamista ja tiedonvaihtoa verkko- ja tietoturvan saralla.

Pääministeri Juha Sipilän hallituksen kärkihankkeena Suomeen rakennetaan digitaalisen liiketoiminnan kasvuympäristö. Yhtenä kärkihankkeen keskeisenä toimenpiteenä valmistellaan ja toimeenpannaan luottamusta internetiin sekä digitaalisiin toimintatapoihin lisäävä kansallinen tietoturvastrategia. Verkko- ja tietoturvadirektiivin kansallisen täytäntöönpanon keskeiset tavoitteet on määritelty tietoturvastrategiassa. Strategian mukaan direktiivin täytäntöönpanon yhteydessä turvataan yritysten mahdollisuudet sovittaa tietoturvariskien hallintaan liittyvät uudet velvoitteet osaksi muiden liiketoiminnan riskiensä hallintaa. Strategian mukaisesti näiden tavoitteiden varmistamiseksi liikenne- ja viestintäministeriö asetti voimaansaattamista tukevan työryhmän arvioimaan nykyisen sääntelyn riittävyys kullakin direktiivin soveltamisalaan kuuluvalla toimialalla.

Hallitusohjelman kärkihankkeena on myös sääntelyn sujuvoittaminen. Kärkihankkeen mukaan säädöspolitiikan ohjausta selkeytetään, tavoitteena sääntelyn nettomääräinen keventäminen ja säädöksille vaihtoehtoisten ohjauskeinojen käytön lisääminen. Tavoitteena on turhan sääntelyn purkaminen ja hallinnollisen taakan keventäminen. Suomen EU-vaikuttamisen yhtenä painopisteenä on nykyistä vähäisempi, parempi ja kevyempi sääntely. EU-säännösten toimeenpanossa pidättäydytään kansallisesta lisäsääntelystä.

2. Verkko- ja tietoturvadirektiivi

2.1 Pääasiallinen sisältö

2.1.1 Viranomaistehtävien määrittely

Direktiivillä jäsenvaltiot velvoitetaan laatimaan kansallinen verkko- ja tietojärjestelmien turvallisuutta koskeva strategia sekä määrittämään direktiivistä johtuvia viranomaistehtäviä tietoturvallisuuden varmistamiseksi ja riskien hallitsemiseksi eri toimialoilla. Jäsenvaltiot velvoitetaan myös osallistumaan keskinäiseen yhteistyöhön uusissa EU-tason yhteistyöryhmissä tietoturvaloukkauksia koskevien tietojen sekä parhaiden kansallisten käytäntöjen vaihtamiseksi.

Toimivaltainen viranomainen

Direktiivin 8 artiklan 1 kohdan mukaan jäsenvaltioiden on nimettävä yksi tai useampi verkko- ja tietojärjestelmien turvallisuudesta vastaava kansallinen toimivaltainen viranomainen, jonka toiminta kattaa ainakin liitteessä II tarkoitetut toimialat ja liitteessä III tarkoitetut palvelut. Jäsenvaltiot voivat antaa tämän tehtävän olemassa olevalle viranomaiselle tai olemassa oleville viranomaisille. 8 artiklan 2 kohdan mukaan toimivaltaisten viranomaisten on seurattava direktiivin soveltamista kansallisesti. Direktiivin 15 ja 17 artiklan mukaan toimivaltaisella viranomaisella on oltava tarvittavat valtuudet ja keinot arvioida, noudattavatko keskeisten palvelujen tarjoajat direktiivin mukaisia velvollisuuksiaan, sekä tämän vaikutuksia verkko- ja tietojärjestelmien turvallisuuteen. Direktiivin 14 ja 16 artiklan mukaan direktiivissä määritellyistä poikkeamista on ilmoitettava toimivaltaiselle viranomaiselle tai CSIRT (Computer security incident response teams)-toimijalle.

Keskitetty kansallinen yhteyspiste

Toimivaltaisten viranomaisten lisäksi jäsenvaltioiden on nimettävä verkko- ja tietojärjestelmien turvallisuudesta vastaava keskitetty kansallinen yhteyspiste. Jäsenvaltiot voivat antaa tämän tehtävän olemassa olevalle viranomaiselle. Keskitetyn yhteyspisteen tehtävänä on yhteydenpito, jotta voidaan varmistaa jäsenvaltion viranomaisten rajat ylittävä yhteistyö ja rajat ylittävä yhteistyö muiden jäsenvaltioiden asiaankuuluvien viranomaisten kanssa. Keskitetyn yhteyspisteen ei pitäisi saada suoraan ilmoituksia poikkeamista, elleivät ne toimi myös toimivaltaisena viranomaisena tai CSIRT-toimijana. Toimivaltaisen viranomaisen tai CSIRT-toimijan olisi kuitenkin voitava antaa keskitetylle yhteyspisteelle tehtäväksi toimittaa poikkeamia koskevia ilmoituksia muiden asiaan liittyvien jäsenvaltioiden keskitetyille yhteyspisteille. Keskitetyn yhteyspisteen olisi toimitettava direktiivin mukaisesti perustetulle jäsenvaltioiden väliselle yhteistyöryhmälle tiivistelmäraportti, joka sisältää tiedot vastaanotettujen ilmoitusten lukumäärästä sekä maininnan ilmoitettujen poikkeamien luonteesta, kuten turvallisuusloukkausten tyypeistä, niiden vakavuudesta tai niiden kestosta.

CSIRT-toimija

Jäsenvaltion on myös nimettävä yksi tai useampi CSIRT-toimija. Toimijan on täytettävä direktiivin liitteessä I asetetut vaatimukset. CSIRT-toimija vastaa riskien ja poikkeamien käsittelystä. CSIRT-toimijan tehtäviin on sisällytettävä vähintään seuraavat:

i) poikkeamien seuranta kansallisella tasolla;
ii) ennakkovaroitusten, varoitusten, ja tiedotusten antaminen sekä tiedon levittäminen riskeistä ja poikkeamista asiaankuuluville sidosryhmille;
iii) poikkeamiin reagointi;
iv) dynaamisen riskin ja poikkeamien analysointi sekä tilannetietoisuus;
v) CSIRT-verkostoon osallistuminen.

Lisäksi CSIRT-toimijoiden on luotava yhteistyösuhteita yksityiseen sektoriin ja edistettävä yhteisten tai standardoitujen toimintatapojen omaksumista ja käyttöä poikkeamien ja riskien käsittelymenettelyissä sekä luokittelujärjestelmissä. Palveluntarjoajat voidaan velvoittaa tekemään poikkeamailmoituksia myös CSIRT-toimijalle.

CSIRT-toimija voidaan perustaa toimivaltaisen viranomaisen yhteyteen.

EU-tason yhteistyö

Lisäksi direktiivissä säädetään, että EU-tasolla perustetaan yhteistyöryhmä jäsenvaltioiden keskinäisen strategisen yhteistyön ja tietojen vaihtamisen tukemiseksi ja helpottamiseksi, luottamuksen ja luotettavuuden kehittämiseksi sekä verkko- ja tietojärjestelmien korkeatasoisen ja yhtenäisen suojan varmistamiseksi unionissa. Yhteistyöryhmä muodostuu jäsenvaltioiden edustajista, komissiosta ja Euroopan unionin verkko- ja tietoturvavirasto ENISAsta (European Union Agency for Network and Information Security). Yhteistyöryhmän tehtävät on määritelty direktiivissä. Yhteistyöryhmä on aloittanut toimintansa 9.2.2017 ja kokoontunut kerran.

Direktiivissä säädetään myös kansallisten CSIRT-toimijoiden verkoston perustamisesta EU-tasolla. CSIRT-verkosto muodostuu jäsenvaltioiden CSIRT-toimijoiden ja EU:n instituutioiden tietotekniikan kriisiryhmän (CERT-EU) edustajista. Verkoston tehtävät on määritelty direktiivissä.

2.1.2 Keskeisten palveluntarjoajien määritteleminen

Jäsenvaltiot velvoitetaan määrittämään direktiivin soveltamisalan mukaisilla toimialoilla sektorikohtaiset keskeisten palvelujen tarjoajat, jotka ovat sijoittautuneet niiden alueelle. Direktiivin soveltamisalan mukaiset toimialat on määritelty direktiivin liitteessä II.

LIITE II

4 ARTIKLAN 4 KOHDASSA TARKOITETTUJEN TOIMIJOIDEN TYYPIT

Toimiala	Osa-alue	Toimijan tyyppi
1. Energia	a) Sähkö	– Sähköalan yritykset, sellaisina kuin ne määritellään Euroopan parlamentin ja neuvoston direktiivin 2009/72/EY (1) 2 artiklan 35 kohdassa, jotka harjoittavat kyseisen direktiivin 2 artiklan 19 kohdassa määriteltyä toimitusta
		– Jakeluverkonhaltijat, sellaisina kuin ne määritellään direktiivin 2009/72/EY 2 artiklan 6 kohdassa
		– Siirtoverkonhaltijat, sellaisina kuin ne määritellään direktiivin 2009/72/EY 2 artiklan 4 kohdassa
	b) Öljy	– Öljynsiirtoputkistojen haltijat
		– Öljyn tuotanto-, jalostus- ja käsittelylaitteistojen haltijat sekä öljyn varastointia ja siirtoa hoitavat operaattorit
	c) Kaasu	– Maakaasun toimittajat, sellaisina kuin ne määritellään Euroopan parlamentin ja neuvoston direktiivin 2009/73/EY (2) 2 artiklan 8 kohdassa
		– Jakeluverkonhaltijat, sellaisina kuin ne määritellään direktiivin 2009/73/EY 2 artiklan 6 kohdassa
		– Siirtoverkonhaltijat, sellaisina kuin ne määritellään direktiivin 2009/73/EY 2 artiklan 4 kohdassa
		– Varastointilaitteiston haltijat, sellaisina kuin ne määritellään direktiivin 2009/73/EY 2 artiklan 10 kohdassa
		– Nesteytetyn maakaasun käsittelylaitteiston haltijat, sellaisina kuin ne määritellään direktiivin 2009/73/EY 2 artiklan 12 kohdassa
		– Maakaasualan yritykset, sellaisina kuin ne määritellään direktiivin 2009/73/EY 2 artiklan 1 kohdassa
		– Maakaasun jalostus- ja käsittelylaitteistojen haltijat
2. Liikenne	a) Lentoliikenne	– Lentoliikenteen harjoittajat, sellaisina kuin ne määritellään Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 300/2008 (3) 3 artiklan 4 kohdassa
		– Lentoaseman pitäjät, sellaisina kuin ne määritellään Euroopan parlamentin ja neuvoston direktiivin 2009/12/EY (4) 2 artiklan 2 kohdassa, lentoasemat, sellaisina kuin ne määritellään kyseisen direktiivin 2 artiklan 1 kohdassa, mukaan lukien Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 1315/2013 (5) liitteessä II olevassa 2 jaksossa luetellut ydinlentoasemat, sekä lentoasemilla sijaitsevia lisärakennelmia ja -laitteita hoitavat toimijat
		– Liikenteenhallinnan ylläpitäjät, jotka tarjoavat lennonjohtopalvelua, sellaisena kuin se määritellään Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 549/2004 (6) 2 artiklan 1 kohdassa
	b) Rautatieliikenne	– Rataverkon haltijat, sellaisina kuin ne määritellään Euroopan parlamentin ja neuvoston direktiivin 2012/34/EU (7) 3 artiklan 2 kohdassa
		– Rautatieyritykset, sellaisina kuin ne määritellään direktiivin 2012/34/EU 3 artiklan 1 kohdassa, mukaan lukien palvelupaikan ylläpitäjät, sellaisina kuin ne määritellään direktiivin 2012/34/EU 3 artiklan 12 kohdassa
	c) Vesiliikenne	– Sisävesillä, merillä ja rannikoilla matkustaja- ja rahtiliikennettä hoitavat yhtiöt, sellaisina kuin ne määritellään meriliikennettä varten Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 725/2004 (8) liitteessä I, lukuun ottamatta noiden yhtiöiden liikennöimiä yksittäisiä aluksia
		– Euroopan parlamentin ja neuvoston direktiivin 2005/65/EY (9) 3 artiklan 1 kohdassa määriteltyjen satamien hallinnointielimet, mukaan lukien niiden satamarakenteet, sellaisina kuin ne määritellään asetuksen (EY) N:o 725/2004 2 artiklan 11 kohdassa, sekä toimijat, jotka huolehtivat tuotantolaitoksista ja laitteista satamien alueella
		– Euroopan parlamentin ja neuvoston direktiivin 2002/59/EY (10) 3 artiklan o alakohdassa määriteltyjen alusliikennepalvelujen tarjoajat

Toimiala	Osa-alue	Toimijan tyyppi
	d) Tieliikenne	– Tieviranomaiset, sellaisina kuin ne määritellään komission delegoidun asetuksen (EU) 2015/962 (11) 2 artiklan 12 kohdassa, jotka vastaavat liikenteenhallinnasta
		– Euroopan parlamentin ja neuvoston direktiivin 2010/40/EU (12) 4 artiklan 1 kohdassa määriteltyjen älykkäiden liikennejärjestelmien ylläpitäjät
3. Pankkiala		– Luottolaitokset, sellaisina kuin ne määritellään Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 575/2013 (13) 4 artiklan 1 kohdassa
4. Finanssimarkkinoiden infrastruktuurit		– Euroopan parlamentin ja neuvoston direktiivin 2014/65/EU (14) 4 artiklan 24 kohdassa määriteltyjen kauppapaikkojen ylläpitäjät
		– Keskusvastapuolet, sellaisina kuin ne määritellään Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 648/2012 (15) 2 artiklan 1 kohdassa
5. Terveydenhuoltoala	Terveydenhuoltolaitokset (mukaan lukien sairaalat ja yksityisklinikat)	– Terveydenhuollon tarjoajat, sellaisina kuin ne määritellään Euroopan parlamentin ja neuvoston direktiivin 2011/24/EU (16) 3 artiklan g alakohdassa
6. Juomaveden toimittaminen ja jakelu		– Neuvoston direktiivin 98/83/EY (17) 2 artiklan 1 kohdan a alakohdassa määritellyn ihmisten käyttöön tarkoitetun veden toimittajat ja jakelijat, lukuun ottamatta jakelijoita, joille ihmisten käyttöön tarkoitetun veden jakelu on ainoastaan osa niiden yleistä toimintaa, joka muodostuu sellaisten muiden hyödykkeiden ja tavaroiden jakelusta, joita ei katsota keskeisiksi palveluiksi.
7. Digitaalinen infrastruktuuri		– IXP
		– Nimipalvelujen tarjoajat
		– Aluetunnusrekisterit

Direktiivissä on määritelty kriteerit keskeisten palvelujen tarjoajien määrittämiseksi. Direktiivin mukaan keskeisen palvelun tarjoajan on tarjottava palvelua, joka on keskeinen yhteiskunnan ja/tai talouden kriittisten toimintojen ylläpitämiseksi. Tämän palvelun on oltava riippuvainen verkko- ja tietojärjestelmistä. Lisäksi palveluun kohdistuvalla poikkeamalla tulisi olla merkittäviä haitallisia vaikutuksia kyseisen palvelun tarjoamiseen.

Direktiivin mukaan jäsenvaltioiden on laadittava luettelo keskeisistä palveluista. Palveluiden luettelon on sisällettävä kaikki jäsenvaltion alueella tarjottavat palvelut, jotka täyttävät direktiivin vaatimukset. Luetteloa on käytettävä viitekohtana määritettäessä keskeisten palvelujen tarjoajia. Luettelon tarkoituksena on määrittää direktiivissä tarkoitettujen toimialojen keskeisten palvelujen tyypit erottaen ne näin muista kuin keskeisistä toiminnoista, joista tietyn toimialan toimija saattaa olla vastuussa.

Jäsenvaltion on myös määriteltävä, mihin toimijoihin sovelletaan verkko- ja tietojärjestelmien turvallisuutta koskevia velvollisuuksia. Direktiivin mukaan tämä voitaisiin tehdä esimerkiksi hyväksymällä luettelo, jossa luetellaan kaikki keskeisten palvelujen tarjoajat tai hyväksymällä toimenpiteitä, joiden avulla palvelun tarjoajat voitaisiin määrittää.

Merkittävää haitallista vaikutusta arvioidessa jäsenvaltioiden on direktiivin mukaan huomioitava direktiivissä määritellyt seikat, kuten esimerkiksi palvelusta riippuvaisten käyttäjien lukumäärä ja toimijan markkinaosuus. Myös toimialakohtaisia tekijöitä olisi otettava huomioon määritettäessä sitä, olisiko poikkeamalla merkittävä haitallinen vaikutus keskeisen palvelun tarjoamiseen. Direktiivin johdanto-osassa on annettu tästä seuraavia esimerkkejä:

”Energiantoimittajien osalta tällaisiin tekijöihin voisi sisältyä tuotetun kansallisen energian määrä tai osuus siitä; öljyntoimittajien osalta päiväkohtainen määrä; lentoliikenteen, mukaan lukien lentoasemat ja lentoliikenteen harjoittajat, sekä rautatieliikenteen ja merisatamien osalta osuus kansallisesta liikennemäärästä ja matkustajien tai rahtikuljetusten lukumäärä vuodessa; pankkialan tai finanssimarkkinoiden infrastruktuurien osalta niiden järjestelmäkohtainen merkitys perustuen kokonaisvaroihin tai näiden kokonaisvarojen ja bruttokansantuotteen suhteeseen; terveydenhuoltoalan osalta palvelun tarjoajan hoidossa olevien potilaiden lukumäärä vuodessa; veden tuotannon, käsittelyn ja toimittamisen osalta vesimäärä sekä käyttäjien lukumäärä ja tyypit, mukaan lukien esimerkiksi sairaalat, julkiset palveluorganisaatiot tai henkilöt, sekä vaihtoehtoisten veden lähteiden olemassaolo saman maantieteellisen alueen kattamiseksi.”[1]

Jäsenvaltioiden on säännöllisesti (vähintään kahden vuoden välein) tarkistettava ja tarvittaessa saatettava ajan tasalle määritettyjen keskeisten palvelujen tarjoajien luettelo. Direktiivin mukaan keskeisten palvelujen tarjoajia määritettäessä sijoittautuminen jäsenvaltioon edellyttää tosiasiallista toimintaa ja kiinteää toimipaikkaa. Mikäli toimijat tarjoavat sekä keskeisiä että muita palveluita, on niihin sovellettava direktiivin vaatimuksia vain keskeisiksi katsottujen palveluiden osalta.

2.1.3 Tietoturva- ja raportointivelvoitteet

Direktiivin mukaan jäsenvaltioiden on velvoitettava keskeisten palveluiden tarjoajat sekä digitaalisen palvelun tarjoajat hallitsemaan verkko- ja tietojärjestelmiensä turvallisuuteen kohdistuvia riskejä sekä raportoimaan poikkeamista toimivaltaiselle viranomaiselle tai CSIRT-toimijalle.

Turvallisuusriskienhallintavelvoitteet

Keskeiset palveluntarjoajat

Direktiivin mukaan keskeiset palvelun tarjoajat tulee kansallisilla säädöksillä velvoittaa tekemään riskienhallintatoimenpiteitä ja ilmoittamaan poikkeamista viranomaiselle. Direktiivin mukaan jäsenvaltioiden on huolehdittava, että keskeisten palvelujen tarjoajat toteuttavat asianmukaiset ja oikeasuhtaiset tekniset ja organisatoriset toimenpiteet hallitakseen riskejä, joita kohdistuu niiden verkko- ja tietojärjestelmien turvallisuuteen, joita nämä keskeisten palvelujen tarjoajat käyttävät toiminnoissaan. Näillä toimenpiteillä on varmistettava riskiin suhteutettu verkko- ja tietojärjestelmien turvallisuuden taso uusin tekniikka huomioon ottaen. Verkko- ja tietojärjestelmien turvallisuudella tarkoitetaan näiden järjestelmien 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.

Palveluntarjoajille määrättävät tekniset ja organisatoriset toimenpiteet eivät saisi edellyttää jonkin tietyn kaupallisen tieto- ja viestintäteknologiatuotteen suunnittelua, kehittämistä tai valmistamista tietyllä tavalla.

Palveluntarjoajien olisi varmistettava käyttämiensä verkko- ja tietojärjestelmien turvallisuus. Näitä ovat ensisijaisesti yksityiset verkko- ja tietojärjestelmät, joita hallinnoi niiden oma tietotekninen henkilöstö tai joiden tietoturvahallinto on ulkoistettu. Turvallisuus- ja

[1] (EU)2016/1148 johdanto-osa kohta 28

ilmoitusvaatimuksia olisi sovellettava huolimatta siitä, huolehtivatko ne verkko- ja tietojärjestelmiensä ylläpidosta sisäisesti vai ulkoistavatko ne sen.

Digitaalisten palveluiden tarjoajat

Direktiivin 16 artiklan mukaan myös digitaalisen palvelun tarjoajat on velvoitettava hallitsemaan verkko- ja tietojärjestelmiin kohdistuvia riskejä ja ilmoittamaan poikkeamista toimivaltaiselle viranomaiselle tai CSIRT-toimijalle.

Digitaalisia palvelun tarjoajia ovat direktiivin liitteen III mukaisesti verkossa toimivat markkinapaikat, verkossa toimivat hakukoneet sekä pilvipalvelut. Koska keskeisten palvelujen tarjoajien ja digitaalisen palvelun tarjoajien välillä on perustavanlaatuisia eroja, kun otetaan huomioon erityisesti edellisten suora yhteys fyysiseen infrastruktuuriin ja jälkimmäisten rajat ylittävä luonne, on tarve yhdenmukaisille säännöille keskeisempää digitaalisten palveluntarjoajien osalta.

Keskeisten palvelujen tarjoajien osalta jäsenvaltioiden olisi voitava määrittää asiaankuuluvat palvelujen tarjoajat ja määrätä vaatimuksia, jotka ovat tiukempia kuin tässä direktiivissä säädetyt. Sen sijaan digitaalisen palvelun tarjoajia ei olisi määritettävä, koska direktiiviä on sovellettava kaikkiin sen soveltamisalaan kuuluviin digitaalisen palvelun tarjoajiin. Komissio voi myös antaa täytäntöönpanosäädöksiä yhdenmukaistaakseen digitaalisen palvelun tarjoajia koskevat turvallisuus- ja ilmoitusvaatimukset. Jäsenvaltiot eivät voisi säätää digitaalisen palvelun tarjoajille direktiiviä pidemmälle meneviä velvollisuuksia.

Raportointivelvollisuus

Jäsenvaltioiden on varmistettava, että keskeisten palvelujen tarjoajat ilmoittavat ilman aiheetonta viivytystä toimivaltaiselle viranomaiselle tai CSIRT-toimijalle poikkeamista, joilla on merkittävä vaikutus niiden tarjoamien keskeisten palvelujen jatkuvuuteen. Poikkeamalla tarkoitetaan direktiivissä mitä tahansa tapahtumaa, joka tosiasiassa vaikuttaa haitallisesti verkko- ja tietojärjestelmien turvallisuuteen. Ilmoituksiin on sisällytettävä tiedot, joiden perusteella toimivaltainen viranomainen tai CSIRT-toimija voi määrittää poikkeaman mahdollisen rajat ylittävän vaikutuksen. Ilmoittaminen ei lisää ilmoituksen tekevän osapuolen vastuuta.

Lisäksi jäsenvaltioiden tulee velvoittaa digitaalisten palveluiden tarjoajat ilmoittamaan kansallisille viranomaisille kaikista poikkeamista, joilla on merkittävä vaikutus sellaisen liitteessä III tarjotun palvelun tarjoamiseen, jota ne tarjoavat unionissa. Ilmoituksiin on sisällytettävä tiedot, joiden perusteella toimivaltainen viranomainen tai CSIRT-toimija voi määrittää mahdollisen rajat ylittävän vaikutuksen merkittävyyden. Direktiivin 16 artiklassa on määritelty tarkemmin miten on arvioitava, onko poikkeamalla merkittävä vaikutus.

3. Nykytila

3.1 Lainsäädäntö ja käytäntö

3.1.1 Johdanto

Tieto- ja viestintäteknologia sekä niihin liittyvät palvelut muuttavat yhteiskunnan toimintaa sekä valtarakenteita mullistavalla tavalla. Esineiden internet, massadatan hyödyntäminen, automatisaatio, robotisaatio, keinoäly, virtuaalitodellisuus ja kehittyvät älyteknologiat ovat esimerkkejä tulevaisuuden digitaalisista muutostekijöistä, joiden muokkaamassa toimintaympäristössä yritykset kilpailevat asiakkaista ja markkinaosuuksista. Tässä murroksessa parhaiten menestyvät ne, jotka kykenevät tarjoamaan asiakkaiden tarpeiden mukaisia korkealaatuisia ja luotettavia tietotekniikkaa hyödyntäviä tavaroita ja palveluita mahdollisimman kannattavasti. Digitalisaatio mahdollistaa toimintatapojen ja liiketoimintamallien tehostamisen ja perustavanlaisen uudistamisen tiedon hyödyntämiseen perustuviksi. Suomella on erinomaiset edellytykset nousta digitalisaatiokilvan kärkisijoille ja profiloitua erityisen luotettavan digitaalisen liiketoiminnan kasvuympäristönä.

Tieto- ja viestintäteknologia-ala muodostaa merkittävän osan Suomen bruttokansantuotteesta. Toimialan yritysten liikevaihto vuonna 2013 oli 43,4 miljardia euroa (josta teleyritykset 4,5 miljardia euroa, ohjelmistot, konsultointi ja tietopalvelut 7,9 miljardia euroa sekä tietokoneiden ja sähkölaitteiden valmistus 31 miljardia euroa).

Toimiala on merkittävällä tavalla vientipainotteinen, sillä Suomen loppukäyttäjäkulutusta kuvaavan IT-markkinan liikevaihto oli vuonna 2014 yhteensä 6 miljardia euroa (josta laitteet 1,5 miljardia euroa, ohjelmistot 1,3 miljardia euroa ja IT-palvelut 3,2 miljardia euroa). Suomen bruttokansantuote vuonna 2012 oli noin 200 miljardia euroa ja niin sanotun internet-talouden osuuden on arvioitu muodostavan siitä noin 10 prosenttia.

Vaikka valtiolla ja kunnilla on merkittävä osuus Suomen IT-markkinan ostovoimasta, on julkisen hallinnon ostovoiman merkitys verrattain pieni suhteessa toimialan kansantaloudelliseen arvoon, joka nojaa pitkälti kansainväliseen vientiin.

Digitalisaatiolla tarkoitetaan tässä yhteydessä muutosta, jossa tieto- ja viestintäteknologiaa sekä siihen perustuvia palveluita hyödyntämällä pyritään muodostamaan aiempaa suurempi osuus liiketoiminnan tai julkisten palveluiden arvosta. Digitalisaatio voi siis toimia taloudellisen toimeliaisuuden katalyyttinä. Toisin sanoen, digitalisaatio voi kiihdyttää arvonlisän muodostamista yrityksissä ja julkishallinnossa.

Suomessa onkin arvioitu voitavan saavuttaa 56 miljardin euron verran uutta liikevaihtoa sekä 48.000 uutta työpaikkaa, jos "suomalaiset yritykset ottavat roolin teollisen internetin alustojen ja ekosysteemien avaintoimijoina".

Kansainvälisillä markkinoilla on keskeinen merkitys Suomessa harjoitettavalle liiketoiminnalle

Viestintäpalveluiden markkinoiden kehittyminen on johtanut internetin eksponentiaaliseen kasvuun. Internet kaksinkertaistuu alle kahden vuoden välein käyttäjämäärällä ja välitetyn datan määrällä mitattuna. Laajeneminen on mahdollistanut yrityksille sellaisen liiketaloudellisen arvon muodostumisen, joka ei ole riippuvaista ajasta, alueesta tai aineesta. Sekä teknologian kehitys, että internetin luonne eräänlaisena "rajattomana"

tuotannontekijänä ovat avanneet Suomessa toimiville yrityksille mahdollisuuksia osallistua maailman markkinoille ja skaalata liiketoimintaansa uusille markkina-alueille erittäin nopeasti ja verrattain pienin muuttuvin kustannuksin.

Näitä mahdollisuuksia ei ole kuitenkaan hyödynnetty täysimääräisesti. Suomen kotimarkkinan pienuudesta sekä ICT-alan vientipainotteisuudesta johtuen on tärkeää turvata eurooppalaisen sisämarkkinan toimivuus sekä Suomessa toimivien yritysten esteetön pääsy kansainvälisille markkinoille. Samalla on erittäin tärkeää huolehtia siitä, että Suomi on jatkossakin houkutteleva kohde sellaisille sijoituksille, joita liiketoimintaansa digitalisoivat yritykset tekevät arvonmuodostusta kehittääkseen. Suomessa on saavutettu sääntelyllä ja julkisen ja yksityisen sektorin yhteistyöllä luotettava toimintaympäristö. Houkuttelevuuteen sijoittumismaana vaikuttavat sekä sääntelyn vaatimusten taso, että sääntelyn ennakoitavuus..

EU:ssa on arvioitu, että digitaalisten sisämarkkinoiden täydellisellä toteutumisella voitaisiin saavuttaa 415 miljardin euron kasvu EU:n bruttokansantuotteeseen. Lisäksi on laskettu, että EU:n kansalaisten henkilötiedoilla on vuositasolla yhteensä 315 miljardin euron liiketaloudellinen arvo. Sisämarkkinoiden esteet ilmenevät muun muassa ylimääräisinä kustannuksina, joita tavaroiden ja palveluiden tarjoaminen toisiin jäsenvaltioihin aiheuttaa. Esimerkiksi rajat ylittävässä kuluttajakaupassa vieraan EU-jäsenvaltion lainsäädännön noudattamisesta aiheutuu yksittäiselle yritykselle keskimäärin 9000 euron kustannukset per jäsenvaltio. On tärkeää huolehtia siitä, ettei EU:n jäsenvaltioiden kansallisen lainsäädännön erilaisuus muodostu uusien markkinoiden kehityksen esteeksi.

Luottamuspula jarruttaa markkinoiden kehitystä

Globalisaation, digitalisaation ja verkostoitumisen kehitystrendit luovat uusia liiketoimintamahdollisuuksia. Samalla ne kuitenkin aiheuttavat myös monenlaista luottamuspulaa markkinatoimijoiden välille. Luottamuksen ansaitseminen on todennäköisesti sitä vaikeampaa, mitä merkittävämmällä tavalla tietotekniikka ottaa ohjat ihmisten arjen palveluissa. Esimerkiksi robottiauton tai täysin automaattisesti ohjautuvan lentokoneen matkustajan luottamus on ansaittava, jotta uudet palvelumuodot hyväksyttäisiin asiakkaiden taholta. Palvelun luotettavuutta on mahdollista hyödyntää kilpailuetuna kilpailijoihin nähden.

Luottamuspulaa kuitenkin ilmenee monin tavoin. Jopa 88 prosenttia haastatelluista 28.000 eurooppalaisesta kertoi muuttaneensa tapojaan käyttää internetiä tietoturvahuolien vuoksi. Suomalaisista 59 prosenttia arvioi tuntevansa digitaalisiin palveluihin liittyvät riskit hyvin, kun EU:n keskiarvo oli 50 prosenttia. Suomalaiset pitävät mahdollisuuksiaan EU:ssa toiseksi parhaina verkkorikollisuudelta suojautumiseen.

Luottamusta voivat heikentää yhtäältä teknisen toteutuksen kuten tietoteknisen ohjelmoinnin tahattomat laadulliset puutteet tai yleisemmin riskien hallinnan laiminlyönti, jotka voivat vaarantaa digitaalisten palveluiden toimintaa ohjauksessa käsitellyn tiedon saatavuuden, eheyden, aitouden tai luottamuksellisuuden. Toisaalta luottamusta voivat heikentää tahalliset tietoturvaloukkaukset, joilla puututaan oikeudettomasti tai rangaistavalla tavalla tiedon saatavuuteen, aitouteen, eheyteen tai luottamuksellisuuteen. Molemmissa tapauksissa tietoturvapoikkeamat voivat estää tai vaarantaa verkkojen ja laitteiden ja sitä kautta palveluiden tarkoituksenmukaisen toiminnan.

Tietoturvapoikkeamien vaikutusta digitalisoitua liiketoimintaa harjoittaville yrityksille on vaikeaa selvittää. Voidaan kuitenkin arvioida, että taloudelliset vahingot voivat olla sitä suurempia, mitä suuremman osan tiedon käsittely muodostaa yrityksen liiketoiminnan arvonmuodostuksesta. Tietoturvapoikkeamien aiheuttamat ongelmat ovat myös omiaan

aiheuttamaan mainehaittaa ja heikentämään asiakkaiden luottamusta yrityksen toimintaan. On selvää, että luottamus laadukkaaseen ja turvalliseen tiedonkäsittelyyn on keskeinen edellytys esimerkiksi eri tavoin automatisoitujen liikennepalvelujen hyväksyttävyydelle.

Myös tahallisten tietoturvaloukkausten vaikutuksia uhreiksi joutuneiden yritysten varallisuudelle, maineelle, suhteille, yrityssalaisuuksille ja työntekijöille on vaikea selvittää, mutta ne voivat olla erittäin merkittäviä. Suuryrityksiltä on yksittäisissä tietomurtotapauksissa viety kymmenien miljoonien käyttäjien tietoja. Yksittäiset tapaukset ovat aiheuttaneet yksittäisille yrityksille satojen miljoonien dollarien vahinkoja. Iso-Britanniassa 81 prosenttia suurista organisaatioista oli joutunut vuoden sisällä tietoturvaloukkauksen kohteeksi. Loukkauksista aiheutuneet kustannukset kaksinkertaistuivat vuoden aikana 0,6–1,15 miljoonan punnan suuruisiksi per organisaatio.

Suomessa lainsäädäntö turvaa jo nykyisin verrattain korkeatasoisen tietosuojan ja tietoturvan tason. Lainsäädäntömme muodostaa yritystoiminnalle kilpailuedun niihin valtioihin nähden, joissa näin ei ole. Kilpailuedun säilyttäminen tuleekin huomioida myös säädettäessä uutta lainsäädäntöä.

Luottamuspulan pienentämiseen pyrkivä liiketoiminta sekä toisaalta julkisen vallan toimintaympäristön kehitystä tukevat toimenpiteet voivat luoda edellytyksiä luotettavasti digitalisoitujen hyödykkeiden uusien markkinoiden kehittymiselle.

Luottamuspulaan liittyvien esteiden poistaminen markkinoilta parantaa samalla julkishallinnon mahdollisuuksia hankkia digitaalisia palveluita hyödynnettäväksi tehokkaasti ja turvallisesti toiminnassaan.

Tietoturvariskien hallinta

Korkealaatuisten ja luotettavien digitaalista tietoa hyödyntävien palveluiden tarjoaminen edellyttää tietoturva-asioiden kokonaisvaltaista huomioimista liiketoimintaa järjestettäessä. Tuotteet ja palvelut on suunniteltava, valmistettava ja ylläpidettävä siten, että tietoturva muodostaa niiden erottamattoman ja sisäänrakennetun osan. Toisin sanoen tietoturva on huomioitava liiketoiminnan koko elinkaaren aikana. Tietoturvariskejä voidaan hallita erilaisin toisiaan täydentävin toimenpitein kuten toimintaympäristön valinnalla, sopimussuhtein, tietoturvaa parantavien tuotteiden avulla, tietoturvaan liittyvän osaamisen parantamisella, tietoturvariskien vakuuttamisella, sertifikaattien ja standardien avulla tai hankkimalla esimerkiksi auditointipalveluita.

Tietoturvariskien hallinnan kannalta on tärkeää, että markkinoilla olisi saatavilla yhteen toimivia tiedon hyödyntämisen liittyviä laitteita, ohjelmistoja ja palveluita. Tätä on mahdollista kehittää yhtäältä yhdenmukaistamalla vaatimuksia esimerkiksi standardisoinnin ja sääntelyn keinoin. Toisaalta riskien hallintaa voidaan edistää myös kehittämällä luottamusverkostoja, joissa tietoa voidaan jakaa eri toimijoiden välillä. Tiedon jakaminen voi mahdollistaa virheistä oppimisen sekä ohjelmistojen laatuvirheiden ja haavoittuvuuksien korjaamisen. Luottamusta riskien hallintaan voi myös lisätä sertifioimalla, todentamalla, hajauttamalla ja vakuuttamalla.

3.1.2 Suomen tietoturvallisuusstrategia

Suomen tietoturvallisuusstrategia hyväksyttiin liikenne- ja viestintäministerin päätöksellä 10.3.2016. Strategia painottuu kilpailukyvyn ja vientiedellytysten varmistamiseen, EU:n digitaalisten sisämarkkinoiden kehittämiseen sekä yksityisyyden suojan ja muiden perusoikeuksien turvaamiseen.

Strategiatyön puitteet on määritelty pääministeri Juha Sipilän hallituksen hallitusohjelman toimintasuunnitelmassa ja esitelty strategian johdannossa. Strategian visio on laadittu näistä lähtökohdista kumpuavien tavoitteiden ja painopisteiden mukaiseksi.

Hallitusohjelman lisäksi strategian sisältöön vaikuttavat verkko- ja tietoturvadirektiiviehdotuksessa strategialle asetetut vaatimukset. Strategiassa tarkastellaan verkko- ja tietoturvadirektiiviehdotuksen edellyttämällä tavalla tietoturvaan liittyvää osaamista ja yleisen tietoisuuden kehittämistä sekä tutkimus- ja kehitystyön merkitystä. Riskienhallinnan ja niiden tunnistamisen osalta strategian keskeinen viesti on, että toimijoilla on oltava mahdollisuus arvioida tietoturvatoimenpiteitään riskiperusteisesti eli suhteuttaa ne osaksi muiden riskien hallintaa. Julkisen ja yksityisen sektorin välistä yhteistyötä verkko- ja tietoturvallisuuteen liittyvässä ennaltaehkäisyssä, reagoinnissa ja korjaavissa toimenpiteissä on myös käsitelty useissa strategian toimenpiteissä.

Strategia on jatkumoa vuosien 2003 ja 2008 tietoturvastrategioille sekä vuoden 2013 kyberturvallisuusstrategialle. Nyt laadittu strategia painottuu toimeksiantonsa mukaisesti erityisesti digitaaliseen liiketoimintaan sekä tulevasta verkko- ja tietoturvadirektiivistä seuraaviin strategisiin vaatimuksiin.

Myös verkko- ja tietoturvadirektiivin kansallisen täytäntöönpanon keskeiset tavoitteet on määritelty tietoturvastrategiassa. Strategian mukaan direktiivin täytäntöönpanon yhteydessä turvataan yritysten mahdollisuudet sovittaa tietoturvariskien hallintaan liittyvät uudet velvoitteet osaksi muiden liiketoiminnan riskiensä hallintaa.

3.1.3 Palveluntarjoajien toimintaan liittyvät turvallisuusvaatimukset ja turvallisuuspoikkeamista ilmoittaminen viranomaisille

Kuten edellä on todettu, globalisaation, digitalisaation ja verkostoitumisen kehitystrendit luovat uusia liiketoimintamahdollisuuksia. Sähköistä tietoa hyödynnetään kiihtyvällä tahdilla erilaisten yhteiskunnallisten hyödykkeiden tuottamiseen. Eri toimialojen hyödyketuotannossa ja viranomaisohjauksessa on entistä huolellisemmin huomioitava tiedon hyödyntämisen hyötyjä ja riskejä. Kunkin toimialan hyödyketuotannossa käytettävät tietoverkot ja sähköiset tietojärjestelmät tulisi suunnitella, rakentaa ja ylläpitää siten, että toiminta täyttää riskienhallinnan perusteella määritellyt laatuvaatimukset. Laatuvaatimukset voidaan määritellä 1) sopimusosapuolten välillä taloudellisen optimoinnin keinoin taikka 2) toimialan ohjauksesta vastaavan viranomaisen toimesta.

Laatuvaatimuksia voidaan määritellä esimerkiksi toimijoiden välisin yksityisoikeudellisin sopimuksin. Sopimuksiin voi liittyä ehtoja, jotka määrittelevät hyödykkeiden ominaisuuksien laadullisen tason.

Monilla yhteiskunnan keskeisestä hyödyketuotannosta vastaavilla eri toimialoilla on myös hyödykkeiden tuottajia ja käyttäjiä koskevia lakisääteisiä velvoitteita, joilla turvataan toiminnan laatu ja turvallisuus. Lakisääteisten laatuvaatimusten taustalla on arvopunninnan keinoin määritelty tarve hallita toiminnan yhteiskunnallisesti merkittäviä vaikutuksia.

Palveluntarjoajien toimintaan liittyvistä turvallisuusvaatimuksista on pidettävä erillään valtionhallinnolle asetetut vaatimukset tietoturvallisuudesta. Valtioneuvoston asetuksessa tietoturvallisuudesta (681/2010) valtionhallinnossa säädetään valtionhallinnon viranomaisten asiakirjojen käsittelyä koskevista yleisistä tietoturvallisuusvaatimuksista sekä asiakirjojen luokittelun perusteista ja luokittelua vastaavista asiakirjojen käsittelyssä noudatettavista tietoturvallisuusvaatimuksista.

Yhtäältä sähköisten viestintä- ja tietojärjestelmien käyttöön perustuvan liiketoiminnan harjoittajaan sovellettavat vaatimukset ovat horisontaalisesti eri toimialoilla toimivia palveluntarjoajia koskevia. Tällaista on esimerkiksi sähköturvallisuutta, sähkömagneettista säteilyä, tuotevastuuta, kuluttajansuojaa ja vahingonkorvausvastuuta koskeva sääntely.

Toisaalta direktiivin soveltamisalalla toimivia palveluntarjoajia koskee monet toiminnan laatua ja turvallisuutta koskevat toimialakohtaiset vaatimukset. Tällaisia ovat erimerkiksi energian toimitusvarmuutta, finanssitoiminnan vakavaraisuutta, ilmailun, meri- tie- ja raideliikenteen turvallisuutta sekä potilasturvallisuutta koskevat toimialakohtaisesta sääntelystä johtuvat vaatimukset.

Hallitusohjelman hengessä on tärkeää, että liiketoiminnan harjoittajia koskevaa horisontaalinen ja toimialakohtainen sääntely olisi kokonaisuutena selkeää ja ennakoitavaa ja niistä aiheutuva hallinnollinen taakka mahdollisimman kevyttä.

Sähköinen viestintä, henkilötietojen käsittely sekä sähköinen tunnistaminen

Tietoyhteiskuntakaaressa (917/2014) säädetään sähköistä viestinnän ja tietoyhteiskunnan palvelujen tarjonnasta. Sähköisen viestintä luo edellytykset digitaalisten järjestelmien käytölle myös eri toimialoilla. Tietoyhteiskuntakaaressa onkin säädetty viestintäverkkojen ja viestintäpalvelujen laatuvaatimuksista. Yleiset viestintäverkot ja -palvelut sekä niihin liitettävät viestintäverkot ja -palvelut on suunniteltava, rakennettava ja ylläpidettävä siten, että sähköinen viestintä on tekniseltä laadultaan hyvää ja tietoturvallista. Lisäksi viestintäverkkojen ja -palvelujen tulee kestää normaalit odotettavissa olevat tietoturvauhat, niiden laatua ja toimintavarmuutta tulee voida seurata, niihin kohdistuvat merkittävät tietoturvaloukkaukset ja -uhat sekä niiden toimivuutta merkittävästi häiritsevät viat ja häiriöt tulee voida havaita eikä kenenkään tietosuojan, tietoturvan tai muiden oikeuksien tule vaarantua.

Tietoyhteiskuntakaaressa säädetään myös niistä EU:n radiolaitedirektiivin (2014/53/EU) mukaisista olennaisista vaatimuksista, jotka EU:ssa markkinoille saatettavien eräiden radiolaitteiden on täytettävä. Näillä vaatimuksilla voidaan huolehtia siitä, että markkinoille saatettavat radiolaitteet toimivat yhteen muiden laitteiden kanssa ja tukevat petoksilta suojaavia ominaisuuksia. Lisäksi radiolaitteet eivät saa vahingoittaa viestintäverkon toimintaa ja niihin tulee sisältyä turvalaitteita, jotka takaavat käyttäjien henkilötietojen ja yksityisyyden suojan.

Tietoyhteiskuntakaaressa säädetään lisäksi viestinnän ja palvelujen jatkuvuuden turvaamisesta tietoturvan ja häiriöiden hallinnasta sekä häiriöistä ilmoittamisesta. Teleyrityksen on ilmoitettava viipymättä Viestintävirastolle, jos sen palveluun kohdistuu tai sitä uhkaa merkittävä tietoturvaloukkaus taikka muu tapahtuma, joka estää viestintäpalvelun toimivuuden tai häiritsee sitä olennaisesti.

Henkilötietojen käsittelystä säädetään henkilötietolaissa (523/1999). Henkilötietolaki on yleislaki, jonka säädöksiä on noudatettava lähtökohtaisesti kaikessa henkilötietojen käsittelyssä. Henkilötietolaissa säädetään henkilötietojen käsittelyn tietoturvallisuudesta ja tietojen säilytyksestä. Lain mukaan rekisterinpitäjän on toteutettava tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi asiattomalta pääsyltä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä taikka muulta laittomalta käsittelyltä. EU:n yleinen tietosuoja-asetus ((EU) 2016/679) on hyväksytty ja se tulee sovellettavaksi toukokuussa 2018.

Vahvasta sähköisestä tunnistamisesta sekä tunnistuspalveluiden tarjoamisesta palveluntarjoajille, yleisölle ja toisille tunnistuspalvelun tarjoajille säädetään laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009). Laissa säädetään sähköisen tunnistamisen järjestelmälle asetettavista tietoturvavaatimuksista. Lain mukaan tunnistamispalvelun tarjoajan on huolehdittava palvelujensa tietojen suojaamisesta sekä riittävästä tietoturvasta. Lain mukaan tunnistuspalvelun tarjoajan on salassapitosäännösten estämättä ilmoitettava ilman aiheetonta viivästystä tunnistuspalveluunsa luottaville osapuolille, tunnistusvälineiden haltijoille, muille luottamusverkostossa toimiville sopimuspuolilleen sekä Viestintävirastolle palvelun toimivuuteen, tietoturvaan tai sähköisen henkilöllisyyden käyttöön kohdistuvista merkittävistä uhkista tai häiriöistä.

EU:n nk. eIDAS-asetuksen (EU) 910/2014 19 artiklassa säädetään sähköisten luottamuspalveluiden tietoturvallisuusvaatimuksista ja velvollisuudesta ilmoittaa valvovalle viranomaiselle tietoturvaloukkauksista ja eheyden menetyksistä.

Verkko- ja tietoturvadirektiivin mukaiset toimialat

Verkko- ja tietoturvadirektiivin liitteessä II on määritelty ne toimialat ja toimialojen osa-alueet, joilla jäsenvaltioiden on määriteltävä keskeiset palvelut ja niiden tarjoajat. Direktiivin mukaiset toimialat ovat energia (sähkö, öljy, kaasu), liikenne (lentoliikenne, rautatieliikenne, vesiliikenne, tieliikenne), pankkiala, finanssimarkkinoiden infrastruktuurit, terveydenhuoltoala (terveydenhuoltolaitokset), juomaveden toimittaminen ja jakelu sekä digitaalinen infrastruktuuri.

Direktiivin liitteessä III on määritelty digitaalisten palveluiden tyypeiksi verkossa toimiva markkinapaikka, verkossa toimiva hakukone sekä pilvipalvelu.

Useimmilla edellä luetelluilla toimialoilla on voimassa olevaa lainsäädäntöä, joka sisältää myös turvallisuusriskienhallintavelvoitteita sekä velvoitteita ilmoittaa toimialan valvovalle viranomaiselle palvelujen laatuun, turvallisuuteen tai jatkuvuuteen liittyvistä poikkeamista.

Energia

Energiasektorilla riskienhallintaan liittyviä velvoitteita sisältyy ainakin sähkömarkkinalakiin (588/2013), ydinenergialakiin (990/1987) sekä maakaasumarkkinalakiin (508/2000).

Sähkönjakelun kantaverkko on suunniteltava ja rakennettava, ja sitä on ylläpidettävä siten, että verkko täyttää verkon käyttövarmuutta ja luotettavuutta koskevat vaatimukset ja järjestelmävastaavalle kantaverkonhaltijalle sähköverkkoluvassa asetetut verkon käyttövarmuutta ja luotettavuutta koskevat ehdot.

Sähköalan yrityksiä, jakeluverkonhaltijoita sekä siirtoverkonhaltijoita koskevat sähkömarkkinalain mukainen verkon kehittämisvelvollisuus, varautumissuunnitteluvelvoite, sekä verkonhaltijan yhteistoimintavelvollisuus häiriötilanteissa. Lisäksi sähköalan yrityksiä sekä jakeluverkonhaltijoita koskevat jakeluverkon toiminnan laatuvaatimukset.

Sähkömarkkinalain mukaan verkonhaltijan on asianmukaisella suunnittelulla varauduttava normaaliolojen häiriötilanteisiin ja valmiuslaissa (1552/2011) tarkoitettuihin poikkeusoloihin. Lisäksi sähkömarkkinalain mukaan jakeluverkonhaltijan on tiedotettava verkon käyttäjille, mikäli sähkönjakelu keskeytyy jakeluverkossa merkittävässä laajuudessa.

Maakaasumarkkinalakiin sisältyy joitakin turvallisuusriskienhallintaa sivuavia velvoitteita. Maakaasumarkkinalain mukaan maakaasumarkkinaviranomainen määrää maakaasuverkkoluvassa yhden siirtoverkonhaltijan vastaamaan maakaasun siirtojärjestelmän teknisestä toimivuudesta ja käyttövarmuudesta sekä huolehtimaan siirtojärjestelmän tasevastuuseen kuuluvista tehtävistä tarkoituksenmukaisella ja maakaasumarkkinoiden osapuolten kannalta tasapuolisella ja syrjimättömällä tavalla (järjestelmävastuu).

Liikenne

Lentoliikenne

Ilmailu on kansainvälistä toimintaa ja siten siviili-ilmailualan sääntely perustuu yhteisiin pelisääntöihin, jotka on sovittu Kansainvälisen siviili-ilmailujärjestön (ICAO), Euroopan unionilainsäädännön, Euroopan lentoturvallisuusviranomaisen (EASA), Euroopan lennonvarmistusjärjestön eli Eurocontrolin ja Euroopan siviili-ilmailukonferenssin (ECAC) puitteissa.

Chicagon yleissopimuksella asetetaan ICAO:lle tehtäväksi hyväksyä ja tarvittaessa muuttaa kansainvälisiä standardeja, suositettuja menetelmiä ja menettelytapoja ilmailun turvallisuuteen, säännöllisyyteen ja tehokkuuteen liittyen.

EU-lainsäädännön vaatimuksilla ja niiden täytäntöönpanemiseksi hyväksytyillä säännöillä varmistetaan, että jäsenvaltiot täyttävät Chicagon yleissopimuksen mukaiset velvoitteensa. Lentotoiminnan yleisistä edellytyksistä on säädetty nk. EASA-asetuksessa ((EY) N.o 216/2008) sekä asetuksen nojalla annetuissa täytäntöönpanosäännöissä.

EASA-asetuksella, sen liitteillä ja asetuksen perusteella annetuilla täytäntöönpanosäännöillä säädetään verrattain kattavista riskienhallintavelvoitteista koskien lentotoiminnan harjoittajaa, lentopaikkoja sekä ilmaliikenteen hallintaa ja lennonvarmistuspalveluja sekä lennonjohtoa.

Kansallisella tasolla ilmailun sääntelyä täydentää ilmailulaki (864/2014). Ilmailulakiin sisältyy kuitenkin vain muutamia turvallisuuteen liittyviä vaatimuksia liittyen esimerkiksi lentokelpoisuuden ylläpitämiseen, lentoaseman hyväksymistodistukseen, maahuolintapalvelujen tarjoamiseen sekä varautumisessa poikkeusoloihin ja häiriötilanteisiin.

Euroopan parlamentin ja neuvoston asetuksessa (EU) N:o 376/2014 (”poikkeama-asetus”) säädetään poikkeamien ilmoittamisesta, analysoinnista ja seurannasta siviili-ilmailun alalla. Asetuksessa säädetään pakollisesta ilmoittamisvelvollisuudesta poikkeamista, jotka voivat muodostaa merkittävän riskin ilmailun turvallisuudelle.

Ilmailulain mukaan siviili-ilmailun onnettomuudesta ja vakavasta vaaratilanteesta on ilmoitettava Trafille. Trafi vastaa ja ylläpitää poikkeama-asetuksen mukaista ilmoitusjärjestelmää, johon ilmoitetaan pakolliset ja vapaaehtoiset poikkeamatiedot.

Rautatieliikenne

Rautateiden turvallisuudesta on säädetty yleisesti EU:n laajuisesti koskien viranomaisia ja toimijoita. Säädöksissä on asetettu vaatimukset mm. turvallisuusjohtamisjärjestelmälle, ilmoitusvelvollisuudelle ja valvonnalle. Keskeiset EU-tason säädökset ovat Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/798 rautateiden turvallisuudesta, Komission

asetus (EU) N:o 1078/2012 rautatieyritysten, turvallisuustodistuksen tai turvallisuusluvan saaneiden infrastruktuurin haltijoiden sekä kunnossapidosta vastaavien yksiköiden soveltamasta omavalvontaa koskevasta yhteisestä turvallisuusmenetelmästä, Komission asetus (EY) N:o 1158/2010 turvallisuustodistuksen arviointikriteereistä, Komission asetus (EY) N:o 1169/2010 turvallisuusluvan arviointikriteereistä, Komission asetus (EU) N:o 1077/2012 yhteisestä turvallisuusmenetelmästä kansallisten turvallisuusviranomaisten turvallisuustodistuksen tai turvallisuusluvan myöntämisen jälkeen harjoittamaa valvontaa varten, Komission täytäntöönpanoasetus (EU) N:o 402/2013 riskien arviointia koskevasta yhteisestä turvallisuusmenetelmästä ja asetuksen (EY) N:o 352/2009 kumoamisesta Komission asetus (EY) N:o 352/2009 yhteisistä turvallisuusmenetelmistä sekä Komission päätös (EY) 460/2009 yhteisistä turvallisuustavoitteista.

Kansallisesti rautateiden turvallisuudesta on säädetty rautatielailla (304/2011), ratalailla (110/2007), rautatiekuljetuslailla (1119/2000), raideliikennevastuulailla (113/1999), rautatiejärjestelmän liikenneturvallisuustehtävistä annetulla lailla (1664/2009). turvallisuustutkintalailla (525/2011), vaarallisten aineiden kuljetuksesta annetulla lailla (719/1994), kaupunkiraideliikenteestä annetulla lailla (1412/2015) valtioneuvoston asetuksella rautatiejärjestelmän turvallisuudesta ja yhteentoimivuudesta (327/2011), valtioneuvoston asetuksella vaarallisten aineiden kuljetuksesta rautatiellä (195/2002), valtioneuvoston asetuksella vaarallisten aineiden maakuljetusten turvallisuusneuvonantajasta (274/2002), valtioneuvoston asetuksella vaarallisten aineiden kuljetukseen tarkoitettujen pakkausten, säiliöiden ja irtotavarakonttien vaatimustenmukaisuuden osoittamisesta ja tähän liittyviä tehtäviä suorittavista tarkastuslaitoksista (124/2015), valtioneuvoston asetuksella rautateiden liikenneturvallisuuskoulutusta antavia oppilaitoksia koskevista vaatimuksista sekä eräistä kelpoisuuksista ja luetteloinneista (13/2013), valtioneuvostona asetuksella rautatiejärjestelmän kelpoisuusrekisteriin ja lisätodistusrekisteriin tallennettavista tiedoista (11/2013) ja kansallisen valvontaviranomaisen eli Trafin määräyksillä. Rautateiden turvallisuutta koskevat Trafin määräykset ovat määräys rautatieliikenteen harjoittajan ja rataverkon haltijan turvallisuusjohtamisjärjestelmästä (TRAFI/1065/03.04.02.00/2012) sekä määräys rautatieliikenteen harjoittajan ja rataverkon haltijan turvallisuuskertomuksesta (TRAFI/19402/03.04.02.00/2014).

Rautatielaissa on säädetty rautatiejärjestelmän turvallisuudesta. Lain mukaan rautatiejärjestelmän turvallisuustaso on säilytettävä, ja sitä on kehitettävä Euroopan unionin lainsäädännön ja alan teknisen ja tieteellisen kehityksen mahdollistamalla tavalla. Rataverkon haltija ja rautatieliikenteen harjoittaja vastaavat rautatiejärjestelmän turvallisesta käytöstä ja käyttöön liittyvien riskien hallinnasta.

Rautatielain mukaan rautatieliikenteen harjoittajalla ja rataverkon haltijalla on oltava rautatieturvallisuutta koskevien säännösten ja määräysten mukainen turvallisuusjohtamisjärjestelmä, joka täyttää rautatieturvallisuusdirektiivissä asetetut vaatimukset. Rautatielaissa on lisäksi säädetty myös varautumisesta poikkeusoloihin, häiriötilanteisiin sekä rautateitä uhkaavaan vaaraan ja onnettomuuteen.

Rautatielain mukaan rautatieliikenteen harjoittajien ja rataverkon haltijoiden tulee ilmoittaa Liikenteen turvallisuusvirastolle niiden tietoon tulleista onnettomuuksista ja vaaratilanteista. Lain mukaan nämä tiedot ovat salassa pidettäviä.

Vesiliikenne

Merenkulun kansainvälisen sääntelyn pohjana ovat YK:n alaisen Kansainvälisen merenkulkujärjestön (IMO) yleissopimukset. Keskeisiä kansainvälisiä yleissopimuksia ovat meriturvallisuutta sääntelevä SOLAS (International Convention for the Safety of Life at Sea, SOLAS-yleissopimus (SopS 11/1981) Vuoden 1974 kansainvälinen yleissopimus ihmishengen turvallisuudesta merellä) sekä ympäristönsuojelua koskeva MARPOL (International Convention for the Prevention of Pollution from Ships).

Riskienhallintaan yleisesti liittyviä velvoitteita on yhtiöiden (varustamot) osalta ISM-säännöstössä eli kansainvälisessä turvallisuusjohtamissäännöstössä (International Safety Management Code), joka perustuu kansainvälisen SOLAS-yleissopimuksen lukuun XI-1 "Special measures to enhance maritime safety" ja siihen liittyvään ISM-säännöstöön. EU:n alueella säännöstö on toimeenpantu asetuksella (EY) N:o 336/2006.

Alusliikennepalvelulain (623/2005) tarkoituksena on alusliikenteen turvallisuuden lisääminen ja tehokkuuden parantaminen sekä alusliikenteestä ympäristölle aiheutuvien haittojen ehkäiseminen. Laissa tarkoitettu VTS-viranomainen on Liikennevirasto. VTS-viranomainen voi tilapäisesti määrätä mm. vesialueen suljettavaksi, aluksia takaisin laituriin ja nopeusrajoituksia poikkeavien sää-, jää- tai vedenkorkeusolosuhteiden vuoksi. Lain mukaan VTS-viranomaisella on lisäksi oikeus kieltää alusta saapumasta VTS-alueelle tai poistumasta VTS-alueelta, tulemasta satamaan tai ankkuroimasta tai lähtemästä satamasta tai ankkuripaikalta. Laissa on lisäksi säädetty merenkulun tiedonhallintajärjestelmästä ja sille asetutuista vaatimuksista.

Satamien osalta turvavelvoitteita on ISPS (International Ship and Port Facility Security Code) säännöstössä, jonka tavoitteena on lisätä turvallisuutta aluksilla ja satamissa. Säännöstön on laatinut Kansainvälinen merenkulkujärjestö IMO. ISPS-säännöstö on myös liitetty kansainväliseen SOLAS-sopimukseen (luku XI-2 "Special measures to enhance maritime security") ja se on toimeenpantu EU:n turvatoimiasetuksella (EY) N:o 725/2004. Kansallisesti laissa eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta (485/2004) säädetään satamissa noudatettavista turvatoimista. Lain mukaan satamalle on tehtävä turva-arviointi, jonka pohjalta tehdään sataman turvallisuussuunnitelma.

Merenkulussa poikkeamaraportointijärjestelmä sisältyy ISM-säännöstön vaatimuksiin. Poikkeamaraportoinnin perusteena on, että analysoimalla läheltä piti -tilanteita ja vähäisiä onnettomuuksia sekä toteuttamalla ennakoivia korjaustoimenpiteitä voidaan pienentää vakavan onnettomuuden riskiä.

Kaupallisen merenkulun onnettomuuksien raportointivelvoitteesta Trafille on säädetty merilailla (674/1994). Lain mukaan merionnettomuusilmoitus on annettava laissa tarkoitetuissa tapauksissa. Alusturvallisuuden valvonnasta annetun lain (370/1995) mukaan valvontaviranomaiselle on tehtävä, mikäli mahdollista, kirjallinen ilmoitus alusturvallisuutta koskevan säännöksen tai määräyksen rikkomisesta.

Alusliikennepalvelulain mukaisella VTS-viranomaisella on velvollisuus ilmoittaa asianomaisille merenkulku-, meripelastus-, ympäristö-, aluevalvonta-, poliisi- tai tulliviranomaisille sekä asianomaisille satamanpitäjille havaitsemistaan tai sille ilmoitetuista tiettyä alusta koskevista aluksen tai siinä olevien ihmisten turvallisuuteen, meripelastukseen, ympäristönsuojeluun tai alue- taikka tullivalvontaan liittyvistä olennaisista seikoista.

Tieliikenne

Liikennejärjestelmä kehittyy ja uudistuu nopeassa tahdissa. Älykkään ja modernin liikennejärjestelmän toiminta perustuu digitaalisessa muodossa olevan tiedon hyödyntämiseen. Ilman toimintoja ohjaavaa luotettavaa tietoa toiminnot eivät voi toteutua.

Älykkäät järjestelmät ja välineet tarvitsevat toimiakseen digitaalisessa muodossa välitettyä tietoa. Tieto koostuu pääasiassa toimintaa ohjaavista tiedosta, liikenneympäristöstä ja olosuhdeominaisuuksista välitetystä tiedosta.

Liikenteeseen liittyvien automaattitoimintojen tarvitsema monimuotoinen tieto, tiedon riittävä määrä ja tiedon luotettavuus sekä tietoyhteyksien turvallisuus ovat avainasemassa varmistettaessa älykkäiden liikennejärjestelmien ja automaattisesti ohjautuvien liikennevälineiden turvallisuus. Tutkimusten mukaan inhimilliset syyt ovat osasyynä jopa 90 prosentissa liikenneonnettomuuksista. Automaatiota hyödyntämällä onnettomuuksia on mahdollista vähentää selvästi.

Automaattisesti ohjautuvat ajoneuvot ovat osa älykkäiden liikennejärjestelmien toteutumista. Älykkäissä liikennejärjestelmissä automaattisesti ohjautuvat ajoneuvot käyttävät liikkumiseensa itse tuottamaansa tietoa, jota ne keräävät ympäristöstä omilla sensoreillaan, tutkillaan ja kameroillaan. Sen lisäksi ne käyttävät sitä laajapohjaista tietoa, mitä ajoneuvoihin välittyy verkon kautta muusta liikenneympäristöstä, muista liikkuvista ajoneuvoista, tieympäristöstä, liikenteen ohjausjärjestelmistä ja kaupallisista palveluista.

EU:n tieliikenteen älykkäiden liikennejärjestelmien käyttöönoton sekä tieliikenteen ja muiden liikennemuotojen rajapintojen puitteista annetun Euroopan parlamentin ja neuvoston direktiivin 2010/40/EU (jäljempänä ITS-direktiivi) tavoitteena on nopeuttaa älykkäiden liikennejärjestelmien koordinoitua käyttöönottoa ja käyttöä tieliikenteessä kaikkialla Euroopassa. Direktiiviä sovelletaan kaikkiin tieliikennealan älykkäisiin liikennejärjestelmiin sekä tieliikenteen ja muiden liikennemuotojen välisiin rajapintoihin. ITS-direktiivi on Suomessa saatettu osaksi liikennekaarta.

Lailla 21/2014 säädetään sähköisistä tietullien keräämisjärjestelmistä sekä eurooppalaisesta sähköisestä tietullipalvelusta (EETS). Lakia sovelletaan sähköisten tietullien keräämisjärjestelmiin, joiden käyttö edellyttää erillisten sähköteknisten laitteiden asentamista tai kiinnittämistä ajoneuvoihin. Laki ei koske pieniä, yksinomaan paikallisia sähköisiä tietullien keräämisjärjestelmiä.

EETS-tietullikohteella tarkoitetaan sähköisten tiemaksujärjestelmien yhteentoimivuudesta yhteisössä annetun Euroopan parlamentin ja neuvoston direktiivin 2004/52/EY soveltamisalaan kuuluvaa tietullikohdetta eli Euroopan unionin alueen osaa, Euroopan tieverkoston osaa taikka rakennetta, kuten tunnelia, siltaa tai lauttaa, jossa tietulli peritään. EETS-palveluntarjoajalla on puolestaan laissa esitetyt vaatimukset täyttävä ja sijoittautumisvaltiossaan rekisteröity oikeushenkilö, joka tarjoaa eurooppalaisen sähköisen tietullipalvelun käyttömahdollisuuden.

Lain tie- ja katuverkon tietojärjestelmästä (991/2003), tarkoituksena on järjestää yleisiä ja yksityisiä teitä sekä katuja koskevat tiedot käsittävä valtakunnallinen tietojärjestelmä ja tietopalvelu.

Pankkiala

Pankkialan ja finanssimarkkinoiden infrastruktuurien alan sääntely ja valvonta on erittäin yhdenmukaistettua unionin tasolla unionin primaari- ja sekundaarioikeuden soveltamisen sekä yhdessä Euroopan valvontaviranomaisten kanssa kehitettyjen standardien käyttämisen myötä.

Pankkialalla riskienhallinnan keskeisenä tavoitteena on turvata riittävät omat varat suhteessa riskien ottoon ja riskienhallintajärjestelmien tasoon. Toimintaan kohdistuvat riskit voidaan jaotella esimerkiksi luottoriskien, operatiivisten riskien, markkinariskien sekä likviditeetin hallintaan.

Operatiivinen riski on keskeinen osa vakavaraisuussääntelyä ja valvontaa pankkialalla ja finanssimarkkinoiden infrastruktuurien alalla. Operatiivisella riskeillä voidaan tarkoittaa esimerkiksi riskiä, joka aiheutuu riittämättömistä tai epäonnistuneista sisäisistä prosesseista, henkilöstöstä, järjestelmistä tai ulkoisista tekijöistä. Operatiivisten riskien hallinta kattaa kaikki toiminnot, mukaan lukien verkko- ja tietojärjestelmien turvallisuuden, eheyden ja häiriönsietokyvyn.

Kansallisessa lainsäädännössä esimerkiksi laissa luottolaitostoiminnasta (610/2014) säädetään, että luottolaitoksella on oltava menetelmät operatiivisten riskien tunnistamiseksi, arvioimiseksi ja hallitsemiseksi. Laitoksen täytyy selkeästi kuvata, mitä se pitää operatiivisina riskeinä. Sillä on oltava operatiivisen riskin hallintaa koskevat kirjalliset toimintaperiaatteet ja menettelytavat.

Arvopaperikeskuksien osalta parlamentin ja neuvoston asetus 909/2014 (ns. I tason asetus) sisältää säännöksiä ulkoistamisesta ja operatiivisten riskien hallinnasta. Se sisältää myös velvollisuuden raportoida ”operational incidentseistä” toimivaltaiselle viranomaiselle.

Finanssivalvonnan määräyksen, 8/2014 operatiivisen riskin hallinta rahoitussektorin valvottavissa, mukaan valvottavan tulee ilmoittaa Finanssivalvonnalle sekä asiakkaille tarjotuissa palveluissa että maksu- ja tietojärjestelmissä esiintyneistä merkittävistä häiriöistä ja virheistä viipymättä niiden ilmaannuttua. Maksujenvälityksessä ja korttimaksamisessa merkittäviksi häiriöiksi katsotaan esimerkiksi suurta määrää asiakkaita koskeva häiriö tai viivästys sekä häiriö, jossa asiakastietoja on joutunut ulkopuoliselle taholle. Finanssivalvonnalle tulee ilmoittaa viipymättä myös sellaiset häiriöt ja virheet, jotka haittaavat tai vaarantavat valvottavan kykyä jatkaa liiketoimintaansa tai vastata velvoitteistaan.

Terveydenhuoltoala

Terveydenhuoltolain mukaan terveydenhuollon toiminnan on oltava laadukasta, turvallista ja asianmukaisesti toteutettua. Tämän lisäksi terveydenhuollon toimintayksikön on laadittava suunnitelma laadunhallinnasta ja potilasturvallisuuden täytäntöönpanosta. Valvira ylläpitää julkista rekisteriä vaatimustenmukaisista tietojärjestelmistä.

Sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain (159/2007) tarkoituksena on edistää sosiaali- ja terveydenhuollon asiakastietojen tietoturvallista sähköistä käsittelyä. Lailla toteutetaan yhtenäinen sähköinen potilastietojen käsittely- ja arkistointijärjestelmä terveydenhuollon palvelujen tuottamiseksi potilasturvallisesti ja tehokkaasti sekä potilaan tiedonsaantimahdollisuuksien edistämiseksi.

Laissa on säädetty sosiaali- tai terveydenhuollon asiakastietojen käsittelyssä käytettävän tietojärjestelmän olennaisista vaatimuksista. Lisäksi laissa on säädetty palvelun tarjoajan velvollisuudesta tehdä nk. omavalvontasuunnitelma, jossa se määrittelee riskienhallintatoimenpiteitä. Lisäksi palvelun tarjoajan on ilmoitettava Valviralle merkittävistä poikkeamista tietojärjestelmän olennaisten vaatimusten täyttymisessä, jos poikkeama voi aiheuttaa merkittävän riskin potilasturvallisuudelle, tietoturvalle tai tietosuojalle.

Terveydenhuollon laitteista ja tarvikkeista annetun lain (629/2010) tarkoituksena on ylläpitää ja edistää terveydenhuollon laitteiden ja tarvikkeiden sekä niiden käytön turvallisuutta. Lakia sovelletaan terveydenhuollon laitteiden ja tarvikkeiden ja niiden lisälaitteiden suunnitteluun ja valmistukseen sekä toimenpidepakkausten ja järjestelmien kokoamiseen. Lisäksi lakia sovelletaan mainittujen tuotteiden markkinoille saattamiseen ja sitä varten steriloimiseen, käyttöönottoon, asennukseen, huoltoon, ammattimaiseen käyttöön, markkinointiin ja jakeluun. Myös ohjelmisto voi olla terveydenhuollon laite.

Laissa on säännökset terveydenhuollon laitteita koskevista vaatimuksista. Laitteen tulee olla käyttötarkoitukseensa sopiva ja sen tulee käyttötarkoituksensa mukaisesti käytettynä saavuttaa sille suunniteltu toimivuus ja suorituskyky. Laitteen asianmukainen käyttö ei saa tarpeettomasti vaarantaa potilaan, käyttäjän tai muun henkilön terveyttä tai turvallisuutta.

Lain mukaan ammattimaisen käyttäjän on ilmoitettava Sosiaali- ja terveysalan lupa- ja valvontavirastolle ja valmistajalle tai valtuutetulle edustajalle vaaratilanteista, jotka ovat johtaneet tai olisivat saattaneet johtaa potilaan, käyttäjän tai muun henkilön terveyden vaarantumiseen ja jotka johtuvat mm. terveydenhuollon laitteen ominaisuuksista tai suorituskyvyn poikkeamasta tai häiriöstä.

Juomaveden toimittaminen ja jakelu

Talousveden turvallisuutta koskevat laatuvaatimukset perustuvat EU:n direktiiviin ihmisten käyttöön tarkoitetun veden laadusta (Euroopan parlamentin ja neuvoston direktiivi 2000/60/EY, annettu 23 lokakuuta 2000, yhteisön vesipolitiikan puitteista).

Terveydensuojelulain (763/1994) mukaan talousvettä toimittavan laitoksen, jolla on omaa veden tuotantoa tai käsittelyä, on haettava toimintansa hyväksymistä kunnan terveydensuojeluviranomaiselta. Talousvettä ei saa toimittaa ennen kuin laitos on hyväksytty. Hakemuksen sisällöstä on säädetty tarkemmin terveydensuojeluasetuksessa (1280/1994). Asetuksen mukaan hakemukseen on käytävä ilmi mm. selvitys raakaveden laadusta, käyttötarkkailusta ja käsittelytavasta, selvitys veden laadun tarkkailun järjestämisestä, sekä selvitys erityistilanteisiin varautumisesta.

Sosiaali- ja terveysministeriö on lisäksi antanut asetuksen talousveden laatuvaatimuksista ja valvontatutkimuksista (1352/2015). Asetuksessa säädetään talousveden laatuvaatimuksista ja -suosituksista ja niiden enimmäisarvoista ja niistä poikkeamisesta. Asetuksessa säädetään lisäksi talousveden desinfioinnista ja säännöllisestä valvonnasta, valvontaa varten tarvittavista tutkimuksista, talousveden radioaktiivisista aineista aiheutuvan säteilyaltistuksen rajoittamisesta sekä erityistilanteisiin varautumista koskevien suunnitelmien sisällöstä ja laatimisesta.

Sosiaali- ja terveysministeriön johdolla laadittu talousveden toimenpideohjelma (WSP, Water Safety Plan) keskittyy talousveden toimittamiseen liittyviin riskeihin ja niihin varautumiseen. WSP pohjautuu Maailman terveysjärjestön (WHO) suosittelemaan malliin.

Digitaalinen infrastruktuuri

Digitaalisen infrastruktuurin toimijoihin kohdistuvien velvoitteiden kannalta merkitystä on sillä, voidaanko ne katsoa tietoyhteiskuntakaaressa tarkoitetuiksi teleyrityksiksi. Tietoyhteiskuntakaaressa teleyrityksellä tarkoitetaan sitä, joka tarjoaa verkkopalvelua tai viestintäpalvelua ennalta rajaamattomalle käyttäjäpiirille eli harjoittaa yleistä teletoimintaa. Teletoiminnan sääntely on teknologianeutraalia ja se voi olla vastikkeellista tai vastikkeetonta.

Viestintävirasto on tulkinnut internetin yhdysliikennepisteet tietoyhteiskuntakaaren tarkoittamaksi yleiseksi teletoiminnaksi ainakin siltä osin, kun niitä käytetään yleisten viestintäverkkojen yhteenliittämiseen. Tällöin tietoyhteiskuntakaaressa ja Viestintäviraston määräyksissä edelletyt edellä kuvatut teleyrityksiä koskevat tietoturvallisuuden ja häiriöiden hallinnan ja häiriöiden ilmoittamisen vaatimukset ulottuvat myös internetin yhdysliikennepisteisiin.

Nimipalvelun (DNS) tarjoaminen on voimassa olevan sääntelyn mukaan yleistä teletoimintaa tai muuta toimintaa riippuen siitä, liittykö se internetyhteyspalvelun tarjontaan vai ei. Silloin kun se on osa internetyhteyspalvelun tarjoamista, sitä koskee tietoyhteiskuntakaaren ja Viestintäviraston määräysten sääntely. Viestintäviraston näkemyksen mukaan DNS on kriittinen ja elimellinen osa internetyhteyspalvelua, joka puolestaan on puhelinpalvelun ohella käyttäjille perusluonteisin teleyritysten tarjoama viestintäpalvelu.

Nimipalvelua tarjotaan myös muuten kuin internetyhteyspalvelun osana. Sitä tarjoavat esimerkiksi verkkotunnusvälittäjät ja muut verkon palveluntarjoajat, esim. Google. DNS-palvelua ei tyypillisesti hankita erikseen vaan osana muuta palvelua.

Suomen lainsäädäntötoimivaltaan kuuluvat .fi ja .ax - domainrekisterit kuuluvat tietoyhteiskuntakaaren soveltamisalaan. Viestintävirasto ylläpitää rekisteriä fi-maatunnukseen päättyvistä verkkotunnuksista (verkkotunnusrekisteri) ja tietokantaa verkkotunnusten teknisistä tiedoista internetliikenteen ohjaamista varten (fi-juuri). Ahvenanmaan maakuntahallitus ylläpitää .ax-juurta.

Viranomaisen toimintaa verkkotunnusrekisterin ja juuren ylläpidossa koskevat tietoyhteiskuntakaaren lisäksi julkisuuslain (621/1999) ja tietoturva-asetuksen tietoturvavaatimukset.

3.1.4 Turvallisuusriskien hallintaan liittyvän viranomaistoiminnan järjestäminen

Valtioneuvoston tilannekeskus

Valtioneuvoston ohjesäännön mukaan valtioneuvoston kanslian toimialaan kuuluu valtioneuvoston yhteinen tilannekuva, varautuminen ja turvallisuus sekä häiriötilanteiden hallinnan yleinen yhteensovittaminen. Valtioneuvoston kansliassa toimii valtioneuvoston tilannekeskus, joka tuottaa reaaliaikaista turvallisuustapahtumatietoa ja toimivaltaisten viranomaisten tiedoista koottua tilannekuvaa. Tilannekeskus yhdistää eri viranomaisilta ja avoimista lähteistä saadut tiedot ja raportoi niiden pohjalta valtionjohdolle ja eri viranomaisille. Tilannekeskus toimii myös Suomen kansallisena yhteyspisteenä muun muassa Euroopan unionin suuntaan erikseen määritellyllä tavalla.

Viestintävirasto

Viestintäviraston tehtävät ja erityiset tehtävät on määritelty tietoyhteiskuntakaaressa ja eräissä muissa laeissa (mm. luottamuspalvelulaki ja eIDAS-asetus). Viestintäviraston tehtävänä on mm. valvoa teletoiminnan tietoturvallisuudelle säädettyjen vaatimusten noudattamista. Sääntelyn tavoitteena on varmistaa, että viestintäverkot ja -palvelut ovat teknisesti kehittyneitä, laadultaan hyviä, toimintavarmoja ja turvallisia.

Viestintäviraston erityisiin tehtäviin kuuluu mm. edistää sähköisen viestinnän toimivuutta, häiriöttömyyttä ja turvallisuutta, kerätä tietoa verkkopalveluihin, viestintäpalveluihin ja lisäarvopalveluihin kohdistuvista tietoturvaloukkauksista ja niiden uhkista sekä viestintäverkkojen ja viestintäpalvelujen vika- ja häiriötilanteista, tiedottaa tietoturva-asioista sekä viestintäverkkojen ja viestintäpalvelujen toimivuudesta sekä selvittää verkkopalveluihin, viestintäpalveluihin ja lisäarvopalveluihin kohdistuvia tietoturvaloukkauksia ja niiden uhkia.

Viestintävirastossa toimivan tilannekeskuksen (CERT-FI) tehtävinä on ennaltaehkäistä tietoturvaloukkauksia ja tiedottaa tietoturva-asioista. CERT-toiminnon tehtävänä on selvittää verkkopalveluihin, viestintäpalveluihin ja lisäarvopalveluihin kohdistuvia tietoturvaloukkauksia ja niiden uhkia kerätä tietoa tällaisista tapahtumista ja tiedottaa tietoturva-asioista yleensä. CERT-toiminnan tavoitteena on yleisten viestintäverkkojen ja viestintäpalveluiden turvallisen ja häiriöttömän toiminnan varmistaminen sekä yhteiskunnan elintärkeiden toimintojen turvaaminen.

Liikenteen turvallisuusvirasto Trafi

Liikenteen turvallisuusvirastosta annetun lain mukaan Liikenteen turvallisuusvirasto Trafi vastaa liikennejärjestelmän sääntely- ja valvontatehtävistä ja edistää liikenteen turvallisuutta. Trafin tehtävistä ja toimivallasta valvonta-asioissa on lisäksi säädetty monissa liikennemuotokohtaisissa erityislaeissa.

Ilmailulaissa säädetään Trafin tehtävistä koskien ilmailun turvallisuusvaatimusten noudattamista ja ilmailutoiminnan vaatimustenmukaisuutta. Sen lisäksi, mitä ilmailulaissa säädetään Liikenteen turvallisuusviraston tehtävistä, virasto toimii mm. EU:n EASA-asetuksessa ja poikkeama-asetuksessa tarkoitettuna toimivaltaisena kansallisena viranomaisena.

Trafi valvoo alusturvallisuudesta annettujen säännösten ja määräysten noudattamista sekä huolehtii Port State Control-direktiivin (Euroopan parlamentin ja neuvoston direktiivi 2009/16/EY) satamavaltioiden suorittamasta valvonnasta ja tarkastusdirektiivin mukaisista tarkastuksista, ilmoituksista sekä niiden mukaisten tietojen antamisesta ja tietojen vaihdosta. Valvontaan kuuluu myös yleinen meriturvallisuuden valvonta.

Trafi valvoo lisäksi rautatiejärjestelmän turvallisuusvaatimusten noudattamista sekä rautatieliikenteen harjoittajan ja rataverkon haltijan turvallisuusjohtamisjärjestelmien vaatimustenmukaisuutta. Valvontaa sääntelee Euroopan komission antama asetus (EU) N:o 1077/2012 kansallisen viranomaisen suorittamasta valvonnasta turvallisuusluvan tai -todistuksen myöntämisen jälkeen.

Trafi valvoo myös auditoinneilla tieverkon haltijoiden johtamis- ja turvallisuudenhallintajärjestelmien toimivuutta ja infran hoitoa (tieturvallisuusdirektiivi 2008/96/EY).

Liikennevirasto

Liikennevirasto toimii alusliikennepalvelulaissa tarkoitettuna VTS-viranomaisena. VTS-viranomaisen tehtävät on määritelty alusliikennepalvelulaissa. Liikennevirasto on myös aluevalvontalaissa tarkoitettu aluevalvontaviranomainen omalla toimialallaan sekä meripelastuslaissa tarkoitettu muu viranomainen. Liikennevirasto voi vesiliikennelain nojalla antaa alueellisia kieltoja ja rajoituksia.

Liikennevirasto toimii maantielaissa tarkoitettuna vastuuviranomaisena sekä tienpitoviranomaisena. Liikennevirasto on myös tieinfrastruktuurin turvallisuuden hallinnasta annetun Euroopan parlamentin ja neuvoston direktiivin 2008/96/EY 2 artiklassa tarkoitettu toimivaltainen organisaatio ja Euroopan laajuisen tieverkon tunnelien turvallisuutta koskevista vähimmäisvaatimuksista annetun Euroopan parlamentin ja neuvoston direktiivin 2004/54/EY 4 artiklassa tarkoitettu hallintoviranomainen.

Liikennevirasto toimii myös rautatielaissa tarkoitettuna valtion rataverkon haltijana ja päättää tässä ominaisuudessa mm. ratakapasiteetista.

Liikenneviraston Liikennekeskukset vastaavat tie-, rata- ja meriliikenteen liikenteenhallinnasta ja pitävät yllä liikenteen tilannekuvaa. Liikennekeskukset tiedottavat ja ohjaavat liikennettä omalla vastuualueellaan tapahtuvissa liikenteellisissä häiriöissä sekä vastaavat viranomais- ja urakoitsijayhteistyöstä häiriötilanteissa. Tieliikennekeskukset seuraavat ja ohjaavat tieliikennettä muuttuvin opastein ja vastaavat tieliikenteelle tiedottamisesta. Rataliikennekeskus valvoo rautatieliikenteen sujuvuutta sekä rataverkon käyttöä. Liikennekeskuksilla on keskeinen rooli ja vastuu operatiivisessa varautumisessa sekä normaali- että poikkeusoloissa. Liikenneviraston VTS-keskukset ehkäisevät vaaratilanteita, reagoivat muuttuviin liikennetilanteisiin (ruuhkat, kapeikot, poikkeukselliset sää- ja jääolosuhteet), tukevat meripelastusjohtajan toimintaa ohjaamalla alusliikennettä. Alusliikenteen turvalliseksi sujumiseksi häiriö- ja poikkeustilanteissa VTS-viranomainen voi antaa viranomaismääräyksiä alusliikennepalvelulain 17 ja 17 a §:n nojalla. VTS-viranomainen tekee suojapaikkapäätöksen ja ohjaa suojapaikkaan. Valmistautuu hoitamaan Valmiuslain 79§ mukaisia tehtäviä. Ohjaa alusliikennettä muuttuvissa turvallisuustilanteissa Liikenneviraston johdon antamien strategisten määräysten ja ohjeiden mukaisesti.

Sosiaali- ja terveysalan lupa- ja valvontavirasto Valvira

Valvira valvoo sosiaali- ja terveydenhuollon asiakas- ja potilastietojen käsittelyyn tarkoitettujen tietojärjestelmien olennaisten vaatimusten toteutumista. Sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain mukaan Valviran tehtävänä on valvoa ja edistää tietojärjestelmien vaatimustenmukaisuutta. Lain mukaan sosiaali- tai terveydenhuollon palvelujen antajan on ilmoitettava Valviralle tietojärjestelmän olennaisten vaatimusten täyttymisessä havaitsemistaan merkittävistä poikkeamista, silloin kun poikkeama voi aiheuttaa merkittävän riskin potilasturvallisuudelle, tietoturvalle tai tietosuojalle.

Terveydenhuollon laitteista ja tarvikkeista annetun lain mukaan Sosiaali- ja terveysalan lupa- ja valvontaviraston (Valvira) tehtävänä on valvoa ja edistää terveydenhuollon laitteiden sekä niiden käytön turvallisuutta ja vaatimustenmukaisuutta.

Tämän tehtävän toteuttamiseksi Valvira ylläpitää vaaratilannerekisteriä. Valviran on arvioitava ilmoitusvelvollisilta tulleet vaaratilanneilmoitukset ja ryhdyttävä tarpeellisiin terveyden ja turvallisuuden edellyttämiin toimiin.

Terveyden ja hyvinvoinnin laitos THL

Sosiaali- ja terveysministeriön alainen Terveyden ja hyvinvoinnin laitos toimii siitä annetun lain (668/2008) mukaan väestön hyvinvoinnin ja terveyden edistämiseksi, sairauksien ja sosiaalisten ongelmien ehkäisemiseksi sekä sosiaali- ja terveydenhuollon ja sen palvelujen kehittämiseksi. Terveyden ja hyvinvoinnin laitoksesta annetun lain mukaan THL:n tehtävänä on vastata sosiaali- ja terveydenhuollon asiakastiedon sähköisen käsittelyn, siihen liittyvän tietohallinnon ja valtakunnallisten tietojärjestelmäpalvelujen käytön ja toteuttamisen suunnittelusta, ohjauksesta ja seurannasta. THL voi tarvittaessa antaa tarkempia määräyksiä sosiaali- tai terveydenhuollon asiakastietojen käsittelyssä käytettävän tietojärjestelmän olennaisten vaatimusten sisällöstä.

Finanssivalvonta

Finanssivalvonnasta annetun lain (878/2008) mukaan Finanssivalvonnan toiminnan tavoitteena on finanssimarkkinoiden vakauden edellyttämä luotto-, vakuutus- ja eläkelaitosten ja muiden valvottaviksi säädettyjen vakaa toiminta, vakuutettujen etujen turvaaminen sekä yleinen luottamus finanssimarkkinoiden toimintaan. Finanssivalvonta valvoo, että finanssimarkkinoilla toimivat noudattavat niihin sovellettavia finanssimarkkinoita koskevia säännöksiä, niiden nojalla annettuja määräyksiä, toimilupansa ehtoja ja toimintaansa koskevia sääntöjä.

Energiavirasto

Energiaviraston tehtävistä on säädetty sähkö- ja maakaasumarkkinoiden valvonnasta annetussa laissa (590/2013). Laissa säädetään Energiaviraston tehtävistä, toimivallasta valvonta-asioista sekä esimerkiksi tiedonsaanti ja tarkastusoikeuksista.

4. Direktiivin saattaminen osaksi kansallista lainsäädäntöä

4.1 Yleistä

Verkko- ja tietoturvadirektiivin voimaansaattamista tukevan työryhmän tehtävän on ollut antaa liikenne- ja viestintäministeriölle asiantuntija-apua direktiivin voimaan saattamiseksi niin, että direktiivin uudet riskienhallinnan ja poikkeamien raportointivelvoitteet saataisiin parhaiten osaksi yritysten normaalien turvallisuusriskienhallintaa. Tarkoituksena on välttää yrityksille ja viranomaisille aiheutuvaa ylimääräistä hallinnollista taakkaa ja mahdollisuuksien mukaan vähentää päällekkäisiä ilmoitusvelvollisuuksien syntyä. Tarkoituksena on lisäksi luoda raportointivelvoitteella lisäarvoa myös yrityksille. Tämä voisi tapahtua esimerkiksi toimialalle kehittyvän paremman tilannekuvan muodossa.

Kuten edellä on kuvattu, voimassa olevaan kansalliseen sektorikohtaiseen lainsäädäntöön sisältyy jo useilla toimialoilla direktiivin velvoitteiden kaltaista turvallisuusriskienhallintalainsäädäntöä. Täytäntöönpanon tueksi työryhmän tehtävänä olikin selvittämää, miltä osin voimassa oleva kansallinen sääntely kattaa direktiivistä johtuvia vaatimuksia ja miten direktiivin velvoitteet voitaisiin kansallisesti implementoida niin, että ne voitaisiin yrityksissä ottaa osaksi niiden normaalia riskinhallintaa. Työryhmälle annettiin lisäksi arvioitavaksi seuraavat kysymykset ja asiakokonaisuudet:

1. *Tulisiko direktiivi saattaa kansallisesti voimaan siten, että direktiivin velvoitteet sisällytettäisiin i) sektorikohtaisiin lakeihin vai ii) erillislakiin?*

2. *Mitkä tahot / mikä taho voisi toimia direktiivin tarkoittamana toimivaltaisena viranomaisena?*

3. *Mikäli toimivaltaisen viranomaisen tehtävät annettaisiin sektorikohtaisesti toimivaltaiselle valvontaviranomaiselle, ovatko voimassa olevan lainsäädännön täytäntöönpanovaltuudet riittäviä?*

4. *Mikä taho voisi toimia kansallisena yhteyspisteenä?*

5. *Keskeisten palveluntarjoajien määrittäminen*

6. *Vähimmäisvelvoitteet korkean verkko- ja tietojärjestelmien turvallisuuden ylläpitämiseksi*

Työryhmän työn tueksi on myös selvitetty millaisia tietoturva- tai muita riskienhallintaan sekä turvallisuuteen liittyviä velvoitteita verkko- ja tietoturvadirektiivin soveltamisalaan kuuluvilla toimialoilla on tällä hetkellä voimassaolevan kansallisen lainsäädännön, EU-lainsäädännön sekä kv-velvoitteiden puitteissa. Arvioinnissa huomioitiin erityisesti verkko- ja tietojärjestelmien turvallisuuteen ja jatkuvuuden varmistamiseen tähtäävät velvoitteet sekä velvoitteet ilmoittaa turvallisuuspoikkeamista viranomaisille. Tavoitteena oli koota toimialakohtainen kattava kuvaus riskienhallinta- ja poikkeamien ilmoitusvelvoitteista, sekä näiden vastaavuudesta NIS-direktiivin velvoitteiden kanssa.

Selvityksen keskeisiä johtopäätöksiä olivat, että kotimainen tietoturvasääntely on fragmentoitunutta. Direktiivin soveltamisalaan kuuluville toimialoille on asetettu melko paljon

turvallisuus- ja riskienhallintavelvoitteita, mutta myös näitä koskeva sääntely on hyvin fragmentoitunutta. Suurimmalla osalla soveltamisalaan kuuluvista toimialoista on säädetty riskienhallintaa ja tietoturvan tasoa koskevia velvoitteita. Turvallisuusvelvoitteet ovat kuitenkin useimmissa tapauksissa yksittäisiin toimintoihin liittyviä, eivät suoraan koko toimialaa tai toimijatyyppiä velvoittavia. Riskienhallintavelvoitteet on osin muotoiltu hyvin avoimiksi siten, ettei suoraan sanamuodosta voida tulkita, voidaanko tietyn velvoitteen katsoa kattavan myös tietojärjestelmien turvaamisen. Ilmoitusvelvollisuuksia on asetettu lähes kaikilla toimialoilla, mutta tietoturvapoikkeamista ilmoittamista koskevia velvoitteita on vain harvoilla toimialoilla. Selvityksen mukaan voimassaoleva kotimainen sääntely ei suurimmalta osin täytä NIS-direktiivissä asetettuja velvoitteita.

Selvityksen mukaan toimialoille on asetettu voimassaolevassa erityislainsäädännössä runsaasti toiminnan turvallisuutta ja riskienhallintaa koskevia velvoitteita, mutta velvoitteiden ei voida suurimmalta osin katsoa kattavan sellaisenaan NIS-direktiivin mukaisia velvoitteita. Ainoastaan yksittäisen toiminnon turvallisuutta koskeva riskienhallintavelvoite ei täytä NIS-direktiivissä asetettuja vaatimuksia ottaen huomioon, että toiminta jää muilta osin sääntelyn ulkopuolelle.

Lisäksi ilmoitus- ja raportointivelvollisuudet koskevat usein tiettyä yksittäistä toimintoa, kuten esimerkiksi onnettomuuksista ilmoittamista. Ilmoitusvelvollisuudet eivät aina kohdistu kaikkeen keskeisten palveluntarjoajien toimintaan. Esimerkiksi terveydenhuoltoalalla velvollisuus ilmoittaa tietoturvapoikkeamasta viranomaiselle koskee tilanteita, joissa se aiheuttaa riskin potilasturvallisuudelle, eikä sairaala ole velvollinen ilmoittamaan järjestelmiin kohdistuvista tietomurroista muilta osin.

Työryhmä on koko ryhmän yhteisten kokousten lisäksi kokoontunut sektorikohtaisesti (liikenne, finanssi, terveydenhuolto, energia, digitaaliset palvelut) arvioimaan toimialakohtaista voimassa olevaa lainsäädäntöä kullakin toimialalla, arvioimaan direktiivin mukaisten velvoitteiden vaikutuksia sektorikohtaisesti sekä millaista toimintaa toimialalla voitaisiin pitää direktiivin tarkoittamalla tavalla yhteiskunnan kannalta keskeisenä.

Sektorikohtaiselle lainsäädännölle tehdyn selvityksen ja työryhmän arvion perusteella sekä kansalliselle täytäntöönpanolle asetetut tavoitteet huomioiden työryhmä katsoo, että NIS-direktiivin mukaiset velvoitteet tulisi lähtökohtaisesti pyrkiä ottamaan kansallisesti osaksi sektorikohtaista lainsäädäntöä. Työryhmän näkemyksen mukaan direktiivin implementointi omaksi erityislaikseen ei täyttäisi samalla tavalla direktiivin täytäntöönpanolle asetettuja tavoitteita ja voisi sen sijaan johtaa päällekkäisiin velvoitteisiin ja raportointikäytäntöihin.

Lisäksi työryhmä katsoo, että direktiivin kansallisessa täytäntöönpanossa olisi arvioitava huolellisesti, miten verkko- ja tietoturvadirektiivin mukaiset turvallisuusriskienhallinta- ja poikkeamailmoitusvelvollisuudet voitaisiin saattaa osaksi kansallista lainsäädäntöä niin, ettei päällekkäisiä velvoitteita muun voimassaolevan lainsäädännön kanssa tarpeettomasti syntyisi. Arvioinnissa on erityisesti huomioitava tietosuoja-asetuksen mukaisten velvollisuuksien suhde verkko- ja tietoturvadirektiivin velvollisuuksiin. Kansalliseen täytäntöönpanon tavoitteena tulisi olla yrityksille syntyvän tarpeettoman hallinnollisen taakan välttäminen.

Työryhmän näkemyksen mukaan direktiivin kansallisen täytäntöönpanon lähtökohdaksi tulisi ottaa, että direktiivin mukaiset velvoitteet tulisi saattaa osaksi kansallisia relevantteja toimialakohtaisia säädöksiä. Täytäntöönpanossa tulee erityisesti kiinnittää huomiota siihen, ettei päällekkäisiä velvoitteita muusta voimassaolevasta lainsäädännöstä johtuvien velvoitteiden kanssa tarpeettomasti syntyisi.

4.2 Tietoturvaloukkauksiin reagoivat ja niitä tutkivat yksiköt (CSIRT-toimijat) (9 artikla)

Tietoturvaloukkauksiin reagoivia ja niitä tutkivia yksiköitä (CSIRT-toimijoita) koskevat vaatimukset on lueteltu direktiivin liitteessä I. Liitteen mukaan CSIRT-toimijoiden on varmistettava viestintäpalvelujensa kattava saatavuus, ja niiden on pidettävä käytössä useita kanavia, joiden kautta niihin voidaan ottaa yhteyttä ja joiden kautta ne itse voivat ottaa yhteyttä muualle milloin tahansa. Lisäksi CSIRT-toimijoiden toimitilat ja niitä tukevat tietojärjestelmät on sijoitettava suojattuihin paikkoihin.

CSIRT- toimijan on huolehdittava myös toiminnan jatkuvuudesta. CSIRT-toimijoilla on oltava tukenaan infrastruktuuri, jonka jatkuvuus on varmistettu. Lisäksi CSIRT-toimijoilla on oltava tarkoituksenmukainen järjestelmä pyyntöjen käsittelyä ja reititystä varten tapauksen edelleenohjauksen helpottamiseksi. CSIRT-toimijoilla on oltava myös riittävä henkilöstö, jotta ne voivat olla käytettävissä jatkuvasti. CSIRT-toimijoilla on oltava myös mahdollisuus halutessaan osallistua kansainvälisiin yhteistyöverkostoihin.

Viestintäviraston lakisääteisiin tehtäviin sisältyy jo CSIRT-toiminnan kaltaista toimintaa. Viestintävirastossa toimivan tilannekeskuksen (CERT-FI) tehtävinä on ennaltaehkäistä tietoturvaloukkauksia ja tiedottaa tietoturva-asioista. CERT-toiminnon tehtävänä on selvittää verkkopalveluihin, viestintäpalveluihin ja lisäarvopalveluihin kohdistuvia tietoturvaloukkauksia ja niiden uhkia kerätä tietoa tällaisista tapahtumista ja tiedottaa tietoturva-asioista yleensä. CERT-toiminnan tavoitteena on yleisten viestintäverkkojen ja viestintäpalveluiden turvallisen ja häiriöttömän toiminnan varmistaminen sekä yhteiskunnan elintärkeiden toimintojen turvaaminen. Viestintäviraston ja erityisesti sen kyberturvallisuuskeskuksen toiminta täyttävät jo käytännössä nykyisellään direktiivissä luetellut vaatimukset.

CSIRT-toimijoiden tehtävät on myös määritelty liitteessä I. Niihin kuuluisivat poikkeamien seuranta, tiedotusten ja varoitusten antaminen, tiedottaminen riskeistä ja poikkeamista, poikkeamiin reagointi, riskin ja poikkeamien analysointi, tilannetietoisuus sekä CSIRT-verkostoon osallistuminen. Lisäksi CSIRT-toimijoiden on luotava yhteistyösuhteita yksityiseen sektoriin sekä edistettävä yhteisten tai standardoitujen toimintatapojen omaksumista ja käyttöä poikkeamien ja riskien käsittelymenettelyissä sekä poikkeamien, riskien ja tietojen luokittelujärjestelmissä.

Nämä tehtävät mahtuisivat ainakin pääosin Viestintäviraston lakisääteisiin tehtäviin, joita ovat mm. edistää sähköisen viestinnän toimivuutta, häiriöttömyyttä ja turvallisuutta, kerätä tietoa verkkopalveluihin, viestintäpalveluihin ja lisäarvopalveluihin kohdistuvista tietoturvaloukkauksista ja niiden uhkista sekä viestintäverkkojen ja viestintäpalvelujen vika- ja häiriötilanteista, tiedottaa tietoturva-asioista sekä viestintäverkkojen ja viestintäpalvelujen toimivuudesta sekä selvittää verkkopalveluihin, viestintäpalveluihin ja lisäarvopalveluihin kohdistuvia tietoturvaloukkauksia ja niiden uhkia.

Työryhmän näkemyksen mukaan Viestintäviraston tulisi toimia direktiivin 9 artiklan tarkoittamana CSIRT-toimijana.

4.3 Kansalliset toimivaltaiset viranomaiset (8 artikla)

Verkko- ja tietoturvadirektiivin mukaan jäsenvaltioiden on nimettävä yksi tai useampi verkko- ja tietojärjestelmien turvallisuudesta vastaava kansallinen toimivaltainen viranomainen. Toimivaltaisen viranomaisen on seurattava direktiivin soveltamista kansallisella tasolla. Toimivaltaisilla viranomaisilla pitää olla tarvittavat valtuudet ja keinot arvioida noudatetaanko direktiivin asettamia riskienhallinta- ja raportointivelvoitteita.

Toimivaltaisen viranomaisen tehtävä on siis valvoa, että direktiivissä tarkoitettujen keskeisten palvelujen tarjoajat ja digitaalisen palvelun tarjoajat noudattavat direktiivillä asetettuja velvollisuuksia.

Kuten edellä on selostettu, verkko- ja tietoturvadirektiivin soveltamisalalla on Suomessa jo useita valvontaviranomaisia, keskeisimpinä Energiavirasto, Finanssivalvonta, Liikenteen turvallisuusvirasto Trafi, Sosiaali- ja terveysalan lupa- ja valvontavirasto Valvira sekä Viestintävirasto.

Tietoturvariskienhallinta velvoitteiden valvomiseksi ei Suomessa ole nimetty vain yhtä viranomaista, kuten Viestintävirastoa. Sen sijaan valvontaviranomaisilla on tyypillisesti toimivalta valvoa lainsäädännössä sille määritettyjä kokonaisuuksia. Esimerkiksi Finanssivalvonta valvoo sen valvottavien osalta operatiivisen riskinhallinnan velvoitteiden noudattamista. Näihin sisältyy myös tietojärjestelmille asetetut turvallisuusvaatimukset. Valvottavat tekevät myös mahdolliset tietoturvaan liittyvät poikkeamailmoitukset Finanssivalvonnalle. Valvontaviranomaisille on tyypillisesti säädetty myös valtuuksia valvontatehtävien hoitamiseen, kuten tiedonsaanti- ja tarkastusoikeuksia. Valvontaviranomaiset voivat myös antaa valvottavia sitovia päätöksiä.

Mikäli tietoturvariskienhallintaan liittyvät viranomaistehtävät keskitettäisiin jatkossa vain yhdelle viranomaiselle, se voisi aiheuttaa päällekkäisiä valvontatoimivaltuuksia sekä raportointivelvollisuuksia palvelun tarjoajille. Ongelmallisena voidaan myös pitää sitä, ettei aina ole selvää johtuuko poikkeama esimerkiksi tietojärjestelmien turvallisuuteen vai onko kyseessä muuhun turvallisuuteen liittyvä poikkeama. Poikkeamilla saattaa todennäköisesti olla myös läheisiä liittymiä verkko- ja tietojärjestelmien turvallisuuden lisäksi esimerkiksi liikenteen osalta liikenteen turvallisuuteen.

Mikäli toimivaltaisen viranomaisen tehtävät annettaisiin olemassa oleville valvontaviranomaisille, voitaisiin näille viranomaisille laissa säädettyjä toimivaltuuksia joutua täydentämään. Lisäksi viranomaisten välinen yhteistyö pitäisi järjestää niin, että sektorikohtaisilla valvontaviranomaisilla olisi mahdollisuus vaihtaa tarvittaessa poikkeamiin liittyvää tietoa yhteistyön vaikuttavuuden lisäämiseksi sekä päällekkäisen työn välttämiseksi, huomioiden kuitenkin tietojen luonteen. Olisi myös arvioitava sitä, voisivatko sektorikohtaiset viranomaiset hyödyntää ja miten Viestintäviraston tietoturvaan liittyvää asiantuntemusta. Kaikkien eri sektoreiden keskeisten palveluiden tarjoajien ja digitaalisten palveluiden tarjoajien tulisi voida halutessaan olla kohdassa 4.2 kuvatun CSIRT-palvelun piirissä ja hyötyä Viestintäviraston CSIRT-toiminnon tietoturvaosaamisesta.

Edellä esitetyn perusteella on katsottava, että direktiivin täytäntöönpanolle asetetut tavoitteet voitaisiin parhaiten saavuttaa niin, että toimivaltaisina viranomaisina toimisivat sektorikohtaiset valvontaviranomaiset. Jatkovalmistelussa on kuitenkin kiinnitettävä erityistä huomiota viranomaisten mahdollisiin resursointitarpeisiin sekä siihen, että toimivaltaisilla viranomaisilla on tarvittavaa osaamista käytössään tehtävien hoitamiseen. Viranomaistoiminnan järjestämisen mahdolliset budjettivaikutukset tulee myös hallituksen esityksessä arvioida huolellisesti.

Työryhmän näkemyksen mukaan toimivaltaisina viranomaisina tulisi toimia ne viranomaiset, jotka vastaavat jo nykytilassa toimialan turvallisuusvelvoitteiden valvonnasta eli nk. sektorikohtaiset valvontaviranomaiset.

4.4 Keskitetty yhteyspiste (8 artikla)

Keskitetyn yhteyspisteen tehtävänä on direktiivin mukaan yhteydenpito, jotta voidaan varmistaa jäsenvaltioiden viranomaisten rajat ylittävä yhteistyö. Kansallinen yhteyspiste voi toimia CSIRT-toimijan yhteydessä tai olla kokonaan erillinen toimija.

Valtioneuvoston ohjesäännön 12 §:n 7 kohdan mukaan valtioneuvoston kanslian toimialaan kuuluu valtioneuvoston yhteinen tilannekuva, varautuminen ja turvallisuus sekä häiriötilanteiden hallinnan yleinen yhteensovittaminen. Tämän johdosta olisi mahdollista, että keskitettynä yhteyspisteenä voisi toimia valtioneuvoston tilannekuvakeskus.

Keskitetyn yhteyspisteen toiminnan voi kuitenkin katsoa olevan läheisellä tavoin sidoksissa direktiivissä tarkoitettuun operatiivisen tason toimintaan. Yhteyspisteen tarkoitus on erityisesti tukea jäsenvaltioiden viranomaisten, CSIRT-toimijoiden sekä direktiivillä perustettujen jäsenvaltioiden välisen yhteistyöryhmän ja CSIRT-verkoston toimintaa. Tämän johdosta keskitetyn yhteyspisteen olisi tarkoituksen mukaista olla parhaalla mahdollisella tavalla tietoinen direktiivin puitteissa suoritettavasta operatiivisen tason yhteistyöstä ja yhteistyöjärjestelyistä.

Työryhmä katsoo, että Viestintäviraston tulisi toimia direktiivin 8 artiklan tarkoittamana keskitettynä yhteyspisteenä.

4.5 Keskeisten palvelujen tarjoajien määrittäminen (5 artikla)

Direktiivissä jäsenvaltiot velvoitetaan määrittelemään keskeiset palvelun tarjoajat direktiivin liitteessä II tarkoitetuilla toimialoilla ja niiden alaluokkien osalta. Jotta keskeiset palvelun tarjoajat voidaan määrittää, on jäsenvaltion määritettävä ensin kullakin toimialalla direktiivin tarkoittamat keskeiset palvelut eli palvelut, jotka ovat keskeisiä yhteiskunnan ja/tai talouden kriittisten toimintojen ylläpitämiseksi.

Direktiivin mukaisia toimialoja ovat energia (sähkö, öljy, kaasu), liikenne (lentoliikenne, rautatieliikenne, vesiliikenne, tieliikenne), pankkiala, finanssimarkkinoiden infrastruktuurit, terveydenhuoltoala (terveydenhuoltolaitokset), juomaveden toimittaminen ja jakelu sekä digitaalinen infrastruktuuri.

Direktiivin mukaan keskeisten palveluiden tarjoajat voidaan määritellä hyväksymällä luettelo keskeisistä palvelun tarjoajista tai hyväksymällä kansallisia toimenpiteitä, joiden avulla voidaan määrittää, mihin toimijoihin sovelletaan verkko- ja tietojärjestelmien turvallisuutta koskevia kriteerejä.

Direktiivin täytäntöönpanoa tukevan työryhmän sektorikohtaisissa kokouksissa on arvioitu keskeisten palveluntarjoajien määrittämistä kullakin sektorilla.

Keskeisten palveluiden tarjoajien määrittämien on toteutettava niin, että palvelun tarjoajille on selvää, että he kuuluvat velvoitteiden piiriin. Velvoitteiden ei tulisi myöskään mielivaltaisesti kohdistua tiettyihin palvelun tarjoajiin. Lisäksi keskeisten palveluiden tarjoajien määrittelemisessä tulee ottaa huomioon direktiivin vaatimukset.

Keskeiset palvelut ja keskeisten palveluiden tarjoajat voitaisiin määritellä lainsäädännöllä. Yksinkertaisin tapa määritellä olisi pitää keskeisinä palveluntarjoajina automaattisesti niitä toimijoita, joihin lainsäädäntövelvoitteet kohdistuvat. Esimerkiksi tietoyhteiskuntakaaren tietoturvapoikkeamien ilmoittamisvelvoite koskee kaikkia teleyrityksiä.

> Teleyrityksen on ilmoitettava viipymättä Viestintävirastolle, jos sen palveluun kohdistuu tai sitä uhkaa merkittävä tietoturvaloukkaus taikka muu tapahtuma, joka estää viestintäpalvelun toimivuuden tai häiritsee sitä olennaisesti.

Voimassa olevaan lainsäädännön sisältyy myös velvoitteita, joidenka soveltamisalaan kuuluvat vain tietyn kynnysarvon ylittävä toiminta. Esimerkiksi sähkömarkkinalaissa on määritelty kriteerit sille, milloin jakeluverkonhaltijan tulee olla nk. oikeudellisesti eriytetty.

> Jos jakeluverkonhaltija, jonka 400 voltin jakeluverkossa siirretty vuotuinen sähkömäärä on ollut kolmen viimeksi päättyneen kalenterivuoden aikana vähintään 200 gigawattituntia, toimii osana sähkön tuotantoa tai toimitusta harjoittavaa yritystä tai saman tahon määräysvallassa olevaa yritysryhmää, tulee verkonhaltijan olla oikeudelliselta muodoltaan, organisaatioltaan ja päätöksenteoltaan riippumaton yrityksen tai yritysryhmän sähköntuotanto- ja sähkönmyyntitoiminnoista (oikeudellisesti eriytetty jakeluverkkotoiminta).

Myös verkko- ja tietoturvadirektiivin riskienhallinta- ja raportointivelvoitteet voitaisiin kohdistaa keskeisille toimijoille jo lainsäädännön tasolla. Tällöin sektorikohtaisesti olisi huolellisesti arvioitava, mille toimijoille velvoitteet kohdistetaan. Toimijoiden joukkoa voitaisiin rajata tarkoituksenmukaisesti esimerkiksi rajaamalla soveltamisalaa vain tietyn kynnysarvokriteerin täyttäviin toimijoihin tai sulkemalla esimerkiksi pieniä yrityksiä pois velvoitteen soveltamisalasta. Perusteet, miksi tiettyjä palveluita tulisi pitää yhteiskunnan toiminnan kannalta keskeisenä sekä toimijoiden joukkoa rajata, tulisi kattavasti kuvata hallituksen esityksen perusteluissa.

Toimialoilla, joilla on jo voimassaolevaa direktiivin sääntelyä vastaavaa kansallista lainsäädäntöä, olisi mahdollista, että kaikkia erityislainsäädännöllä velvoitettuja toimijoita pidettäisiin suoraan keskeisten palveluiden tarjoajina, eikä näin erillistä määritysprosessia tarvitsisi tehdä.

Sen sijaan, mikäli palveluntarjoajat määriteltäisiin luettelona, olisi lainsäädännössä säädettävä niistä kriteereistä, joilla luettelo laadittaisiin. Luetteloiden laatiminen ja ylläpitäminen olisi omiaan lisäämään huomattavasti viranomaisten ja yritysten hallinnollista taakkaa.

Työryhmä katsoo, että tarkoituksenmukaisin keino määrittää keskeisten palveluiden tarjoajat olisi lainsäädännöllisin kriteerein. Kriteerit on arvioitava huolellisesti toimialakohtaisesti niin, että direktiivin mukaiset velvoitteet voitaisiin toimialakohtaiset erityispiirteet ja voimassa oleva lainsäädäntö huomioiden osoittaa tarkoituksenmukaisimmalle joukolle toimijoita.

4.6 Keskeisten palvelujen tarjoajia koskevat turvallisuusvaatimukset ja poikkeamien ilmoittaminen (14 artikla)

Direktiivin mukaan jäsenvaltioiden on velvoitettava keskeisten palvelujen tarjoajat hallitsemaan käyttämiinsä verkko- ja tietojärjestelmien turvallisuuteen liittyviä riskejä. Lisäksi keskeisten palveluiden tarjoajat on velvoitettava ilmoittamaan turvallisuuspoikkeamista, joilla on merkittävä vaikutus niiden tarjoamien palvelujen jatkuvuuteen.

Kuten edellä on kuvattu, voimassa olevaan kansalliseen sektorikohtaiseen lainsäädäntöön sisältyy jo useilla toimialoilla direktiivin velvoitteiden kaltaista turvallisuusriskienhallintalainsäädäntöä. Joillakin direktiivin soveltamisalueen mukaisilla toimialoilla on myös lakisääteisiä poikkeamaraportointivelvoitteita. Poikkeamista ilmoitetaan pääsääntöisesti toiminnan turvallisuutta valvovalle viranomaiselle. Esimerkiksi finanssisektorilla osana operatiivisten riskien hallintaa valvottavien on ilmoitettava Finanssivalvonnalle myös järjestelmien tietoturvaan liittyvistä poikkeamista.

Vaikka useilla toimialoilla on lakisääteisiä direktiivin velvoitteiden kaltaista turvallisuusriskienhallinta- ja poikkeamaraportointivelvoitteita, ei niissä välttämättä ole yksiselitteisesti säädetty verkko- ja tietojärjestelmien turvallisuudesta ja turvallisuuspoikkeamien ilmoittamisesta, vaan velvoitteet voivat olla yleisempiä. Tämän vuoksi voimassa oleva lainsäädäntö ei ole välttämättä riittävää täyttämään direktiivin asettamat velvoitteet. Lainsäädäntöön voikin olla tarpeellista lisätä säännöksiä verkko- ja tietojärjestelmien riskienhallintaan sekä turvallisuuspoikkeamailmoituksiin liittyen.

Työryhmä katsoo, että kansalliselle täytäntöönpanolle asetetut tavoitteet huomioiden direktiivin velvoitteet keskeisten palveluiden tarjoajien verkko- ja tietojärjestelmien riskienhallinnasta sekä turvallisuuspoikkeamailmoituksista tulisi saattaa mahdollisuuksien mukaan osaksi kansallisia relevantteja toimialakohtaisia säädöksiä.

4.7 Digitaalisen palvelun tarjoajaa koskevat turvallisuusvaatimukset ja poikkeamien ilmoittaminen (16 artikla)

Direktiivin mukaan jäsenvaltioiden on velvoitettava myös digitaalisen palvelun (verkossa toimiva markkinapaikka, verkossa toimiva hakukone, pilvipalvelu) tarjoajat hallitsemaan käyttämiinsä verkko- ja tietojärjestelmien turvallisuuteen liittyviä riskejä. Lisäksi digitaalisen palvelun tarjoajat on velvoitettava ilmoittamaan turvallisuuspoikkeamista, joilla on merkittävä vaikutus niiden tarjoamien palvelujen jatkuvuuteen. Toisin kuin keskeisten palvelujen tarjoajien osalta, komissio voi antaa täytäntöönpanosäädöksiä täsmentääkseen digitaalisen palvelun tarjoajalle asetettuja turvallisuuskriteerejä sekä poikkeamailmoituskynnystä.

Direktiivin mukaisien digitaalisen palvelun tarjoajien riskienhallintaa ei ole toistaiseksi varsinaisesti säännelty kansallisesti eikä EU:n tasolla. Niitä koskevat riskienhallinta- ja poikkeamaraportointivelvoitteet voitaisiin mahdollisesti jatkossa ottaa osaksi tietoyhteiskuntakaarta. Tietoyhteiskuntakaari sisältää jo vastaavantapaista sääntelyä teleyrityksille.

Työryhmä katsoo, että digitaalisen palvelun tarjoajaa koskevat turvallisuusvaatimukset ja poikkeamien ilmoittamista koskevat velvollisuudet voitaisiin ottaa osaksi tietoyhteiskuntakaarta.

4.8 Vähimmäisvelvoitteet korkean verkko- ja tietojärjestelmien turvallisuuden ylläpitämiseksi

Direktiivissä määritellään vähimmäisvelvoitteet korkean verkko- ja tietojärjestelmien turvallisuuden ylläpitämiseksi. Jäsenvaltiot voivat ottaa käyttöön myös direktiiviä pidemmälle meneviä oikeuksia ja velvoitteita. Direktiivin luonteesta johtuen ei kuitenkaan ole täysin selvää, mitä on pidettävä direktiivin vähimmäisvelvoitteina. Esimerkiksi jäsenvaltioiden on määriteltävä keskeiset palvelut direktiivin määrittämillä toimialoilla. Jäsenvaltioille on annettu suhteellisen laaja harkintavalta siinä, mitä nämä palvelut ovat.