Tietoturvan ja tietosuojan parantaminen yhteiskunnan kriittisillä toimialoilla

Työryhmän loppuraportti

LIIKENNE- JA VIESTINTÄMINISTERIÖ

Liikenne- ja viestintäministeriön julkaisuja **2021:1**

lvm.fi

Liikenne- ja viestintäministeriön julkaisuja 2021:1

Tietoturvan ja tietosuojan parantaminen yhteiskunnan kriittisillä toimialoilla

Työryhmän loppuraportti

Olli Lehtilä, Piia Nyström, Niko-Matti Ronikonmäki,
Tom-Henrik Sirviö

Liikenne- ja viestintäministeriö 2021

Julkaisujen jakelu
Distribution av publikationer

Valtioneuvoston julkaisuarkisto Valto

Publikations-
arkivet Valto

julkaisut.valtioneuvosto.fi

Julkaisumyynti
Beställningar av publikationer

Valtioneuvoston verkkokirjakauppa

Statsrådets
nätbokhandel

vnjulkaisumyynti.fi

Liikenne- ja viestintäministeriö

ISBN pdf 978-952-243-614-6

ISSN pdf 1795-4045

Taitto Valtioneuvoston hallintoyksikkö, Julkaisutuotanto

Helsinki 2021

Kuvailulehti
1.2.2021

Tietoturvan ja tietosuojan parantaminen yhteiskunnan kriittisillä toimialoilla

Työryhmän loppuraportti

Liikenne- ja viestintäministeriön julkaisuja 2021:1		**Teema**	-
Julkaisija	Liikenne- ja viestintäministeriö		
Toimittaja/t	Olli Lehtilä, Piia Nyström, Niko-Matti Ronikonmäki, Tom-Henrik Sirviö		
Kieli	Suomi	**Sivumäärä**	67

Tiivistelmä

Liikenne- ja viestintäministeriö asetti ajalle 9.11.2020 – 31.1.2021 työryhmän selvittämään tietoturvan ja tietosuojan parantamista yhteiskunnan kriittisillä toimialoilla. Taustalla on loppuvuodesta 2020 ilmi tullut psykoterapiayritykseen kohdistunut tietomurto, jonka seurauksena ihmisten terapiatietoja päätyi ulkopuolisille tahoille ja internetiin. Työryhmä on tarkastellut tietoturvan ja tietosuojan parantamista useilla kriittisillä toimialoilla, joita ovat terveydenhuolto, rahoitusmarkkinat, energiahuolto, vesihuolto, liikenne ja digitaalinen infrastruktuuri. Lisäksi tarkasteltavana ovat julkisen hallinnon merkittävät kriittiset tietojärjestelmät (pl. turvallisuusviranomaisten verkot ja järjestelmät).

Työryhmä esittää loppuraportissaan lainsäädännön muutostarpeita ja muita toimenpiteitä tietoturvan ja tietosuoja parantamiseksi yhteiskunnan kriittisillä toimialoilla. Toimenpiteissä painotetaan erityisesti viranomaisten entistä tehokkaampaa ja järjestäytyneempää yhteistyötä sekä tarvetta velvoittaviin tietoturvavaatimuksiin ja vaatimusten säännölliseen arviointiin ja valvontaan. Tietoturva-asioiden rinnalla huomiota tulee kiinnittää tietosuojasääntelyyn ja sen toimivuuteen.

Työryhmä julkaisi 15.12.2020 työstään väliraportin, joka oli lausunnoilla 15.12.2020–6.1.2021. Lausuntopalaute on huomioitu loppuraportissa.

Asiasanat	Tietoturva, tietosuoja, turvallisuus, digitalisaatio		
ISBN PDF	978-952-243-614-6	**ISSN PDF**	1795-4045
Asianumero	VN/24348/2020	**Hankenumero**	LVM073:00/2020
Julkaisun osoite	http://urn.fi/URN:ISBN:978-952-243-614-6		

Presentationsblad
1.2.2021

Förbättring av informationssäkerheten och dataskyddet inom kritiska sektorer i samhället

Arbetsgruppens slutrapport

Kommunikationsministeriets publikationer 2021:1		**Tema**	-
Utgivare	Kommunikationsministeriet		
Redigerare	Olli Lehtilä, Piia Nyström, Niko-Matti Ronikonmäki, Tom-Henrik Sirviö		
Språk	finska	**Sidantal**	67

Referat

Kommunikationsministeriet tillsatte för tiden 9.11.2020–31.1.2021 en arbetsgrupp med uppdrag att utreda förbättringen av informationssäkerheten och dataskyddet inom kritiska sektorer i samhället. Bagrunden till detta är det dataintrång som inträffade i databasen hos ett psykoterapiföretag i slutet av 2020 och som ledde till att uppgifter om människors terapi läckte ut till utomstående parter och internet. Arbetsgruppen har undersökt hur informationssäkerheten och dataskyddet kan förbättras inom flera kritiska sektorer, såsom hälso- och sjukvården, finansmarknaden, energiförsörjning, vattenförsörjning, transporter och digital infrastruktur. Dessutom synar arbetsgruppen betydande, kritiska informationssystem inom den offentliga förvaltningen (med undantag av säkerhetsmyndigheternas nät och system).

Arbetsgruppen föreslår i sin slutrapport att de ändringar i lagstiftningen som behövs och andra åtgärder ska vidtas för att förbättra informationssäkerheten och dataskyddet inom kritiska sektorer i samhället. Bland åtgärderna betonas i synnerhet ett effektivare och mer organiserat samarbete mellan myndigheterna samt behovet av bindande informationssäkerhetskrav och en regelbunden utvärdering och övervakning av kraven. Vid sidan av informationssäkerhetsfrågor bör uppmärksamhet ägnas dataskyddslagstiftningen och hur den fungerar.

Den 15 december 2020 offentliggjorde arbetsgruppen en halvtidsrapport om sitt arbete. Rapporten var på remiss under tiden 15 december 2020 till 6 januari 2021. Remissresponsen har beaktats i slutrapporten.

Nyckelord	informationssäkerhet, dataskydd, säkerhet, digitalisering		
ISBN PDF	978-952-243-614-6	**ISSN PDF**	1795-4045
Ärendenr.	VN/24348/2020	**Projektnr.**	LVM073:00/2020
URN-adress	http://urn.fi/URN:ISBN:978-952-243-614-6		

Description sheet
1 February 2021

Improving information security and data protection in the critical sectors of society

Working group final report

Publications of the Ministry of Transport and Communications 2021:1		**Subject**	-
Publisher	Ministry of Transport and Communications		
Editors	Olli Lehtilä, Piia Nyström, Niko-Matti Ronikonmäki, Tom-Henrik Sirviö		
Language	Finnish	**Pages**	67

Abstract

The Ministry of Transport and Communications appointed a working group for a period from 9 November 2020 to 31 January 2021 to examine how to improve information security and data protection in sectors that are critical to the functioning of society. The basis for setting up the group is a recent data breach against a service providing psychotherapy services. As a result of the breach, clients' therapy data became available for third parties and in the internet. The working group has examined how to improve the information security and data protection in several critical sectors, including health care, financial market, energy supply, water services, transport and digital infrastructure. Under review are also critical information systems in public administration (excluding networks and systems of security authorities).

In its final report, the working group proposes legislative amendments and other measures to improve information security and data protection in the critical sectors of society. The focus in the measures is on more efficient and organised cooperation between the authorities and the need to impose binding information security requirements that are regularly assessed and monitored. In addition to information security, attention should be paid to effective data protection regulation.

The working group released an interim report on 15 December 2020 that was available for comments from 15 December 2020 to 6 January 2021. The comments were considered in drafting the final report.

Keywords	information security, data protection, security, digitalisation		
ISBN PDF	978-952-243-614-6	**ISSN PDF**	1795-4045
Reference no.	VN/24348/2020	**Project no.**	LVM073:00/2020
URN address	http://urn.fi/URN:ISBN:978-952-243-614-6		

Sisältö

1 Ehdotukset poliittisiksi linjauksiksi

1.1 Viranomaiset toimivat yhdessä, Kyberturvallisuuskeskus tukee ja vahvistaa viranomaisia

1. Viranomaisten väliselle yhteistyölle tietoturvaloukkaustilanteissa luodaan yhtenäinen säädöspohja. Laki viranomaisten yhteistoiminnasta tietoturvaloukkausten ehkäisemisessä ja selvittämisessä sisältäisi säännökset yhteistyöryhmän perustamisesta tietoturvaloukkaustilanteissa, viranomaisten välisestä ennakoivasta ja tapahtumakohtaisesta keskinäisestä tiedonvaihdosta sekä välineistön, tilojen ja henkilöstön tilapäisestä luovuttamisesta toisen viranomaisen käyttöön. Säädöspohjan valmistelussa arvioidaan lisäksi nykyisten toimivaksi todettujen yhteistyömenettelyjen vahvistamista ja yhteistyötä yksityisen sektorin kanssa. Viranomaisille taataan riittävät resurssit yhteistoimintaan.
   Vastuutaho: LVM, muut yhteistyöviranomaisten hallinnonalat
   Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1–2 vuoden kuluessa)
2. Varmistetaan valtion budjetista riittävät viranomaisvalvonnan resurssit tämän raportin linjausten toteuttamiseen.
   Vastuutaho: LVM, VM, STM, TEM, OM, MMM, SM
   Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1–2 vuoden kuluessa)
3. Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen resursseja vahvistetaan, jotta se pystyy tukemaan ja antamaan toimialakohtaista neuvontaa muille hallinnonaloille. Kyberturvallisuuskeskukseen perustetaan jokaiselle kriittiselle toimjialle oma asiantuntijapalvelu, joiden vas-

tuuvirkamiehet tukevat päätoimisesti tietyn yksittäisen toimialan tietoturvasta vastaavaa sektoriviranomaista.
Vastuutaho: LVM, Liikenne- ja viestintävirasto, NIS-sektoriviranomaiset
Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1–2 vuoden kuluessa)

4. Liikenne- ja viestintäviraston Kyberturvallisuuskeskus tarjoaa koulutusta NIS-sektoreiden tietoturvaa valvoville viranomaisille. Työnantajavirastot sitoutuvat siihen, että Kyberturvallisuuskeskuksen koulutus tai muu vastaava tietoturvakoulutus on tietoturvavalvonnan parissa työskenteleville virkamiehille pakollinen. Työnantajavirastojen tulee kyetä esittämään koulutuksen perusteella, että tietoturvavalvonnan parissa työskentelevien asiantuntijoiden tietotaito on riittävällä tasolla.
   Vastuutaho: Liikenne- ja viestintävirasto, NIS-sektoriviranomaiset
   Toimenpiteen kiireellisyys: Kiireellisyysluokka 2 (toteutettava 2–4 vuoden kuluessa)

5. Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen tarjoama tietoturvallisuuden kartoituspalvelu mahdollistetaan kaikille kriittisille toimialoille. Palvelun avulla on mahdollista löytää ja korjata ulkoverkon tietoturvahaavoittuvuuksia. Tehdään tarvittavat lainsäädäntömuutokset. Varmistetaan, että kriittisten toimialojen viranomaisilla on riittävä osaaminen kartoituspalvelujen tulosten tulkitsemiseksi.
   Vastuutaho: LVM, Liikenne- ja viestintävirasto
   Toimenpiteen kiireellisyys: Kiireellisyysluokka 2 (toteutettava 2–4 vuoden kuluessa)

6. Selvitetään viranomaisten tarpeet teknologisille ratkaisuille salassa pidettävän ja turvaluokitellun tiedon käsittely-ympäristöjen luomiseen. Selvityksen kohteena ovat muun muassa viranomaisten yhdenmukainen salattu sähköpostiviestintä, turvalliset neuvotteluyhteydet ja -palvelut sekä turvallinen tiedonsiirtopalvelu. Selvitys tehdään vuonna 2021 ja selvityksen pohjalta haetaan ja toteutetaan nykyaikaiset ratkaisut vuosina 2022–2023. Selvityksessä arvioidaan myös tiedonvaihdon yhteentoimivuutta kolmansien tahojen kanssa.
   Vastuutaho: VM
   Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1–2 vuoden kuluessa)

7. Varmistetaan, että tietoturvaloukkausten havainnointi- ja varoitusjärjestelmä Havaro on laajasti kriittisten toimialojen käytettävissä. Tehdään tarvittavat lainsäädäntömuutokset, jotka mahdollistavat Havaro-palvelun tarjoamisen nykyistä laajemmalle joukolle.
   Vastuutaho: LVM ja Liikenne- ja viestintävirasto
   Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1–2 vuoden kuluessa)

1.2 Kaikilla kriittisillä toimialoilla on lakisääteiset tietoturvavaatimukset

8. Kriittisille toimialoille määritellään selkeät ja oikeasuhtaiset tietoturvavaatimukset lainsäädännössä. Määrittely tehdään riskiperusteisesti. Viranomaisilla on oltava laissa riittävät valtuudet antaa tietoturvaa koskevia sitovia määräyksiä kriittisille toimialoille. Olemassa olevat määräykset käydään läpi ja varmistetaan, että ne ovat ajan tasalla. Tietoturvavaatimusten valmistelussa huomioidaan kansainvälinen lainsäädäntö ja sen asettamat rajoitteet ja vaatimukset.
   Vastuutaho: LVM, TEM, MMM, STM, VM
   Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1–2 vuoden kuluessa)

9. Tietoturvavaatimusten laatimisesta vastaaville viranomaisille säädetään velvoite pyytää Liikenne- ja viestintäviraston Kyberturvallisuuskeskukselta lausunto tietoturvaa koskevista vaatimuksista ennen niiden hyväksymistä ja tarvittaessa myös vaatimusten toimeenpanosta.
   Vastuutaho: LVM, TEM, MMM, STM, VM
   Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1–2 vuoden kuluessa)

10. Liikenne- ja viestintäviraston Kyberturvallisuuskeskus, Tiedonhallintalautakunta sekä Tietosuojavaltuutettu laativat ennakollisen ohjeen yleisistä tietoturvavaatimuksissa huomioitavista asioista.
    Vastuutaho: Liikenne- ja viestintävirasto, Tiedonhallintalautakunta, Tietosuojavaltuutetun toimisto
    Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1–2 vuoden kuluessa)

1.3 Kriittisten toimintojen ja järjestelmien vaatimustenmukaisuutta arvioidaan säännöllisesti

11. Kriittisille toimialoille säädetään velvoite määritellä kriittiset tieto- ja tietoliikennetekniset prosessit ja toiminnot. Määrittelyssä huomioidaan erityisesti prosesseissa ja toiminnoissa käsiteltävien tietojen ja tietoaineistojen sekä käytettävien tietojärjestelmien kriittisyys sekä prosessien ja toimintojen merkitys yhteiskunnan keskeisille toiminnoille ja arkaluontoisille henkilötiedoille. Kriittisyyden määrittelyn reunaehdot määritellään lain-

säädännössä. Määrittelyssä huomioidaan myös EU:ssa tehtävä työ kriittisten toimintojen ja infrastruktuurin tunnistamiseksi. Määrittelyssä huomioidaan taloudelliset vaikutukset.
Vastuutaho: LVM, TEM, MMM, STM, VM
Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1–2 vuoden kuluessa)

12. Kriittisille toimialoille säädetään velvoite säännöllisesti auditoida kriittiset tieto- ja tietoliikennetekniset prosessit ja toiminnot. Auditointimalli määräytyy laissa riskiperusteisesti sen mukaan, kuinka kriittistä tietoa sisältävästä järjestelmästä tai toimintaa ohjaavasta prosessista on kyse. Auditointimallissa voidaan ottaa huomioon toimialakohtaisia erityispiirteitä. Määrittelyssä huomioidaan taloudelliset vaikutukset ja toimenpiteiden oikeasuhtaisuus eri kokoisten toimijoiden osalta.
Vastuutaho: LVM, TEM, MMM, STM, VM
Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1–2 vuoden kuluessa)

13. Kriittisten toimialojen suurimpien ja yhteiskunnan keskeisten toimintojen kannalta merkittävimpien toimijoiden tulee osoittaa käyttävänsä tietoturvallisuuden hallintajärjestelmää ISO 27001 –sertifioinnilla tai sitä vastaavalla yleiseen tietoturvastandardiin perustuvalla sertifioinnilla vuoden 2025 loppuun mennessä. Kyseessä olevat toimijat määritellään sektorikohtaisesti toimenpiteen täytäntöönpanovaiheessa.
Vastuutaho: NIS-direktiivissä määritellyt toimialat
Toimenpiteen kiireellisyys: Kiireellisyysluokka 2 (toteutus aloitettava 2–4 vuoden kuluessa)

14. Tietoturvallisuuden arviointilaitosten määrää lisätään tehostamalla arviointilaitosten hyväksymismenettelyä ja valmistelemalla tämän mahdollistavat lakimuutokset. Lakimuutoksien yhteydessä varmistetaan, että arviointilaitoksien toiminnan korkea laatu ja ammattitaito säilyy.
Vastuutaho: VM
Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1–2 vuoden kuluessa)

1.4 Kriittisten toimialojen erityispiirteet tunnistetaan ja huomioidaan

15. Säädetään tietoturva täsmällisemmin osaksi sähköverkkoyhtiöiden varautumisvelvoitetta ja varautumissuunnitelmaa.
    Vastuutaho: TEM
    Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1–2 vuoden kuluessa)

16. Varmistetaan ydinvoimaloiden tietoturvallisuusvaatimuksia koskevan ohjeistuksen velvoittavuus.
    Vastuutaho: TEM ja Säteilyturvakeskus (STUK)
    Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1–2 vuoden kuluessa)

17. Varmistetaan, että tietoturvallisuus on otettu huomioon vesihuoltolaitosten suunnitelmissa häiriötilanteisiin varautumiseksi. Laaditaan vesihuoltolaitoksia koskevia tietoturvaohjeistuksia ja varmistetaan, että vesihuoltolaitokset noudattavat niitä toiminnassaan.
    Vastuutaho: MMM
    Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1–2 vuoden kuluessa)

18. Tehdään lainsäädäntömuutokset, joilla varmistetaan, että Liikenne- ja viestintävirastolla on mahdollisuus antaa määräyksiä kaikkien liikennemuotojen tietoturvasta.
    Vastuutaho: LVM
    Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1–2 vuoden kuluessa)

19. Tietoverkkorikoksiin liittyen poliisin toimivaltuuksia selvitetään pakkokeinolainsäädännön tarkastelutarpeita koskevassa työryhmässä kysymyksen eri näkökannat huolellisesti punniten.
    Vastuutaho: OM:n työryhmä
    Toimenpiteen kiireellisyys: Työryhmälle annetussa aikataulussa

20. Lisätään poliisin tietoverkkorikostorjunnan resursseja, jotta se voi tehokkaasti ennalta estää, selvittää ja tutkia kriittisiin toimialoihin kohdistuvia tietoverkkorikoksia.
    Vastuutaho: SM
    Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1–2 vuoden kuluessa)

21. Valvovat viranomaiset ohjeistavat toimijoita tekemään tietoturvaloukkauksista rikosilmoituksen poliisille aina, kun epäilevät, että kyseessä on rikos.

Vastuutaho: NIS-sektoriviranomaiset
Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1–2 vuoden kuluessa)

22. Vaikutetaan NIS-direktiivin uudelleenarviointityössä EU:ssa, jotta tulevassa sääntelyssä otetaan huomioon Suomen kannalta keskeiset toimijat.
Vastuutaho: LVM
Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1–2 vuoden kuluessa)

1.5 Julkisen sektorin merkitys kriittisenä toimialana tunnistetaan ja huomioidaan

23. Valtion tieto- ja viestintätekniikkakeskus (Valtori) auditoi järjestelmänsä ja prosessinsa valtiovarainministeriön marraskuussa 2020 antaman ohjauksen mukaisesti[1]. Lisäksi Valtorin on vuoden 2021 loppuun mennessä varmistettava, että tietosuojaa koskevat vaikutusarvioinnit on yleisen tietosuoja-asetuksen mukaisesti tehty siltä osin, kun käsittely todennäköisesti aiheuttaa korkean riskin ihmisten oikeuksille ja vapauksille.
Vastuutaho: Valtori ja VM
Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1–2 vuoden kuluessa)

24. Arvioidaan valtion yhteisten tieto- ja viestintäteknisten palveluiden tuottajien tietosuojaa ja tietoturvaa koskevia vastuita ja velvoitteita. Lähtökohtana on, että yhteisille palveluille asetetaan palvelukohtaisesti turvallisuus-, tietosuoja- sekä toimintavarmuusvaatimukset ja palvelujen vaatimuksenmukaisuus arvioidaan hyväksytyn arviointityökalun kriteerien mukaisesti (esim. Katakri TL IV –tason vaatimukset)
Vastuutaho: VM
Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1–2 vuoden kuluessa)

25. Arvioidaan Valtorin tietoturvan ja tietosuojan vaatimia resursseja ja arvioinnin pohjalta tehdään tarvittavat resursoinnit. Resurssit tulee kohdistaa nimenomaisesti tietoturva- ja tietosuojaosaamiseen.
Vastuutaho: VM, Valtori
Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1–2 vuoden kuluessa)

[1] Valtiovarainministeriön ohjauskirje Valtorille 20.11.2020, VN/1411/2020

26. Varmistetaan Tiedonhallintalautakunnan vuoden 2020 suositusten toimeenpano hyödyntämällä Haukka-hankkeessa vuonna 2021 laadittavaa Julkri-kriteeristöä, jota julkisen sektorin toimijat käyttävät pilvipalveluiden tietoturvallisuusvaatimusten määrittämisessä sekä pilvipalveluntarjoajien ja pilvipalveluihin perustuvien valmistuotteiden tietoturvallisuuden tason arvioimisessa hankintoja tehdessään.
Vastuutaho: VM, Liikenne- ja viestintävirasto, Digi- ja väestötietovirasto
Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1–2 vuoden kuluessa)

27. Selvitetään, miten tietoturvaan ja tietosuojaan liittyvää osaamista voidaan vahvistaa julkisissa hankinnoissa esimerkiksi yhteishankintayhtiö Hansel Oy:n kautta.
Vastuutaho: VM
Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1–2 vuoden kuluessa)

28. Selvitetään Suomen 15 suurimman kunnan tietoturvan ja tietosuojan taso terveydenhuollossa, sosiaalihuollossa, energiahuollossa ja vesihuollossa. Selvityksessä hyödynnetään toimenpiteessä 4 mainittua Kyberturvallisuuskeskuksen tarjoamaa tietoturvallisuuden kartoituspalvelua.
Vastuutaho: VM, Liikenne- ja viestintävirasto
Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1–2 vuoden kuluessa)

1.6 Tietosuojasääntelyllä pystytään tehokkaasti puuttumaan oikeudenloukkauksiin

29. Selvitetään kriittisten toimialojen tietosuojaa koskeva kyvykkyystaso samaan tapaan kuin kyberturvallisuudessa.
Vastuutaho: Tietosuojavaltuutetun toimisto, Huoltovarmuuskeskus (siltä osin kun kytkös huoltovarmuuteen)
Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1–2 vuoden kuluessa)

30. Kriittisten toimialojen rekisterinpitäjien on varmistettava vuoden 2021 loppuun mennessä, että tietosuojaa koskevat vaikutusarvioinnit on yleisen tietosuoja-asetuksen mukaisesti tehty siltä osin, kun käsittely todennäköisesti aiheuttaa korkean riskin ihmisten oikeuksille ja vapauksille.

Vastuutaho: Kriittisten toimialojen rekisterinpitäjät, Tietosuojavaltuutetun toimisto
Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1–2 vuoden kuluessa)

31. Tietosuojan sertifiointielinten toiminta käynnistetään tehostamalla sertifiointielinten hyväksymismenettelyä.
Vastuutaho: Tietosuojavaltuutetun toimisto
Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1–2 vuoden kuluessa)

32. Sertifiointielimet luovat kriteerit tietosuojasertifioinnille ja tuovat ne tietosuojavaltuutetulle hyväksyttäväksi. Työssä huomioidaan olemassa olevat kansainväliset standardit. Arvioidaan mahdollisuudet hyväksyä kriittisiä toimialoja valvovien viranomaisten tietoturvamääräykset tai olemassa olevat tietoturvan arviointikriteerit yleisen tietosuoja-asetuksen mukaisiksi sertifiointikriteereiksi.
Vastuutaho: Tietosuojavaltuutetun toimisto
Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1–2 vuoden kuluessa)

33. Kannustetaan laajasti erityisiin henkilötietoryhmiin kuuluvia tai valtiosääntöoikeudellisesti arkaluonteisia tietoja käsitteleviä kriittisten toimialojen rekisterinpitäjiä osoittamaan keskeisen toimintansa tietosuojasääntelyn mukaisuus tietosuojasertifioinneilla.
Vastuutaho: Tietosuojavaltuutetun toimisto
Toimenpiteen kiireellisyys: Kiireellisyysluokka 2 (toteutettava 2–4 vuoden kuluessa)

34. Varmistetaan Tietosuojavaltuutetun toimistolle riittävät resurssit valvoa sektoreita tehokkaasti ja puuttua henkilötietojen tietoturvaloukkauksiin. Lisäksi Tietosuojavaltuutetun ratkaisukäytäntöä pyritään saattamaan nykyistä paremmin saataville.
Vastuutaho: OM, Tietosuojavaltuutetun toimisto
Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1–2 vuoden kuluessa)

35. Seurataan tietosuojalain mukaisen seuraamusjärjestelmän soveltamista ja toimivuutta.
Vastuutaho: OM
Toimenpiteen kiireellisyys: Kiireellisyysluokka 2 (toteutettava 2–4 vuoden kuluessa)

1.7 Etsitään uusia toimintatapoja tietoturvauhkista ja -loukkauksista viestimiseksi ja ilmoittamiseksi

36. Kehitetään yksityishenkilöille ja organisaatioiden edustajille palvelu (esimerkiksi mobiilipäätelaitteeseen asennettava sovellus), jonka kautta on mahdollista saada kohdennetusti ajankohtaista tietoa tietoturvauhkista ja -loukkauksista ja tietoturvallisuutta koskevista ohjeista sekä ilmoittaa tietoturvauhkista ja -loukkauksista Kyberturvallisuuskeskukselle, kriittisen toimialan valvovalle viranomaiselle ja/tai poliisille. Lisäksi palvelun avulla voisi ilmoittaa henkilötietojen tietoturvaloukkauksesta Tietosuojavaltuutetun toimistolle. Palvelu (sovellus ja palveluun liittyvät järjestelmät) toteutetaan turvallisen ohjelmistokehityksen sekä hyvän tietoturvan ja -suojan periaatteita noudattaen.
    Vastuutaho: Liikenne- ja viestintävirasto
    Toimenpiteen kiireellisyys: Kiireellisyysluokka 2 (toteutettava 2–4 vuoden kuluessa)

Työryhmä esittää, että linjausehdotusten pohjalta valmistellaan valtioneuvoston periaatepäätös. Työryhmä pitää tärkeänä, että periaatepäätöksessä linjattujen toimenpiteiden täytäntöönpanoa seurataan esimerkiksi puolivuosittain.

2 Johdanto

Yhteiskunnan eri sektorit ovat yhä riippuvaisempia digitaalisten palveluiden käytöstä niin Suomessa kuin maailmanlaajuisesti. Yhteiskunnan keskeiset palvelut, kuten sähkön ja juomaveden jakelu sekä terveydenhuollon palvelut, tarvitsevat luotettavia yhteyksiä ja tietojärjestelmiä toimiakseen. Eri toimialoilla tulee viimeistään nyt ottaa huomioon, että tietoturvallisuuden ja tietosuojan merkitys palveluiden laadulle ja turvallisuudelle on perusedellytys digitaalisessa yhteiskunnassa.

Lainsäädännössä on asetettu yleisiä tietoturvallisuutta ja tietosuojaa koskevia velvollisuuksia, joita on erityisesti henkilötietosääntelyssä ja viranomaisia koskevissa yleislaeissa. Lisäksi Suomessa on useilla toimialoilla sektorikohtaisia velvoitteita huolehtia palveluiden ja tietojärjestelmien tietoturvasta ja tietosuojasta. Hyviä esimerkkejä tällaisista toimialoista ovat viestintä- ja finanssisektorit. Eri sektoreiden kyvykkyydet vastata kasvaviin tietoturva- ja tietosuojahaasteisiin vaihtelevat kuitenkin suuresti. Yhteiskunnan eri sektoreille asetetaan toisistaan poikkeavia tietoturva- ja tietosuojavaatimuksia, joissa on pyritty huomioimaan kunkin toimialan erityispiirteitä. Myös lainsäädännön yhtenäistäminen EU:n tietosuojalainsäädännön vaatimusten kanssa on vielä kesken, vaikka usea ministeriö on jo toteuttanutkin uudistuksia. Yksin lakisääteiset velvoitteet ja määräykset eivät kuitenkaan ole riittäviä tietoturvallisuuden ja tietosuojan parantamisessa, vaan velvoitteita täydentävät eri toimialojen toimintakulttuuri, yhteinen tilannekuva, ymmärrys toimintaympäristön muutoksista sekä vapaaehtoinen yhteistyö viranomaisten sekä palveluiden tarjoajien välillä.

Tietoturvaa koskevat häiriöt ja loukkaukset sekä tietosuojaa koskevat loukkaukset voivat vaikuttaa merkittävästi toimialojen toimintaan ja palveluihin. Tämä pätee nykyään myös esineisiin, laitteisiin ja kulkuneuvoihin, joista yhä suurempi osa on yhteydessä internetiin, ja joiden toimintaa ohjataan digitaalista tietoa käsittelemällä. Käytössä olevien yhteyksien, palveluiden ja laitteiden tietoturvallisuuden taso vaikuttaa suoraan kansalaisten digitaalisia palveluita ja tuotteita kohtaan kokemaan luottamukseen. Tuotteet, palvelut ja tietojärjestelmät on suunniteltava, valmistettava ja ylläpidettävä siten, että tietoturva ja tietosuoja muodostavat niiden erottamattoman ja sisäänrakennetun osan. Toisin sanoen tietosuoja ja tietoturva on huomioitava toiminnan koko elinkaaren aikana tuote-, järjestelmä- ja palvelukehityksen lähtökohtana, eikä jälkikäteen päälle liimattavana tarrana tai laastarina.

Digitaalista toimintaympäristöä koskevan tiedon ja ymmärryksen lisääminen sekä toimivien ja turvallisten toimintamallien opastaminen yksityisille ja julkisille organisaatioille sekä yksittäisille käyttäjille on tärkeässä asemassa digitaalisessa yhteiskunnassa ja kansalaisten luottamuksen saavuttamisessa. Kyseessä on vahvasti myös riskien hallintaa koskeva kysymys, johon toimijoiden tulee vastata säilyttääkseen verkko- ja

tietojärjestelmiensä turvallisuuden eheyden ja häiriönsietokyvyn. Yritystasolla häiriöt ja loukkaukset voivat aiheuttaa merkittäviä taloudellisia vahinkoja ja laajemmassa mittakaavassa häiriöillä voi olla vaikutusta koko yhteiskunnan huoltovarmuudelle ja peruspalveluiden saatavuudelle.

Psykoterapiakeskus Vastaamoon kohdistunut tietomurto osoitti, miten tietomurto tai kyberhyökkäys voi vaikuttaa merkittävästi tavallisten ihmisten arkeen ja paljastaa erittäin arkaluonteisia tietoja ihmisten elämästä. Tietomurrot ja tietosuojaloukkaukset voivat taloudellisten vaikutusten lisäksi aiheuttaa myös syvää inhimillistä kärsimystä, jonka merkitystä yhteiskunnallisena ja oikeudellisena epäkohtana ei pidä väheksyä. Julkisen vallan tehtävänä on perustuslain nojalla turvata kansalaisten yksityiselämän suoja ja muut perusoikeudet. Yksin viranomaistoimilla riittävää turvallisuustasoa ei kuitenkaan ole mahdollista saavuttaa, vaan tietoturvan ja tietosuojan merkitys on tunnistettava kaikkialla yhteiskunnassa ja myös yksityisen sektorin toimijoiden on sitouduttava siihen.

Vastaamon tietomurtotapaukseen liittyvien näkökohtien selvittäminen on osoittanut, että Suomessa on tietojärjestelmiä, joiden tietoturvan ja tietosuojan taso ei ole riittävällä tasolla siten kuin EU:n tietosuojalainsäädäntö ja toimialan erityislainsäädäntö edellyttävät. Osa näistä järjestelmistä on yhteiskunnan toiminnan kannalta kriittisillä toimialoilla. Lähtöoletuksena voidaan pitää, että tällaisia tietojärjestelmiä koskevaa sääntelyä ja valvontaa on vahvistettava. Tuloksekas toiminnan kehittäminen edellyttää sääntelyn, ohjeistuksen ja valvonnan rinnalla, että taloudelliset voimavarat suunnataan tehokkaasti niin julkisella sektorilla kuin elinkeinoelämässä. Viime kädessä yritykset ja viranomaiset kuitenkin vastaavat omien palveluidensa, tuotteidensa ja tietojärjestelmiensä tietoturvan ja tietosuojan tasosta.

Havaittuihin puutteisiin ja tietoturvan sekä tietosuojan korkean tason edellyttämiin kehittämistoimenpiteisiin on tartuttu Suomessa nopeasti. Liikenne- ja viestintäministeriön asettama työryhmä on selvittänyt tarvittavia toimenpiteitä tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla[2]. Tarkasteltavia toimialoja ovat olleet EU:n verkko- ja tietoturvadirektiivin (NIS-direktiivi) mukaisesti erityisesti terveydenhuolto, rahoitusmarkkinat, energiahuolto, vesihuolto, liikenne ja digitaalinen infrastruk-

[2] Työryhmä kokoontui toimikaudellaan kahdeksan kertaa. Työryhmässä kuultiin työryhmän ulkopuolisina tahoina Keskusrikospoliisia, Valviraa, Finanssivalvontaa, Energiavirastoa, Valtioneuvoston tietosuojaverkostoa, tietoturvallisuuden arviointilaitoksia (KMPG Oy ja Nixu Oyj), CSC Tieteen tietotekniikan keskus Oy:tä ja Suojelupoliisia. Työryhmä julkaisi 15.12.2020 työstään väliraportin, joka oli lausunnoilla 15.12.2020-6.1.2021. Väliraportista annettiin 55 lausuntoa, joista saatua palautetta hyödynnettiin lopullisessa selvityksessä.

tuuri, sekä viestintäverkot. Lisäksi tarkasteltavana ovat olleet valtion ja kuntien merkittävät tietojärjestelmät, joita voidaan pitää kriittisinä yhteiskunnan toiminnan kannalta. Turvallisuusviranomaisten verkot ja järjestelmät rajattiin selvityksen ulkopuolelle, koska katsottiin, että tällaisia erittäin turvallisuuskriittisiä toimintoja on tarkoituksenmukaista tarkastella erillisenä kokonaisuutena.

Työryhmän asiantuntijakuulemisissa ja lausuntopalautteessa on tuotu esille, että myös muilla kuin nyt tarkasteltavilla toimialoilla on tarpeita kehittää tietoturvallisuutta ja tietoturvavaatimusten valvontaa. Työryhmä on kuitenkin sille annettu aikataulu huomioiden katsonut, ettei selvityksen laajentaminen muille kuin edellä mainituille toimialoille ole tässä vaiheessa mahdollista. Työryhmä on keskittynyt etsimään tehokkaita lyhyen aikavälin toimenpiteitä, joilla tietoturvaa ja tietosuojaa voidaan parantaa yhteiskunnan toiminnan kannalta kriittisiksi tunnistetuilla toimialoilla.

Työryhmä esittää selvityksessä konkreettisia toimenpide-ehdotuksia, joiden avulla tietoturvaan ja tietosuojaan liittyviin puutteisiin pystyttäisiin tulevaisuudessa tehokkaammin puuttumaan. Osana toimenpide-ehdotuksia työryhmä on arvioinut erilaisia vaihtoehtoja tavoitteiden saavuttamiseksi ja kartoittanut tarvittavia lainsäädäntömuutoksia. Lisäksi työryhmä on arvioinut tarvittavia resursseja ja taloudellisia vaikutuksia liittyen toimenpide-ehdotuksiin. Työryhmän tavoitteena on, että resurssiarviot sisältyvät kevään 2021 ja 2022 lisätalousarvioihin. Esitetyt resurssi- ja määrärahatarpeet tulisi osoittaa viranomaisille mahdollisimman pian, jotta tietoturvan ja tietosuojan tasoon saadaan välittömiä parannuksia kriittisillä toimialoilla.

Tietosuojan osalta on keskeistä huomata, että tietoturva on vain yksi keino suojata henkilötietoja. Tietoturvan lisäksi henkilötietoja suojataan esimerkiksi minimoimalla käsiteltävien henkilötietojen määrä vain välttämättömään tai käsittelemällä tiedot siten, etteivät ne ole suoraan yhdistettävissä yksittäiseen henkilöön. Tässä selvityksessä tietosuojaa on käsitelty pääasiassa tietoturvan näkökulmasta. Tämä ei kuitenkaan vähennä muiden henkilötietojen käsittelyä ohjaavien periaatteiden ja säännösten merkitystä kansalaisten tietosuojan ja tiedollisen itsemääräämisoikeuden turvaamisessa. Selvityksessä käytettyjen termien osalta on syytä huomata, että tässä selvityksessä käytetään synonyymeina termejä kyberturvallisuus ja tietoturvallisuus.

Suomessa kybertuvallisuuden kehittämistä on tarkasteltu laajasti vuonna 2019 valmistuneessa Suomen kyberturvallisuusstrategiassa ja sen toimeenpano-ohjelmassa, joka valmistuu keväällä 2021[3]. Kyberturvallisuusstrategian toimeenpanossa keskitytään erityisesti pitkän aikavälin toimiin kyberturvallisuuden kehittämiseksi, kuten osaami-

[3] https://turvallisuuskomitea.fi/suomen-kyberturvallisuusstrategia-2019/.

sen- ja tietoturvakulttuurin parantamiseen. Tästä syystä vastaavia, esimerkiksi kansainväliseen yhteistyöhön, osaamiseen tai harjoitustoimintaan kohdistuvia, pitkän aikavälin toimenpiteitä ei ole tarkasteltu tässä selvityksessä. Toimenpide-ohjelman ja tämän selvityksen toimenpiteiden on tarkoitus muodostaa yhdenmukainen ja toisiaan tukeva kokonaisuus, joilla tietoturvan ja tietosuojan toteutumiseen liittyviin haasteisiin pystytään puuttumaan sekä pitkällä että lyhyellä aikavälillä. Tavoitteena on yhteiskunta, jossa on maailman luotettavimmat ja turvallisimmat digitaaliset palvelut kaikille yhteiskunnan toimijoille.

3 Tietoturva ja tietosuoja yhteiskunnallisina ja taloustieteellisinä ilmiöinä

3.1 Yksityinen ja julkinen vastuu

Tietoturvan ja tietosuojan kehittämisessä ovat vastakkain yhtäältä yksittäisten toimijoiden velvollisuudet ja toisaalta yhteiskunnan vastuut ja tarpeet. Taloustieteellinen kirjallisuus tarjoaa välineitä aihepiirin haasteiden kuvaamiseen. Laaja aihepiiriin liittyvä haaste on, että yksittäisten toimijoiden ja yhteiskunnan toiminta eivät ole sopusoinnussa[4]. Tietoturvaan ja tietosuojaan liittyvissä haasteissa on hyödyllistä erottaa yksittäisiin toimijoihin, kuten kansalaisiin tai yrityksiin, ja kansantalouteen kohdistuvat vaikutukset.

Taloustieteellisessä tarkastelussa tietoturvaan ja tietosuojaan liittyvät haasteet nähdään erityisesti kannustinongelmana. Yhteiskunnan näkökulmasta jokaisen toimijan tulisi suojata tuotteensa ja palvelunsa riittävillä keinoilla. Lisäksi yksityishenkilöiden tulisi varmistaa omien laitteidensa tietoturvallisuus. Näillä toimenpiteillä tietomurtojen ja muiden ongelmatilanteiden riski pienenee. Toimijat eivät kuitenkaan välttämättä päädy hankkimaan riittävää tietoturvan tasoa. Tämä johtuu erityisesti siitä, että ongelmatilanteissa yksittäinen toimija ei joudu kantamaan kaikkia seurauksia vaan osa kaatuu yhteiskunnan kannettavaksi. Taloustieteellisessä kirjallisuudessa tilannetta, jossa toiminnan haitat koskevat muitakin kuin yksittäistä toimijaa, sanotaan negatiiviseksi ulkoisvaikutukseksi.

Esimerkiksi psykoterapiakeskus Vastaamon tapauksessa on nähtävissä, että osa tietomurron kustannuksista jää yhteiskunnan ja yksittäisten rekisteröityjen kannettavaksi. Yhteiskunta esimerkiksi tarjoaa tietomurron uhreille tukipalveluita ja neuvontaa. Uhrit kokevat henkistä kärsimystä, joutuvat elämään sen tiedon kanssa, että tietoja voidaan käyttää myöhemmin hyväksi, sekä käyttämään aikaa ja rahaa suojautuakseen tietojen myöhemmältä hyväksikäytöltä. Toisaalta tietomurto on herättänyt tarpeen keskustella sääntelyn tasosta ja sen uudistamisesta. Lisäksi tietosuojaan ja tietoturvaan liittyvät ongelmatilanteet voivat johtaa suoriin laite- tai palveluinvestointeihin.

[4] Katso esimerkiksi Moore (2010).

Yksittäisen toimijan ongelmaa voidaan kuvata myös yksityisyysparadoksin käsitteen avulla. Tällä tarkoitetaan tilannetta, jossa toimijat antavat ymmärtää olevansa kiinnostuneita tietosuojaan ja tietoturvaan liittyvistä asioista, mutta käyttäytyvät niistä jokseenkin välittämättä[5]. Esimerkiksi Vastaamoon liittyvässä tietomurrossa voidaan nähdä sekä kannustinongelmaan että yksityisyysparadoksiin liittyviä piirteitä, kun toimijan valmistautuminen on ollut puutteellista ja julkinen sektori on joutunut kantamaan tietomurrosta vastuuta.

Kannustinongelman ratkaisemiseksi sääntelijän tehtävänä on luoda järjestelmä, jossa yksittäisellä toimijalla on riittävät kannustimet hankkia ja ylläpitää riittävä tietosuojan ja tietoturvan taso. Taloustieteellistä tietoturvan ja tietosuojan kansantaloudellisten vaikutusten mallintamiseen liittyvää tutkimusta on suhteellisen vähän. Tietoturvan ja tietosuojan haasteiden ja ratkaisujen mallintamiseen voi kuitenkin hyödyntää esimerkiksi veronkiertoon liittyviä perusmallinnuksia, joissa päätös kiertää veroa tehdään kahden eri vaihtoehdon (kiertää veroa, ei kierrä veroa) odotettujen rahallisten hyötyjen ja tappioiden välillä[6]. Asetelma voidaan kääntää yksittäisen toimijan tietosuojan hankintaa ja ylläpitoa koskevaksi valintatilanteeksi.

Yksinkertaistettuna voidaan ajatella, että toimija valitsee riittävän ja riittämättömän tietosuojan ja tietoturvan tason välillä. Riittävä taso on kalliimpi hankkia, sillä se voi aiheuttaa suurempia kustannuksia esimerkiksi tietoturvavälineissä ja ylläpidossa. Sen sijaan riittämättömän tietoturvan valinta on edullisempi vaihtoehto, kun alkuinvestointi ja ylläpito eivät vie niin paljon resursseja. Molempiin tilanteisiin liittyy tietomurrosta seuraava odotettu haitta, joka voi olla molemmille valinnoille sama. Kun rahallinen hyöty on suurempi riittämättömän tietosuojan tapauksessa, on todennäköistä, että toimija valitsee riittämättömän tietosuojan ja tietoturvan tason.

On kuitenkin mahdollista, että valintapäätökseen liittyy myös muita huomioonotettavia asioita. Jos tietomurto tapahtuu ja toimijalla on ollut riittämätön tietosuojan ja tietoturvan taso, voi toimijan maine laskea ja vähentää esimerkiksi asiakkaiden määrää. Mainehaitan vaikutukset yrityksen pitkän aikavälin toimintaedellytyksiin ovat kuitenkin epäselvät. Tutkimusten mukaan tietomurto ei ole vaikuttanut yritysten pitkän aikavälin markkina-arvoon, vaikka kyberhyökkäys vaikuttaa negatiivisesti niiden osakkeiden arvoon lyhyellä aikavälillä[7].

[5] Katso esimerkiksi Brown (2016).

[6] Katso esimerkiksi Allingham ja Sandmo (1972).

[7] Sen (2018) kokoaa tutkimustuloksia.

Mainehaitan merkitys tietosuojan ja tietoturvan tason valinnassa on tärkeä hahmottaa, jotta sen vaikutus riittävän tason valintaan selviää. Jos mainehaitan riski on suuri, toimijat valitsevat todennäköisemmin riittävän tason. On kuitenkin hyödyllistä huomata, että mainehaitan tasoon julkinen valta ei varsinaisesti pysty vaikuttamaan. Sen sijaan julkinen valta voi kannustaa tai sääntelyllä velvoittaa valitsemaan riittävän tietoturvan ja tietosuojan tason, jotta tietomurtojen todennäköisyys pienenisi.

Julkisen vallan näkökulmasta riittävän tietosuojan ja tietoturvan tason valitseminen on olennaista, sillä riittämätön taso heikentää kansalaisten hyvinvointia sekä resurssien että muiden mekanismien kautta. Riittämättömästä tasosta johtuvat tietomurrot kasvattavat resurssitarvetta ja ovat pois muista käyttökohteista. Toisaalta esimerkiksi Vastaamon kaltaisessa tapauksessa tietomurrosta aiheutuu inhimillisiä kustannuksia, kun yksityiset tiedot leviävät tarkoitettua laajemmalle. Lisäksi tietojen leviäminen voi kasvattaa epäluottamusta yhteiskunnassa, jos yksilöt eivät uskalla jakaa omia tietojaan esimerkiksi Vastaamon kaltaisille yrityksille.

Kansantalouden tasolla riittävän tietosuojan ja tietoturvan tason toteutumiseen viime kädessä vaikuttavat poliittiset linjaukset. On kuitenkin syytä huomata, että henkilötietojen suojan osalta EU:n tietosuojasääntelyn mukaisista vaatimuksista ei voi poiketa. Järjestelmän tavoitteena voi olla se, että käytännössä kaikki toimijat hankkivat riittävän tietoturvan ja tietosuojan tason, jolloin niiden murtuminen on hyvin epätodennäköistä. On myös mahdollista, että tätä ei tavoitella. Täydellinen tietoturvan taso ei välttämättä ole siinä mielessä optimaalinen, että toiminnan tehokkuuden ja tietosuojan välillä on tehtävä valinta. Enemmän tietoturvaa ja tietosuojaa tarkoittaa tehottomampaa toimintaa[8]. Tietoturvaan ja tietosuojaan kuluu enemmän resursseja, kun on enemmän tehtävää. Lisäksi suurempi tietoturvan ja tietosuojan määrä voi aiheuttaa epätehokkuuksia tuotannossa, kun esimerkiksi järjestelmän ylläpitoon kuluu resursseja. Toisaalta vähemmän tietoturvaa tarkoittaa tehokkaampaa toimintaa, mutta suurempaa riskiä tietomurroille.

Riittävän tietoturvan ja tietosuojan tasoon liittyen on myös hyvä huomioida, etteivät ne ole staattisia tilanteita vaan vaativat säännöllistä huomiota. Erityisesti tietoturva on dynaaminen ja muuttuva tila, joka vaatii säännöllistä riskien arviointia ja kehittämistä.

[8] Moore (2010).

3.2 Lähestymistapoja tietoturvan ja tietosuojan parantamiseen

Keinot tavoiteltavan tietosuojan ja tietoturvan tason saavuttamiseksi on päätettävä, kun tavoiteltu taso on tiedossa. Keinojen keskiössä on toimijan kannustaminen valitsemaan riittävä taso riittämättömän sijaan. Kannustinjärjestelmän luomiseen on erilaisia keinoja. Toimivan järjestelmän tulee sisältää sekä ennaltaehkäiseviä (ex ante) että jälkikäteisiä (ex post) toimia[9]. Käytännössä lainsäädännön lisäksi valvonta ja jonkinlaiset sanktiot riittämättömästä tasosta voivat olla tarpeellisia keinoja. Kuva 1 kokoaa erilaisia lähestymistapoja aihepiirin sääntelyyn.

Kuva 1. Lähestymistapoja tietoturvan ja tietosuojan parantamiseksi

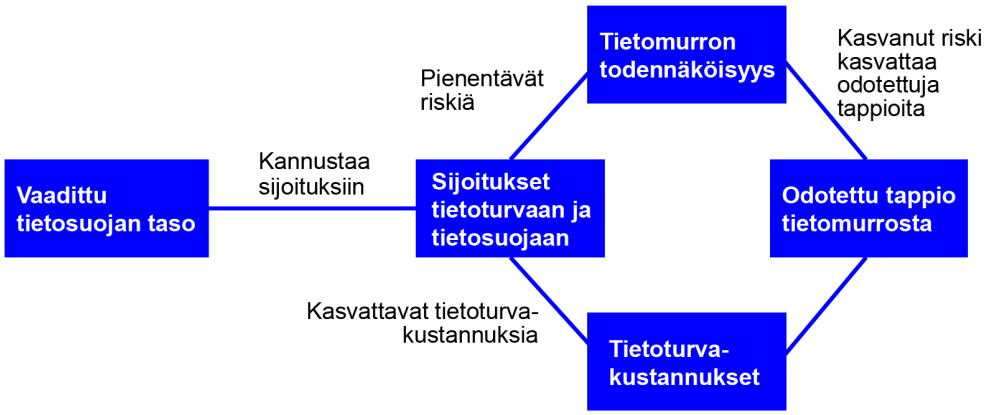
Lähestymistapoja		
Ennaltaehkäisevä sääntely	**Tiedonsaantioikeudet (information disclosure)**	**Jälkikäteiset velvollisuudet**
Mekanismi, jolla tapahtuma on tarkoitus estää etukäteen. Tarkoitus kannustaa minimivaatimusten omaksumiseen, mikä vähentää haitallisen tapahtuman todennäköisyyttä.	Kannusteita korjaava mekanismi, jossa mahdollisesta haitasta tehdään kannustinmekanismi.	Mekanismi, jolla on tarkoitus korjata vahinkoja jälkeenpäin. Tämä voi tarkoittaa esimerkiksi haittojen korvaamista uhreille.

Lähde: Romanosky ja Acquisti (2009)

Ennaltaehkäisevien toimien tarkoituksena on luoda haitallisia tapahtumia estäviä mekanismeja. Esimerkiksi tietosuoja- ja tietoturvalainsäädäntö, jolla säädetään minimivaatimuksista, on ennaltaehkäisevää sääntelyä. Ennaltaehkäisevien toimien täydennykseksi voi olla hyvä luoda kannustinmekanismeja ja jälkikäteisiä velvollisuuksia, joilla toimijoita voidaan asettaa jälkikäteiseen korvausvastuuseen. Kuvassa yksi esiteltyjen lähestymistapojen tarkempia toimintamekanismeja on kuvattu kuvissa 2-4. Kuvissa vaikutusmekanismeilla vertaillaan tilannetta, jossa sääntely on tilanteeseen, jossa sitä ei ole.

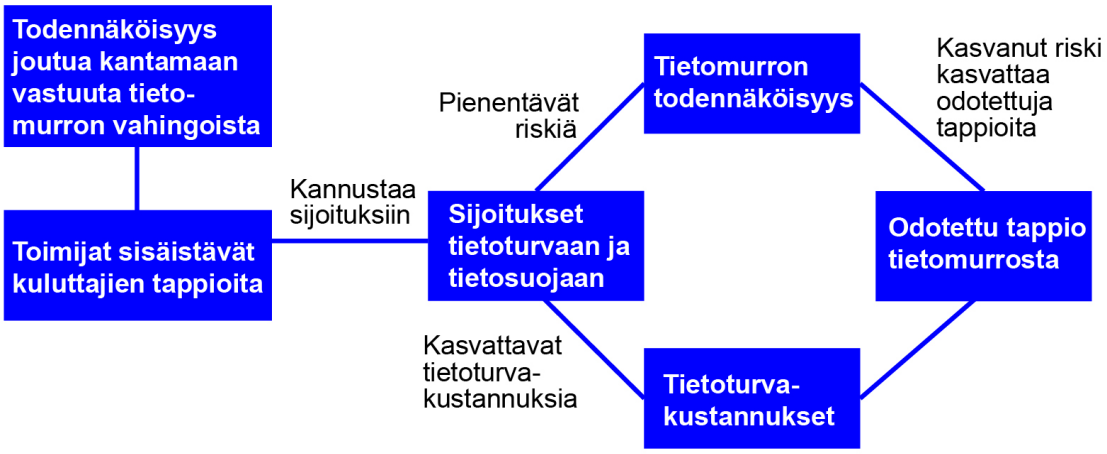
[9] Katso esimerkiksi Moore (2010).

Kuva 2. Ex ante -sääntelyn vaikutusmekanismi (Lähde: mukaillen Romanosky ja Acquisti 2009)



Verrattaessa tilanteeseen ilman ennaltaehkäisevän sääntelyn mekanismia toimijat käyttävät enemmän resursseja tietoturvaan ja tietosuojaan liittyviin menoihin. Tämä pienentää tietomurron todennäköisyyttä ja toisaalta kasvattaa tietoturvakustannuksia. Tietoturvakustannukset voivat kuitenkin kokonaisuudessa jäädä pienemmiksi, kun tietoturvauhkiin varaudutaan ennakolta sen sijaan, että jälkikäteen maksettaisiin varautumattomuudesta. Tietomurron pienentynyt riski pienentää myös tietomurron odotettuja tappioita.

Kuva 3. Jälkikäteisen sääntelyn vaikutuskanavat (Lähde: mukaillen Romanosky ja Acquisti 2009)



Toinen lähestymistapa on jälkikäteisten vastuiden säätäminen. Kuvassa kolme kuvattu mekanismi on samankaltainen kuin kuvan kaksi mekanismi, mutta lähtökohtana on, että toimija joutuu jollain todennäköisyydellä kantamaan jälkikäteistä vastuuta tietomurron vahingoista, jos tietoturva ei ole ollut riittävällä tasolla. Tällaisen vastuun säätäminen kannustaa toimijoita sisäistämään kuluttajien kustannuksia (esimerkiksi yksityisten tietojen leviämisen aiheuttama harmi). Se taas saa toimijat sijoittamaan enemmän resursseja tietoturvaan ja tietosuojaan.

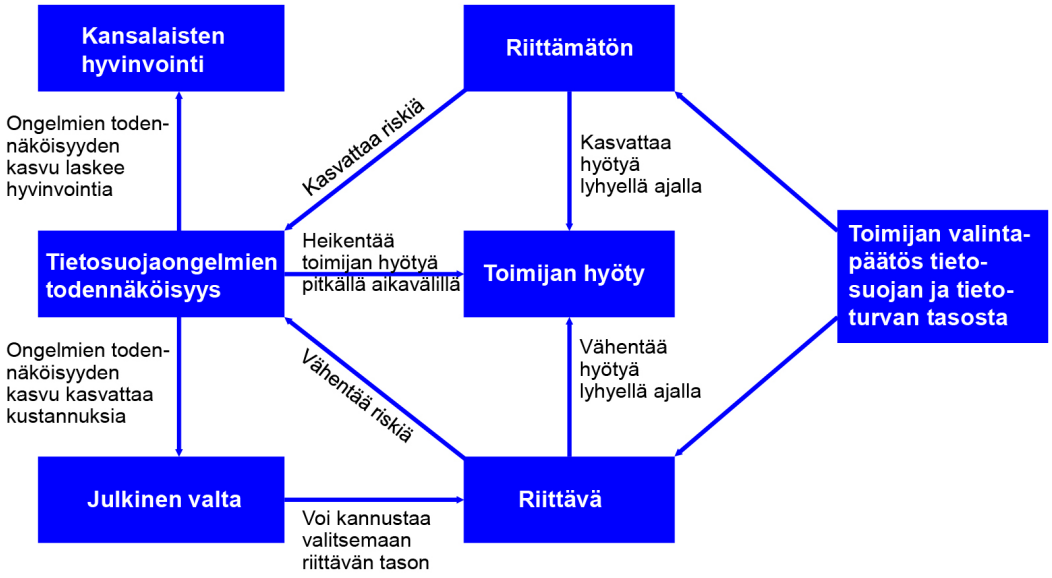
Yksi tapa kannustaa valitsemaan riittävä tietosuojan ja tietoturvan taso on tehdä riittämättömän tason valitsemisesta vähemmän houkuttelevaa. Julkinen valta voi esimerkiksi määrätä toimijoille satunnaisia tarkastuksia, joista seuraa sanktioita siinä tapauksessa, että tietosuojan ja tietoturvan taso on riittämätön. Silloin toimijoiden hyöty riittämättömän tason valinnasta pienenee, kun tarkastus ja sanktiot ovat mahdollisia. Toimijat tiedostavat pienentyneen hyödyn ja valitsevat todennäköisemmin riittävän tietosuojan ja tietoturvan tason.

Edellä kuvatussa mallissa sääntelijän tehtävä olisi määrittää tarpeellinen määrä tarkastuksia suhteessa toimialan kokoon nähden niin, että tarkastuksen todennäköisyys ja sanktio ovat toimijan kannalta tarpeeksi suuria. Tarkastusten määrässä olisi syytä kiinnittää huomiota siihen, että toimijan näkökulmasta tarkastuksen mahdollisuus on niin suuri, että se vaikuttaa valintapäätökseen riittävän tietosuojan ja tietoturvan tason valinnan todennäköisyyttä kasvattavasti. Päätöksentekijän tulee määritellä tavoiteltava taso, johon päästään hyödyntämällä edellä mainittua tai jotain vaihtoehtoista mallia.

Tarkastusmahdollisuuden ja sanktioiden lisäksi hyödyllinen ja kustannustehokas malli voi olla myös aiheesta tiedottaminen niitä koskeville toimijoille. Veronkiertokirjallisuudessa on havaittu, että kirjeitse tapahtuva muistuttaminen verovelvollisuudesta vähentää veronkiertoa[10]. Samankaltainen ajatus voi toimia tietoturvaan ja tietosuojaan liittyen. Kaikki toimijat eivät välttämättä ole lainsäädännöstä huolimatta tietoisia riittävästä tietosuojan ja tietoturvan tasosta ja niiden saavuttamiseksi vaadituista välineistä taikka riittämättömästä tietosuojan ja tietoturvan tasosta seuraavista sanktioista. Tällöin riittävän konkreettinen tiedottaminen vaatimuksista, niiden saavuttamiseksi tehtävistä toimista sekä sanktioista tapauksissa, jossa tietoturvan ja tietosuojan taso ei ole tarkastuksessa riittävällä tasolla, voi kannustaa yksittäisiä toimijoita huolehtimaan tietosuojan ja tietoturvan hankinnasta ja kunnossapidosta.

[10] Slemrod (2018) kokoaa aihepiirin tutkimustuloksia.

Kuva 4. Yksittäisen toimijan tietosuojan ja tietoturvan tason valintapäätöksen vaikutukset



Kuviossa neljä toimija tekee ensimmäisenä valintapäätöksen, jossa valitaan riittävä tai riittämätön tietosuojan ja tietoturvan taso. Päätöksentekijä on määritellyt riittävän tason. Riittämättömän tason valinta kasvattaa toimijan hyötyä lyhyellä aikavälillä, koska se on kustannuksiltaan edullisempi. Riittävä taso vähentää toimijan hyötyä lyhyellä aikavälillä, koska kustannukset kasvavat. Samaan aikaan riittävän tason valinta pienentää tietosuojaongelmien riskiä ja riittämättömän tason valinta kasvattaa sitä. Tietosuojaongelmien riskin kasvaminen heikentää toimijan hyötyä, julkisen vallan toimintaedellytyksiä ja viimeksi kansalaisten hyvinvointia. Julkinen valta voi kuitenkin erilaisin keinoin kannustaa toimijoita valitsemaan riittävän tietosuojan ja tietoturvan tason. Esimerkkejä keinoiksi on esitelty yllä.

4 Nykytilan arviointi

4.1 Lainsäädännössä asetetut tietoturvaa ja tietosuojaa koskevat vaatimukset

Nykyisin käytössä olevista ennaltaehkäisevistä toimenpiteistä työryhmä tarkasteli toimialojen tietoturvaan ja tietosuojaan liittyviä lainsäädännöstä johtuvia vaatimuksia. Tarkastelun perusteella toimialojen välillä on merkittäviä eroavaisuuksia sen suhteen, kuinka tarkkoja tietoturva- ja tietosuojavaatimuksia on säädetty suoraan laissa. Tämän osalta eroavaisuudet korostuivat erityisesti sen osalta, miten toimintojen tietoturvallisuuden toteuttamisesta on säädetty. Esimerkiksi tietoturvaloukkauksia koskevat ilmoitusvelvoitteet ovat lainsäädännön tasolla pääosin yhtenäiset. Huomionarvoista on myös, että joissain varsin merkittävissäkin yhteiskunnan toiminnoissa, kuten ydinlaitoksissa, tietoturvaa koskeva sääntely on velvoittavan lain, asetuksen tai määräyksen sijasta viranomaisen ohje[11]. Toimialoja koskevat keskeiset tietoturvavaatimukset on koottu selvityksen liitteenä olevaan taulukkoon.

Työryhmän saaman selvityksen perusteella tietoturvallisuuden kannalta paras tilanne on rahoitus- ja televiestintäaloilla, joissa on pitkät perinteet tietoturvaa koskevasta alan toimijoita velvoittavasta sääntelystä. Muiden toimialojen (energia, terveydenhuolto, liikenne, vesihuolto) osalta tilanne on huonompi ja hajonta yksittäisen toimialan sisällä on suurta. Osasyynä asiaan on se, että eri sektoreilla on asetettu toisistaan niin määrällisesti kuin laadullisesti poikkeavia tietoturva- ja tietosuojavaatimuksia. Lisäksi on huomioitava, että eri toimialat ovat digitaalisessa kehityksessä eri vaiheessa ja toimijoiden kokoluokassa voi olla merkittäviä eroja. Kaikilla toimialoilla on tunnistettu erityisesti viranomaisvalvontaan liittyviä resurssitarpeita. Yleisesti voidaan sanoa, että tietoturvaa koskevalla sääntelyllä on positiivinen vaikutus siihen, miten hyvin tietoturvallisuus on huomioitu ja toteutuu toimialoilla.[12]

Erityisesti tietoturvaa valvovien sektoriviranomaisten ja tietoturva-arviointeja tekevien toimijoiden kuulemisissa korostui tarve nykyistä yksityiskohtaisemmille tietoturvavaatimuksille. Konkreettiset vaatimukset tehostaisivat valvontaa, koska niiden täyttyminen

[11] STUK:n on antanut ydinenergialain 7 r §:n nojalla ohjeen ydinlaitoksen tietoturvallisuuden hallinnasta: https://www.stuklex.fi/fi/ohje/YVLA-12
[12] Huoltovarmuuskeskuksen raportti kybertuvallisuuden nykytilasta eri toimialoilla: https://cdn.huoltovarmuuskeskus.fi/app/uploads/2020/10/05091400/Kyberturvallisuuden-nykytila-eri-toimialoilla.pdf

olisi helpompi todentaa kuin laissa olevien hyvin yleistasoisesti muotoiltujen huolellisuusvelvoitteiden. Etenkin energia-, liikenne- ja vesihuoltosektorilla lain nojalla annettuja vaatimuksia on vähän tai ei lainkaan. Laissa ei myöskään kaikissa tapauksessa ole valtuutusta antaa alemman aseista sääntelyä tai vaihtoehtoisesti valtuutusta ei ole käytetty. Vastaava tilanne on julkisen sektorin tiedonhallinnassa erityisesti alemman asteisen sääntelyn osalta.

Terveydenhuollossa haasteet liittyvät erityisesti niin sanottuihin B-luokan järjestelmiin, joita koskevat turvallisuusvaatimukset ovat olleet hyvin yleisluonteisia ja joiden valvontaan on ollut huomattavan vähän resursseja. Eduskunnan käsiteltävänä on sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain (159/2007, jäljempänä asiakastietolaki) kokonaisuudistus (HE 212/2020), jossa ehdotetaan, että liittymisvelvoite Kanta-palveluihin laajentuu kaikkiin palvelunantajiin, joilla on käytettävissään asiakas- tai potilastietojärjestelmä. Kaikkien sosiaali-ja terveydenhuollon palvelunantajien käyttämät Kanta-palveluun liitettävät asiakas- ja potilastietojärjestelmät on niin sanottuun A-luokkaan kuuluvina sertifioitava. Jo nykyinen asiakastietolaki mahdollistaa tietoturvavaatimuksia koskevan THL:n määräyksen ulottamisen muihin kuin Kanta-palveluihin liitettäviin eli niin sanottuihin B-luokan järjestelmiin.

Julkisen sektorin tietoturvan tasoa selvitetään parhaillaan valtiovarainministeriön Haukka-ohjelmassa, joka perustuu julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelmaan vuosille 2020–2023[13]. Työn keskeisenä havaintona voidaan todeta, että digitaalisen turvallisuuden tilanne on kunnissa pääosin heikompi kuin valtiotasolla. Vastaava havainto tuli esille työryhmän järjestämissä kuulemisissa, joissa kiinnitettiin huomiota siihen, että esimerkiksi terveydenhuollon, energiahuollon ja vesihuolloin kriittisistä toiminnoista merkittävä osa on kuntien vastuulla.

Täsmennettävää on myös valtiotasolla. Valtiovarainministeriö on marraskuussa 2020 edellyttänyt osana Valtion tieto- ja viestintäkeskus Valtorin toiminnan kehittämistä, että Valtori käynnistää useita tietoturvan varmistamiseen ja kehittämiseen sekä hallinnollisiin prosesseihin kohdistuvia toimenpiteitä. Työryhmässä tunnistettiin tarve myös mahdollisille lainsäädäntömuutoksille. Työryhmässä esitettyjen asiantuntijanäkemysten mukaan Valtorille tulisi esimerkiksi säätää TORI-palveluihin nimenomaiset tietoturvavaatimukset ja Valtorin roolista henkilötietojen käsittelijänä ja rekisterinpitäjänä tulisi säätää laissa. Tähän liittyen valtiovarainministeriössä on valmisteilla selvitys turvallisuusverkkolain ja sen nojalla annetun asetuksen (valtioneuvoston asetus julkisen hallinnon turvallisuusverkkotoiminnasta, 1109/2015) mukaisten tietoturvallisuusvaatimusten sisällyttämisestä soveltuvin osin yhteisten tieto- ja viestintäteknisten palvelujen jär-

[13] Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelma 2020-2023 (Haukka): https://julkaisut.valtioneuvosto.fi/handle/10024/162191

jestämisestä annettuun lakiin (1226/2013, TORI-laki) tai asetukseen. Selvitys on tarkoitus toteuttaa vuoden 2021 aikana ja sen pohjalta valmistellaan mahdolliset säädösmuutosehdotukset vuonna 2022.

Huomiota kiinnitettiin myös julkisiin hankintoihin liittyvään tietoturva- ja tietosuojaosaamiseen. Esimerkiksi järjestelmähankintoja tehtäessä tietoturva ja tietosuoja tulisi ottaa huomioon jo hankintaprosessin alussa, sillä näin voidaan parhaiten varmistua siitä, että tietosuoja- ja tietoturvavaatimukset ovat sisäänrakennettuna erilaisiin prosesseihin ja järjestelmiin. Kilpailutus- ja hankintaprosesseissa tulisikin kiinnittää aktiivisemmin huomiota esimerkiksi eri toimijoiden tarjoamien palvelujen ja järjestelmien sertifioinnin tasoon. Työryhmä katsoi, että tietosuojaan ja tietoturvaan liittyvää hankintaosaamista olisi mahdollista kehittää esimerkiksi julkishallinnolle tukitoimintoja tarjoavan Hansel Oy:n kautta.

Suoraan sovellettavasta EU:n yleisestä tietosuoja-asetuksesta seuraa yksityiskohtaisia vaatimuksia, jotka koskevat henkilötietojen suojan ja tietoturvallisuuden osalta kaikkia rekisterinpitäjiä. Näillä on merkitystä laajemminkin tietojärjestelmien tietoturvallisuuden kannalta, koska useimmissa tietojärjestelmissä käsitellään samalla henkilötietoja. EU:n tietosuojalainsäädännön uudistamisen tarkoituksena on ollut, että henkilötietojen tietoturvallisuus taataan ensisijaisesti yleislaeilla. Erityislainsäädännön tarve on pystyttävä perustelemaan käsittelyyn liittyvillä riskeillä. Toisaalta on huomioitava myös muiden salassa pidettävien tietojen tietoturvallisuus.

Tietosuojan osalta henkilötietojen käsittelyä koskevan yleissääntelyn on arvioitu olevan pääosin ajan tasalla. EU:n yleisessä tietosuoja-asetuksessa säädetään muun muassa tietosuojariskien arvioinnista, sisäänrakennetusta tietosuoja velvoitteesta, henkilötietojen käsittelyn turvallisuudesta, tietoturvaloukkauksesta ilmoittamisesta ja valvonnasta. Yleissääntelyn lisäksi voimassa on sektorikohtaista erityissääntelyä, jota voidaan antaa tietosuoja-asetuksen mukaisen kansallisen liikkumavaran puitteissa.

Yleisen tietosuoja-asetuksen turvallisuutta koskeva sääntely on riskiperusteista. Sen lähtökohtana on, että rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava henkilötietojen käsittelyn riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet. Tietoturvaa koskevat vaatimukset suhteutetaan käsiteltävien tietojen laatuun ja laajuuteen. Tietosuojariskiä arvioitaessa on otettava huomioon muun muassa henkilötietojen luvaton luovuttaminen tai henkilötietoihin pääsy, mikä voi aiheuttaa etenkin fyysisiä, aineellisia ja aineettomia vahinkoja. Lainsäädännön lisäksi on erityisesti merkitystä sillä, millä tavalla rekisterinpitäjät määrittelevät henkilötietojen käsittelytavat ja toteuttavat käytännössä menettelylliset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi sekä sillä, miten henkilötietoja käsittelevä henkilöstö on omaksunut nämä toimenpiteet.

Yleisesti sovellettavaa tietosuojalainsäädäntöä täydentävästä sääntelystä tulisi lähtökohtaisesti pidättäytyä ja myös erityislainsäädännön tarvetta olisi arvioitava riskiperusteisesti (PeVL 14/2018 vp). Erityistä huomiota arvioinnissa on kiinnitettävä arkaluonteisiin henkilötietoihin sekä muihin tilanteisiin, joissa henkilötietoja on erityisesti suojattava niihin kohdistuvilta riskeiltä. Tietosuojalakia (1050/2018) valmisteltaessa eri sektoreiden erityislainsäädäntöä kartoitettiin ja todettiin, että Suomessa on voimassa useita satoja erityislakeja, jotka sisältävät henkilötietojen käsittelyä koskevaa sääntelyä. Osa ministeriöistä on myös toteuttanut henkilötietojen käsittelyä koskevia lainsäädännön uudistuksia.

Eri sektoreiden tietosuojan kypsyystasosta ei ole tehty samalaista kattavaa sektorikohtaista selvitystä kuin kyberturvallisuuden nykytilasta, mutta tarve tällaiselle selvitykselle on tunnistettu. Viranomaisvalvonnassa saatujen havaintojen perusteella myös tietosuojan osalta vahvasti säännellyt toimialat, kuten tele- ja finanssisektorit, ovat tietosuojatyön osalta valveutuneempia ja paremmin resursoituja kuin valtaosa muista sektoreista. Tämä näkyy sekä henkilötietojen suojaa koskevissa tietoturvaloukkausilmoituksissa että tietoisuudessa yleisen sääntelyn vaatimuksista ja niiden noudattamisessa.

4.2 Viranomaisten toimivalta

Riittävät viranomaistoimivaltuudet sisältävät sekä ennaltaehkäiseviä että jälkikäteisiä puuttumiskeinoja valvonnan kohteiden tietoturvassa ja tietosuojassa havaittuihin puutteisiin. Ennaltaehkäisevää puuttumista on sitovien viranomaismääräysten ja niiden noudattamisen valvonnan lisäksi esimerkiksi yleinen viranomaisen tarjoama ohjaus ja neuvonta. Jälkikäteisiä puuttumiskeinoja on esimerkiksi toimivalta huomauttaa lainvastaisista käytännöistä, määrätä toimijoita korjaamaan tietoturvassa tai tietosuojassa havaittuja puutteita tai jopa kieltää puutteellisesta suojattujen tietojen käsittely, sekä mahdollisuus määrätä sanktio tietoturvaan tai tietosuojaan liittyvistä rikkomuksista.

Työryhmä kiinnitti tehtävänsä mukaisesti huomiota erityisesti EU:n verkko- ja tietoturvadirektiivin (*jäljempänä NIS-direktiivi*) mukaisia velvoitteita valvoviin viranomaisiin ja niiden toimivaltuuksiin. Verkko- ja tietoturvadirektiivissä säädetään verkko- ja tietojärjestelmien turvallisuuden varmistamisesta. Direktiivi tuli voimaan toukokuussa 2018[14]. Direktiivin keskeisin sisältö on, että direktiivin soveltamisalan piiriin kuuluvat toimijat

[14] Euroopan parlamentin ja neuvoston direktiivi toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa, (EU) 2016/1148.

ovat velvollisia huolehtimaan käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta ja niiden on ilmoitettava valvovalle viranomaiselle tietoverkkoihin tai tietojärjestelmiin kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä häiriöstä.

Direktiivi on Suomessa pantu täytäntöön eri sektoreita koskevaan lainsäädäntöön tehdyillä muutoksilla. Direktiivin osittain tai kokonaan kattamat toimialat ovat energia, liikenne, pankkiala, finanssialan infrastruktuurit, terveydenhuoltoala, juomaveden toimittaminen ja jakelu, digitaalinen infrastruktuuri ja digitaaliset palvelut. Toimialaa valvovalla viranomaisella on oikeus velvoittaa toimija tiedottamaan häiriöstä tai tiedottaa asiasta itse sekä ilmoittaa tarvittaessa häiriöstä Liikenne- ja viestintävirastolle tai tarvittaessa muille asiaan liittyville Euroopan Unionin jäsenvaltioille.

Sääntelyä valvovien sektoriviranomaisten toimivalta velvoittaa valvottavia ryhtymään toimenpiteisiin havaittujen tietoturvapuutteiden korjaamiseksi vaihtelee sektorikohtaisesti. NIS-direktiivin toimeenpanossa viranomaisille ei annettu uusia nimenomaisia toimivaltuuksia, vaan viranomaisten toimivalta pohjautuu kyseisten viranomaisten muuhun toimivaltasääntelyyn. Aiemmassa kyberturvallisuutta koskevassa selvitystyössä toimivaltuuksia on näiltä osin pidetty jossain määrin epäselvinä, koska sääntelystä ei ole kaikissa tapauksissa yksiselitteisesti pääteltävissä, kuinka pitkälle meneviin toimenpiteisiin viranomainen voi tietoturvan varmistamiseksi ryhtyä. [15]

Työryhmän saaman selvityksen perusteella NIS-viranomaisten toimivaltuuksissa ei sinänsä tunnistettu merkittäviä puutteita. Valvovilla viranomaisilla on lähtökohtaisesti eri asteisia keinoja puuttua sekä etukäteen että jälkikäteen tietoturvassa tai tietosuojassa havaittuihin puutteisiin. Toimivaltuuksien sijasta ongelmana vaikuttaa olevan se, ettei viranomaisilla ole valvontaan ja toimivaltuuksien hyödyntämiseen riittäviä tosiasiallisia resursseja, eikä konkreettisia tietoturva- tai tietosuojavaatimuksia, joita valvoa.

Viranomaisten resursseihin ja toimintakykyyn vaikuttavana tekijänä tunnistettiin myös tietoturva- ja tietosuojaosaajien puute työmarkkinoilla. Tämä vaikeuttaa viranomaisten rekrytointeja, kun harvoista osaajista kilpaillaan yksityisen sektorin ja muiden viranomaisten kanssa. Sama ongelma on tunnistettu yrityspuolella ja kyberturvallisuusalalla laajemminkin. Osaamiskysymykseen haetaan pitkän aikavälin ratkaisua Suo-

[15] Viranomaisten toimivaltuudet häiriötilanteissa, oikeusministeriön julkaisuja, selvityksiä ja ohjeita 2019:18 https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161604/OM_2019_18_Viranomaisten_toimivaltuudet_hairiotilanteissa.pdf?sequence=1&isAllowed=y

men kyberturvallisuusstrategian (2019) toimeenpano-ohjelmassa, joka valmistuu keväällä 2021. Tästä huolimatta työryhmä tunnisti tarpeen myös lyhyen aikavälin toimille, vaikkakin nopeiden ratkaisujen löytäminen koettiin haastavaksi.

4.3 Tietosuojavaltuutetun tehtävät

Tietosuojavaltuutetun toimisto on itsenäinen ja riippumaton viranomainen, joka valvoo tietosuojalainsäädännön ja muiden henkilötietojen käsittelyä koskevien lakien noudattamista. Tietosuojavaltuutetun toimisto edistää tietoisuutta henkilötietojen käsittelyyn liittyvistä oikeuksista ja velvollisuuksista, määrää tarvittaessa hallinnollisia seuraamuksia EU:n yleisen tietosuoja-asetuksen rikkomisesta, tekee selvityksiä ja tarkastuksia sekä antaa lausuntoja lainsäädännöllisistä ja hallinnollisista uudistuksista. Tietosuojavaltuutettu tekee yhteistyötä muiden valtioiden valvontaviranomaisten kanssa ja edustaa Suomea Euroopan tietosuojaneuvostossa.

Tietosuojavaltuutetulla on tietosuojasäännösten noudattamisen valvonnan yleistoimivaltaisena viranomaisena laajat tutkintatoimivaltuudet ja korjaavat toimivaltuudet. Selkeimmät viranomaistoiminnan kehittämiskohteet liittyvät tältä osin resursseihin, jotka mahdollistavat lainsäädännön vaatimusten tosiasiallisen täytäntöönpanon valvonnan ja toteuttamisen. Tietosuojavaltuutetun toimiston arvion mukaan noin 40 prosenttia sille käsiteltäväksi tulevista tapauksista on tällä hetkellä ilmoituksia henkilötietojen tietoturvaloukkauksesta. Tästä syystä erityisesti tietoturvaa koskevaan asiantuntemukseen tarvittaisiin lisää resursseja. Henkilötietojen tietoturvaloukkauksesta täytyy yleisen tietosuoja-asetuksen mukaan ilmoittaa tietosuojavaltuutetun toimistolle, jos loukkauksesta voi aiheutua riski luonnollisten henkilöiden oikeuksille ja vapauksille. Kriittisten toimialojen osalta tietoturvaloukkauksesta voi joutua tekemään kaksi erillistä ilmoitusta; tietosuojavaltuutetun toimistoon sekä sektorikohtaiselle valvontaviranomaiselle.

Tietosuoja-asetuksen myötä tietosuojavaltuutetun toimistolla on mahdollisuus käyttää eriasteisia korjaavia toimivaltuuksia. Toimisto on antanut rekisterinpitäjille määräyksiä, jotka kohdistuivat rekisteröidyn oikeuksien toteuttamiseen ja käsittelytoimien muuttamiseen sekä tietoturvaloukkauksesta ilmoittamiseen rekisteröidyille. Lisäksi on annettu huomautuksia puutteista henkilötietojen käsittelyssä. Hallinnollisten seuraamusmaksujen määräämisestä vastaa seuraamuskollegio, jonka muodostavat tietosuojavaltuutettu ja kaksi apulaistietosuojavaltuutettua. Vuoden 2020 aikana hallinnollisia seuraamusmaksuja on määrätty viidessä tapauksessa.

Tietosuojavaltuutettu antaa yleistä ohjausta ja neuvontaa tietosuojasta sekä henkilötietojen käsittelystä. Vaikka neuvonta on yleisluontoista, eikä siinä voida antaa yksityiskohtaisia tai sitovia kannanottoja yksittäistapauksiin, neuvontapalvelu on koettu hyvin tarpeelliseksi niin rekisteröityjen kuin rekisterinpitäjien keskuudessa. Toimisto pyrkii antamaan tukea organisaatioissa tehtävään tietosuojatyöhön kokoamalla yhteen uusia päätöksiä, ohjeita ja muita ajankohtaisia tietosuoja-asioita.

Toimistoon tulevien yhteydenottojen perusteella on havaittavissa, että tietosuojaosaamisen taso on rekisterinpitäjinä toimivissa organisaatioissa vaihtelevaa. Tarvetta neuvonnalle ja opastukselle tietosuoja-asioissa on yhä enemmän.

4.4 Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen tehtävät

Liikenne- ja viestintäviraston Kyberturvallisuuskeskus palvelee koko suomalaista yhteiskuntaa luottamuksen kasvattamisessa ja tietoturvallisuuden edistämisessä. Kyberturvallisuuskeskuksen toiminnassa yhdistyvät erilaiset tietojärjestelmien ja -liikenteen turvallisuusviranomaistehtävät ja tietoturvayhteyspisteenä toimiminen. Toiminnan järjestäminen tällä tavoin on mahdollistanut merkittäviä synergiaetuja, joiden ansiosta Kyberturvallisuuskeskus nauttii suurta arvostusta myös kansainvälisesti.

Kyberturvallisuuskeskuksen yhtenä pääasiallisista tehtävistä on valvoa sähköisen viestinnän palveluista annetun lain tietosuojaan ja tietoturvallisuuteen liittyvien velvoitteiden noudattamista. Laissa edellytetään, että teleyritysten on huolehdittava palvelujensa tietoturvasta. Virastolla on lain mukaan laajat toimivaltuudet antaa myös tarkempia määräyksiä siitä, miten teleyritysten on varmistettava palvelujensa tietoturvallisuus ja ilmoittaa häiriöistä.

Sähköisen viestinnän palveluista annetun lain mukaan teleyrityksen on ilmoitettava virastolle, jos sen palveluun kohdistuu tai sitä uhkaa merkittävä tietoturvaloukkaus taikka muu tapahtuma, joka estää viestintäpalvelun toimivuuden tai häiritsee sitä olennaisesti. Laissa säädetään tarkasti myös siitä, mitä toimenpiteitä teleyritykset voivat tehdä tietoturvan varmistamiseksi. Tarvittaessa laki mahdollistaa myös sen, että viestintäverkko, viestintäpalvelu tai laite voidaan kytkeä pois yleisestä viestintäverkosta, jos se aiheuttaa merkittävää haittaa tai häiriötä esimerkiksi muiden viestintäpalvelujen toimintaan. Näistä toimenpiteistä voi päättää lain mukaan Liikenne- ja viestintävirasto. Säädös on kansainvälisesti arvioiden uniikki.

Viraston Kyberturvallisuuskeskuksen tehtäviä on viime vuosina laajennettu koskemaan myös muuta kuin teleyritysten ja viestinnän välittäjien tietoturvallisuutta. Kyberturvallisuuskeskuksen tietoturvaneuvonta on muun muassa valtionhallinnolle sekä huoltovarmuuskriittisille toimijoille tarkoitettu palvelu, jonka tarkoituksena on varmistaa organisaatioiden tietoisuus kybertoimintaympäristön uhkista sekä tukea asiakkaitansa niiden toiminnan ja järjestelmien turvallisuuden varmistamisessa. Liikenne- ja viestintäviraston tehtäviin kuuluu myös viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen arviointi, jos siltä pyydetään niiden arviointia.

Kyberturvallisuuskeskus valvoo myös vahvaa sähköistä tunnistamista koskevan lainsäädännön noudattamista. Vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetussa laissa (617/2009, jäljempänä tunnistamislaki) tunnistuspalvelun tarjoaja on velvoitettu säännöllisesti teettämään palvelulleen ulkoisen arvioinnin siitä, täyttääkö palvelu esimerkiksi tietoturvaa ja tietosuojaa koskevat vaatimukset. Kyberturvallisuuskeskus valvoo vaatimusten noudattamista, antaa tunnistamislakia tarkentavia määräyksiä ja ylläpitää julkista rekisteriä vaatimukset täyttävistä tunnistuspalvelun tarjoajista.

Varsinaisten valvontatehtäviensä lisäksi Kyberturvallisuuskeskus tukee suoraan yhteiskunnan eri sektoreiden toimijoita. Eri toimialojen riittävä tukeminen vaatii Kyberturvallisuuskeskukselta riittävää ymmärrystä niiden toiminnasta ja toimintaympäristöstä. Toimintaa on resursoitava riittävästi, jotta mahdollistetaan tilannekuvan jatkuva tuottaminen ja analysointi kunkin toimialan tarpeet huomioiden. Nykyresursoinnilla Kyberturvallisuuskeskus ei pysty tarjoamaan riittäviä palveluita kaikille yhteiskunnan kriittisille toimialoille. Resursseilla saavutettavat hyödyt ovat merkittäviä, koska Kyberturvallisuuskeskuksen tietojen avulla koko yhteiskunta pystyy varautumaan ja reagoimaan tietoturvauhkiin ja -loukkauksiin nykyistä merkittävästi paremmin.

Kyberturvallisuuskeskus myös selvittää ja ennaltaehkäisee tietoturvaloukkauksia, ylläpitää ja jakaa kansallisen kyberturvallisuuden tilannekuvaa sekä julkaisee tietoturvallisuuden ohjeita ja oppaita tukemaan organisaatioiden tietoturvallisuuden kehittämistä ja yksittäisten henkilöiden tietoturvallista asiointia internetissä ja sähköisissä palveluissa. Näitä palveluja tarjotaan kaikille toimialoille ja kaikille kansalaisille. Toiminta on erityisen riippuvaista Kyberturvallisuuskeskukselle vapaaehtoisesti ja luottamuksellisesti annettavista ilmoituksista.

Suomen kyky tunnistaa tietoturvauhkia ja varoittaa niistä pohjautuu laaja-alaiseen ja tehokkaasti toimivaan kansalliseen ja kansainväliseen kumppaniverkostoon, jota on rakennettu pitkäjänteisesti ja leimallisesti yhden organisaation sisällä jo 16 vuotta. Yhteistyö perustuu Liikenne- ja viestintävirastoa ja sen henkilöstöä kohtaan tunnettuun luottamukseen. Verkostoista saatu tieto ajankohtaisista uhkista ja ilmiöistä on välttämätöntä kansallisen kyberturvallisuuden varmistamisessa.

Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen nauttima luottamus erityisesti yksityisen sektorin parissa perustuu merkittävästi siihen, että se koetaan neutraaliksi toimijaksi suomalaisessa yhteiskunnassa. Se ei ole sotilaallinen organisaatio, eikä tiedusteluorganisaatio, eikä toimi tällaisesta toiminnasta vastaavien ministeriöiden alla. Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen erityinen vahvuus on, että se on nimenomaan siviiliorganisaatio, jonka ensisijainen asiakaskunta muodostuu elinkeinoelämästä ja yrityksistä. Tämä on rakentanut Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen koko yhteiskuntaa palvelevan toiminnan uskottavuutta myös kansainvälisesti, niin EU:ssa kuin sen ulkopuolella.

Suomessa Kyberturvallisuuskeskuksen ja elinkeinoelämän yhteistyö on kansainvälisestikin vertailtuna poikkeuksellisen toimivaa.

4.5 Viranomaisyhteistyö

Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksessa toimii sektorikohtaisten valvontaviranomaisten edustajista koottu yhteistyöryhmä, joka vaihtaa tietoa tietoturvauhista ja -loukkauksista, huolehtii lainsäädännön ajantasaisuudesta, neuvoo ja auttaa huoltovarmuuskriittisiä toimijoita riskien osalta sekä valvoo tietoturvavelvoitteiden toteutumista.[16] Yhteistyöryhmän jäsenet neuvovat, auttavat ja tiedottavat omilla toimialoillaan huoltovarmuuskriittisiä toimijoita riskinhallinnan osalta sekä valvovat lakisääteisten tietoturvavelvoitteiden toteutumista. Ryhmän jäsenet osallistuvat aktiivisesti myös EU:n NIS Cooperation Groupin alla toimiviin toimialakohtaisiin alatyöryhmiin ja välittävät näistä tietoa kansalliselle yhteistyöryhmälle. Kansallinen yhteistyöryhmä on toiminut vuodesta 2018 ja kokoontuu keskimäärin neljä kertaa vuodessa. Yhteistyöryhmän toiminta perustuu hallinnon yleislainsäädäntöön ja NIS-direktiivin sääntelyyn.

Lainsäädännössä viranomaisten välinen yhteistyö perustuu erityisesti virka-apuun sekä tiedonvaihtoa koskevaan sääntelyyn. Esimerkiksi Liikenne- ja viestintävirastolla on salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus luovuttaa laissa säädettyjen tehtäviensä hoitamisen yhteydessä saamansa tai laatimansa asiakirja sekä ilmaista salassa pidettävä tieto Energiavirastolle, Finanssivalvonnalle, Valviralle, tietosuojavaltuutetun toimistolle sekä elinkeino-, liikenne- ja ympäristökeskukselle, jos se on näille säädettyjen tietoturvallisuuteen liittyvien tehtävien hoitamiseksi välttämätöntä. Vastaavasti esimerkiksi Energiavirastolla on oikeus tehdä valvontayhteistyötä Liikenne- ja viestintäviraston kanssa ja luovuttaa

[16] https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/nis-koordinointi-ja-viranomaisyhteistyo

salassa pidettäviä tietoja Liikenne- ja viestintävirastolle. Finanssivalvonnalle on säädetty velvollisuus tehdä yhteistyötä verkko- ja tietoturvadirektiivin mukaisten tehtävien hoitamisessa Liikenne- ja viestintäviraston kanssa sekä oikeus tätä tarkoitusta varten luovuttaa salassapitosäännösten estämättä tietoja Liikenne- ja viestintävirastolle. Myös vesihuoltolaissa (119/2001) säädetään oikeudesta antaa tietoja Liikenne- ja viestintävirastolle silloin kun tämä on välttämätöntä tietoturvallisuuteen liittyvien tehtävien hoitamiseksi.

Edellä kuvattu sääntely ilmentää periaatetta, jonka mukaan tietoturvallisuudesta huolehtivien viranomaisten on oltava yhteistyössä, silloin kun niiden tehtävät sitä edellyttävät. Myös NIS-direktiivi edellyttää, että tietoturvallisuudesta vastaavat viranomaiset tekevät tarvittavaa yhteistyötä direktiivin mukaisten velvoitteiden valvomiseksi. NIS-direktiivin ulkopuolella viranomaisyhteistyö ilmenee esimerkiksi rikosten selvittämistä koskevassa yhteistyössä. Psykoterapiakeskus Vastaamon tapauksessa toimivaltaisia viranomaisia olivat poliisin lisäksi ainakin Valvira, aluehallintovirastot, tietosuojavaltuutettu ja Liikenne- ja viestintävirasto.

Viranomaisten välisestä yhteistyöstä on säädettävä lailla aina, jos kyse on virka-avusta, jolla puututaan yksittäisen oikeussubjektin perustuslailla suojattuihin oikeuksiin tai kyse on perustuslaissa tarkoitetusta julkisen vallan käytöstä. Myös viranomaisyhteistyöhön liittyvä tietojen vaihto saattaa edellyttää laintasoista sääntelyä. Jos viranomaisyhteistyötä varten perustetaan päätösvaltaa käyttävä yhteistyöelin, on tästäkin säädettävä laissa. Lisäksi viranomaisyhteistyöstä voi olla tarkoituksenmukaista säätää, vaikka se ei olisi oikeudellisesti välttämätöntä. Erityiset lain tasoiset säännökset yhteistyöstä korostavat yhteistyön merkitystä siihen osallistuville viranomaisille ja saattavat ohjata sen järjestäytyneisiin muotoihin.

Työryhmän saaman selvityksen perusteella Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen asiantuntemuksen hyödyntämistä eri sektoreiden tietoturvavalvonnassa pidetään erittäin tärkeänä. Tästä syystä Kyberturvallisuuskeskuksen roolia sektorikohtaisia viranomaisia tukevana tietoturvaviranomaisena tulisi työryhmän näkemyksen mukaan entisestään vahvistaa. Lisäksi työryhmän näkemyksen mukaan on tärkeää, että vastuu sektorikohtaisesta valvonnasta säilyy sektoriviranomaisilla, joilla on paras asiantuntemus oman sektorinsa erityispiirteistä. Viranomaisten väliselle yhteistoiminnalle olisi mahdollista luoda nykyistä vakiintuneemmat rakenteet lainsäädännössä.

4.6 Tietoturvaan ja tietosuojaan liittyvien rikosten selvittäminen

Poliisi vastaa tietosuojaan ja tietoturvaan liittyvien rikosten ennalta estämisestä, paljastamisesta, selvittämisestä ja syyteharkintaan saattamisesta. Tietosuojaan ja tietoturvaan kytkeytyviä rikosnimikkeitä ovat esimerkiksi useimmat rikoslain 38 luvun tieto- ja viestintärikokset, kuten tietosuojarikos (RL 38:9) tai tietomurto (RL 38:8). Suomessa Keskusrikospoliisi ja sen yhteydessä toimiva Poliisin kyberrikostorjuntakeskus vastaa vakavimpien tietoverkkorikosten selvittämisestä, kuten Vastaamo-tapaukseen liittyvistä rikosepäilyistä. Keskusrikospoliisin lisäksi tietoverkkorikoksia tutkitaan poliisilaitoksilla aluevastuuperiaatteen mukaisesti.

Työryhmän saaman selvityksen perusteella tietoverkoissa tapahtuvien rikosten ympärillä suurimmat poliisitoiminnan haasteet liittyvät nykyisin erityisesti käytettävissä olevien tiedonhankintakeinojen ja tiedon säilyvyyden rajallisuuteen sekä rikosten ilmoittamiseen ylipäänsä. Epäiltyjen rikosten korkea tai myöhäinen ilmoittamiskynnys pahentaa myös tiedon säilyvyyteen ja käytettäviin tiedonhankintakeinoihin liittyviä ongelmia. Poliisin kybertoimivaltuuksien kehittämistä tarkastellaan oikeusministeriön vuonna 2021 asettamassa esitutkinta- ja pakkokeinolain uudistamistarpeita käsittelevässä työryhmässä. Lisäksi tietoverkkorikollisuuden torjuntaa on käsitelty valtioneuvoston vuonna 2017 valmistuneessa selvityksessä[17].

Poliisitoiminnan yhteydessä työryhmässä keskusteltiin yleisen tietosuoja-asetuksen voimaatulon vuoksi uudistetusta tietosuojarikosta koskevasta sääntelystä. Uudistuksessa osa aiemman lainsäädännön mukaisista henkilötietorikoksena kriminalisoiduista teoista siirtyi rikosoikeudellisesta sääntelystä hallinnollisten sanktiomenettelyiden piiriin. Uudistuksen jälkeen esimerkiksi rekisterinpitäjä ja henkilötietojen käsittelijä eivät voi syyllistyä rikoslain mukaiseen tietosuojarikokseen, vaan toimintaa arvioidaan vain hallinnollisten seuraamusten kautta. Tarkoituksena on kuitenkin ollut yritysten osalta, että niihin sovelletaan ensisijaisesti hallinnollista seuraamusjärjestelmää. Tämä perustuu suoraan tietosuoja-asetukseen. Hallinnollisten sakkojen on katsottu olevan niin ankaria, ettei vakavienkaan tietosuoja-asetuksen rikkomisten saattaminen rikosoikeudellisen järjestelmän piiriin ole välttämätöntä eikä tarpeellista.[18]

[17] https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79866/Tietoverkkotorjunta-selvitys_VERKKO_.pdf?sequence=1
[18] HaVM 13/2018 vp

4.7 Digitaalinen toimintaympäristö osana kansallista turvallisuutta

Perinteisen rikollisuuden ohella digitaaliseen toimintaympäristöön kohdistuu myös kansallista turvallisuutta vaarantavia uhkia. Tällaiset uhat voivat ilmetä esimerkiksi vieraan valtion tiedustelutoimintana tai suuren ihmismäärän henkeä ja terveyttä taikka yhteiskunnan elintärkeitä toimintoja uhkaavana toimintana. Suojelupoliisin tehtävänä on suojata kansallista turvallisuutta, mihin kuuluu myös digitaalisen toimintaympäristön suojaaminen. Perinteisesti kansallisen turvallisuuden yhteydessä korostuu myös maanpuolustuksen merkitys. Muuttuneessa digitaalisessa toimintaympäristössä myös kyberpuolustuksella on aiempaa tärkeämpi rooli.

Kun tietoturvalle tai -suojalle vahinkoa aiheuttava toiminta vaarantaa myös kansallista turvallisuutta, ei riitä, että tekninen poikkeama selvitetään. Vahingon rajaamiseksi on selvitettävä myös sen syy ja taustatekijät. Suojelupoliisi tuottaa ennakoivaa ja merkityksellistä tietoa kansallista turvallisuutta vaarantavasta toiminnasta omilla toimivaltuuksillaan. Tietoa ja tilannekuvaa tuotetaan valtiojohdon lisäksi viranomaisille, kuten Kyberturvallisuuskeskukselle. Tämän lisäksi Suojelupoliisi torjuu kansallisen turvallisuuden uhkia ilmoittamalla havaitsemistaan uhkista kriittistä infrastruktuuria ylläpitäville organisaatioille sekä avustamalla näitä estämään vahinkoja omalla toiminnallaan.

4.8 Kansainvälinen yhteistyö

Kansainvälinen yhteistyö on tietoturvallisuutta ja tietosuojaa koskevalle turvalliselle toimintaympäristölle elintärkeää. Euroopan unioni on Suomelle merkittävin viitekehys kansainväliselle yhteistyölle eri valtioiden ja toimijoiden kanssa. EU:n sääntely luo keskeisen alustan Suomen kansalliselle tietoturvaa ja tietosuojaa koskevalle politiikalle. EU:n yhteisen tietoturvaa ja tietosuojaa koskevan sääntelyn johdosta jäsenvaltiot toimivat tiiviissä yhteistyössä ja vaihtavat esimerkiksi aktiivisesti tietoturvaa ja rajat ylittäviä henkilötietojen käsittelykäytäntöjä koskevia tietoja. Tätä yhteistyötä on tärkeää tiivistää jatkossa yhteisen tilannekuvan ylläpitämiseksi ja kehittämiseksi.

Rajat ylittävän yhteistyön ja tiedonvaihdon merkitys korostuu, koska mahdolliset tietoturvaa tai tietosuojaa koskevat loukkaukset eivät tunne fyysisiä valtion rajoja. Tietoturvaloukkauksia ja -häiriöitä koskevissa tapauksissa korostuu rajat ylittävän tiedonvaihdon, varoittamisen ja parhaiden käytänteiden jakamisen merkitys. Tämän johdosta Suomi on tiiviisti mukana muun muassa EU-maiden CSIRT-verkostossa, EGC-luottamusverkostossa, Pohjoismaiden valtiollisten CERT-toimijoiden verkostossa ja lainvalvontaviranomaisten kyberturvallisuutta koskevassa yhteistyöverkostossa. Verkostojen

kautta Suomella on mahdollisuus saada ja jakaa tietoja esimerkiksi ajankohtaisista tietojärjestelmiä koskevista haavoittuvuuksista. Mainittujen verkostojen lisäksi Euroopan kyberturvallisuusvirasto (ENISA) on jo toiminut pitkään yhteistyöelimenä jäsenvaltioiden välillä ja pyrkinyt toiminnassaan kehittämään koko EU:n kyberturvallisuuden tasoa.

Tietosuoja-asioissa yhteistyötä tehdään EU-tasolla erityisesti Euroopan tietosuojaneuvostossa (EDPB). Euroopan tietosuojaneuvosto on riippumaton EU:n elin, joka koostuu EU:n jäsenmaiden kansallisista tietosuojaviranomaisista ja Euroopan tietosuojavaltuutetun edustajista. Myös ETA-maat Islanti, Norja ja Liechtenstein ovat tietosuojaneuvoston jäseniä. Euroopan tietosuojaneuvosto vastaa EU:n yleisen tietosuoja-asetuksen ja poliisi- ja rikosoikeusviranomaisia koskevan tietosuojadirektiivin yhdenmukaisesta soveltamisesta. Tietosuojaneuvosto on muun muassa julkaissut ohjeistuksen henkilötietojen tietoturvaloukkauksista ilmoittamisesta[19]. Tietosuojaan liittyvää kansainvälistä yhteistyötä tehdään myös Euroopan neuvoston ja OECD:n puitteissa.

4.9 Kybertoimintaympäristön muutokset kansainvälisestä näkökulmasta

Tieto- ja kyberturvallisuuden ja tietosuojan kehittäminen edellyttävät myös ymmärrystä kybertoimintaympäristön muutoksista kansallisella ja kansainvälisellä tasolla. Kriittisillä toimialoilla tämä edellyttää, että eri toimijat jakavat ja ylläpitävät kybertoimintaympäristön tilannekuvaa koordinoidusti ja kohdennetuin tilannekatsauksin. Toimintaympäristön osalta on tärkeää huomata, että pahantahtoista kybertoimintaa ja -loukkauksia kohdistuu yksityisten yritysten lisäksi valtion instituutioihin. Tekijänä voivat tällöin olla yksityisen toimijan lisäksi valtiotoimija tai sen käyttämä bulvaani. Valtiolähtöisissä loukkauksissa korostuvat haavoittuvuuksien havaitsemisen ja korjaamisen ohella yhteisesti koordinoidut poliittiset toimet ja signaloinnit. Suomi on osallistunut aktiivisesti yhteisen EU-politiikan ja välineiden kehittämiseen ja hyödyntämiseen, joiden avulla edistetään vastuullista valtiokäyttäytymistä kybertoimintaympäristössä. Tällaisia välineitä pahantahtoisen kybertoiminnan torjuntaan EU:n tasolla ovat olleet esimerkiksi kyberdiplomatian työkalupakki ja kyberpakotteet.

Tieto- ja kyberturvallisuuteen sekä tietosuojaan liittyviä lakisääteisiä velvoitteita täydentämään on tarpeen luoda yhteinen tilannekuva sekä ymmärrys kybertoimintaym-

[19] https://tietosuoja.fi/documents/6927448/8316711/Henkil%C3%B6tietojen+tietoturvaloukkauksesta+ilmoittaminen+en.pdf/9d539a27-8ffa-4ac9-89bc-c4fa0e3073c7/Henkil%C3%B6tietojen+tietoturvaloukkauksesta+ilmoittaminen+en.pdf

päristön muutoksista. Edellä mainittuihin tekijöihin voidaan kansallisen ja kansainvälisen sääntelyn ohella vaikuttaa toimialojen toimintakulttuureja kehittämällä, vapaaehtoisella yhteistyöllä viranomaisten ja palveluiden tarjoajien välillä sekä kehittämällä sekä hyödyntämällä EU-politiikkoja ja välineitä. Lisäksi on tärkeää osallistua aktiivisena osapuolena kansainväliseen yhteistyöhön, jossa edellytetään vastuullista valtiokäyttäytymistä kybertoimintaympäristössä. On selvää, että hallinnonalojen välistä yhteistyötä EU- ja kansainvälisen tason vaikuttamisen tehostamiseksi kehitetään jatkuvasti. Kansainvälisen kybertoimintaympäristön kehitystä koskevaa tilannekuvaa jaetaan hallinnonalojen välillä ja tämä huomioidaan myös Suomen kansallisen toimintaympäristön arvioinnissa. Näitä laajempia kybertoimintaympäristöön liittyviä kysymyksiä ja kansainvälistä yhteistyötä kyberuhkien torjunnassa ei kuitenkaan käsitellä tämän raportin suosituksissa, vaan niihin liittyvää kehitystyötä tehdään jatkuvasti muun muassa kansallisen kyberturvallisuusstrategian toimeenpanon puitteissa.

4.10 Auditoinnit ja sertifioinnit

Työryhmän työssä on tunnistettu, että kriittisten toimialojen tietoturvan ja tietosuojan tasoa voidaan parantaa prosessien ja toimintojen auditoinnilla ja sertifioinnilla. Auditointeja voidaan toteuttaa usealla eri tasolla ja auditoinnissa käytettävät kriteerit sekä vaatimukset voidaan mukauttaa tarkastettavan kohteen perusteella. Eri auditointimallien erot perustuvat muun muassa siihen, toteutetaanko auditointi ennalta määrättyjen kriteerien pohjalta vai kiinnitetäänkö huomiota enemmän käytettäviin tarkastusmenetelmiin ja vaatimuksiin. Auditoinnin kohteena olevat toimijat saavat joka tapauksessa arvokasta tietoa toteutettavasta tarkastuksesta. Auditoinnin suorittamisen jälkeen kohteella on tarvittava tieto tarkastuksen kohteena olleen prosessin, toiminnon tai tietojärjestelmän mahdollisista puutteista, jotka edellyttävät korjaustoimenpiteitä. Samalla auditointiraportit voivat tarjota viranomaisille työkalun eri toimijoiden valvontaan. Raporttien avulla voidaan tarkastella sitä, täyttääkö toiminta ennalta annetut ja asetetut vaatimukset. Toteutetusta auditoinnista riippuen organisaatiolla on mahdollisuus hakea toiminnoilleen, prosesseilleen tai tietojärjestelmilleen sertifikaattia.

Auditointitoimintaa voidaan pitää esiasteena tietoturvaa tai tietosuojaa koskevan sertifikaatin hankkimiseksi. Toimijan hakema sertifikaatti toimii todistuksena sekä sovellettavien standardien että auditoinnissa käytettyjen kriteerien ja vaatimusten täyttämisestä. Yksi tapa parantaa kriittisten toimialojen tietoturvaa ja tietosuojaa on velvoittaa toimijoita hankkimaan sertifikaatteja (esimerkiksi ISO sertfikaatit) toiminnalleen tai sen tietyille osa-alueille. Työryhmässä on arvioitu, että myös tietosuojaa koskevien arviointien osalta erityisesti yleisen tietosuoja-asetuksen mukaisten tietosuojan sertifiointimekanismien käyttöä olisi mahdollista lisätä.

Yksi tyypillisimmistä tietoturvaa koskevista todistuksista on ISO 27001 -sertifikaatti, joka todistaa, että arvioidun organisaation tietoturvan hallintajärjestelmä on arvioitu parhaiden käytäntöjen mukaisesti ja että se täyttää ISO 27001 -standardin asettamat vaatimukset. Standardi keskittyy erityisesti siihen, miten tietoturva on hallinnollisesti järjestetty organisaatiossa ja sen toiminnassa, eli onko esimerkiksi kriittiset tietojärjestelmät ja niihin kohdistuvat riskit tunnistettu. Standardin vaatimukset ovat yleisluonteisia, jonka vuoksi ne soveltuvat eri toimijoille. ISO 27001- ja 27002-standardeihin on luotu myös täydentävät tietosuojan hallintaa koskevat vaatimukset ja ohjeet[20].

Suomessa hyödynnetään muun muassa kansallista turvallisuusauditointikriteeristöä Katakria. Katakri-kriteeristö itsessään ei aseta tietoturvallisuudelle ehdottomia vaatimuksia, vaan siihen kootut vaatimukset perustuvat voimassa olevaan lainsäädäntöön ja Suomea sitoviin kansainvälisiin tietoturvavelvoitteisiin. Vaikka Katakri-kriteeristöä käytetään ensisijaisesti turvallisuusluokitellun tiedon käsittelyn arviointien yhteydessä, kriteeristöä voidaan hyödyntää myös yksityisen ja julkisen sektorin muussa turvallisuustyössä ja sen kehittämisessä. Lisäksi Kyberturvallisuuskeskus on laatinut pilvipalveluiden turvallisuuden arviointikriteeristön (PiTuKri), jonka tavoitteena on edistää viranomaisten salassa pidettävän tiedon turvallisuutta tilanteissa, joissa tietoja käsitellään pilvipalveluissa[21].

Tällä hetkellä vain osa yhteiskunnan kriittisen toimialan toimijoista tilaa auditointipalveluja tai omaa tietoturvaa koskevia sertifikaatteja. Erityisesti kuntasektorilla, logistiikassa, elintarvikehuollossa ja teollisuustuotannossa auditointeja tehdään työryhmän saaman selvityksen mukaan vähän. Myös terveydenhuollon B-luokan järjestelmien auditointi on vähäistä. Auditointien vähäinen käyttöaste osalla toimialoista on vaikuttanut siihen, että prosessien, toimintojen ja tietojärjestelmien tietoturvallisuuden taso voi vaihdella merkittävästi eri toimialoilla. Prosessien ja toimintojen auditoinnin pitäisi olla luonnollinen osa kriittisten toimialojen riskinhallintaa.

Auditointien määrän lisääminen edellyttää sääntelyn tarkastelun ohella toimintakulttuurin muutosta niin julkisella kuin yksityisellä sektorilla. Kaikki auditointitoiminta edellyttää toiminnan kohteelta rahallisia panostuksia. Tämän osalta tulee kuitenkin huomioida, että auditoinnin yksityiskohtaisuus ja tarkistettavan kohteen laajuus vaikuttavat suoraan kyseessä olevan auditoinnin kustannuksiin. Näin ollen yksittäisten, kriittisiksi

[20] ISO/IEC 27701:2019 Security techniques -- Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management -- Requirements and guidelines
[21] https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf

tunnistettujen, tietojärjestelmien tai prosessien auditoinnit ovat kokoluokaltaan moninkertaisesti pienempiä panostuksia kuin suuryrityksen tai kunnan digitaalisen palveluympäristön laajamittainen auditointi.

Tietoturvaa koskevia auditointeja tekevät Suomessa Liikenne- ja viestintäviraston Kyberturvallisuuskeskus, erikseen hyväksytyt arviointilaitokset (mm. KPMG ja Nixu), eräät tietoturvayritykset ja organisaatioiden sisäiset riippumattomat toimijat. Korkeimmasta tarkastustasosta vastaavat Kyberturvallisuuskeskus ja erikseen hyväksytyt arviointilaitokset, joita on Suomessa tällä hetkellä vain muutamia. Toimijoiden omavalvonta ja sisäiset riippumattomat auditoinnit ja tarkastukset eivät vastaa ulkopuolisen arviointilaitoksen tekemää tarkastusta, mutta ne voidaan nähdä yhtenä lisäkeinona tietoturvan ja tietosuojan parantamiseksi. Lisäksi yksityisen sektorin toimijoilta on mahdollista hankkia erilaisia koulutus- ja konsultointipalveluita tietoturvan ja tietosuojan parantamiseksi.

Yleisen tietosuoja-asetuksen 42 artiklan mukaisia hyväksyttyjä tietosuojasertifiointimekanismeja ei vielä ole käytössä. Näiden käyttöä olisi syytä kannustaa eri toimialoilla täydentämään rekisterinpitäjän sisäistä valvontaa ja viranomaisvalvontaa vastaavalla tavalla kuin nyt käytetään tietoturva-auditointeja.

Ulkopuolisten sertifiointielinten myöntämät tietosuojasertifioinnit olisivat yksi tietosuoja-asetuksen mukainen keino rekisterinpitäjän osoittaa, että tietosuoja-asetusta ja erityisesti käsittelyn turvallisuuteen liittyviä vaatimuksia noudatetaan. Ulkopuolisten riippumattomien sertifiointielinten tekemät arviot lisäisivät toiminnan uskottavuutta, laajentaisivat merkittävästi kyvykkyyksiä arvioida säännösten mukaisuutta (valvontaa) ja samalla se toisi rekisterinpitäjille tärkeää osaamista tietosuojan kehittämiseen. Tämä edellyttäisi sertifiointielinten akkreditointia, joka on tietosuojavaltuutetun tehtävä, sekä tietosuojan sertifioinnin liiketoiminnan käynnistämistä.

4.11 Tietoturvan ja tietosuojan vaikutus talousjärjestelmälle

Työryhmän työssä huomio on erityisesti kriittisten toimialojen tietoturvan ja tietosuojan parantamisessa. Kriittisten toimialojen toiminnalla on olennainen rooli muiden toimialojen ja yhteiskunnallisten toimintojen ylläpidossa. Kriittisillä toimialoilla on myös suoraa kansantaloudellista vaikutusta. Taulukossa yksi on kuvattu näiden toimialojen työllisyyttä ja osuutta bruttokansantuotteesta. Toimialoilla työskentelee yhteensä yli 350 000 henkilöä ja ne muodostavat neljänneksen Suomen kansantaloudesta.

Taulukko 1. Tilastotietoa toimialoista

Toimiala	Henkilötyö-vuodet	Osuus arvonlisästä	Liikevaihto (1000 euroa)
Tele	11065	1,16%	4802769
Finanssiala	44055	2,95%	
Terveydenhuolto	105637	9,41%	8493940
Vesihuolto	8755	0,89%	2998318
Energia	12213	3,06%	14506486
ICT ja ohjelmisto	*58960*	3,17%	12025614
Liikenne	122729	4,63%	23715094
Yhteensä	363414	25,27%	

Lähde: Tilastokeskus

Kriittisten toimialojen tietoturvan ja tietosuojan kansantaloudellinen merkitys on suuri. Tietoturvan ja tietosuojan murtumisesta aiheutuneet häiriöt vaikuttaisivat suoraan toimialojen satoihin tuhansiin palkansaajiin ja bruttokansantuotteen kehitykseen. Kriittisten toimialojen kohdalla tietoturvan ja tietosuojan murtuminen vaikuttaisi kuitenkin myös muilla tavoilla kansantalouden toimintaan ja kehitykseen. Toimialojen väliset keskinäisriippuvuudet ja epäsuorat kustannukset ovat vaikutuksista olennaisimpia. Osittain keskinäisriippuvuudet ja epäsuorat kustannukset hahmottavat samoja asioita eri suunnista.

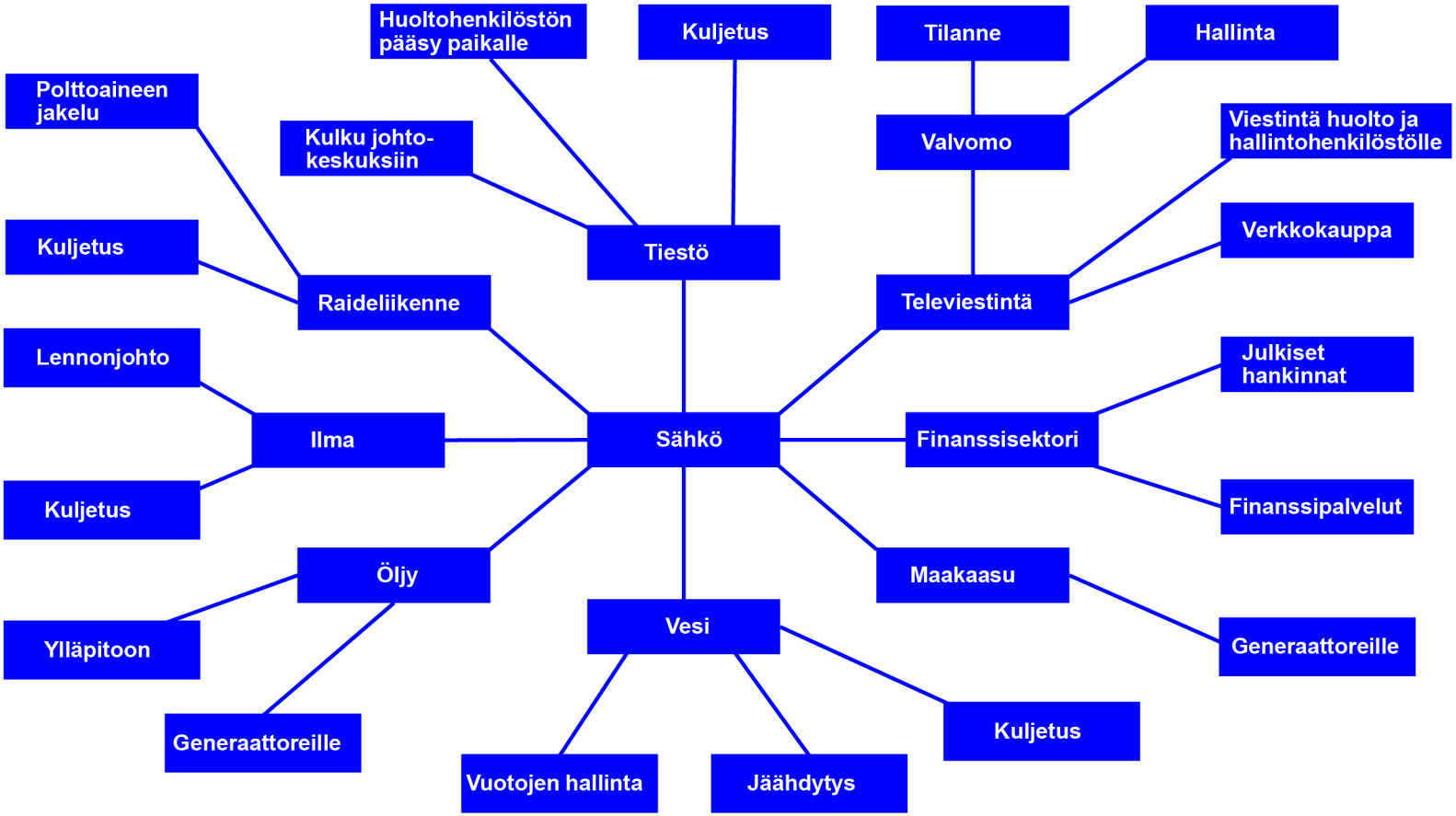
Keskinäisriippuvuuksilla tarkoitetaan suhteita, joiden kautta yhden kriittisen toimialan häiriöt vaikuttavat muiden kriittisten toimialojen ja kansantalouden toimintaan. On esimerkiksi mahdollista, että vesihuollon häiriötilanteissa saastunutta vettä pääsee vesijohtoverkkoon. Tällöin vesihuolto joudutaan toteuttamaan väliaikaisjärjestelyin. Mahdolliset väliaikaisjärjestelyt ovat esimerkki suorasta vaikutuksesta. Keskinäisriippuvuudesta esimerkkinä voisi olla tilanne, jossa saastunut vesi aiheuttaa pandemian. Tällöin ihmisten terveyden lisäksi myös yritysten toimintaedellytykset ja kansantalouden kehitys ovat hankalassa tilanteessa [22].

[22] Heino ym. (2019).

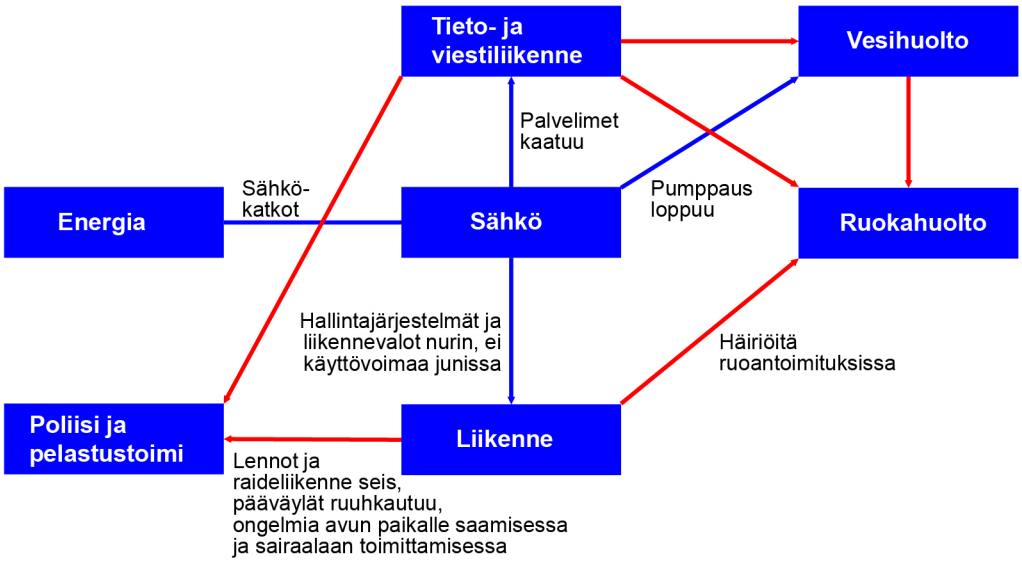
Keskinäisriippuvuudet muodostavat monimutkaisen verkoston. Erityisen paljon keskinäisriippuvuuksia on sähköllä, sillä se toimii virtana monella toimialalla ja monissa yhteiskunnan tärkeissä toiminnoissa. Sähkön keskinäisriippuvuuksia hahmottaa kuva viisi, johon on listattu sähkön vaikutukset eri toimialoihin.

Kuvassa viisi esitetty keskinäisriippuvuuksien verkosto on staattinen. Tämä tarkoittaa, että esimerkiksi sähkön katkeamisen seurauksia voi hahmottaa toimialojen sisällä. Esimerkiksi lennonjohdon palvelut voivat kaatua sähkön katketessa. Keskinäisriippuvaisuuksien toinen idea kuitenkin on hahmottaa dynaamisia suhteita. Näillä tarkoitetaan niitä tapahtumia, joissa sähkönsaannin katkeaminen yhdellä alalla vaikuttaa sen alan kautta myös toisen toimialan toimintaan. Keskinäisriippuvaisuuksien dynamiikkaa tarkastellaan kuvassa kuusi.

Kuva 5. Sähkön keskinäisriippuvuuksia (Lähde: Rinaldi ym. 2001 mukaillen)



Kuva 6. Keskinäisriippuvuuksien dynamiikka sähkönsaannin pettäessä (Lähde: Kröger ja Zio 2011; Heino ym. 2019 mukaillen)



Kuvassa kuusi tarkastelun lähtökohtana on tilanne, jossa sähkö katkeaa. Kuviossa siniset viivat kuvaavat sähkökatkon suoria vaikutuksia eri toimialojen toimintaan. Punaiset viivat sen sijaan kuvaavat keskinäisriippuvuuksien kautta tulevia epäsuoria vaikutuksia, kun sähkökatko vaikuttaa toisen toimialan vaikutuksen kautta esimerkiksi vesihuoltoon.

Sähkökatkon suorana vaikutuksena on liikenteen hallintajärjestelmien pettäminen lentoliikenteessä, liikennevalojen sammuminen maanteillä ja junien käyttövoiman loppuminen. Toisaalta tieto- ja viestiliikenteen palvelimet kaatuvat ja vedenpumppaus loppuu. Toimialoja voitaisiin lisätä kuvan kaksi mukaisesti ja hahmotella lisävaikutuksia.

Suorat vaikutukset kertautuvat keskinäisriippuvuuksien kautta. Esimerkiksi liikenteen ongelmat tarkoittavat, että ruoantoimituksessa ja avunsaannissa on ongelmia. Toisaalta tieto- ja viestiliikenteen ongelmat vaikuttavat niin pelastustoimeen, ruokahuoltoon kuin vesihuoltoonkin. Lisäksi vesihuollon ongelmat varsinkin pitemmällä aikavälillä vaikuttavat ruokahuoltoon. Kuva kaksi ei esitä kaikkia mahdollisia vaikutusketjua ja keskinäisriippuvuuksia vaan pyrkii hahmottelemaan keskinäisriippuvuuksien merkitystä.

Sähköä tarvitaan myös kriittisten finanssipalveluiden kuten päivittäisen maksuliikenteen ylläpitoon. Kuvassa kuusi ei ole erikseen esitetty finanssialan vaikutuksia. Säh-

kön saanti on kuitenkin olennaista maksujärjestelmien toiminnalle ja ongelmat maksuliikenteessä voivat johtaa esimerkiksi ongelmiin ruokahuollon turvaamisessa. Vaikka monilla kriittisillä toimialoilla on vaikutussuhteita muihin kriittisiin toimialoihin ja yhteiskunnan toimivuuteen, eivät vaikutussuhteet ole kaikilla toimialoilla niin merkittäviä kuin energiasektorilla.

Kansantalouden näkökulmasta keskinäisriippuvuuksien dynamiikka tarkoittaa, että tietoturvan tai tietosuojan murtumisen kustannukset kertautuvat muiden toimialojen vaikutuksien kautta. Suorien kustannusten lisäksi muille kriittisille toimialoille tietoturvan ja tietosuojan murtumisesta aiheutuvat kustannukset vaikuttavat kokonaiskustannuksiin. Toisaalta on hyvä huomata, että tähän mennessä keskinäisriippuvaisuuksia on keskitytty kuvaamaan kriittisten toimialojen kautta. Laajojen järjestelmäongelmien tapauksessa vaikutukset kuitenkin levittäytyvät kansantalouteen myös muiden toimialojen kautta. Ilman sähköä tai energiaa teollisuus ei pysty toimimaan samoin kuin suuri osa asiantuntijatyöstä pysähtyy ilman sähkövirtaa.

Toisaalta tietoturvan ja tietosuojan murtumisella voi olla laajempia vaikutuksia yritysten toimintaedellytyksiin ja kansantalouden toimintaan, jos esimerkiksi tietomurto vaikuttaa kansalaisten luottamukseen yhteiskunnan toimivuudesta tai yritysten odotuksiin. Jos yritykset esimerkiksi alkavat odottaa tietomurtoja, voivat ne ryhtyä toimenpiteisiin suojatakseen toimintaansa tai toisaalta päätyä siirtämään toimintaansa maihin, joissa ei ole vahvoja odotuksia tietomurroista. Kotitalouksien luottamus digitaalisen talousjärjestelmän toimintaan voi järkkyä ja esimerkiksi tietojen analoginen säilyttäminen tai käteisen käyttäminen voi lisääntyä, vaikka analogisten palveluiden tarjoaminen ja käteisen käyttäminen ovat yleensä kalliimpia toimintatapoja. Instituutioita kohtaan koettu epäluottamus voi lisääntyä, jos nähdään toiminnan olevan heikoilla kantimilla.

Toisaalta tietoturvan ja tietosuojan murtumisen vaikutuksia voi hahmotella edellä mainittujen käsitteiden avulla kotitalouksien ja yritysten kannalta. Kotitalouksien kannalta tietosuojan ja tietoturvan murtuminen aiheuttaa yleisellä tasolla kustannuksia suoraan, jos hyödykkeitä joudutaan hankkimaan toista kautta tietoturvan pettäessä tai pääsy hyödykkeisiin katkeaa. Suora kustannus on myös kansalaisen kohdistamat lisäresurssit esimerkiksi uuden palveluntarjoajan etsimiseen tai oman tietoturvan ja tietosuojan tason parantamiseen. Lisäksi se voi aiheuttaa epäsuoria kustannuksia, jos kansalaisen luottamus palveluun järkkyy, mistä seuraa esimerkiksi pienempää hyödykkeiden kulutusta.

Yrityksille tietoturvan ja tietosuojan pettäminen tarkoittaa tuotantokustannusten nousemista. Tietoturvan ja tietosuojan pettäminen johtaa suoraan kasvaneisiin kustannuksiin ongelmien hallinnassa (esimerkiksi viestintä asiakkaille), oman tietoturvan ja tietosuojan tason parantamisessa. Lisäksi tietoturvan ja tietosuojan pettäminen voi

johtaa epäsuoriin kustannuksiin, jos asiakkaiden luottamus yritykseen järkkyy, mikä taas johtaa pienentyneisiin asiakasmääriin ja pienentyneeseen myyntiin.

Tähän mennessä tekstissä on kuvattu tietoturvan ja tietosuojan murtumisen aiheuttamia erilaisia vaikutuksia. Työryhmän tavoitteena on parantaa kriittisten toimialojen tietoturvaa ja tietosuojaa, millä on yhteiskunnallisia sekä kansantaloudellisia vaikutuksia. Kansantaloudelliset vaikutukset riippuvat mekanismeista, joilla tietoturvaa ja tietosuojaa pyritään parantamaan. Yksi esillä olleista vaihtoehdoista on erilainen sääntely, jolla kriittisten toimialojen toimijoita velvoitetaan parantamaan tietoturvansa ja tietosuojansa tasoa.

Sääntelyn vaikutukset ovat moninaiset. Suurempi sääntelytaakka tarkoittaa, että yritykset joutuvat käyttämään lisää resursseja tietoturvaan ja tietosuojaan. Tämä voi pienentää voittoja, mutta on myös mahdollista, että tietoturvaan ja tietosuojaan kohdennetut lisäresurssit ovat pois muusta toiminnasta. Toisaalta hyvä tietoturvan ja tietosuojan taso voi tarjota ne omaksuville yrityksille maine-edun ja siten edesauttaa liiketoiminnan menestymistä.

On hyödyllistä huomioida, että uusi sääntely ei välttämättä oikein kohdistettuna vaikuta pelkästään toimijoiden valintapäätöksiin, sillä sääntely voi vaikuttaa myös laajamittaisemmin muihinkin kuin sen kohteena oleviin toimijoihin. Yksityisyydensuojan, sääntelyn ja innovaatioiden välillä on erotettavissa kaksi näkökulmaa. Ensimmäisen mukaan sääntely estää innovaatiot luomalla lisää kustannuksia esimerkiksi tietojenvaihtoon liittyen. Toinen näkökulma korostaa, että laajempi sääntely edistää tietojen luovuttamista, kun yksilöt näkevät sen turvallisemmaksi[23].

Tietoturvan ja tietosuojan tason määrittämisessä yksi oleellinen näkökulma on taloudellisen tehokkuuden ja tietoturvan välinen valinta. On mahdollista, että tavoitteena on se, että kaikki toimijat valitsevat riittävän tietoturvan tason ja että tietoturva on teknisesti edistynyt eli uusimman teknologian mukainen. Tällöin taloudellinen tehokkuus kuitenkin lyhyellä aikavälillä kärsii. Tehokkuutta voi tässä yhteydessä verrata tietoturva- ja tietosuojapalveluiden käytettävyyteen. Suurella tietoturvan ja tietosuojan tasolla arjessa kuluu paljon resursseja sen ylläpitoon ja esimerkiksi erilaisten tunnistautumistietojen täyttämiseen. Toisaalta pitkällä aikavälillä suuri tietoturvan ja tietosuojan taso vähentää edellä kuvattujen riskien todennäköisyyttä ja pienentää siten pitkän aikavälin kustannuksia.

[23] Acquisti ym. (2016).

5 Tavoitteet ja keinot

Tietoturvan ja tietosuojan tasoa on kehitettävä kaikilla yhteiskunnan kriittisillä sektoreilla. Lisäksi sektoreiden välisiä osaamis- ja kyvykkyyseroja on kavennettava. Digitaalinen yhteiskunta koostuu suuresta joukosta toisistaan riippuvaisia toimijoita. Esimerkiksi useat kriittiset toimialat tarvitsevat energiahuoltoa tai viestintäverkkoja oman sektorinsa perustoimintoihin. Yhteiskunnan toiminnan jatkuvuuden kannalta on välttämätöntä varmistaa kaikkien keskeisten toimialojen toimintaedellytykset myös erilaisten häiriöiden varalta. Kriittisten toimintojen osalta yksikään toimiala ei voi olla heikko lenkki.

Riittävästä tietoturvasta ja tietosuojasta huolehtimisella vahvistetaan myös kansalaisten luottamusta digitaaliseen yhteiskuntaan. Ihmisten tietojen siirtyessä yhä enenevässä määrin digitaaliseen muotoon on kansalaisten kyettävä luottamaan siihen, että tietoja käsitellään asianmukaisesti ja ne ovat turvassa tietomurroilta ja muilta oikeudenloukkauksilta. Ilman luottamusta yhteiskunnan digitaaliset palvelut eivät kehity ja digitalisaation hyödyt menetetään.

Tavoitteisiin pääsemiseksi tarvitaan toimenpiteitä, joilla saadaan aikaan sektorirajat ylittäviä vaikutuksia. Tällaisia toimenpiteitä ovat esimerkiksi viranomaisten välisen yhteistyön ja yhteisen tilannekuvan kehittäminen, joka vaatii sekä lainsäädännön vahvistamista että riittävää resursointia. Tietoturva- ja tietosuojaloukkausten ehkäisemiseksi ja selvittämiseksi viranomaisille tulisi säätää nykyistä vakiintuneemmat yhteistyörakenteet. Yhteistyön osalta korostuu myös viranomaisten yhteistyö yksityisen sektorin toimijoiden kanssa. Lisäksi Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen tarjoamat asiantuntija- ja tietoturvapalvelut on saatava entistä laajemmin kaikkien kriittisten toimialojen käyttöön.

Toiminnan kehittäminen ja sektoreiden välisten erojen kaventamien vaatii kattavaa sääntelyä ja sen tehokasta valvontaa. Lainsäädännössä on oltava riittävät tietoturvaa ja tietosuojaa koskevat vaatimukset ja määräyksenantovaltuudet, joita voidaan täydentää velvoittavilla alemman asteen määräyksillä. Aikaisempien selvitysten mukaan sääntelyllä on ollut positiivinen vaikutus tietoturvan toteutukseen.[24] Lainsäädännön tasolla korostuu lisäksi vähimmäisvaatimusten määritys. Eri sektoreilla tarkemmat tieto-

[24] Huoltovarmuuskeskuksen raportti kyberturvallisuuden nykytilasta eri toimialoilla: https://cdn.huoltovarmuuskeskus.fi/app/uploads/2020/10/05091400/Kyberturvallisuuden-nykytila-eri-toimialoilla.pdf

turvavaatimukset asetetaan tyypillisesti määräyksissä tai ohjeistuksissa. Riittävän tietoturvallisuuden ja tietosuojan tason varmistamiseksi vaatimusten tulisi perustua velvoittaviin määräyksiin.

Sääntelyn vahvistaminen ei yksin riitä, vaan myös sääntelyn toimeenpanoon ja valvontaan sekä toimijoiden ohjaamiseen ja neuvontaan tarvitaan riittävät resurssit. Tällä hetkellä useilla yhteiskunnan kriittisillä toimialoilla tietoturvaan ja tietosuojaan osoitetut resurssit ovat riittämättömiä. Resurssien riittämättömyys koskee myös toimialakohtaista viranomaisvalvontaa, eikä viranomaisilla ole edes mahdollisuutta käyttää lainsäädännössä annettuja toimivaltuuksia. Toiminnan kehittäminen ja resurssien kohdentaminen tietoturvan ja tietosuojan kehittämiseen edellyttää uskallusta johtotasolta.

Vaikka tehokkaalla viranomaisvalvonnalla voidaan katsoa olevan merkittävä vaikutus tietoturvan ja tietosuojan parantamiseen yhteiskunnassa, ensisijainen vastuu tietoturvan ja tietosuojan toteutumisesta on jokaisella toimijalla itsellään. Mikään määrä valvontaa ei yksin riitä tekemään yhteiskunnasta ja sen kriittisistä toiminnoista turvallisia. Tietoturvan ja tietosuojan on jo lähtökohtaisesti oltava sisäänrakennettuna kriittisten toimialojen toimintakulttuuriin ja toimijoiden on itse kannettava siitä vastuu.

Yhteenvetona työryhmä toteaa, että tietoturvan ja tietosuojan parantaminen kriittisillä toimialoilla vaatii, että:

1. Lainsäädännössä on riittävät tietoturva- ja tietosuojavaatimukset ja -velvoitteet, joita toimialoilla noudatetaan, sekä säännökset antaa tarkempia määräyksiä tietoturvan ja tietosuojan toteuttamisesta.
2. Toimijoilla on riittävä tietämys ja osaaminen velvoitteiden noudattamisessa.
3. Viranomaisilla on riittävät toimivaltuudet valvoa tietoturvan ja tietosuojan toteutumista ja tehdä sektorirajat ylittävää yhteistyötä.
4. Viranomaisilla on riittävä osaaminen ja uskallus käyttää niille lainsäädännössä annettua toimivaltaa ja ohjata toimialaansa.
5. Viranomaisilla on riittävät tosiasialliset aineelliset ja henkilöresurssit käyttää toimivaltaansa.
6. Jokainen toimija kantaa itse vastuun oman toimintansa tietoturvasta ja tietosuojasta.
7. Pidetään yllä yhteistä tietoturvaa ja tietosuojaa koskevan toimintaympäristön tilannekuvaa ml. säännöllisellä koordinaatiolla, tiedonvaihdolla ja tilannekatsauksilla.

6 Arvio keskeisistä vaikutuksista

6.1 Tietoturvan ja tietosuojan murtumisen kustannukset

Tietoturvan ja tietosuojan murtuminen kriittisillä toimialoilla aiheuttaa monenlaisia kustannuksia. Yritystason kustannusten lisäksi kustannuksia aiheutuu yhteiskunnalle laajemmin esimerkiksi aiemmin kuvattujen mekanismien, kuten keskinäisriippuvuuksien, kautta. Pienten ja keskisuurten yritysten tietomurtojen kokonaiskustannukset vuonna 2015 olivat noin 50 000 dollaria. Sen sijaan suurilla, yli 1500 henkilöä työllistävillä, yrityksillä kokonaiskustannukset olivat noin 620 000 dollaria.[25]

Psykoterapiakeskus Vastaamoon kohdistuneen tietomurron kokonaiskustannusten hahmottaminen on kesken, mutta Suomesta ja maailmalta on arvioita aiempien tietomurtojen kustannuksista. Arviot perustuvat julkisuudessa olleisiin tietoihin. Kesäkuussa 2019 Lahden kaupungin tietojärjestelmiin kohdistetun hyökkäyksen suoriksi kustannuksiksi on arvioitu lähes 700 000 euroa. Myös Kokemäen ja Porin kaupunkien verkkoon on tunkeuduttu vuonna 2019, mutta näistä ei ole toistaiseksi kustannusarvioita. Toisaalta hyökkäykset voivat kohdistua myös yksittäisiin yrityksiin kuten vuonna 2019, kun mineraaliyhtiö Omyan joutui kyberhyökkäyksen seurauksena sulkemaan kaikkien tehtaidensa toiminnan.

Kyberhyökkäyksistä ja tietomurroista on myös kansainvälisiä esimerkkejä. Vuonna 2017 moni yritys Euroopassa joutui kyberhyökkäyksen seurauksena lunnasvaatimusten uhriksi ja seurauksena tuhansia servereitä ja kymmeniä tuhansia tietokoneita jouduttiin asentamaan uudestaan. Esimerkiksi kansainvälinen FedEx kertoi joutuneensa hyökkäyksen uhriksi ja arvioi menetysten olevan noin 300 miljoonaa puntaa.

Suomea koskevat ja kansainväliset esimerkit kertovat kyberhyökkäysten ja tietomurtojen aiheuttamista kustannuksista. Tämän hetkisen tiedon perusteella voi olla hankala hahmottaa kyberhyökkäysten kokonaiskustannuksia yhteiskunnalle. Esimerkiksi Lahden kaupungin tapauksessa epäsuorien kustannusten arvioiminen on hankalaa. Kirjallisuudesta kuitenkin löytyy erilaisiin mallinnusmenetelmiin perustuvia arvioita kriittisten toimialojen häiriötilanteiden kokonaiskustannuksista. Esimerkit kustannuksista perustuvat usein sellaisiin tietomurtoihin, joissa murto ja sen seuraukset tapahtuvat kerralla.

[25] Iivanainen (2019) käy läpi erilaisille yrityksille tietomurroista aiheutuneita kustannuksia.

Lausuntopalautteessa esiin nousseissa kommenteissa tuotiin kuitenkin esille, että jatkossa myös pitkäaikaisempi tietopohjan vääristyminen voi aiheuttaa haasteita.

Kriittisillä toimialoilla tietomurrot ja muut tietoturvaongelmat voivat heikentää muiden toimintojen toimintamahdollisuuksia tai jopa estää ne. Koska kriittisen infrastruktuurin toimintaan liittyy keskinäisriippuvuuksia ja monivaiheisia epäsuoria kustannuksia, yhteiskunnalliset kustannukset tietomurrosta ovat yleisiä yrityskohtaisia kustannuksia huomattavasti suurempia. Taulukko kaksi kuvaa aiempia tutkimuksia, joissa kriittisten toimialojen toimintojen pysähtymisen kustannuksia on kartoitettu. Vaikka osa arvioista mallintaa esimerkiksi myrskyn kokonaistaloudellisia vaikutuksia, on mekanismi ja idea sama kuin kyberhyökkäyksessä. Esimerkiksi myrskyn sijaan myös kyberhyökkäys voi tehdä useita kriittisiä toimialoja toimimattomiksi. Tällöin aiheutuneita kustannuksia voidaan verrata eri tapauksien välillä.

Taulukko 2. Toimintahäiriöiden kokonaiskustannuksia

Tutkimus	Maa	Häiriö	Häiriön kesto	Taloudelliset vaikutukset
Jonkeren ja Giannonpoulos (2014)	Alankomaat	Myrsky	Useita viikkoja	2,3–3,4 miljardia euroa
Jonkeren ym. (2015)	Italia	Sähkökatko	0,5-18 tuntia	46–173 miljoonaa euroa
Oughton (2019)	Iso-Britannia	Kyber-hyökkäys		21–111 miljoonaa puntaa

Siirryttäessä yritysvaikutuksista kansantalouden tasolle ja kriittisten toimialojen toimintaan, kustannukset kasvavat huomattavasti. Esimerkiksi Ison-Britannian kansantaloudelle laajamittaisen kyberhyökkäyksen on simuloitu kustantavan 21–111 miljoonaa puntaa. Kaksi muuta tutkimusta käsittelevät erilaisia tilanteita, mutta niiden toimintamekanismit ovat sovellettavissa myös tietoturvan tai tietosuojan murtumisen tilanteeseen. Esimerkiksi myrsky voi jättää kriittisten toimialojen toimintoja toimimattomaksi, mikä voi olla tilanne myös tietoturvan tai tietosuojan murtuessa. Tällaisen tilanteen kustannukset voivat olla erittäin korkeat. Vaikutusarvioinnin näkökulmasta yksi kriittisten toimialojen tietoturvan ja tietosuojan parantamisen hyödyistä on se, että edellä kuvattua kokoluokkaa olevat kustannukset realisoituvat epätodennäköisemmin.

Suuressa osassa linjausehdotuksia varsinainen lainsäädäntö- ja toimeenpanotyö tapahtuu vasta myöhemmin, jolloin myös esitetään niiden tarkemmat vaikutusarviot.

Tässä vaiheessa on kuitenkin mahdollista eritellä yleisellä tasolla poliittisten linjausehdotusten vaikutuksia. Yleisesti linjausehdotukset lisäävät erilaisia viranomaisyhteistyön muotoja ja viranomaisten resurssitarvetta. Osa ehdotuksista vaikuttaa myös yksityisen sektorin toimintaan.

Linjausehdotukset ohjaavat resursseja erityisesti toimenpiteisiin liittyvään lainsäädäntötyöhön ja valvovien viranomaisten nykyisten resurssien vahvistamiseen (osassa linjausehdotuksista nimenomaisesti esitetään lisää resursseja viranomaisille). Osa linjausehdotuksista voi tietoturvan ja tietosuojan parantamisen lisäksi vaikuttaa myös muuhun toimintaan. Auditointilaitosten määrän lisääminen voi esimerkiksi tuottaa yksityiselle sektorille uusia liiketoimintamahdollisuuksia. Osa linjausehdotusten yhteydessä esitetystä selvitystyöstä voi ohjautua tutkimusyhteisöjen lisäksi muille kilpaillun tutkimusrahoituksen hakijoille, jos selvityksiä ei päädytä toteuttamaan yksin virkatyönä. Myös esimerkiksi linjausehdotus 36 voi toteutustavasta riippuen tuoda yksityiselle sektorille liiketoimintamahdollisuuksia, jos palvelun kehittämiseen hyödynnetään yksityisen sektorin osaamista. Työryhmän ehdottamista toimenpiteistä osa on sellaisia, että niiden toteuttaminen edellyttää myös lisärahoituksen saamista. Lisäksi toimenpiteistä osan toteutumiseen voi vaikuttaa se, missä määrin tarvittavaa aineistoa on käytettävissä.

Vaatimuksenmukaisuuden arviointia koskevien linjausehdotusten 11–14 vaikutukset ovat epäselvemmät. Erityisesti sertifiointitoiminnalla voi olla erilaisia vaikutuksia kansantalouden dynamiikkaan. Näitä vaikutuksia esitellään alla.

6.2 Sertifioinnin taloudelliset vaikutukset

Yksi tapa parantaa kriittisten toimialojen tietoturvaa ja tietosuojaa on velvoittaa toimijoita hankkimaan sertifikaatteja (esimerkiksi ISO -sertifikaatit) toiminnalleen tai sen tietyille osa-alueille. Sertifikaatin hankkiminen parantaa toimijoiden tietoturvaa, koska tietoturvastandardin vaatimukset suojaavat yritystä ja toisaalta ohjaavat sitä tietoturvan jatkuvaan parantamiseen. Sertifikaateilla myös pystyy viestimään esimerkiksi asiakkaiden suuntaan, että toimijan tietoturva on kestävällä tasolla[26]. Toisaalta tietoturvasertifiointi ei välttämättä vaikuta positiivisesti yrityksen markkina-arvoon[27].

Kriittisten toimialojen sertifiointivelvoitteessa on hyvä tarkastella toimijoiden kykyä hankkia sertifikaatteja. Erilaisten tietoturvasertifikaattien hankkiminen vie huomattavan

[26] Iivanainen (2019).
[27] Hsu ym. (2016).

määrän resursseja ja on epäselvää, onko pienemmillä yrityksillä taloudellisia mahdollisuuksia sertifikaattien hankkimiseen. ISO 27001 –tietoturvasertifikaatin hankkimisen kokonaiskustannuksiksi on arvioitu 76 480 euroa[28]. Kattavia arvioita eri kokoisten ja erilaista lähtötasoa edustavien yritysten tietoturvasertifioinnin kustannuksista on kuitenkin vaikea esittää. Lisäksi on selvää, että muun muassa yrityksen toimiala, koko ja järjestelmien monimutkaisuus vaikuttavat tietoturvasertifioinnin kustannuksiin. Arvioitu kokonaiskustannus onkin vain yksi esimerkki tietoturvasertifioinnin kustannuksista.

Taulukko 3. Kriittisten toimialojen yritysten lukumäärä henkilöstön mukaan

Toimiala	Yrityksiä yhteensä	0–4 henkeä	5–9 henkeä	10–19 henkeä	20–49 henkeä	50–99 henkeä	100–249 henkeä	250–499 henkeä	500–999 henkeä	≥1000 henkeä
Tele	393	286	41	32	13	9	8	1		3
Finanssiala	8709	8034	286	159	114	57	34	10	8	7
Terveyden-huolto	18364	16710	655	490	309	100	53	23	14	10
Vesihuolto	1506	1201	127	89	60	18	7	3	1	
Energia	950	717	67	60	66	24	9	4	2	1
ICT ja ohjelmisto	7958	6491	558	418	275	120	68	20	4	4
Liikenne	20069	17046	1508	787	479	138	70	23	9	9
Yhteensä	57949									

Lähde: Tilastokeskus

Sertifiointien kustannukset voivat siis olla esimerkkitapausta huomattavasti korkeammat. Kustannukset jakautuvat useammalle vuodelle ja sertifiointeihin joudutaan käyttämään paljon aikaa. Taulukko kolme kokoaa yhteen kriittisten toimialojen yritysten lukumäärät jaoteltuna henkilöstön määrän mukaan. Taulukosta huomataan, että monilla kriittisillä toimialoilla yritykset ovat pieniä vain muutaman hengen kokoisia toimijoita.

[28] Iivanainen (2019).

Esimerkiksi terveydenhuollossa lähes 95% prosenttia yrityksistä on alle kymmenen hengen toimijoita.

Sertifioinnin kustannukset voivat olla varsinkin pienemmille toimijoille suuret. Onkin epäselvää, miten toimijat reagoivat mahdolliseen sertifiointipakkoon. Jos yritys, jonka liiketoiminnan suuruusluokka ei mahdollista vähintään kymmenien tuhansien eurojen arvoisen sertifikaatin käyttöönottoa, velvoitetaan ottamaan sertifikaatin käyttöön, tulokset voivat olla moninaiset. On mahdollista, että liiketoiminta jatkuu ennallaan ilman sertifikaattia. Mikäli sertifioinnin valvonta on kattavaa ja mahdolliset sanktiot suuria, on mahdollista, että yritykset lopettavat liiketoimintaansa tämän takia.

Toisaalta kasvavan sääntelyn vaikutuksena voi myös olla yritysten yhteenliittymisten ja fuusioiden kasvu. Jos toimijalla ei ole taloudellista mahdollisuutta sertifikaatin hankintaan, mutta toimintaa halutaan jatkaa, on mahdollista, että sertifikaattivaatimus lisää kannusteita luoda yhteenliittymiä pienten toimijoiden välillä tai fuusioita isompien ja pienempien toimijoiden välillä. Yhteenliittymien tai fuusioiden kasvulla voi olla myös muita talousvaikutuksia. Toisaalta suurempien toimijoiden osalta vaikutus voi myös olla toiminnan siirto (ainakin nimellisesti) maihin, joissa sertifiointivelvoitetta ei ole.

Fuusioiden kasvu tarkoittaa, että alalla on entistä vähemmän toimijoita, jotka ovat entistä suurempia. Tällöin on mahdollista, että yksittäisille toimijoille muodostuu markkina-asema, jonka kautta ne voivat vaikuttaa esimerkiksi hintatasoon. Tällainen asetelma johtaisi kilpailun vähenemiseen ja todennäköisesti kuluttajahintojen nousuun sekä toimijoiden voittojen kasvuun. Kilpailun väheneminen voi vaikuttaa negatiivisesti myös esimerkiksi talouskasvun edellytyksiin. Myös toiminnan tai voittojen siirto ulkomaille todennäköisesti vaikuttaisi negatiivisesti Suomen kansantalouden toimintaedellytyksiin.

Kansantalouden kannalta sertifioinnin kustannukset ovat siis epäselvät. Tutkimuskirjallisuus sertifioinnin kansantaloudellisista vaikutuksista on pieni ja keskittyy suurilta osin sertifioinnin vaikutuksiin yritysten toimintaan. Erityisen paljon esitetty kysymys on, vaikuttaako sertifiointi pitkällä aikavälillä positiivisesti yritysten maineeseen ja heijastuuko se liiketoimintaan. Toisaalta sertifioinnit voivat auttaa välttämään taulukossa 2 kuvattua kokoluokkaa olevia haasteita. Toisaalta ne ovat kalliita erityisesti pienille yksittäisille toimijoille ja sertifiointivaatimusten asettamisten vaikutukset yksittäisten toimijoiden käyttäytymiseen ovat epäselvät.

7 Yhteenveto ja lisäresurssitarpeet

Työryhmän raportin kriittisten toimialojen tietoturvaa ja tietosuojaa parantavat ehdotukset koostuvat 36 poliittisesta linjausehdotuksesta. Linjausehdotuksissa painotetaan ensinnäkin viranomaisten tehokkaampaa ja järjestäytyneempää yhteistyötä. Toiseksi korostetaan sitä, että kaikilla kriittisillä toimialoilla tulisi olla lakisääteiset tietoturvavaatimukset. Kolmanneksi kriittisten tietojärjestelmien vaatimustenmukaisuutta tulisi arvioida nykyistä kattavammin. Neljänneksi kaikkien selvityksen kohteena olevien toimialojen erityispiirteet tulee huomioida, jotta toimialoille voidaan asettaa oikeasuhtaisia ja tehokkaita velvoitteita. Viidenneksi julkisen sektorin tietoturvaa ja tietosuojaa pitää vahvistaa. Tietoturva-asioiden rinnalla huomiota tulee kiinnittää tietosuojaa koskeviin vaatimuksiin ja niiden noudattamiseen, jotta pystytään tehokkaasti puuttumaan oikeudenloukkauksiin. Samalla on eräiltä osin tarkasteltava lainsäädännön toimivuutta. Kaikkien edellä mainittujen kokonaisuuksien toteuttaminen ja tietoturvan sekä tietosuojan yleisen tason parantaminen kriittisillä toimialoilla edellyttää merkittäviä lisäresursseja niin julkiselle kuin yksityiselle sektorille.

Työryhmä on arvioinut konkreettiset lisäresurssitarpeet kultakin hallinnonalalta sektoriviranomaisten tehokkaan tietoturvavalvonnan mahdollistamiseksi. Tarkasteltavia toimialoja ovat olleet NIS-direktiivin mukaisesti erityisesti terveydenhuolto, rahoitusmarkkinat, energiahuolto, vesihuolto, liikenne ja digitaalinen infrastruktuuri, sekä viestintäverkot. Tarkasteltavana ovat olleet myös valtion ja kuntien merkittävät tietojärjestelmät, joiden osalta lisäresurssiarvioita on tarkasteltu erityisesti valtion järjestelmien osalta. Lisäksi tarkastelussa ovat olleet poliisin resurssit erityisesti tietoverkkorikosten torjunnan näkökulmasta. Turvallisuusviranomaisten verkkoja ja järjestelmiä ei ole tarkasteltu tämän työryhmän työn puitteissa, koska katsottiin, että tällaisia erittäin turvallisuuskriittisiä toimintoja on tarkoituksenmukaista tarkastella erikseen.

Työryhmän arvion mukaan mainituilla toimialoilla tarvitaan yhteensä 109 henkilötyövuotta lisää viranomaistoiminnoissa, jotta työryhmän esittämät linjausehdotukset voitaisiin toteuttaa ja tietoturvan sekä tietosuojan valvonnan, ohjauksen ja neuvonnan tasoa voitaisiin kehittää tarvittavalle tasolle. Henkilötyövuosien lisäys kustantaisi työryhmän arvion mukaan noin 10 miljoonaa euroa vuodessa.

Sekä työryhmän toimenpide-ehdotukset että niihin kohdistetut resurssit on tarkoitettu toisiaan tukeviksi ja niitä tulisi tarkastella kokonaisuutena. Tämä tarkoittaa sitä, että yksittäisen toimenpiteen tehokkuus on usein riippuvainen muiden ehdotettujen toimenpiteiden toteutumisesta.

Liite 1 Tietoturvavaatimuksia koskeva sääntely kriittisillä toimialoilla

Tietoturvavaatimuksia koskeva sääntely kriittisillä toimialoilla*

Lain nojalla ei ole annettu tietoturvaa koskevaa alemman asteista velvoittavaa sääntelyä (asetus / määräys)
Pykälä sisältää asetuksen tai määräyksenantovaltuutuksen tietoturvavaatimuksista
Lakia täydentää delegoitu EU-asetus
* Taulukossa on huomioitu erityisesti toimialojen erityislainsäädännön vaatimuksia. Lisäksi toimialoilla sovelletaan myös yleislaeista, kuten yleisestä tietosuoja-asetuksesta, johtuvia vaatimuksia.

Toimiala	Lainsäädäntö	Asetukset / määräykset	Ohjeet / muut ei velvoittavat	Valvoja
Terveydenhuolto	Asiakastietolaki 159/2007 5a luku, 19 a § Toisiolaki 552/2019 3 luku, 24 §	**Asiakastietolain** nojalla THL voi antaa määräyksiä tietojärjestelmien olennaisista vaatimuksista, vaatimusten todentamisen menettelyistä ja omavalvontasuunnitelman selvityksistä ja vaatimuksista. THL:n voimassa olevat tietoturvan kannalta relevantit määräykset: Määräys 1/2015: A-luokkaan kuuluvien sosiaali- ja terveydenhuollon tietojärjestelmien olennaiset tietoturvavaatimukset Määräys 2/2015: Omavalvontasuunnitelmaan sisällytettävät selvitykset ja vaatimukset **Toisiolain** nojalla Tietolupaviranomainen (Findata) antaa tarkemmat määräykset muiden palveluntarjoajien tietoturvallisille käyttöympäristöille asetettavista vaatimuksista. Määräys 1/2020: Määräys muiden palveluntarjoajien tietoturvallisille käyttöympäristöille asetettavat vaatimukset		Valvira TSV

Tietoturvavaatimuksia koskeva sääntely kriittisillä toimialoilla*

Lain nojalla ei ole annettu tietoturvaa koskevaa alemman asteista velvoittavaa sääntelyä (asetus / määräys)
Pykälä sisältää asetuksen tai määräyksenantovaltuutuksen tietoturvavaatimuksista
Lakia täydentää delegoitu EU-asetus

* Taulukossa on huomioitu erityisesti toimialojen erityislainsäädännön vaatimuksia. Lisäksi toimialoilla sovelletaan myös yleislaeista, kuten yleisestä tietosuoja-asetuksesta, johtuvia vaatimuksia.

Toimiala	Lainsäädäntö	Asetukset / määräykset	Ohjeet / muut ei velvoittavat	Valvoja
Energia-markkinat	Sähkömarkkinalaki (588/2013) 19 § 2-3 kohdat, 28 §, 29 a §, 45 §, 49 §, 49 a §, 52 §, 75 b § Maakaasumarkkinalaki (587/2017) 27 §, 29 §, 32 a §, 32 b §, 34 a §, 58 b § Valvontalaki (590/2013) 9 §, 16 §, 30 §, 31 § Ydinenergialaki (990/1987) 7 §, 7 a §, 7r §	Ydinenergia-asetus (161/1988) 108 §, 110 §, 111 §:t	Ohje: Tietoturvallisuuteen liittyvän häiriön ilmoittamisesta, sähköverkonhaltijoiden varautumis- ja valmiussuunnittelusta sekä sähköverkonhaltijan varautumissuunnitelman mallipohja. STUK on antanut ydinenergialain 7 r §:n nojalla erityisen ns. YVL-ohjeen ydinlaitoksen tietoturvallisuuden hallinnasta.	Energiavirasto, STUK

Rahoitus-markkinat	Finanssivalvonnasta annettu laki (878/2008) 18 § 2 mom. Laki luottolaitostoiminnasta 610/2014 5:10-11, 5:16, 9:2, 9:16, 9:24 Laki talletuspankkien yhteenliittymästä 599/2010 3:17.3 CRR (EU) No 575/2013 Art 288, 368, 320-322 CRD 2013/36/EU Art 74 Maksulaitoslaki 297/2010 19 a §, 19 b § Maksupalvelulaki 290/2010 85 c § PSD2 (EU) 2015/2366 Art 5, 19-20, 95, 96 Laki rahoitus- ja vakuutusryhmittymien valvonnasta 699/2004 2:16, 2:16.3 Sijoituspalvelulaki 747/2012 7:5, 7:8 MiFID II 2014/65/EU Art. 16 Laki kaupankäynnistä rahoitusvälineillä (295/2019) 3 luku, 3:36.1, 3:36.2 MiFID II 2014/65/EU Art. 47, 48	Komission delegoitu asetus 2017/565 (sijoituspalvelut) Komission delegoitu asetus 231/2013 (vaihtoehtorahastot) Komission delegoitu asetus 2017/565 (kauppapaikat) Komission delegoitu asetus 2017/584 (kauppapaikat) Komission delegoitu asetus 2017/392 (arvopaperikeskukset)	MOK 8/2014 Operatiivisen riskin hallinta rahoitussektorin valvottavissa MOK 1/2012 Ulkoistaminen rahoitussektoriin kuuluvissa valvottavissa EBA Guidelines on outsourcing arrangements 25.2.2019 (EBA/GL/2019/02) EBA Guidelines on ICT and security risk management 29.11.2019 (EBA/GL/2019/04) EBA Recommendations on outsourcing to cloud service providers (EBA/REC/2017/03) IOSCO guidelines Committee on Payments and Market Infrastructures, Board of the International Organization of Securities Commissions, Guidance on cyber resilience for financial market infrastructures, 6/2016	Fiva

Tietoturvavaatimuksia koskeva sääntely kriittisillä toimialoilla*

Lain nojalla ei ole annettu tietoturvaa koskevaa alemman asteista velvoittavaa sääntelyä (asetus / määräys)
Pykälä sisältää asetuksen tai määräyksenantovaltuutuksen tietoturvavaatimuksista
Lakia täydentää delegoitu EU-asetus

* Taulukossa on huomioitu erityisesti toimialojen erityislainsäädännön vaatimuksia. Lisäksi toimialoilla sovelletaan myös yleislaeista, kuten yleisestä tietosuoja-asetuksesta, johtuvia vaatimuksia.

Toimiala	Lainsäädäntö	Asetukset / määräykset	Ohjeet / muut ei velvoittavat	Valvoja
Vesihuolto	Vesihuoltolaki 119/2001 15 a § Patoturvallisuuslaki 494/2009 7 § ,16 §, 24 §			ELY:t
Digitaalinen infrastruktuuri	Laki sähköisen viestinnän palveluista 917/2014 170 §, 171 §, 243 § 244 §, Ahvenanmaan itsehallintolaki 1144/1991 32 §	Liikenne- ja viestintäviraston määräykset: M66 teletoiminnan häiriötilanteista, M67 teletoiminnan tietoturvallisuudesta M68 Verkkotunnusmääräys	FI-verkkotunnusvälittäjille on laadittu opas, jossa on ohjeistettu tietoturvavelvollisuuksien toteuttamisesta ja varautumissuunnitelman tekemisestä. Suositus DNSSEC käytöstä. Lisäksi viraston määräysten perustelumuistioissa on runsaasti neuvontaa, jota voi luonnehtia ohjeeksi tai suositukseksi.	
Ilmailu	Ilmailulaki 864/2014 128 a §, 128 b §	Yhteiseurooppalainen sääntely on valmisteilla.	Yhteiseurooppalainen sääntely ja sen suositukset ovat työn alla.	Traficom
Raideliikenne	Raideliikennelaki 1302/2018 169 §		Suositus raideliikenteen kyberturvallisuuden edistämisestä (Traficom)	Traficom
Merenkulku	Laki eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta 485/2004 7 e §, 7 f § Alusliikennepalvelulaki 623/2005 16 §, 18 a §			Traficom
Tieliikenne	Laki liikenteen palveluista 320/2017 140 § (tieliikenteen ohjaus- ja hallintapalvelun tarjoajat) 161 § (älykkään liikennejärjestelmän ylläpitäjät)	Tietunnelien hallinnointia ja turvallisuutta koskevat määräykset ja ohjeet (Liikenneviraston ohjeita 33/2016)	Tietunnelien osalta on ohje vakavien vaaratilanteiden ja onnettomuuksien raportoinnista (Liikenneviraston ohjeita 17/2015) jota sovelletaan myös tietoturvapoikkeamien raportointiin tunnelikohteissa.	Traficom

Tietoturvavaatimuksia koskeva sääntely kriittisillä toimialoilla*

Lain nojalla ei ole annettu tietoturvaa koskevaa alemman asteista velvoittavaa sääntelyä (asetus / määräys)
Pykälä sisältää asetuksen tai määräyksenantovaltuutuksen tietoturvavaatimuksista
Lakia täydentää delegoitu EU-asetus

* Taulukossa on huomioitu erityisesti toimialojen erityislainsäädännön vaatimuksia. Lisäksi toimialoilla sovelletaan myös yleislaeista, kuten yleisestä tietosuoja-asetuksesta, johtuvia vaatimuksia.

Toimiala	Lainsäädäntö	Asetukset / määräykset	Ohjeet / muut ei velvoittavat	Valvoja
Julkinen sektori	Tiedonhallintalaki 906/2019 18 § TORI-laki 1226/2013 2 §, 4 §, 5 § Laki digitaalisten palvelujen tarjoamisesta 306/2019 4 § Laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista 571/2016 16 §, 17 §, 18 §, 22 § Laki väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista 661/2009 44 § 5 luku Kuntalaki 410/2015 98 §, 99 a § Julkisuuslaki 621/1999 6 luku, 7 luku Laki kansainvälisistä tietoturvallisuusvelvoitteista 588/2004 3 luku, 9 §, 10 § Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista 1406/2011	Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa 1101/2019	Tiedonhallintalautakunta on vuonna 2020 julkaissut suosituksia, jotka opastavat tiedonhallintayksiköitä ja viranomaisia laissa ja asetuksessa säädettyjen tietoturvallisuusvaatimusten toteuttamisessa.	VM

Liite 2

Työryhmän kokoonpano

Puheenjohtaja:	Ylijohtaja Laura Vilkkonen, Liikenne- ja viestintäministeriö
Varapuheenjohtaja:	Turvallisuusyksikön johtaja Elina Immonen, Liikenne- ja viestintäministeriö
Jäsenet:	Kyberturvallisuusjohtaja Rauli Paananen, Liikenne- ja viestintäministeriö
	Hallitusneuvos Joni Komulainen, sosiaali- ja terveysministeriö (varajäsen erityisasiantuntija Marja Penttilä, sosiaali- ja terveysministeriö)
	Tietohallintoneuvos Tuija Kuusisto, valtiovarainministeriö (varajäsen hallitussihteeri Jonna Kuparinen, valtiovarainministeriö)
	Ylitarkastaja Tatu Pahkala, työ- ja elinkeinoministeriö (varajäsen ylitarkastaja Bettina Lemström, työ- ja elinkeinoministeriö)
	Lainsäädäntöneuvos Virpi Koivu, oikeusministeriö (varajäsen johtava asiantuntija Johanna Järvinen, oikeusministeriö)
	Neuvotteleva virkamies Katri Saukkonen, maa- ja metsätalousministeriö
	Tietohallintojohtaja Ari Uusikartano, ulkoministeriö (varajäsen turvallisuuspolitiikan yksikön päällikkö Sari Rautio, ulkoministeriö)
	Tietoturvapäällikkö Harri Mäntylä, puolustusministeriö (varajäsen everstiluutnantti Lauri Noronen, puolustusvoimat)
	Johtaja Jukka-Pekka Juutinen, Liikenne- ja viestintävirasto

Poliisitarkastaja Kimmo Ulkuniemi, Poliisihallitus

Apulaistietosuojavaltuutettu Jari Råman, Tietosuojavaltuutetun toimisto (varajäsen ylitarkastaja Erika Leinonen, Tietosuojavaltuutetun toimisto)

Johtaja Sauli Savisalo, Huoltovarmuuskeskus

Sihteeristö: Neuvotteleva virkamies Olli Lehtilä, Liikenne- ja viestintäministeriö

Lainsäädäntöneuvos Piia Nyström, Liikenne- ja viestintäministeriö

Johtava asiantuntija Niko-Matti Ronikonmäki, Liikenne- ja viestintäministeriö

Liite 3

Valtiovarainministeriön eriävä mielipide

Linjauksen numero 24 tulisi olla seuraava: ” 24. Arvioidaan valtion yhteisten tieto- ja viestintäteknisten palveluiden tuottajien tietosuojaa ja tietoturvaa koskevia vastuita ja velvoitteita. Lähtökohtana on, että yhteisille palveluille asetetaan palvelukohtaisesti turvallisuus, tietosuoja sekä toimintavarmuusvaatimukset ja palvelujen vaatimuksenmukaisuus arvioidaan.”

Perustelut

Valtion tieto- ja viestintäteknisten palvelujen ja palvelutuottajien ohjaus kuuluu valtiovarainministeriön tehtäviin. Niiden tietoturvallisuuden ja varautumisen vaatimusten asettaminen ja valvonta kuuluu tähän ohjaukseen. Tiedonhallintalaissa säädetään tiedonhallintayksiköiden, kuten Valtorin ja muiden valtion virastojen ja laitosten, tietoturvallisuuden vähimmäistason vaatimuksista. Näiden kanssa päällekkäisiä velvoittavia vaatimuksia ei voi olla. Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista on myös valtiovarainministeriön toimialaan kuuluva laki. Viranomaisten tietoturvallisuuden arviointiin ja auditointiin liittyvien menettelyjen kehittäminen on arvioitava tämän lainsäädännön kehittämisen yhteydessä. Ennen perusteellista arviota menettelyissä mahdollisesti sovellettavien lainsäädännön velvoitteita tarkentavien alemman tason säädösten tai muiden vaatimusten tai kriteerien taloudellisesta ja toiminnallisesta vaikutuksesta palvelutuotantoon, ei arviointia voida kiinnittää mihinkään muuhun kuin voimassa olevaan lainsäädäntöön eikä tällaista lähtökohtaa antavaa linjausta tai päätöstä voida tehdä.

Tuija Kuusisto, tietohallintoneuvos, Julkisen hallinnon ICT, Valtiovarainministeriö

Lähteet

Acquist, Alessandro, Taylor, Curtis ja Wagman, Liad (2016): The Economics of Privacy. Journal of Economic Literature, 54, 442-492.

Allingham, Michael G. ja Sandmo, Agnar (1972): Income Tax Evasion: A Theoretical Analysis. Journal of Public Economics, 1, 323-338.

Brown, Ian (2016): The economics of privacy, data protection and surveillance teoksessa Bauer, Johannes M. ja Latzer Michael (toim.) Handbook on the economics of the internet. ElgarOnline.

Heino, Ossi, Jukarainen, Pirjo, Kalalahti, Joanna, Kekki, Tuula, Mansikkamäki, Suvi-Tuuli, Takala, Annina ja Verho, Pekka (2019): Kriittisen infrastruktuurin haavoittuvuus ja viranomaisen toimintakyky. KIVI-hankkeen loppuraportti.

Huoltovarmuusorganisaation Digipooli (2020):Kyberturvallisuuden nykytila eri toimialoilla – kartoituksen keskeiset havainnot.

Hsu, Carol, Wang, Tawei ja Lu, Ang (2016): The Impact of ISO 27001 Certification on Firm Performance. 2016 49th Hawaii International Conference on System Sciences, 4842-4848.

Iivanainen, Tuomas (2019): ISO/IEC 27001 –tietoturvasertifikaatin kokonaiskustannukset. Opinnäytetyö, liiketalouden koulutusohjelma, Satakunnan ammattikorkeakoulu.

Jonkeren, Olaf, Azzini, Ivano, Galbusera, Luca, Ntalampiras, Stavros ja Giannopoulos, Georgios (2015): Analysis of Critical Infrastructure Network Failure in the European Union: A Combined Systems Engineer and Economic Model. Networks and Spatial Economics, 15, 252-270.

Jonkeren, Olaf ja Giannopoulos, Georgios (2014): Analysing Critical Infrastructure Failure with a Resilience Inoperability Input-Output Model. Economic Systems Research, 26, 39-59.

Kröger, Wolfgang ja Zio, Enrico (2011): Vulnerable Systems. London: Springer.

Liikenne- ja viestintävirasto Traficom (2020): Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri). Traficomin julkaisuja 13/2020.

Moore, Tyler (2010): The economics of cybersecurity: Principles and policy options. International Journal of Critical Infrastructure Protection, 3, 103-117.

Oikeusministeriö (2019): Viranomaisen toimivaltuudet häiriötilanteissa. Oikeusministeriön julkaisuja 2019:18.

Oughton, Edward J., Ralph, Daniel, Pant, Raghav, Leverett, Eireann, Copic, Jennifer, Thacker, Scott, Dada, Rabia, Ruffle, Simon, Tuveson, Michelle ja Hall, Jim W. (2019): Stochastic Counterfactual Risk Analysis for the Vulnerability Assessment of Cyber-Physical Attacks on Electricity Distribution Infrastructure Networks. Risk Analysis, 39, 2012- 2031.

Rinaldi, Steven M., Peerenboom, James P. ja Kelly, Terrence K. (2001): Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies. IEEE Control Systems Magazine, December 2001, 11-25.

Romanosky, Sasha ja Acquisti, Alessandro (2009): Privacy Costs and Personal Data Protection: Economic and Legal Perspectives. Berkeley Technology Law Journal, 24, 1061-1102.

Sen, Ravi (2018): Challenges to Cybersecurity: Current State of Affairs. Communications of the Association for Information Systems, 43, 22-44.

Sisäministeriö (2017): Tietoverkkorikollisuuden torjuntaa koskeva selvitys. Sisäministeriön julkaisuja 14/2017.

Slemrod, Joel (2018): Tax Compliance and Enforcement. NBER Working Paper 24799.

Turvallisuuskomitea (2019): Suomen kyberturvallisuusstrategia 2019. Valtioneuvoston periaatepäätös, 3.10.2019.

Valtiovarainministeriö (2020): Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelma 2020-2023 (Haukka). Valtiovarainministeriön julkaisuja 2020:33.

Twitter: @lvm.fi
Instagram: lvmfi
Facebook.com/lvmfi
Youtube.com/lvm.fi
LinkedIn: Liikenne- ja viestintäministeriö

lvm.fi

LIIKENNE- JA
VIESTINTÄMINISTERIÖ

ISSN 1795-4045
ISBN 978-952-243-614-6