



VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Julkisen hallinnon digitaalinen turvallisuus

Julkisen hallinnon ICT

Valtiovarainministeriön julkaisuja – 2020:23

Valtiovarainministeriön julkaisuja 2020:23

Julkisen hallinnon digitaalinen turvallisuus

Valtiovarainministeriö

ISBN PDF: 978-952-287-857-1

Taitto: Valtioneuvoston hallintoyksikkö, Julkaisutuotanto

Helsinki 2020

Kuvailulehti

Julkaisija	Valtiovarainministeriö	8.4.2020
Tekijät		
Julkaisun nimi	Julkisen hallinnon digitaalinen turvallisuus	
Julkaisusarjan nimi ja numero	Valtiovarainministeriön julkaisuja 2020:23	
Diaari/hankenumero	VN/1465/2020	Teema Julkisen hallinnon ICT
ISBN PDF	978-952-287-857-1	ISSN PDF 1797-9714
URN-osoite	http://urn.fi/URN:ISBN:978-952-287-857-1	
Sivumäärä	42	Kieli suomi
Asiasanat	julkisen hallinnon ICT, tietopolitiikka, riskienhallinta, kyberturvallisuus, varautuminen, tieto- ja viestintäteknikka	
Tiivistelmä	<p>Julkisen hallinnon digitaalisen turvallisuuden periaatepäätöksessä määritetään kehittämisen periaatteet ja keskeiset palvelut turvallisuuden edistämiseksi digitaalisessa toimintaympäristössä. Tavoitteena on kokonaisturvallisuuden viitekehyksessä suojata kansalaisia, yhteisöjä ja yhteiskuntaa niiltä riskeiltä ja uhkilta, jotka voivat kohdistua tietoihin, palveluihin ja yhteiskunnan toimintaan digitaalisessa toimintaympäristössä. Kansalaisten, yritysten ja yhteisöjen tulee voida luottaa eettisesti kestäviin, avointa ja läpinäkyvää toimintaa tukeviin ja turvallisiin julkisen hallinnon palveluihin. Suomi tunnetaan edelläkävijänä sekä yhteiskunnan digitalisoitumisen edellytysten osalta että kansalaisten ja yhteisöjen digitaalisten palveluiden tarjoajana. Digitalisoitumiseen sekä digitaalisen toiminnan ja palveluiden turvaamiseen on siten panostettava tasapainoisesti.</p> <p>Periaatepäätös ja sen linjauksia edistävä toimeenpanosuunnitelma valmisteltiin valtiovarainministeriön asettamassa poikkihallinnollisessa koordinaatioryhmässä. Digitaalisen turvallisuuden kehittämisen koordinaatiota ja yhteistyötä sekä taloudellisen vaikuttavuuden arviointia vahvistetaan. Kansalaisten ja henkilöstön osaamista sekä palveluiden turvallisuutta edistetään. Tämä tukee kyberturvallisuusstrategian 2019 toteuttamista julkisessa hallinnossa.</p> <p>Tietohallintoneuvos Tuija Kuusisto Valmisteluryhmän puheenjohtaja</p>	
Kustantaja	Valtiovarainministeriö	
Julkaisun jakaja/myynti	Sähköinen versio: julkaisut.valtioneuvosto.fi Julkaisumyynti: vnjulkaisumyynti.fi	

Presentationsblad

Utgivare	Finansministeriet	8.4.2020	
Författare			
Publikationens titel	Digital säkerhet inom den offentliga förvaltningen		
Publikationsseriens namn och nummer	Finansministeriets publikationer 2020:23		
Diarie-/ projektnummer	VN/1465/2020	Tema	Offentliga förvaltningens ICT
ISBN PDF	978-952-287-857-1	ISSN PDF	1797-9714
URN-adress	http://urn.fi/URN:ISBN:978-952-287-857-1		
Sidantal	42	Språk	finska
Nyckelord	offentliga förvaltningens IKT, informationspolitik, riskhantering, cybersäkerhet, beredskap, informations- och kommunikationsteknik		
Referat	<p>I ett principbeslut om digital säkerhet inom den offentliga förvaltningen fastställer statsrådet principer för utvecklingsarbetet och de centrala tjänsterna för att främja säkerhet i en digital miljö. Målet är att inom ramen för den övergripande säkerheten skydda medborgarna, sammanslutningarna och samhället mot de risker och hot som kan riktas mot information, tjänster och samhällets verksamhet i en digital miljö. Medborgare, företag och sammanslutningar ska kunna lita på att den offentliga förvaltningens tjänster är etiskt hållbara, stöder en öppen och transparent verksamhet och är säkra. Finland känt som en föregångare både när det gäller förutsättningarna för digitaliseringen i samhället och som tillhandahållare av digitala tjänster för medborgare och sammanslutningar. Vi måste på ett välbalanserat sätt satsa på digitalisering och på att den digitala verksamheten och tjänsterna är säkra.</p> <p>Principbeslutet och genomförandeplanen, som ska stödja riktlinjerna i det, bereddes i en förvaltningsövergripande samordningsgrupp tillsatt av finansministeriet. Samordningen och samarbetet för att utveckla den digitala säkerheten och bedömningen av de ekonomiska effekterna ska förbättras. Medborgarnas och personalens kompetens samt tjänsternas säkerhet ska stärkas. Detta arbete stöder genomförandet av strategin för cybersäkerhet (2019) i den offentliga förvaltningen.</p> <p>Tuija Kuusisto informationsförvaltningsråd beredningsgruppens ordförande</p>		
Förläggare	Finansministeriet		
Distribution/ beställningar	Elektronisk version: julkaisut.valtioneuvosto.fi Beställningar: vnjulkaisumyynti.fi		

Description sheet

Published by	Ministry of Finance	8 April 2020	
Authors			
Title of publication	Digital security in public sector		
Series and publication number	Publications of the Ministry of Finance 2020:23		
Register number	VN/1465/2020	Subject	Public Sector ICT
ISBN PDF	978-952-287-857-1	ISSN (PDF)	1797-9714
Website address (URN)	http://urn.fi/URN:ISBN:978-952-287-857-1		
Pages	42	Language	Finnish
Keywords	public administration ICT, information policy, risk management, cybersecurity, preparedness, information and communications technologies		
Abstract	<p>The Government Resolution on digital security in public sector defines the principles of development and key services for advancing security in the digital environment. Within the framework of comprehensive security, the goal is to protect citizens, communities and society from the risks and threats that may affect information, services and the functioning of society in the digital environment. Citizens, businesses and communities must be able to rely on ethically sustainable public services that support open and transparent activities and are secure. Finland is known as a leader both in terms of the prerequisites for the digitalisation of society and in providing digital services for citizens and communities. A balanced approach to digitalisation and ensuring the security of digital activities and services is therefore needed.</p> <p>The Government Resolution and the implementation plan to advance its policies were prepared by an intersectoral coordination group set up by the Ministry of Finance. In line with these, measures are being taken to strengthen coordination and cooperation on the development of digital security and improve economic impact assessment practices. A further objective is to promote the skills of citizens and staff and the security of services. This supports the implementation of the cybersecurity strategy for 2019 in public administration.</p> <p>Tuija Kuusisto Senior Ministerial Adviser Chair of the preparation group</p>		
Publisher	Ministry of Finance		
Distributed by/ Publication sales	Online version: julkaisut.valtioneuvosto.fi Publication sales: vnjulkaisumyynti.fi		

Sisältö

Yhteenveto	9
Julkisen hallinnon digitaalisen turvallisuuden kehittämisen periaatteet ja keskeiset palvelut	11
Liitteet	16
Liite 1. Termit.....	16
Liite 2. Digitaalisen turvallisuuden nykytilasta.....	18
Liite 3. Julkisen hallinnon digitaalisen turvallisuuden kansainvälinen vertailu.....	26
Liite 4. Julkisen hallinnon digitaalisen turvallisuuden toimijat ja tehtävät	30
Liite 5. Valmisteluryhmä	40

Yhteenveto

Kansalaisten, yritysten ja yhteisöjen tulee voida luottaa eettisesti kestäviin, avointa ja läpinäkyvää toimintaa tukeviin ja turvallisiin julkisen hallinnon palveluihin. Digitalisoitumisen nopea edistyminen, tietojen laittomaan käyttöön ja virheellisillä tiedoilla vaikuttamiseen liittyvät uhkat sekä lisääntynyt kansallinen ja kansainvälinen keskinäisriippuvuus asettavat uusia vaatimuksia koko julkisen hallinnon digitaaliselle turvallisuudelle ja sen ohjaukselle. Tämän johdosta on perusteltua linjata digitaalisen turvallisuuden kehittämisestä julkisessa hallinnossa, sekä suunnitella ja toteuttaa linjausten mukaiset kehittämistehtävät. Näin tarkennetaan kyberturvallisuusstrategiaa 2019 julkisen hallinnon osalta sekä tuetaan myös käynnistymässä olevaa kyberturvallisuusstrategian kehittämisohjelman valmistelua ja toteuttamista.

Digitaalisen turvallisuuden tavoitteena on kokonaisturvallisuuden viitekehyksessä suojata kansalaisia, yhteisöjä ja yhteiskuntaa niiltä riskeiltä ja uhkilta, jotka voivat kohdistua henkilötietoihin ja kansalaisten palveluihin sekä yhteiskunnan ja viranomaisten toimintaan, prosesseihin, palveluihin ja tietoaisteihin digitaalisessa toimintaympäristössä. Julkisen hallinnon digitaalisen turvallisuuden kehittämisen periaatteet ovat:

- Johdamme digitaalisen yhteiskunnan turvallisuutta yhdessä tilannetietoon ja riskiarvioon perustuen.
- Suunnittelemme ja seuraamme julkisen hallinnon digitaalisen turvallisuuden vaikuttavuutta ja kustannuksia.
- Kehitämme kansalaisten ja henkilöstön ymmärrystä digitaalisen turvallisuuden riskien vaikutuksista ja vastuista.
- Edistämme digitaalista turvallisuutta julkisen hallinnon, yhteisöjen ja kansalaisten yhteistyönä.
- Vaikutamme EU- ja kansainväliseen digitaaliseen turvallisuuteen ja hyödynnämme yhteistyön tuloksia.
- Edellytämme teknologioilta ja palvelutuotannolta turvallisuutta.

Keskeiset kehitettävät toiminnan prosesseja ja palveluita tukevat digitaalisen turvallisuuden palvelut ovat: julkisen hallinnon digitaalisen turvallisuuden kansallinen ja

kansainvälinen yhteistoimintamalli sekä riskien hallinta, kunnille tarkoitetut yhteiset digitaalista turvallisuutta edistävät palvelut, digitaalisen identiteetin hallinta, kansalaisten ja henkilöstön osaamisen kehittäminen, julkisen hallinnon digitaalisen turvallisuuden asiantuntijapalvelut, palveluiden ja palvelutuotannon digitaalisen turvallisuuden arviointi, digitaalisen infrastruktuurin suojaaminen sekä autonomisten ja oppivien järjestelmien ja palveluiden turvallinen kehittäminen.

Yhteiskunnan toiminta ja palvelut sekä tiedon yhteiskäyttö perustuvat keskinäiselle luottamukselle turvallisuuden hallinnasta. Turvallisuusongelmat julkisen hallinnon digitaalisissa palveluissa voivat rapauttaa kansalaisten ja yhteisöjen luottamuksen viranomaisiin. Yhteiskunnan on tämän vuoksi panostettava digitalisoitumiseen sekä digitaalisen toiminnan ja palveluiden turvaamiseen tasapainoisesti. Digitaalisen turvallisuuden kehityshankkeiden tavoitteiden tulee hyödyttää yhteiskuntaa ja hyötyjen tulee olla mitattavissa.

Julkisen hallinnon digitaalisen turvallisuuden kehittämisen periaatteet ja keskeiset palvelut

Kansalaisten, yritysten ja yhteisöjen tulee voida luottaa eettisesti kestäviin, avointa ja läpinäkyvää toimintaa tukeviin ja turvallisiin julkisen hallinnon palveluihin. Kansainvälisten digitalisointumista koskevien arviointien perusteella Suomi tunnetaan edelläkävijänä sekä yhteiskunnan digitalisoinnin edellytysten osalta¹ että kansalaisten ja yhteisöjen digitaalisten palveluiden tarjoajana². Kyberturvallisuuden hallintaa ja varautumista koskevissa kansainvälisissä arvioinneissa³ Suomi on sijoittunut lähelle kärkivaltioita.

Kyberturvallisuusstrategiassa 2019 asetetaan keskeisimmät kansalliset tavoitteet kybertoimintaympäristön kehittämiseksi ja siihen liittyvien elintärkeiden toimintojen turvaamiseksi. Usein digitaalisen toimintaympäristön turvallisuudella eli digitaalisella turvallisuudella tarkoitetaan samaa kuin kyberturvallisuudella. Digitaalisen turvallisuuden viitekehykseen sisältyy niin kyberturvallisuuteen kuin riskienhallintaan, toiminnan jatkuvuudenhallintaan ja varautumiseen, tietoturvaluuteen ja tietosuojaan liittyviä asioita. Digitaalisen turvallisuuden tavoitteena on kokonaisturvallisuuden viitekehyksessä suojata kansalaisia, yhteisöjä ja yhteiskuntaa niiltä riskeiltä ja uhkilta, jotka voivat kohdistua henkilötietoihin ja kansalaisten palveluihin sekä yhteiskunnan ja viranomaisten toimintaan, prosesseihin, palveluihin ja tietoaisteistoihin digitaalisessa toimintaympäristössä. Julkisen hallinnon digitaalisen turvallisuuden linjauksilla turvataan koko julkista hallintoa ja sen palveluiden toimivuutta rajoittumatta yhteiskunnan elintärkeiden toimintojen turvaamiseen.

Digitalisoinnin nopea edistyminen, tietojen laittomaan käyttöön ja virheellisillä tiedoilla vaikuttamiseen liittyvät uhkat sekä lisääntynyt kansallinen ja kansainvälinen keskinäisriippuvuus kasvattavat yhteiskunnan haavoittuvuutta sekä asettavat uusia vaatimuksia

1 EU (2019) The Digital Economy and Society Index (DESI)

2 United Nations (2018) E-Government Survey 2018, Gearing E-Government to Support Transformation Towards Sustainable and Resilient Societies. United Nations, Economic & Social Affairs

3 International Telecommunications Union (2019) Global Cybersecurity Index (GCI); e-Governance Academy (2019) National Cyber Security Index (NCSI)

koko julkisen hallinnon digitaaliselle turvallisuudelle ja sen ohjaukselle. Tarve kansalliselle ja kansainväliselle yhteistyölle ja ymmärrykselle sekä turvallisuustekijöiden huomioimiselle julkisen hallinnon, yritysten, järjestöjen ja kansalaisten muodostamissa ekosysteemeissä on yhä suurempi. Tämän johdosta on perusteltua linjata digitaalisen turvallisuuden kehittämisestä julkisessa hallinnossa, sekä suunnitella ja toteuttaa linjausten mukaiset kehittämistehtävät. Näin tuetaan myös käynnistymässä olevaa kyberturvallisuusstrategian 2019 kehittämisohjelman valmistelua ja toteuttamista, sekä osaltaan pannaan täytäntöön valtioneuvoston päätöstä huoltovarmuuden tavoitteista (1048/2018). Tavoitetasolla julkisen hallinnon toiminta, digitaaliset palvelut ja tiedot sekä niiden tarvitsema infrastruktuuri ovat luotettavia, ja palveluiden sekä tietojen luottamuksellisuus, eheys ja saatavuus on turvattu. Digitaalinen turvallisuus mahdollistaa myös uusien palveluiden kehittämisen ja näiden turvallisuuden.

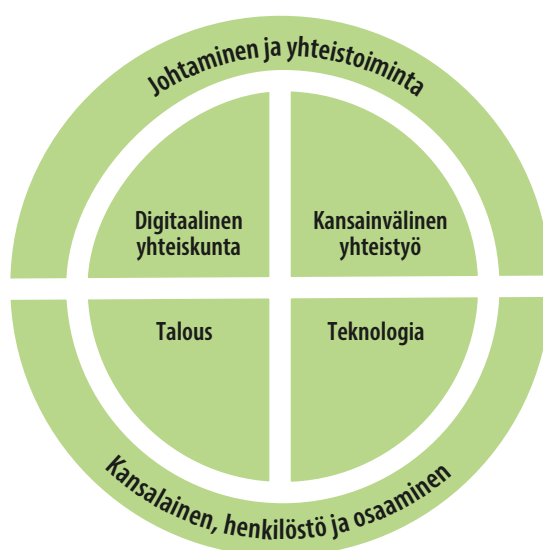
Kansainvälisessä vertailussa arvioitiin Suomeen verrattuna digitaalisen turvallisuuden ohjausta, tehtäviä, rakenteita, riskejä ja resursseja Alankomaissa, Australiassa, Isonsa-Britanniassa, Israelissa, Ruotsissa, Saksassa, Venäjällä ja Virossa⁴. Verrokkivaltioissa lainsäädäntöä on pyritty kehittämään vastaamaan digitaalisen toimintaympäristön nopeita muutoksia. Digitaalisen turvallisuuden johtamista keskitetään ja virastoja yhdistetään suuremmiksi kokonaisuuksiksi. Vertailun perusteella Suomen tulee arvioida digitaalisen turvallisuuden johtamisrakenteita, vastuita ja rooleja sekä uudistaa niitä kansainvälisen kehityksen mukaisesti. Verrokkivaltioissa digitaalisen turvallisuuden aktiivisina toimijoina tunnustetaan yleisesti julkinen hallinto, elinkeinoelämä, korkeakoulut ja tutkimuslaitokset sekä kansalaiset. Näillä kaikilla tulee olla aktiivinen rooli digitaalisen turvallisuuden toimijoina. Digitaalisen turvallisuuden taitojen kehittämisen tulee olla strateginen painopiste koko yhteiskunnan laajuisesti. Hallinnolle, kansalaisille ja yhteisöille on tarjottava tukea tunnistettuihin digitaalisen turvallisuuden häiriötilanteisiin. Suomen tulee kuvata digitaaliseen turvallisuuteen liittyvät uhkat selkeästi kaikkien yhteiskunnan toimijoiden ymmärtämään muotoon. Verrokkivaltioissa digitaalinen infrastruktuuri nähdään osana palvelurakenteita ja digitaalinen turvallisuus osana palvelukokonaisuutta. Palveluntarjoajan tulee vastata digitaalisen turvallisuuden vaatimuksista sekä taata turvallinen palvelun käyttö. Suomessa tulee systemaattisesti edellyttää digitaalisen turvallisuuden kansainvälisten standardien soveltamista.

Julkisen hallinnon digitaalisen turvallisuuden nykytilaselvityksen ja kansainvälisen vertailun perusteella on valittu julkisen hallinnon kehittämisalueet ja kehittämisen periaatteet sekä keskeisiä hallinnon toimintaa ja prosesseja tukevat digitaalisen turvallisuuden palvelut. Julkisen hallinnon digitaalisen turvallisuuden palveluita keskeisesti edistävät tehtävät kuvataan julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelmassa

4 Digitaalisen turvallisuuden kansainvälinen vertailu, KPMG, helmikuu 2020

2020–2023. Toimeenpanosuunnitelmaa ylläpidetään tarvittaessa toimintaympäristön muutosten ja kyberturvallisuusstrategian 2019 kehittämisohjelman asettamien vaatimusten mukaisesti.

Julkisen hallinnon digitaalisen turvallisuuden **kehittämisaalueet** ovat: johtaminen ja yhteistoiminta; digitaalinen yhteiskunta; kansainvälinen toiminta; talous; teknologia; kansalainen, henkilöstö ja osaaminen:



Kehittämisaalueisiin liittyvät julkisen hallinnon digitaalisen turvallisuuden kehittämisen periaatteet ovat:

- Johdamme digitaalisen yhteiskunnan turvallisuutta yhdessä **tilannetietoon** ja **riskiarvioon** perustuen.
- Suunnittelemme ja seuraamme julkisen hallinnon digitaalisen turvallisuuden **vaikuttavuutta** ja **kustannuksia**.
- Kehitämme kansalaisten ja henkilöstön **ymmärrystä** digitaalisen turvallisuuden riskien vaikutuksista ja vastuista.
- Edistämme digitaalista turvallisuutta julkisen hallinnon, yhteisöjen ja kansalaisten **yhteistyönä**.
- Vaikutamme **EU- ja kansainväliseen** digitaaliseen turvallisuuteen ja hyödynnämme yhteistyön tuloksia.
- Edellytämme **teknologioilta** ja palvelutuotannolta turvallisuutta.

Keskeiset kehitettävät toiminnan prosesseja ja palveluita tukevat **digitaalisen turvallisuuden palvelut** ovat:

1. Julkisen hallinnon digitaalisen turvallisuuden kansallinen ja kansainvälinen yhteistoimintamalli
Kansallisen ja kansainvälisen yhteistyön kautta tehostetaan digitaalisen turvallisuuden koordinoitua ja vaikuttavuutta sekä edistetään Suomen kilpailukykyä.
2. Julkisen hallinnon digitaalisen turvallisuuden riskien hallinta
Digitaalisen turvallisuuden nykytila-arvion ja kokonaiskuvan perusteella tuotettavien riskianalyyseiden ja vaikutusarviointien avulla valitaan kehityskohteet, joihin suunnataan resursseja.
3. Kunnille tarkoitetut yhteiset, digitaalista turvallisuutta edistävät palvelut
Kuntien digitaalisen turvallisuuden kehittämisen tiekarttaa ylläpidetään ja sen toteutumista seurataan.
4. Digitaalisen identiteetin hallinta
Edistetään Suomen kansalaisille ja kaikille Suomessa asuville mahdollisuutta sähköiseen tunnistautumiseen. Edistetään toimivien sähköisten tunnistusratkaisujen kehittymistä, jotka mahdollistavat erilaisten välineiden käytön.
5. Kansalaisten ja henkilöstön osaamisen kehittäminen
Kehitetään julkisen hallinnon ja yhteisöjen kaikkien henkilöryhmien sekä yksityisten kansalaisten digitaalisen turvallisuuden taitoja ja tietoisuutta.
6. Julkisen hallinnon digitaalisen turvallisuuden asiantuntijapalvelut
Digitaalisen turvallisuuden keskitettyjä asiantuntijapalveluita kehitetään ja tarjotaan laajasti koko julkisen hallinnon käyttöön.
7. Julkisen hallinnon palveluiden ja palvelutuotannon digitaalisen turvallisuuden arviointi
Edistetään normeihin ja standardeihin perustuvaa digitaalisten palveluiden ja palvelutuottajien arviointia ja varmentamista.
8. Julkisen hallinnon tarvitseman digitaalisen infrastruktuurin suojaaminen
Keskeisten yhteisten teknologioiden ja palveluiden turvallisuutta edistetään siten, että julkisen hallinnon toiminnan, prosessien ja palveluiden jatkuvuus ja tiedot ovat turvatut.
9. Julkisen hallinnon autonomisten ja oppivien järjestelmien sekä palveluiden turvallinen kehittäminen
Autonomisten ja oppivien järjestelmien sekä digitaalisten palveluiden turvallisuudesta huolehditaan riskienhallinnan avulla.

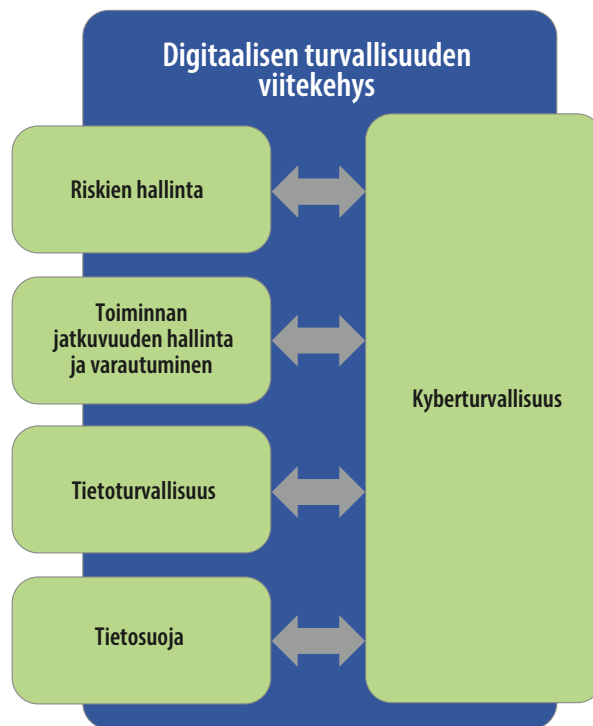
Julkisen hallinnon digitaalisen turvallisuuden kehittämisen periaatteiden toteuttamisella tavoiteltava muutos on strategisen ja operatiivisen tason digitaalisen turvallisuuden kehittämisen ohjauksen, koordinaation ja yhteistyön vahvistaminen ja ulottaminen koko julkisen hallinnon alueelle. Tämän ilmentymiä ovat uusi julkisen hallinnon digitaalisen turvallisuuden strategisen tason ohjausryhmä sekä julkisen hallinnon digitaalisen turvallisuuden toiminnallisen tason kehittämisen ohjauksen vahvistaminen ja kuntien digitaalisen turvallisuuden tiekartan kautta tapahtuvan kehittämisen ohjaus.

Kehittämistä mahdollistetaan kansalaisten ja henkilöstön osaamisen kasvattamisen ja harjoitustoiminnan sekä asiantuntijapalveluiden saatavuuden parantamisen avulla. Lisäksi toteutetaan turvallisuuden arkkitehtuurin valmisteluun liittyvä palveluiden, prosessien, infrastruktuurin ja tietojen kriittisyysluokittelu sekä kriittisten kehittämiskohteiden tunnistaminen, kehityssuunnitelmien laadinta ja arviointi. Julkisen hallinnon digitaalisen turvallisuuden tilan arvioimiseksi tietoturvallisuuden arvioinnin hallintaa edistetään säädösvalmistelun kautta ja kasvatetaan julkisen hallinnon digitaalisen infrastruktuurin ja palveluiden tilan analysointikykyä. Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelman keskeiset toteuttajat ovat valtiovarainministeriö, Digi- ja väestötietovirasto, ja Liikenne- ja viestintävirasto, sekä hankittavia palveluita tuottavat yritykset.

Liite 1. Termit

Digitaalinen turvallisuus

Usein kyberturvallisuuden synonyymi. Digitaalisen turvallisuuden viitekehykseen sisältyy riskienhallintaan, toiminnan jatkuvuudenhallintaan ja varautumiseen sekä kyberturvallisuuteen, tietoturvaluuteen ja tietosuojaan liittyviä asioita⁵. Terminä uusi ja vakiintumaton. Kansainvälistä yhteisymmärrystä termeistä ei ole.



Digitaalisen turvallisuuden kehittäminen on riskienhallintaan perustuvaa toiminnan jatkuvuuden ja varautumisen, tietoturvaluuden ja tietosuojan avulla tapahtuvaa turvallisuuden kehittämistä, joka samalla on myös kyberturvallisuuden kehittämistä.

Kyberturvallisuus sisältää etenkin kansainvälisissä yhteyksissä myös sellaisia osa-alueita, joihin kohdistuu laajasti muutakin kuin digitaalisen turvallisuuden piiristä lähtevää intressiä. Näitä osa-alueita ovat esimerkiksi kyberdiplomatia, kybervaikuttaminen, kyberresilienssi ja hybrdivaikuttaminen.

⁵ Pilkahduksia tulevaisuuteen, Tietopolitiikka, tekoäly ja robotisaatio hyvinvoinnin ja taloudellisen menestyksen mahdollistajana Suomessa, Valtiovarainministeriön julkaisuja 2019:22

OECD:ssä on käytössä termi digital security⁶, koska se on yhdenmukaisempi termi kuin kyberturvallisuus termien digitalisoituminen, digitaalinen transformaatio ja digitaalinen talous kanssa. Digitaalinen turvallisuus kuten kyberturvallisuuskin vaikuttavat myös fyysisen maailman turvallisuuteen samoin kuin fyysisen maailman kautta vaikutetaan digitaaliseen turvallisuuteen.

- Kyberturvallisuus** Tavoitetilä, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. Kyberturvallisuus tarkoittaa digitaalisen ja verkottuneen yhteiskunnan tai organisaation turvallisuutta ja sen vaikutusta niiden toimintoihin.⁷ Kybertoimintaympäristön synonyyminä voidaan käyttää termiä digitaalinen toimintaympäristö.
- Tietoturvallisuus** Järjestelyt, joilla pyritään varmistamaan tiedon luottamuksellisuus, eheys ja saatavuus⁸.
- Tietosuoja** Ihmisten yksityisyyden suojeleminen ja yksilöä koskevien tietojen suojaaminen oikeudettomalta käytöltä henkilötietoja käsiteltäessä⁹.
- Riskienhallinta** Järjestelmällinen toiminta, joka sisältää riskianalyysin sekä tarvittavien toimenpiteiden suunnittelun, toteutuksen, seurannan ja korjaavat toimenpiteet¹⁰.
- Jäännösriski** Riskiin käsittelyn jälkeen jäävä riski, jota ei voida tai ei haluta poistaa. Jäännösriskeihin voi sisältyä tunnistamattomia riskejä.¹¹
- Jatkuvuudenhallinta** Organisaation prosessi, jolla tunnistetaan toiminnan uhkat ja arvioidaan niiden vaikutukset organisaatiossa ja sen toimijaverkostossa sekä luodaan toimintatapa häiriötilanteiden hallinnalle ja toiminnan jatkuvuudelle kaikissa olosuhteissa¹².
- Varautuminen** Toiminta, jolla varmistetaan tehtävien mahdollisimman häiriötön hoitaminen ja mahdollisesti tarvittavat tavanomaisesta poikkeavat toimenpiteet häiriötilanteissa ja poikkeusoloissa¹³.

6 Digital Security Risk Management for Economic and Social Prosperity, OECD Recommendation and Companion Document, 2015

7 Sanastokeskus TSK TEPA-termipankki, Kyberturvallisuuden sanasto (TSK 52, 2018)

8 Sanastokeskus TSK TEPA-termipankki, Kyberturvallisuuden sanasto (TSK 52, 2018)

9 Sanastokeskus TSK TEPA-termipankki, Tieteen termipankki 06.08.2019

10 Sanastokeskus TSK TEPA-termipankki, Kokonaisturvallisuuden sanasto (TSK 50, 2017)

11 Valtiovarainministeriö, Ohje riskienhallintaan, valtiovarainministeriön julkaisu 22/2017, liite

12 Sanastokeskus TSK TEPA-termipankki, Kyberturvallisuuden sanasto (TSK 52, 2018)

13 Sanastokeskus TSK TEPA-termipankki, Kokonaisturvallisuuden sanasto (TSK 50, 2017)

Liite 2. Digitaalisen turvallisuuden nykytilasta

Pääministeri Sanna Marinin hallitusohjelman mukaisesti julkisen hallinnon strategisen tason johtamista tehostetaan sekä linjataan yhteiskunnan toiminnan turvaamisen kannalta kriittisten tietojen, tietoverkkojen ja tietojärjestelmien kehittämistoimista digitaalisessa toimintaympäristössä. Tuorein valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä on vuodelta 2009. Tämän jälkeen niin julkisen hallinnon rakenteet ja toiminta kuin strategiat, säädökset ja ohjeet ovat muuttuneet merkittävästi ja digitaaliseen toimintaympäristöön kohdistuvat uhkat ovat kasvaneet. Keskeisiä muutoksia ovat yhteiskunnan eri toimijoiden yhteistyön ja keskinäisriippuvuuksien kasvaminen, tieto- ja viestintätekniikan sääntelyn tarkentuminen, tuoreimpana laki julkisen hallinnon tiedonhallinnasta (906/2019), sekä Yhteiskunnan turvallisuusstrategia vuodelta 2017, kyberturvallisuusstrategia vuodelta 2019 ja ICT-palvelutuotannon keskittäminen kunnissa, kuntayhtymissä ja valtion hallinnossa. Valtion tieto- ja viestintätekniikkakeskus Valtori perustettiin vuonna 2014 sekä Digi- ja väestötietovirasto vuonna 2020.

Suomen kyberturvallisuusstrategiassa 2019 asetetaan keskeisimmät kansalliset tavoitteet kybertoimintaympäristön kehittämiseksi ja siihen liittyvien elintärkeiden toimintojen turvaamiseksi. Se nojautuu kyberturvallisuusstrategian 2013 yleisiin periaatteisiin. Kolme strategista linjausta ovat: kansainvälinen yhteistyö, kyberturvallisuuden johtamisen, suunnittelun ja varautumisen parempi koordinaatio sekä kyberturvallisuuden osaamisen kehittäminen. Kyberturvallisuuden voimavarojen kohdentamista ja yhteistoimintaa on tarkoitus parantaa hallituskausien yli ulottuvalla kyberturvallisuuden kehittämisohjelmalla. Ohjelman tavoitteena on konkretisoida kansallisia linjauksia sekä selkiyttää hankkeiden, tutkimuksen ja kehittämisohjelmien kokonaisuutta. Kyberturvallisuuden kansallista kehittämistä koordinoimaan on liikenne- ja viestintäministeriöön perustettu kyberturvallisuusjohtajan tehtävä.

Yhteiskunnassa tapahtuneiden muutosten johdosta, ja Suomen kyberturvallisuusstrategian 2019 tarkentamiseksi julkisen hallinnon osalta, on tarpeen arvioida julkisen hallinnon digitaalisen turvallisuuden nykytilaa ja arvioinnin perusteella linjata digitaalisen turvallisuuden kehittämisestä julkisessa hallinnossa. Julkisen hallinnon digitaalisen turvallisuuden linjausten tavoitteena on turvata koko julkisen hallinnon ja sen palveluiden toimivuus rajoittumatta yhteiskunnan elintärkeiden toimintojen turvaamiseen.

Digitaalinen yhteiskunta

Viime vuosina digitaalinen toimintaympäristö ja sen vaikutukset yhteiskunnan ja julkisen hallinnon toimintaan ovat muuttuneet merkittävästi. Digitalisoitumisen edetessä tietoa on

ryhdytty hyödyntämään yhä laajemmin ja sen käyttöä tehostamaan uusien teknologioiden kuten ohjelmistorobotiikan ja tekoälyn avulla. **Kansalaisille** suunnitellaan tarjottavan ihmiskeskeisiä elämäntapahtumiin perustuvia palveluita ja yhteisöille liiketoimintatapah-tumiin perustuvia palveluita.

Kyberturvallisuuden hallintaa ja varautumista koskevissa kansainvälisissä arvioinneissa¹⁴ Suomi on sijoittunut lähelle kärkivaltioita. Suomessa ei ole tapahtunut laajoja tietovuo-toja. Julkisen hallinnon digitaalisen turvallisuuden kehittämistä tehdään hajautetusti eri hallinnon organisaatioissa. Hallinnon organisaatioiden sisäiset digitaalisen turvallisuuden vastuut ovat useimmiten selkeät. Laajavaikutteisen kyberloukkaustilanteen operatiivista johtamista ei kuitenkaan ole määritelty ja kyberturvallisuuden operatiivisen tilannekuvan muodostamista on syytä parantaa¹⁵. Koko yhteiskuntaa koskevia digitaalisen turvallisuuden linjauksia puuttuu ja vastuunjaot vaativat paikoitellen selkiyttämistä. Päätöksenteon tueksi ei kattavasti käytetä yhteisiä riskienhallinnan menetelmiä.

Keskeisiä kansallisia ja kansainvälisiä digitaalisen turvallisuuden toimijoita ovat ministeriöt, digitaalisen turvallisuuden kysymyksiä käsittelevät viranomaiset ja yhteistyöelimet, sekä digitaalisen turvallisuuden julkiset ja yksityiset palveluiden tuottajat¹⁶ (Liite 4). Digitaalisen turvallisuuden edistäminen **valtion, kuntien, yksityisen sektorin, tutkimusmaailman, kansalaisjärjestöjen ja kansalaisten yhteistyönä** vaatii edelleen kehittämistä nykytilanteeseen verrattuna.

Kansainvälinen toiminta

Digitaalisen turvallisuuden ja kyberturvallisuuden kysymykset ovat yhä kasvavassa määrin kansainvälisen politiikan kysymyksiä, joita poliittiset ristiriidat leimaavat. Kansainvälisessä yhteisössä on viime vuosina herännyt tarve **vahvistaa yhteistyötä** digitaalisen toiminta-ympäristön turvallisuuskysymyksissä. EU:ssa on perustettu EU:n neuvoston pysyvä hori-sontaalinen kyberturvallisuuden työryhmä ja useat muut neuvoston työryhmät käsitte-levät kyberturvallisuuden kysymyksiä oman toimialansa näkökulmasta. Toimintakenttä ei ole staattinen, vaan uusien teknologioiden ja tekoälyn tuomat muutokset näkyvät kan-sainvälisistä pelisäännöistä käytävissä keskustelussa. Suomi osallistuu kansainväliseen kyberturvallisuusyhteistyöhön tavoitteenaan vahvistaa sääntömääräistä kansainvälistä jär-jestystä sekä edistää demokratiaa, sananvapautta ja oikeusvaltioperiaatteen toteutumista.

14 International Telecommunications Union (2019) Global Cybersecurity Index (GCI); e-Governance Academy (2019) National Cyber Security Index (NCSI)

15 Valtiontalouden tarkastusvirasto, Kybersuojauksen järjestäminen, Tarkastuskertomus 16/2017

16 Lehto, Limnell, Kokkomäki, Pöyhönen, Salminen. Kyberturvallisuuden strateginen johtaminen Suomessa. Valtioneuvoston tutkimus- ja selvitystoiminnan julkaisusarja 28/2018

Johtaminen ja yhteistoiminta

Julkisen hallinnon sisäinen sekä julkisen hallinnon ja yhteisöjen välinen yhteistyö digitaalisen turvallisuuden alueella on Suomessa erittäin hyvällä tasolla. Julkisen hallinnon **johtamisen** haasteena on edistää rohkeasti uusien digitaalisten palveluiden käyttööntotoa arvioiden samalla vastuullisesti niihin kohdistuvat riskit sekä käsitellä jäljelle jäävät jäännösriskit. Julkisen hallinnon digitaalisen turvallisuuden tilaa ei arvioida kattavasti. Selkeät periaatteet puuttuvat siitä, mitä digitaalisia palveluita ja digitaalisen turvallisuuden palveluita on perusteltua toteuttaa yhteisesti.

Tekniset ongelmat ja häiriöt, luonnonilmiöt sekä eri tavoin tapahtuva vaikuttaminen edellyttävät jatkuvaa ja kriittisten toimintojen osalta keskitetysti ohjattua toimintavarmuuden kehittämistä. Nykyinen julkisen hallinnon toimialakohtaisesti tapahtunut kehittäminen ei ole johtanut riittävään lopputulokseen. Yhteiskunnan toiminnan kannalta kriittisten tietovarantojen, tietoverkkojen ja palveluiden kehittämistä ei ole ohjattu ja resursoitu keskitetysti eikä kehittämisen tavoitetilaa ole selkeästi asetettu.¹⁷

Nopeasti muuttuvassa toimintaympäristössä tarvittavia joustavia ja jatkuvasti kehitettäviä **yhteistyön edellytyksiä ja toimintamalleja** ei ole riittävästi saatavilla viranomaisten ja yhteisöjen käyttöön. Näitä ovat yhteiset käsitteet ja toimintaperiaatteet, tietojen kriittisyysluokittelu ja digitaalisten palveluiden hallinta sekä vastuu- ja riippuvuuskuvaukset.

Julkisesta hallinnosta puuttuu tietoturvallisuuden **teknistä tarkastamista** järjestävä organisaatio, jonka vastuulla olisi esimerkiksi tunnettujen haavoittuvuuksien kattava skannaaminen. Yhteiskunnan toiminnan jatkuvuuden kannalta välttämätön kaikkien keskeisten toimialojen toimintaedellytysten varmistaminen myös tietoturvallisuusloukkausten ja kyberhäiriöiden varalta on osin riittämätöntä.

Kansalainen, henkilöstö ja osaaminen

Kansalaisten ja asukkaiden rooli yhteiskunnan digitaalisen turvallisuuden tuottajana on ohuelti tunnistettu ja määritetty. Digitaalisessa turvallisuudessa korostuvat asiakaslähtöisyyden sijasta usein teknologiset ratkaisut. Toteutuksissa etsitään vielä menettelyjä, joilla sovitetaan yhteen sekä turvallisuuden että yksityisyyden suojaamisen osittain ristiriitaisetkin tavoitteet.

Osaamisen hankinta ja ylläpito ovat Suomessakin merkittäviä haasteita. Digitaalisen turvallisuuden erityisosaajia on liian vähän ja rekrytointi on vaikeaa niin julkisessa hallinnossa

¹⁷ Uudistuva, vakaa ja kestävä yhteiskunta. Valtiovarainministeriön virkamiespuheenvuoro. Valtiovarainministeriön julkaisuja 2019:11

kuin yksityisillä palveluntuottajillakin. Palveluiden ulkoistuksissa organisaatioiden oman osaamisen kehittyminen siirtyy palvelutoimittajille, mikä heikentää syväosaamisen kehittymistä ja hiljaisen tiedon siirtymistä organisaation sisällä. Julkisen hallinnon henkilöstön digitaalisen turvallisuuden osaamisen kehittämiseksi on saatavilla koulutusmateriaalia, mutta systemaattinen osaamisen kehittämisen taso vaihtelee.

Talous

Julkisen hallinnon digitaalisen turvallisuuden yleisesti käytössä olevaa **investointien kustannus-/hyötymallia** ei ole määritetty, eikä digitaalisen turvallisuuden vaikuttavuutta tunneta tarkasti. Tämä johtuu osittain siitä, että digitaalisen turvallisuuden kehittämisen tarkkaa osuutta tieto- ja viestintätekniikan infrastruktuurin ja palveluiden kehittämisestä on vaikea tunnistaa. Täten digitaalisen turvallisuuden kehittämiseen kohdennettujen taloudellisten resurssien riittävyttä nykytilanteessa on vaikea arvioida. Puutteellisista resursseista aiheutuvat turvallisuuspoikkeamat kuitenkin aiheuttavat useimmiten moninkertaisesti kustannuksia verrattuna siihen, että riskejä kyetään ehkäisemään ennalta tai torjumaan tehokkaasti. Hallinnon toiminnan jatkuvuuden ja luottamuksen menettämisen kustannusta on hankala mitata rahamääräisesti.

Digitalisoitumisen laajeneminen ja ICT-palvelutuotannon keskittyminen ovat tuoneet kustannussäästöjä ja kehittäneet asiakkaiden palveluita, mutta samalla palveluiden jatkuvuuteen, sekä tietojen luotettavuuteen, saatavuuteen ja eheyteen on muodostunut uusia haavoittuvuuksia. Hyökkääjien monimuotoisuus lisääntyy ja hyökkäysten tekninen edistyneisyys kehittyy jatkuvasti, jolloin organisaatioiden kyky reagoida tehokkaasti kasvaviin ulkopuolisiin uhkiin voi heikentyä vakavasti. Palveluita digitalisoitaessa kustannussäästöjen merkitys on korostunut toiminnan muuttuessa. **Riskienhallintaa** ei ole riittävästi käytetty digitaalisen turvallisuuden **vaikuttavuuden arvioinnissa** ja tasapainon saavuttamisessa kustannussäästöjen sekä palveluiden ja niiden turvallisuuden parantamisen välillä.

Teknologiat

Havainnointikyvyn, järjestelmien **valvonnan** ja haavoittuvuuksien hallinnan kehittäminen sekä havaintojen perusteella tapahtuva julkisen hallinnon ja yritysten yhteinen kehittämisen toimeenpano lisäävät resurssitarpeita. Ne myös luovat vaatimusta kohdentaa henkilöstön työaikaa entistä enemmän digitaalisen turvallisuuden tehtäviin. **Proaktiivista tietoturvallisuutta** ja rutiinitehtävien digitaalisen turvallisuuden **automatisointia** ei hyödynnetä laajasti tarvittavan henkilötyöpanoksen vähentämiseksi.

Pilvipalvelut ovat digitaalisen turvallisuuden näkökulmasta sekä mahdollisuus että uhka. Pilvipalveluihin tukeutumalla voidaan kasvattaa joidenkin julkisen hallinnon palveluiden toimintavarmuutta. Pilvipalveluiden käytöllä voidaan mahdollisesti myös ehkäistä

palvelunestohyökkäysten vaikutuksia tehokkaasti. Pilvipalveluiden tietoturvallista käyttöä, sekä tietosuojaa ja toiminnan jatkuvuuden hallintaa koskevia linjauksia ei ole riittävästi, mikä hankaloittaa palveluiden hyödyntämistä julkisessa hallinnossa. Digitalisoituminen kasvattaa jatkuvasti avoimen ja rakenteisen tiedon kysyntää, eivätkä paikalliset ja suljetut tietojärjestelmät tue tätä kehitystä. Tietoturvallisia tiedonkäsittely-ympäristöjä, kuten turvallisia julkisia ja yksityisiä pilvipalveluita tai paikallisia ratkaisuja, joihin data, algoritmit ja jalostettu data voidaan sijoittaa, ei ole saatavilla riittävästi. Pilvipalveluiden haasteina ovat usein eri valtioiden erilaiset säädökset. Tämä aiheuttaa riskejä ja epävarmuutta palveluiden käyttäjille, jos palvelu tuotetaan Suomen ulkopuolelta noudattaen kyseisen maan säädöksiä.

Tekoälyn hyödyntäminen ja kvanttiteknologia ovat uusia teknologioita, joiden käyttö on vielä vähäistä. Tekoälyn kehittämisen yhteydessä käydään keskustelua siitä, miten järjestelmien opettamisessa käytettävä data vaikuttaa tekoälyn toimintaan ja millaisia eettisiä periaatteita tulisi huomioida. **Kvanttitekniikan** kehittymisen nopeutta ja sen käyttöönoton aiheuttamien riskien realisoitumista muun muassa salausalgoritmien purkamisessa on vaikea arvioida.

Uhka-arviot

Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä VAHTI julkaisi vuonna 2019 digitaalisen toimintaympäristön turvallisuusraportin, jonka mukaan keskeiset turvallisuushaasteissa tapahtuneet muutokset osoittavat, että tällä hetkellä eniten organisaatioiden toimintaan vaikuttavat erilaiset – niin pienet kuin laajavaikutteisetkin – **ICT-palvelutuotantoon** liittyvät häiriöt. Tällaisissa tilanteissa palveluiden toiminta tyypillisesti estyy, mikä vaikuttaa samalla palveluiden ja niissä käsiteltävien tietojen saatavuuteen. Näin palvelutuotannon häiriöt ovat usein myös digitaaliseen turvallisuuteen liittyviä häiriöitä.

Säädöksin on pyritty varmistamaan yhteisten, **keskitettyjen digitaalisten palveluiden** ja niiden palvelutuotannon turvallisuus. Digitaalista turvallisuutta ei ole mahdollista toteuttaa aukottomasti, mikä korostaa riskienhallinnan merkitystä osana toiminnan johtamista. Organisaatioiden toimintamalleja digitaalisen turvallisuuden alueella haastavat pyrkimys jatkuvaan ympärivuorokautiseen palveluun, mikä vaatisi toimintakulttuurien yhtenäistämistä sekä esimerkiksi häiriötilanteiden hallinnan selkiyttämistä. Myös yksityishenkilöt ja yhteisöt odottavat usein digitaalisilta palveluilta ympärivuorokautista toimintavarmuutta, mutta valtionhallinnossa ei ole tätä varten tarvittavaa keskitettyä ja jatkuvaa valvomotoimintaa (SOC) ja palveluiden hallintajärjestelmää.

Ulkopuolisten **palveluntuottajien** tuottamien ICT-palveluiden turvallisuuden varmistaminen on organisaatioille haasteellista. Tätä haastetta yritetään hallita sopimuksin, mutta ongelmana on saada monikansallisten toimittajien kanssa tehtäviin sopimuksiin riittäviä

ehtoja. Sekä julkisen hallinnon ulkopuolisten, että hallinnon sisäisten **tuotantoketjujen** haasteina ovat riskitasot, tietoturvaluus, osaaminen ja tuotantokapasiteetti. Yhteisten järjestelmien uhkat ovat jaettuja, mutta substanssi ja riskiprofiilit ovat erilaisia. Kunnissa ja kuntayhtymissä digitaalisen turvallisuuden toimintamalleja ei ole parannettu riittävästi keskeisiksi tunnistettujen ICT-toimittajien kanssa.

Toistuvasti onnistuneet tietoturvaluusloukkaukset julkisen hallinnon organisaatioihin ja yksityishenkilöiden henkilökohtaisten laitteiden valjastaminen näiden loukkausten toteuttamiseen osoittavat, että digitaalisen turvallisuuden vähimmäisvaatimukset eivät kaikilta osin täyty. Tietomurtojen lisäksi myös tunnistautumisen menettelyjen tai **identiteetin hallinnan** käytön hankaluudet heikentävät luottamusta julkisen hallinnon digitaalisiin palveluihin ja vaarantavat käyttäjien turvallisuuden ja yksityisyyden. Julkinen hallinto ei saa siirtää riskejään palveluiden käyttäjien huolehdittavaksi, eivätkä turvallisuusvaatimukset saa estää palveluiden käyttäjien tahtoa toteutumasta¹⁸.

Nykyisellään erilaisten **IoT-laitteiden** sisäänrakennettu tietoturvaluus on usein heikko, kun valmistuksessa tavoitellaan mahdollisimman pieniä kustannuksia. Kyseisiä laitteita kytketään kuitenkin yhä enemmän osaksi teollisuus- ja muita automaattioratkaisuja. Kyberturvaluuskeskuksen tietoturvamerkki, joka osoittaa laitteen täyttävän ainakin tietoturvan perusvaatimukset, on tässä suhteessa merkittävä parannus.

Vanhoissa perustietojärjestelmissä on usein puutteellinen **arkkitehtuuri**, eivätkä teknologiset ratkaisut täytä nykyisiä vaatimuksia. Tilaaja-tuottajamallissa ongelmien paikallistamista hankaloittaa ulkoistetun ja keskitetyn palveluntuotannon yhteydessä usein ilmenevät haasteet kokonaisuuden hallinnassa ja valvonnassa. Digitaalisen turvallisuuden osa-alueiden kehittämisessä ei aina hyödynnetä riittävästi kansainvälisiä standardeja. Esimerkiksi linjauksia tavoitteesta hyödyntää sertifiointeja ja sertifioituja tuotteita hankintojen kilpailutuksissa ei ole riittävästi. Kotimaisten viitekehysten kansainvälisestä yhteensopivuudesta ei huolehdita, vertaa Suomessa laaditut tietoturvaluuden vaatimus-/auditointikriteeristöt.

Uusia innovaatioita ja teknologiaratkaisuja kehitettäessä ei vastuullisuutta ja eettisten pelisääntöjen luomista useinkaan huomioida riittävästi. Turvallisia toimintamalleja ei ole aina integroitu ohjelmistokehityksen, testaamisen ja ylläpidon automatisointiin pyrkivissä kehittämisprosesseissa (DevOps).

18 Palvelujen käyttäjien näkökulmasta yhtenä haasteena ovat julkisen hallinnon digitaalisten palveluiden käyttöhäiriöt tilanteissa, jotka edellyttävät käyttäjiltä tiettyjen määräaikaisten noudattamista. Esimerkiksi tulotietojen ilmoittaminen, veroprosentin muutos tai työvoimatoimistoon ilmoittautuminen voi osoittautua haasteelliseksi määräajan mukaisesti, jos tätä tarkoitusta varten tarjottu digitaalinen palvelu ei ole käytettävissä teknisen tai muun häiriötilanteen vuoksi. Tarvittaisiin selkeitä linjauksia siitä, miten asiakkaita ohjeistetaan pitkäkestoisten häiriötilanteiden varalta.

Yhteenveto ja johtopäätökset

Yhteiskunnan on ratkaistava, mitä **turvallisuuden** toteuttaminen digitaalisessa toimintaympäristössä tarkoittaa. Mitkä asiat digitaalisen turvallisuuden hallinnasta ovat yksityishenkilöiden vastuulla, mitkä yhteisöjen kuten teknisen infrastruktuurin tai palveluiden kaupallisten tuottajien vastuulla, ja mitkä kuuluvat kuntien ja kuntayhtymien tai valtion viranomaisten vastuulle? Vastuiden tulisi olla selkeät ja kaikkien toimijoiden samalla tavalla ymmärtämät.

Digitaalisen toimintaympäristön ilmiöt ja piirteet ovat erilaiset kuin fyysisen toimintaympäristön, joten **tehtäviä ja vastuuta** tulisi selkiyttää vastaamaan paremmin digitalisoinnin aiheuttamaan toimintaympäristön nopeaan muutokseen. Kansalaisten, yritysten ja erilaisten yhteisöjen on voitava liittyä hallinnon tarjoamiin tavanomaisiin digitaalisiin palveluihin turvallisesti. Eri tahojen on myös voitava luottaa palveluiden toimivuuteen ja viime kädessä viranomaisten apuun häiriötilanteissa. Samoin kunnallisten toimijoiden on voitava tukeutua valtiollisiin toimijoihin laajoissa häiriötilanteissa.

Yhteiskunnallinen keskustelu digitaalisen toimintaympäristön turvallisuudesta ja siinä esiintyvien uhkien torjunnasta on painottunut operatiivisen tason toiminnan kehittämiseen, nykyisten tiedostettujen uhkien ja häiriöiden hallitsemiseksi. Erityisesti on korostettu havainnointikyvyn ja häiriöiden hallintakyvyn kehittämistä sekä tietosuoja- ja tietoturvalisuekysymyksiä. Tutkimusta ja hallinnon ohjausta tulee suunnata vahvemmin **strategisesti** pitkällä aikavälillä vaikuttavimpiin asioihin. Kehittämistä ohjaavia linjauksia tarvitaan uusien palveluratkaisuiden hyödyntämisestä, hallinnon ja yritysten yhteistoiminnasta sekä kansainvälisestä yhteistyöstä. Nykyistä selkeämmin tulee ohjata sitä, miltä osin palveluita tuotetaan ja infrastruktuuria rakennetaan kansallisin toimin ja resurssein, miltä osin tukeudutaan esimerkiksi EU:n yhteiseen kehittämiseen tai muuhun kansainväliseen yhteistyöhön ja erityisesti julkisessa hallinnossa siihen, kuinka julkisten digitaalisten palveluiden tuotannossa tulisi ja voidaan hyödyntää erilaisia uusia palvelumalleja ja teknologian tarjoamia mahdollisuuksia.¹⁹

Investointien **tuottavuuden mittaaminen** on välttämätöntä, jotta rajalliset resurssit voidaan kohdentaa mahdollisimman tehokkaasti. Digitaalisen turvallisuuden kehityshankkeiden tavoitteiden tulee hyödyttää yhteiskuntaa ja niiden tulee olla mitattavissa. Sekä mittaustuloksia että riskianalyseja tulee soveltaa tulevien investointiohjelmien suunnittelussa.

Tietoliikenteen ja sähkön syötön toimitusvarmuus ovat digitaalisen toimintaympäristön perusedellytyksiä. Tietoverkkojen turvallisuus ja sähkön syötön toimitusvarmuus ovat tällä

¹⁹ Uudistuva, vakaa ja kestävä yhteiskunta. Valtiovarainministeriön virkamiespuheenvuoro. Valtiovarainministeriön julkaisuja 2019:11

hetkellä Suomessa hyvällä tasolla. Digitaalisen toimintaympäristön kehittyminen edellyttää tietoliikenneoperaattoreilta ja sähköverkkotoimijoilta jatkuvaa turvallisuuden, hallinnan ja valvonnan parantamista. **Kansalaisten** käytössä tulee olla turvallinen digitaalinen toimintaympäristö, jossa turvallisuus vastaa kokemusta fyysisen toimintaympäristön turvallisuudesta. Tämä tarkoittaa muun muassa hyökkäysten torjumista jo tietoverkossa, haittaohjelmien suodatusta sekä palvelunestohyökkäysten estämistä. Myös viranomaisten toimivaltuudet sekä valvonnan vastuiden ja velvoitteiden jäsentyminen suhteessa digitaalisen infrastruktuurin palveluntarjoajiin on arvioitava.

Digitalisoinnin tavoitteena on olennainen toimintaprosessien kehittäminen ja samalla tavalla digitaaliseen turvallisuuteen tulee suhtautua **innovatiivisella**, uutta luovalla ajattelulla. Turvallisuuden periaatteet eivät digitalisoinnissa sinänsä muutu, mutta vanhat turvallisuustoimenpiteet saatetaan ohittaa, jos ne koetaan toimintaa rajoittaviksi piirteiksi. Turvallisuustavoitteet tulee kuitenkin uudessakin toimintamallissa saavuttaa, vaikka toteutus muuttuisikin.

Liite 3. Julkisen hallinnon digitaalisen turvallisuuden kansainvälinen vertailu

Digitaalisen turvallisuuden kansainvälisessä vertailussa tarkasteltiin digitaalisen turvallisuuden ohjausta, tehtäviä, rakenteita, riskejä ja resursseja verrokkivaltioissa²⁰. Verrokkivaltiot olivat Alankomaat, Australia, Iso-Britannia, Israel, Ruotsi, Saksa, Venäjä ja Viro. Vertailutieto kerättiin verrokkivaltioiden julkisista dokumenteista perustuen tiedonhaku-kysymyksiin, jotka käsittelivät lainsäädäntöä, strategisia linjauksia, toiminnan organisointia ja resursseja.

Digitaalisen turvallisuuden **termit** ovat verrokkivaltioissa kirjavia. Käsitteet ”digitaalinen turvallisuus (digiturva)”, ”kyberturvallisuus” ja ”tietoturvallisuus” eivät ole täysin vakiintuneita Suomessakaan ja käsitteiden väliset erot vaikuttavat osin keinotekoisilta. Tässä vertailussa digitaalinen turvallisuus koostuu tietoturvaluuteen, kyberturvaluuteen, toiminnan jatkuvuuteen ja varautumiseen, riskienhallintaan sekä tietosuojan kuuluvista asioista. Vertailun tausta-aineistoon on koottu materiaalia kustakin verrokkivaltiosta kaikilta osa-alueilta sen mukaan kuin aineistoa oli saatavilla. Käsitteiden ja määritelmien erot näkyvät myös selvityksen tausta-aineistossa: verrokkivaltioiden digitaalista turvallisuutta käsiteltiin pääasiassa kyberturvallisuusstrategiassa. Ruotsissa linjaukset on kirjattu tieto- ja kyberturvallisuusstrategiaan sekä digitalisaatiostrategiaan. Alankomaissa kyberturvallisuusstrategian lisäksi on erillinen yhteiskunnan digitalisaatiostrategia. Saksassa ja Isonsa-Britanniassa on lisäksi erillinen hallinnon digitalisointistrategia. Vertailun tausta-aineistossa käytettiin lisäksi kansallisia riskiarvioita, sekä kriittisen infrastruktuurin suojaamista ja tietosuoja ja muita digitaalista turvallisuutta käsitteleviä dokumentteja, milloin niitä oli saatavilla.

Digitaalista turvallisuutta koskeva **lainsäädäntö** on vaihtelevaa, mutta EU:n yleinen tietosuoja-asetus (GDPR) sekä verkko- ja tietoturvadirektiivi (NIS) yhtenäistävät käytäntöjä. Uusi EU:n asetus kyberturvallisuusvirastosta ENISA:sta ja asetuksen (EU) 526/2013 kumoamisesta sekä tieto- ja viestintäteknikan kyberturvallisuussertifiointista (”kyberturvallisuus-asetus”) vahvistaa EU:n yhteisen viranomaisen (ENISA) kyberturvallisuuden koordinoijan ja neuvonantajan roolia ja määrittelee prosessien, palveluiden ja tuotteiden sertifiointijärjestelmän. Israel edellyttää henkilökohtaista **sertifiointia** henkilöiltä, jotka työskentelevät kyberpuolustuksen, tunkeutumistestauksen, tietoturvaloukkausten tutkimisen, kyberturvallisuuden metodologioiden tai kyberturvallisuusteknologioiden parissa. Isonsa-Britanniassa Cyber Essentials -sertifikaatin voivat yritysten ja ammattilaisten lisäksi hankkia

²⁰ Digitaalisen turvallisuuden kansainvälinen vertailu, KPMG, helmikuu 2020

myös yksityishenkilöt. Suomen Tietoturvamerkki on esimerkki mallista, jolla tuotteiden ja palveluiden sertifiointia voitaisiin toteuttaa myös EU:n laajuisesti.

Digitaalista infrastruktuuria ei verokkivaltioissa käsitellä erillisenä kokonaisuutena. Sen sijaan digitaalisen infrastruktuurin ajatellaan sisältyvän fyysisen maailman rakenteisiin, toimintoihin, palveluihin ja tuotteisiin ja sen turvaamisen olevan vastaavasti osa yleistä varautumista ja jatkuvuuden hallintaa. Energiahuolto ja tietoliikenteen toimivuus nähdään digitalisoituvan yhteiskunnan keskeisinä edellytyksinä.

Digitaalisen turvallisuuden ohjauksessa suuntaus näyttää olevan kohti **keskitettyjä malleja**, jossa yhden ministeriön alaisuuteen on sijoitettu toimivaltainen viranomainen, joka ohjaa ja koordinoi mutta myös ohjeistaa ja kouluttaa sekä valvoo ja reagoi. Vahvasti hajautetussa mallissa toimijoiden välinen kommunikointi ja toimivaltakysymykset voivat muodostua haasteellisiksi. Tietosuojasta vastaa EU-valtioissa GDPR:n mukainen tietosuojaviranomainen, joiden resursoinnissa on kuitenkin suuria eroja: Suomessa tietosuojavaltuutetun toimistossa on vakituisesti kolme henkilöä, Virossa 19, Ruotsissa 75 ja Saksan liittovaltion virastossa 190. Myös Israelissa ja Australiassa on tietosuojaviranomainen, jonka tehtävät ovat samankaltaisia kuin EU-valtioiden viranomaisilla.

Verokkivaltioiden digitaaliseen turvallisuuteen liittyvät riskit on käsitelty kansallisissa riskiarvioissa tai kyberturvallisuusstrategioissa. Näissä strategiseksi riskiksi tunnistetaan vieraiden valtioiden tai näiden tukemien ryhmittymien **vihamielinen vaikuttaminen** lähes poikkeuksetta. Kyberhyökkäyksiä pidetään merkittävänä uhkina mm. siksi, että niiden katsotaan voivan horjuttaa yhteiskunnan vakautta esimerkiksi hybrdivaikuttamisen tai valeututisten kautta. Hyökkäyksiin tarvittavaa teknologiaa on lisäksi helposti saatavilla ja hyökkääjän kiinnijäämisen riski on pieni. Digitaalisen toimintaympäristön turvallisuuden parantamiseksi tarvitaan konkreettisia, yhteiskunnan eri alueet kattavia toimenpiteitä, joiden toteutumista seurataan säännöllisesti esimerkiksi Ison-Britannian tavoin kyberturvallisuusstrategian avulla.

Verokkimaissa kansallisen digitaalisen turvallisuuden aktiivisina toimijoina tunnistetaan yleisesti julkinen hallinto, elinkeinoelämä, korkeakoulut ja tutkimuslaitokset sekä kansalaiset. Kaikkien toimijoiden **yhteistyö** tuottaa kattavamman digitaalisen turvallisuuden tilannekuvan. Uusien digitaalisten tuotteiden ja palveluiden kehittyminen kasvattaa koko kybertoimialaa ja tarjoaa uusia vientimahdollisuuksia. Israel ja Alankomaat ovat esimerkkejä valtioista, joissa toimialaa ja tutkimusta kehittämällä tavoitellaan kansantaloudellista hyötyä.

Suomessa **kansalaisten** roolia ja vastuita aktiivisina yhteiskunnan turvallisuuden tekijöinä ei ole määritelty, toisin kuin verokkivaltioissa. Niissä koko yhteiskunnan kattava osaamisen kehittäminen on strateginen painopiste ja digitaalisen turvallisuuden taitojen ja osaamisen kehittäminen eräs strateginen päätavoite.

Nopeasti kehittyvän digitaalisen toimintaympäristön muutokset edellyttävät nopeaa ja kansainvälisesti tehokasta **havainnointi- ja reagointikykyä**. Kybertoimintaympäristö ja siihen kohdistuvat uhkat, kuten kybervakoilu, -terrorismi tai muu kyberrikollisuus, eivät noudata valtioiden rajoja, joten uudenlainen erityisosaaminen, tiedonvaihto ja turvallisuusviranomaisten yhteistyö ovat välttämätöntä niin kansallisesti kuin kansainvälisestikin.

Kansainvälisen vertailun johtopäätökset

Digitaalisen infrastruktuurin tulee olla **osa palvelurakenteita** ja digitaalisen turvallisuuden osa palvelukokonaisuutta. Palveluntarjoajan tulee vastata digitaalisen turvallisuuden vaatimuksiin sekä taata turvallinen palvelun käyttö. Suomen tulee systemaattisesti edellyttää digitaalisen turvallisuuden kansainvälisten **standardien** ja kriteeristöjen soveltamista. Kansallisia digitaalisen turvallisuuden osa-alueiden vaatimuksia tulee käyttää kansainvälisten standardien täydentämiseksi, ei niiden korvaamiseksi.

Digitaalisen turvallisuuden merkitys on tunnistettu laajasti ja monissa maissa (muun muassa Ruotsi, Alankomaat, Saksa, Viro) **lainsäädäntöä** on pyritty kehittämään vastaamaan digitaalisen toimintaympäristön nopeita muutoksia. Kuten edellä on todettu, yhteiskunnan digitalisoinnista käsitellään tyypillisesti valtioiden kyberturvallisuusstrategioissa. Saksassa viranomaisjärjestelmien ja verkkojen tietoturva on nostettu perustuslain tasolle. Koska digitaalinen toimintaympäristö ylittää kansalliset rajat, on digitaaliseen turvallisuuteen liittyvän lainsäädännön oltava kansainvälistä, mikä edellyttää Suomen aktiivista osallistumista EU:n säädösvalmisteluun: yhteiskunnan sääntelyn tarvetta tulee seurata ja muutostarpeisiin tulee reagoida nopeasti. Suomen tulee esimerkiksi olla mukana laatimassa oppivien järjestelmien eettisiä periaatteita ja käytön valvonnan ohjeistusta sekä ottaa nämä käyttöön.

Verrokkivaltiossa digitaalisen turvallisuuden johtamista **keskitetään** ja virastoja yhdistetään suuremmiksi kokonaisuuksiksi ja Ruotsissa valmistellaan uuden, keskitetyn kyberturvallisuusviranomaisen perustamista. Kansainvälinen yhteistoiminta edellyttää selkeitä vastuualueita ja rooleja. Suomen tulee arvioida digitaalisen turvallisuuden **johtamisrakenteita, vastuita ja rooleja** sekä uudistaa niitä kansainvälisen kehityksen mukaisesti. Koordinointi- ja toteutusvastuut voidaan jakaa osiin, mutta vastuualueet tulee määrittää selkeästi toimivan kansallisen ja kansainvälisen yhteistyön takaamiseksi. Toimivaltakysymysten ei tule haitata digitaalisen turvallisuuden kehitystyötä. Suomen tulee lisätä yhteistoimintaa kaikkien digitaalisen turvallisuuden toimijoiden välillä turvallisen digitaalisen yhteiskunnan vahvistamiseksi.

Verrokkivaltioiden digitaaliseen turvallisuuteen kohdistettujen investointien arvioiminen ei ole kerätyn tiedon pohjalta mahdollista. Digitaalisen toimintaympäristön turvallisuuden kehityshankkeiden tavoitteiden tulee hyödyttää yhteiskuntaa ja hyötyjen on oltava mitattavissa. Mittaustuloksia ja riskianalyysia tulee soveltaa tulevien investointiohjelmien

suunnittelussa. Yhteiskunnan palveluissa käytettävälle teknologialle on asetettava digitaalisen turvallisuuden vähimmäisvaatimukset ja niiden toteutumista on valvottava. Turvallisuuden kannalta kriittisimmille tehtäville on määriteltävä henkilöstön digitaalisen turvallisuusosaamisen vähimmäisvaatimukset.

Digitaalisen turvallisuuden **osaamisen kehittäminen** on mukana lähes kaikkien verrokkivaltioiden strategioissa. Verrokkivaltioiden viranomaiset (esimerkiksi Ruotsin Myndigheten för samhällsskydd och beredskap, Ison-Britannian National Cyber Security Centre ja Alankomaiden Autoriteit Persoonsgegevens) tarjoavat kukin ohjeita ja koulutusta julkiselle hallinnolle, elinkeinoelämälle ja yksityishenkilöille. Kaikilla Suomen yhteiskunnan toimijoilla – hallinnolla, elinkeinoelämällä, korkeakouluilla ja tutkimuslaitoksilla sekä kansalaisilla – tulee olla aktiivinen rooli digitaalisen turvallisuuden tekijöinä. Digitaalisen turvallisuuden taitojen kehittäminen tulee olla strateginen painopiste koko yhteiskunnan laajuisesti. Esimerkiksi kansalaisten puutteelliset digitaalisen toimintaympäristön turvallisuustaidot ja -ratkaisut avaavat laajan hyökkäyspinnan digitaalisten palveluiden tuotantoa kohtaan. Ruotsin, Alankomaiden ja Viron tavoitteena on lisätä digitaalisia taitoja, (mm. medialukutaito ja kyberturvallisuus) jo ensimmäisen ja toisen asteen opetusohjelmiin, valmistamaan koululaisten ja opiskelijoiden valmiuksia. Israelissa toteutus on jo pidemällä ja kyberturvallisuus on mukana myös varusmiespalveluksessa. Isossa-Britanniassa teini-ikäisille on suunnattu erilaisia kyberturvallisuuskursseja, joiden tavoitteena on paitsi lisätä nuorten valmiuksia, myös houkuttaa nuoria kyberturvallisuusosalalle.

Verrokkivaltioiden uhka-analyysit ovat pääsääntöisesti samankaltaisia keskenään, mutta kokonaisuus ei ole erityisen selkeä yhdelläkään tarkastellulla valtiolla. Suomen tulee kuvata digitaaliseen turvallisuuteen liittyvät **uhkat** selkeästi kaikkien yhteiskunnan toimijoiden ymmärtämään muotoon. Uhkien vaikutusten pienentämiseen liittyvät strategiset linjaukset tulee avata toimeenpanosuunnitelmassa konkreettisiksi operatiivisiksi tehtäviksi. Tiivistä yhteistyötä viranomaisten ja elinkeinoelämän välillä korostetaan lähes kaikissa verrokkivaltioissa. Hallinnolle, kansalaisille ja yhteisöille on **tarjottava tukea** tunnistettuihin digitaalisen turvallisuuden häiriötilanteisiin. Iso-Britannia on esimerkiksi perustanut kyberrikollisuuden erikoistuneen yksikön kaikkiin paikallisiin poliisiosastoihin.

Liite 4. Julkisen hallinnon digitaalisen turvallisuuden toimijat ja tehtävät

Julkinen hallinto on pitkälle digitalisoitunut, joten kaikki julkisen hallinnon toimijat tarvitsevat digitaalista turvallisuutta. Nykytilanteessa julkisen hallinnon keskeisiä digitaalisen turvallisuuden toimijoita ovat:

Eduskunta

Eduskunnan kanslian tehtävänä on luoda eduskunnalle edellytykset hoitaa sille valtioon kuuluvat valtiopäivätehtävät. Kanslian palveluilla tuetaan myös digitaaliseen turvallisuuteen liittyvää lainsäädäntötyötä, päätöksentekoa ja kansainvälistä yhteistyötä. Eduskunta edistää avoimuutta, tiedon käytettävyyttä ja demokratiaa.

Digitaalisen turvaamisen tavoitteena eduskunnassa on eduskunnan toiminnan jatkuvuuden turvaaminen ja ulkopuolisen häirinnän estäminen. Koska eduskunta on ylin valtioelin, on toiminnan jatkuvuus varmistettava kaikissa olosuhteissa. Viestinnän luotettavuus ja oikea-aikaisuus ovat tärkeä osa digitaalista turvaamista eduskunnassa.

Valtiontalouden tarkastusvirasto

Valtiontalouden tarkastusvirasto, VTV, tarkastaa valtion taloudenhoitoa ja omaisuuden hallintaa sekä valvoo finanssipolitiikkaa ja puolue- ja vaalirahoitusta. Toiminnallaan VTV varmistaa, että valtion varoja käytetään eduskunnan osoittamiin kohteisiin lakia noudattaen ja järkevästi ja valvoo, että finanssipolitiikkaa hoidetaan kestävällä tavalla. VTV varmistaa osaltaan oikeusvaltion, kansanvallan ja kestävä talouden periaatteita myös Euroopan unionin taloudenhoidossa ja muussa kansainvälisessä yhteistyössä.

Digitaalisen turvallisuuden kannalta järkevä varojen käyttö tarkoittaa sitä, että digitaalisesti toimivan hallinnon palvelut ovat helposti saatavilla, helppoja ja turvallisia käyttää ja lisäksi ne tuotetaan taloudellisesti kestävällä tavalla. Tällöin palveluiden jatkuvuuden turvaamisesta on myös huolehdittu. VTV:n tavoitteena on vahvistaa luottamusta siihen, että suomalainen valtionhallinto toimii avoimesti, tuloksellisesti ja kestävästi myös digitaalisena.

Kansaneläkelaitos (Kela)

Kansaneläkelaitos (Kela) on itsenäinen julkisoikeudellinen laitos, jonka hallintoa ja toimintaa valvovat eduskunnan valitsemat valtuutetut. Kela huolehtii Suomessa asuvien ja monien ulkomailla asuvien suomalaisten sosiaaliturvasta eri elämäntilanteissa. Itsenäisen

asemansa lisäksi Kela on merkittävä valtakunnallisten tietojärjestelmäpalveluiden tuottaja. Kelan IT-palveluissa työskentelee yli 700 IT-alan ammattilaista, kuten sovelluskehittäjiä, tietoturva-arkkitehtejä, verkkoliikenne sekä palvelin asiantuntijoita. Kelan tuottamien tietojärjestelmien tieto- ja kyberturvallisuus ovat erittäin tärkeitä valtakunnallisten tietojärjestelmien tietosisältöjen sekä Kelan tuottamien palveluiden saatavuuden turvaamisen vuoksi. Tavoitetilassa Kelan tuottamien valtakunnallisten tietojärjestelmäpalveluiden toiminnan jatkuvuus on varmistettu kaikissa tilanteissa.

Suomen Pankki

Yhteiskunnan kannalta kriittisten finanssisektorin infrastruktuurien kuten maksu- ja selvitysjärjestelmien kyberturvallisuutta tukevien periaatteiden ja kehikoiden käyttöönotto ja yleisvalvonta.

Finanssivalvonta

Finanssivalvonnalla on keskeinen rooli finanssialan digitaalisen turvallisuuden valvojana. Finanssivalvonta vastaa sen valvonnassa olevien toimijoiden operatiivisten riskien, kyberturvallisuuden ja maksujärjestelmien valvonnasta ja tarkastamisesta. Lisäksi Finanssivalvonta antaa aihealueen määräyksiä ja ohjeita. Finanssivalvonta myös osallistuu huoltovarmuustyöhön Finanssisektorin alaisuudessa toimivien poolien jäsenenä. Lisäksi Finanssivalvonnalla on vahva rooli finanssialan digitaalisen turvallisuuden ja kyberturvallisuuden tilannekuvan muodostamisessa normaaliolojen ja poikkeusolojen yhteydessä sen valvottavien Finanssivalvonnalle lähettämien häiriö- ja poikkeamailmoitusten seurannan kautta.

Valtioneuvoston kanslia

Valtioneuvoston kanslia vastaa pääministerin johdolla hallitusohjelman toimeenpanon valvonnasta ja avustaa pääministeriä valtioneuvoston johtamisessa. Kanslia turvaa pääministerin ja hallituksen toimintaedellytykset kaikissa olosuhteissa. Valtioneuvoston kanslian toimialaan kuuluvat muun muassa valtioneuvoston yhteinen tilannekuva, varautuminen ja turvallisuus, häiriötilanteiden hallinnan yleinen yhteensovittaminen sekä valtioneuvoston ja sen ministeriöiden yhteinen tietohallinto ja asiakirjahallinto.

Suomen Erillisverkot Oy

Suomen Erillisverkot Oy on Suomen valtion kokonaan omistama erityistehtävayhtiö. Se turvaa yhteiskunnan kriittistä johtamista ja tietoyhteiskunnan palveluja kaikissa olosuhteissa. Yhtiö tarjoaa viranomaisille ja huoltovarmuuskriittisille toimijoille turvalliset ja toimintavarmat ICT-palvelut. Yhtiö kehittää yhteiskunnan kokonaisturvallisuutta ja vaikuttaa toiminnallaan kansalaisten elämään.

Ulkoministeriö

Kybertoimintaympäristö ja kyberturvallisuus ovat nousseet tärkeäksi osaksi Suomen ulko- ja turvallisuuspolitiikkaa. Kyberuhkat eivät tunne valtioiden rajoja. Kyberturvallisuuden vahvistaminen edellyttää syvenevää kansainvälistä yhteistyötä. Ulkoministeriö osaltaan koordinoi tätä kansainvälistä toimintaa. Ulkoministeriö toimii myös kansallisena turvallisuusviranomaisena (National Security Authority, NSA). Kansallisen turvallisuusviranomaisen tehtävä on kansainvälisen tietoturvallisuusvelvoitelain mukaisesti ohjata ja valvoa, että Suomelle toimitettu kansainvälinen turvallisuusluokiteltu tieto suojataan ja sitä käsitellään asianmukaisesti. NSA ohjaa kansallista toimintaa ja vastaa muun muassa kansainvälisten tietoturvaluussopimusten valmistelusta.

Tietosuojavaltuutetun toimisto

Tietosuojavaltuutettu on kansallinen valvontaviranomainen, joka valvoo tietosuojalainsäädännön noudattamista. Tietosuojavaltuutettu ja apulaistietosuojavaltuutetut ovat tehtävässään itsenäisiä ja riippumattomia. Tietosuojavaltuutetun tehtävänä on edesauttaa tiedollisten ja muiden perusoikeuksien toteutumista henkilötietojen käsittelyssä ja luottamuksen rakentamisessa. Tietosuojavaltuutettu käsittelee muun muassa tietosuojaloukkauksilmoituksia, hyväksyy sertifikaattien myöntäjiä ja tekee tietojärjestelmiin kohdistuvia tarkastuksia. Tietosuojavaltuutettu voi tarvittaessa määrätä hallinnollisia seuraamuksia ja käyttää muita toimivaltuuksiaan. Tietosuojavaltuutettu edustaa Suomea Euroopan tietosuojaneuvostossa.

Sisäministeriö

Sisäministeriö valmistelee poliisia, pelastustoimea, hätäkeskustoimintaa, rajavalvontaa, meripelastusta ja maahanmuuttoa koskevan lainsäädäntöä.

Poliisi

Poliisin tehtävänä on rikosten ennalta estäminen, paljastaminen, selvittäminen ja syyteharjintaan saattaminen. Kyberrikokset tutkitaan poliisilaitoksissa alueperiaatteen mukaisesti.

Suojelupoliisi

Suojelupoliisin tehtävänä on ennaltaehkäistä ja torjua kaikkein vakavimpia kansallisen turvallisuuden uhkia, kuten terrorismia ja vieraiden valtioiden Suomeen kohdistamaa laitonta tiedustelua. Suojelupoliisi suorittaa näitä tehtäviään myös digitaalisessa toimintaympäristössä. Suojelupoliisi tekee lisäksi ennakoivaa tiedusteluanalyysiä kansallista turvallisuutta uhkaavista ilmiöistä valtiovahdun ja muiden viranomaisten päätöksenteon tueksi.

Keskusrikospoliisi, Kyberrikostorjuntakeskus

Keskusrikospoliisin kyberrikostorjuntakeskuksen päätehtävinä kyberrikollisuuden torjunnassa ovat: Vakavimpien tietoverkkorikosten tutkinta, tietoverkkorikollisuuden tilannekuvan ylläpito, internet- ja verkkotiedustelu, tietotekninen tutkinta, sekä esitutkintaan liittyvät asiantuntijapalvelut poliisille ja muille viranomaisille.

Puolustusministeriö

Puolustusministeriö vastaa valtioneuvoston osana ja hallinnonalansa ohjaajana kansallisesta puolustuspolitiikasta ja turvallisuudesta sekä kansainvälisestä puolustuspoliittisesta yhteistyöstä. Puolustusministeriö vastaa sotilaallisen maanpuolustuksen voimavaroista ja puolustusvoimien toimintaedellytyksistä. Sen vastuulla on Suomen osallistuminen kansainväliseen kriisinhallintaan sekä Euroopan turvallisuusrakenteisiin vaikuttaminen kansallisten etujen turvaamiseksi. Puolustusministeriö vastaa myös kokonaismaanpuolustuksen koordinoinnista ja kestävästä maanpuolustustahdosta. Se antaa pyynnöstä virka-apua muille viranomaisille.

Turvallisuuskomitea

Turvallisuuskomitea avustaa valtioneuvostoa ja ministeriöitä laajoissa kokonaisturvallisuuteen liittyvissä asioissa. Komitea seuraa Suomen turvallisuusympäristön ja yhteiskunnan kehitystä sekä yhteensovittaa kokonaisturvallisuuteen liittyvää ennakoivaa varautumista. Kansallinen kyberturvallisuusstrategia 2019 nojautuu Suomen kyberturvallisuusstrategian 2013 yleisiin periaatteisiin. Strategian (2013) linjausten mukaisesti Turvallisuuskomitea seuraa ja yhteen sovittaa strategian toimeenpanoa. Kyberturvallisuuden yhteen sovittamisen päämääriä ovat päällekkäisen toiminnan välttäminen, mahdollisten puutteiden tunnistaminen ja varmistuminen vastuutahoista. Varsinaiset päätökset tekee toimivaltainen viranomainen sen mukaisesti, mitä asiasta on säädetty.

Puolustusvoimat

Puolustusvoimat on luomassa kokonaisvaltaista kyberpuolustuskykyä lakisäätteisiä tehtäviään varten osana yhteiskunnan elintärkeiden toimintojen turvaamista. 'Kyberpuolustuksella' tarkoitetaan kansallisen kyberturvallisuuden maanpuolustuksellista osa-aluetta, joka muodostuu tiedustelun, vaikuttamisen ja suojautumisen suorituskyvyistä. Kyberpuolustuksen suorituskyvyillä tuotetaan tiedustelutietoa valtionjohdon ja puolustusvoimien johdon päätöksenteon tueksi sekä tuetaan puolustusvoimien operaatioita suojaamalla oman päätöksenteon edellytykset.

Kybertoimintaympäristöön kohdistuvat uhkat ovat muuttuneet vaikutuksiltaan yhteiskunnan kannalta aiempaa vaarallisemmiksi. Kybertoimintaympäristössä toteutettavia

hyökkäyksiä voidaan käyttää poliittisen ja taloudellisen painostuksen välineinä sekä vakavassa kriisissä yhtenä vaikuttamiskeinona perinteisten sotilaallisten voimakeinojen ohella. Puolustusjärjestelmä on riippuvainen kybertoimintaympäristön käytettävyydestä ja sotilaallisen toiminnan kannalta se tulee nähdä myös mahdollisuutena ja voimavarana.

Valtiovarainministeriö

Valtiovarainministeriö vastaa valtioneuvoston osana vakaan ja kestäväen kasvun edellytyksiä vahvistavasta talouspolitiikasta, valtiontalouden hyvästä hoidosta ja kestäväen kuntatalouden toimintaedellytyksistä sekä tuloksellisesta julkisesta hallinnosta. Valtiovarainministeriön tehtäviin kuuluvat julkisen hallinnon tietopolitiikan, tiedonhallinnan ja sähköisen asioinnin yleiset perusteet. Tähän liittyen valtiovarainministeriö valmistelee julkisen hallinnon ICT-infrastruktuurin, digitaalisten palveluiden ja tietojen digitaalisen turvallisuuden yleisiä perusteita ja vaatimuksia, sekä julkisen hallinnon digitaalisen turvallisuuden linjauksia, säädöksiä ja kehittämissuunnitelmia ja ohjaa näiden toimeenpanoa, sekä asettaa tarvittavat johtoryhmät ja yhteistyöverkostot. Valtiovarainministeriö on asettanut julkisen hallinnon digitaalisen turvallisuuden strategisen johtoryhmän digitalisoitumisen ja digitaalisen turvallisuuden tasapainoista edistämistä varten.

Valtiovarain controller -toiminto

Valtiovarain controller -toiminnon tehtävänä on mm. seurata, arvioida ja kehittää sisäisen valvonnan ja sen osana olevan riskienhallinnan järjestämistä valtionhallinnossa. Toiminto voi esittää valtioneuvostolle ja ministeriölle sekä valtion virastolle, laitokselle, liikelaitokselle ja rahastolle raportin havainnoistaan ja esittää siinä mahdolliset toimenpide-ehdotuksensa.

Valtiovarain controller -toiminto johtaa valtioneuvoston asettamaa sisäisen valvonnan ja riskienhallinnan neuvottelukuntaa, joka seuraa ja arvio sisäisen valvonnan ja riskienhallinnan menetelmiä ja yleistä kehitystä sekä sisäisen valvonnan toimivuutta ja menettelyiden hyödyntämistä talouden ja toiminnan ohjauksessa ja johtamisessa sekä tehdä aloitteita sisäisen valvonnan ja sen osana olevan riskienhallinnan kehittämiseksi.

Tiedonhallintalautakunta

Tiedonhallintalautakunnan yhtenä tehtävänä on edistää tiedonhallinnan ja tietoturvallisuuden menettelytapoja sekä vaatimusten toteuttamista. Tiedonhallintalautakunta voi asettaa väliaikaisia jaostoja sekä julkaista suosituksia ja järjestää seminaareja ja muita tilaisuuksia.

Digi- ja väestötietovirasto

Digi- ja väestötietoviraston tehtävänä on edistää yhteiskunnan digitalisaatiota, turvata tietojen saatavuutta ja tarjota palveluita asiakkaiden elämäntapahtumiin. Viraston vastuulla on monia palvelukokonaisuuksia, joiden häiriötön, turvallinen ja sujuva toiminta on yhteiskunnan toiminnan kannalta tärkeää. Laadukkaat väestötiedot, varmennepalvelut sekä sähköisen asioinnin tukipalvelut luovat osaltaan edellytyksiä, joiden varaan digitalisaatiota voidaan rakentaa. Viraston tehtävänä on taata näiden palveluiden toimintavarmuus ja turvallisuus. Viraston vastuulla on digitaalisen turvallisuuden asiantuntijapalvelut ja se valmistelee suosituksia ja ohjeita. Virasto vastaa myös julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (Vahti) toiminnasta. Virasto on asettanut julkisen hallinnon digitaalisen turvallisuuden kehittämissuunnitelman (JUDO-ohjelma) vuosille 2019–2021.

Valtion tieto- ja viestintätekniikkakeskus Valtori

Valtori tuottaa valtionhallinnon toimialariippumattomat ICT-palvelut sekä korkean varautumisen ja turvallisuuden vaatimukset täyttäviä tieto- ja viestintätekniisiä palveluja ja integraatiopalveluja. Valtorin tehtävänä on varmistaa, että sen vastuulla olevien palveluiden tieto- ja kyberturvallisuus sekä jatkuvuuden ja varautumisen hallinta täyttävät asetetut vaatimukset nopeasti muuttuvassa toimintaympäristössä. Vaatimusten täyttämiseksi Valtori luo ja edelleen kehittää kyberturvallisuuden osalta kattavan tilannekuvan sekä havainnointikyvykkyyden. Näiden avulla mahdollistetaan nopea reagointi tietoturvatapahtumiin ja häiriötilanteisiin. Havainnointikykyä toteutetaan viranomaisyhteistyössä Valtorin molemmat liiketoimintaympäristöt kattavassa kyberoperaatiokeskuksessa (CSOC). Edelleen tieto- ja digiturvallisuuden osalta käytössä on määrämuotoinen tietoturvallisuuden hallintamalli, jolla varmistetaan yhteiset toimintaprosessit sekä mahdollistetaan liiketoimintakeskeinen riskien- ja poikkeamienhallinta.

Opetus- ja kulttuuriministeriö

Opetus- ja kulttuuriministeriö vastaa Suomen koulutus-, tiede-, kulttuuri-, liikunta- ja nuorisopolitiikan kehittämisestä sekä kansainvälisestä yhteistyöstä. Digitaalisen turvallisuuden liittyviä opetus- ja kulttuuriministeriön tehtäviä ovat muun muassa koulutus- ja tutkimusjärjestelmän sekä osaamisen ylläpitäminen, kirjasto- ja muiden kulttuuripalvelujen ylläpitämisen edellytysten turvaaminen ja kulttuuriomaisuuden suojeleminen.

Opetus- ja kulttuuriministeriö ohjaa useita koulutuksen digitaalisia palveluita ja rekistereitä. Ministeriön toimiala vastaa riittävän ammattitaitoisen työvoiman saannista sekä kansalaisten digitaalisissa toimintaympäristöissä vaadittavien taitojen ja osaamisen kuten medialukutaitojen kehittämisestä kaikilla koulutusasteilla. Osaamisen kehittäminen vahvistaa kansalaisten luottamusta ja osallisuutta digitalisoituvassa yhteiskunnassa. Opetus- ja kulttuuriministeriön toimialan toimijat vastaavat myös digitaaliseen turvallisuuteen

liittyvän erityisosaamisen ja tutkimuksen kehittämisestä. Lisäksi ministeriön hallinnonalan tehtävänä on säilyttää pitkäaikaisesti tai pysyvästi ja ymmärrettävässä muodossa valtionhallinnossa syntyvä digitaalinen tietoaaineisto ja keskeinen digitaalisessa muodossa oleva kulttuuriperintö. Ministeriö ohjaa muita julkisen hallinnon toimijoita asiassa.

Liikenne- ja viestintäministeriö

Liikenne- ja viestintäministeriö vastaa sähköisten viestintäpalvelujen ja –verkkojen tietoturvallisuuden kehittämisestä. Tämä tarkoittaa esimerkiksi sähköisten viestintäpalvelujen tai sähköisten viestintäverkkojen tietoturvaa koskevan sääntelyn kehittämistä, strategia-työtä tai muuta yleistä ohjausta. Liikenne- ja viestintäministeriön alaisuudessa toimii vuoden 2019 alussa muodostettu Liikenne- ja viestintävirasto. Kansainvälisestikin arvostettu Kyberturvallisuuskeskus toimii osana Liikenne- ja viestintävirastoa.

Liikenne- ja viestintävirasto, Kyberturvallisuuskeskus

Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksella on keskeinen rooli digitaalisen yhteiskunnan varautumisessa. Toiminnallaan virasto huolehtii yhteiskunnan toiminnasta myös normaaliolojen häiriötilanteissa ja poikkeusoloissa muun muassa varmistamalla yleisten viestintäverkkojen ja -palvelujen sekä niihin liitettyjen muiden viestintäverkkojen ja -palvelujen toimivuuden ja tietoturvallisuuden sekä taajuuksien ja salausteknisen aineiston saatavuuden esimerkiksi turvallisuusviranomaisten tarpeisiin. Lisäksi virasto vastaa Suomen kansallisesta verkkotunnuspäätteestä .fi ja ylläpitää fi-juurinimipalvelimia ja valvoo verkkotunnusvälittäjiä.

Virasto edistää viestinnän luottamuksellisuutta ja valvoo säädetysti yksityisyyden suojaa televiestinnässä. Viraston Kyberturvallisuuskeskuksen CERT-toiminto (Computer Emergency Response Team) huolehtii virastolle säädetystä tietoturvaloukkausten ennaltaehkäisy-, selvitys- ja tiedotustehtävistä sekä kyberturvallisuuden tilannekuvan ylläpitämisestä ja jakamisesta. CERT-toiminto tuottaa ja ylläpitää kyberturvallisuuden tilannekuvaa yhdessä luotettujen koti- ja ulkomaisten yhteistyökumppaneiden ja vastintahojen kanssa. Kyberturvallisuuskeskuksen CERT on tunnettu ja luotettu yhteistyökumppani useissa kansainvälisissä verkostoissa, joiden rakentamiseen on käytetty 19 vuotta CERT-toiminnon perustamisen alusta lähtien.

Sosiaali- ja terveysministeriö

Sosiaali- ja terveysministeriö ohjaa useita yhteiskunnan kannalta merkittäviä tehtäviä. Sosiaaliturva vastaa kaikista sosiaalietuuksista ja muun muassa vakuutuksista ja eläkkeistä. Sosiaali- ja terveyspalvelut puolestaan sosiaalihuollon ja terveydenhuollon palveluista. Lisäksi alueeseen kuuluu muun muassa ympäristöterveydenhuolto. Varsinaisen toiminnan

ohella ministeriö ohjaa myös näihin liittyviä turvallisuusasioita. On huomattava, että näillä alueilla olevat toimijat eivät ole yksinomaan julkista hallintoa vaan mukana on paljon yksityisiä toimijoita ja myös kolmatta sektoria. Turvallisuusvaatimukset voivat liittyä potilasturvallisuuteen, jossa tietojen saatavuus ja oikeellisuus näyttelevät suurta roolia, lääkintälaitteasetukseen, jolla varmistetaan lääkinnällisten laitteiden, jotka ovat nykyään usein verkkoon kytkettyjä tietokoneita, turvallinen toiminta, tai tietosuojasetukseen, koska alalla käsitellään paljon arkaluontoisia henkilötietoja. Näiden vaatimusten lisäksi kansallisiin sähköisiin palveluihin kytkettyihin järjestelmiin kohdistuu joukko turvallisuusvaatimuksia ja järjestelmät on sertifioitava. Ministeriö ohjaa toimintaa ja vastaa lainsäädännöstä toteutuksen jäädessä alaisen hallinnon virastojen (erityisesti THL, Fimea ja Valvira) vastuulle.

Tietolupaviranomainen Findata

Findata on palvelu sosiaali- ja terveysalan tietojen toissijaiseen käyttöön. Se myöntää luvat sosiaali- ja terveystietojen toissijaiseen käyttöön silloin, kun tietoja yhdistellään useammalta rekisterinpitäjältä, rekisteritiedot ovat peräisin yksityisiltä sosiaali- ja terveydenhuollon palvelunjärjestäjiltä tai kyse on Kanta-palveluihin tallennetuista tiedoista. Findata toimii THL:n yhteydessä, eriyttynä THL:n muusta toiminnasta.

Maa- ja metsätalousministeriö

Maa- ja metsätalousministeriö ohjaa, edistää ja seuraa digitaalista turvallisuutta omalla toimialallaan. Digitaalisen turvallisuuden kannalta keskeisiä tehtäviä ovat kiinteistötietojärjestelmän (KTJ) ja maastotietojärjestelmän (MTJ) ylläpito ja jatkuvuuden turvaaminen kaikissa turvallisuustilanteissa, tilastotietojen saatavuuden turvaaminen sekä maksajavirasto-tehtävien toimeenpanto ISO27001-sertifikaatin mukaisesti. NIS-direktiivi velvoittaa huoltovarmuuskriittisiä yrityksiä ja keskeisiä digitaalisten palveluiden tarjoajia ilmoittamaan tietoturvapoikkeamasta toimialansa valvontaviranomaiselle. MMM:n toimialalla NIS-ilmoitusvelvollisuus koskee vähintään 5 000 kuutiometriä vuorokaudessa vettä toimittavia tai jäteveettä vastaanottavia vesihuoltolaitoksia.

Maanmittauslaitos

Maanmittauslaitoksen toimialaan kuuluvat kiinteistöjen ja osakehuoneistojen omistuksen, kiinteistöjen ja muiden rekisteriyksiköiden hallinnan, luototusjärjestelmän ja paikantamisen turvaamiseksi tarvittaviin rekistereihin liittyvä toiminta, paikkatietojen yhteentoimivuuden ja käytön edistäminen sekä paikkatieto- ja kiinteistöalan tutkimus. Lisäksi Maanmittauslaitos huolehtii paikantamisen perustasta ja peruspaikkatietojen tuottamisesta sekä tuottaa asiantuntijapalveluita yhteiskunnan käyttöön.

Ruokavirasto

Ruokavirasto vastaa Suomen maksajavirastotehtävistä komission vaatimusten mukaisesti. Vaatimuksena on maksajaviraston ISO/IEC 27001 -sertifioitu hallintajärjestelmä sekä maksajaviraston delegoitujen tehtävien osalta maksajaviraston toimintaa vastaava ISO/IEC 27001 ja 27002 standardeihin perustuva tietoturvallisuuden varmistaminen. Maksajaviraston delegoituja tehtäviä on siirretty ELY-keskuksille, YT-alueille, Tullille ja Ahvenanmaalle.

Työ- ja elinkeinoministeriö

Työ- ja elinkeinoministeriö ohjaa ja vastaa osaltaan hallinnonalan toimintojen ja tietovarantojen tietoturvallisuudesta sekä tehtäviä ja toimintoja ohjaavasta lainsäädännöstä. Palveluiden toteutus on hallinnonalan virastoiden ja laitosten vastuulla. Keskeisiä turvattavia toimintoja ovat yritysten ja yhteisöiden perusrekisterit ja niiden toiminta (oikeellisuus ja saatavuus), työvoimatoimintojen kokonaisuus (tietosuoja ja saatavuus), energihuollon varmistaminen sekä elinkeinoelämälle suunnatut liiketoimintasalaisia tietoja sisältävät rahoituspalvelut (prosessiturvallisuus).

Huoltovarmuuskeskus

Huoltovarmuuskeskus on työ- ja elinkeinoministeriön hallinnonalan laitos, jonka tehtävänä on maan huoltovarmuuden ylläpitämiseen ja kehittämiseen liittyvä suunnittelu ja operatiivinen toiminta. Yhteistyössä muiden viranomaisten ja elinkeinoelämän kanssa Huoltovarmuuskeskus varmistaa, että yhteiskunnalle kriittisimmät järjestelmät toimivat kaikissa tilanteissa. Huoltovarmuuskeskus johtaa ja resursoi huoltovarmuuskriittisen elinkeinoelämän tarpeisiin kohdennettua kyber- ja digitaalisen infrastruktuurin turvallisuutta parantavaa Digitaalinen turvallisuus 2030 -ohjelmaa.

Teknologian tutkimuskeskus VTT Oy

Teknologian tutkimuskeskus VTT Oy on valtion kokonaan omistama erityistehtävää toteuttava voittoa tavoittelematon yhtiö. VTT tarjoaa digitaalisen turvallisuuden palveluja yrityksille sekä julkiselle hallinnolle.

Ympäristöministeriö

Ympäristöministeriön visio on ”parempi ympäristö tuleville sukupolville”. Ministeriöllä on kolme strategista vaikuttavuustavoitetta, jotka kaikki ovat hallinnonrajat ylittäviä: 1. Hyvä ympäristö ja monimuotoinen luonto, 2. Hiilineutraali kiertotalousyhteiskunta, 3. Kestävä kaupunkikehitys. Ympäristöministeriö vastaa yhdessä Suomen ympäristökeskuksen kanssa ympäristötietojärjestelmien digitaalisesta turvallisuudesta ja käytävyydestä, sekä ohjaa ja edistää rakennetun ympäristön tietojärjestelmien digitaalisen

turvallisuuden toimintaa. Ympäristöministeriön johtamana on käynnistynyt syksyllä 2019 yhteistyössä muiden ministeriöiden kanssa rakennetun ympäristön tietotalustan kehittäminen, joka pitää sisällään laajoja tietokokonaisuuksia niin kyberturvallisuuden kuin tietosuojakysymysten osalta. Ympäristöministeriö osaltaan huomioi digitaalisen turvallisuuden vaatimukset tietotalustan valmistumisessa ja käytössä.

Kunnat ja kuntayhtymät

Kunnat järjestävät asukkailleen palveluita, joista suurin osa on määritelty kuntien tehtäviksi laissa. Kuntayhtymät hoitavat jäsenkuntiansa puolesta kuntayhtymän perussopimuksen mukaisia tehtäviä. Kuntien toiminta on monialaista, mikä asettaa haasteita digitaaliselle turvallisuudelle. Kunnanhallituksen tehtävänä on huolehtia riskienhallinnan järjestämisestä. Kuntaliiton selvityksen perusteella perustietotekniikka, tietoturva, tietotekniikan hankinnat ja kilpailutukset, kehittäminen ja ylläpito hoidetaan kunnissa ja kuntayhtymissä pitkälti omana työnä. Kuntien ja kuntayhtymien välillä on eroja ja kuntakoolla on merkitystä järjestämistapaan. Kuntien ja kuntayhtymien omistamien yhtiöiden kautta tietoturvan hoitaa arviolta noin kolmannes, ja ostopalvelua käyttää arviolta noin viidennes.²¹ Kunnat on veloitettu toteuttamaan tiedonhallintalain mukaiset tietoturvallisuuden vähimmäisvaatimukset vuoden 2023 loppuun mennessä.

Kuntaliitto

Kuntaliiton tehtävänä on edesauttaa digitaalisen turvallisuuden ja yhteentoimivuuden menetelmien ja käytänteitten soveltamisessa kuntakentässä, toimien yhteistyössä kunta-toimijoiden kanssa. Digitaalisen turvallisuuden määräykset on sopeutettava kuntatoimijoiden toimintaan, ja yhteentoimivuuden keskeisenä tehtävänä on varmistaa toimivat palvelukokonaisuudet. Digitaalisen turvallisuuden käytänteitten tulee omalta osaltaan auttaa yhteentoimivuuden saavuttamista. Sähköisen asioinnin merkityksen lisääntyessä palvelukokonaisuuksien osalta on turvallisten ja laadullisten palveluiden toteuttaminen osa kuntalaisen arkea, osa arjen turvallisuutta. Määrityksiä ja käytänteitä toteutettaessa tulee voida osoittaa tarvittavaa tukea soveltajille, kuntatoimijoiden kokoluokka huomioituna.

Järjestöt

Järjestöjen rooli digitaalisen turvallisuuden osaamisen kehittämisessä, sekä yhteiskunnan erilaisiin häiriötilanteisiin varautumisessa ja onnettomuuksien hallinnassa on merkittävä. Järjestöillä on kokemusta vapaaehtoistoiminnan järjestämisestä kansalaisten ja asukkaiden kanssa.

21 Hyvärinen & Parviainen, Kuntien tietotekniikkakartoitus 2018, Kuntaliitto

Liite 5. Valmisteluryhmä

Julkisen hallinnon digitaalisen turvallisuuden kehittämisen periaatteiden ja toimeenpanosuunnitelman 2020–2023 valmistelun koordinoitua varten 1.9.2019–28.2.2020 väliseksi ajaksi asetettuun työryhmään kuuluivat:

- tietohallintoneuvos *Tuija Kuusisto*, valtiovarainministeriö, puheenjohtaja
- erityisasiantuntija *Mika Tuikkanen*, valtiovarainministeriö, varapuheenjohtaja, virkavapaalla 1.9.2019–
- erityisasiantuntija *Jaakko Poikonen*, 31.12.2019 saakka, valtiovarainministeriö
- neuvotteleva virkamies *Petri Puhakainen*, valtioneuvoston kanslia
- tietohallintojohtaja *Ari Uusikartano*,
varajäsen tietoturvapääällikkö *Antti Savolainen*, ulkoministeriö
- johtava asiantuntija *Ismo Parviainen*,
varajäsen turvallisuuspääällikkö *Kari Santalahti*, sisäministeriö
- tietoturvapääällikkö *Harri Mäntylä*, puolustusministeriö
- erityisasiantuntija *Liisi Hakalisto*, opetus- ja kulttuuriministeriö
- johtaja *Ari Huvinen*, maanmittauslaitos, varajäsen johtava
tietohallintoasiantuntija *Jaana Merta*, maa- ja metsätalousministeriö
- neuvotteleva virkamies *Olli Lehtilä*, varajäsen erityisasiantuntija *Maija Rekola*,
liikenne- ja viestintäministeriö
- erityisasiantuntija *Teemupekka Virtanen*, sosiaali- ja terveysministeriö
- hallitusneuvos *Kari Klemm*, varajäsen kehittämispääällikkö *Jaakko Jokela*;
kehittämispääällikkö *Petteri Ohvo* 31.1.2020 saakka, varajäsen teollisuusneuvos
Sirpa Alitalo, työ- ja elinkeinoministeriö
- ylitarkastaja *Roni Kiviharju*, erityisasiantuntija *Tomi Marjamäki*,
ympäristöministeriö

- erityisasiantuntija, tietoturvavastaava *Outi Juntura*, Eduskunta
- erikoistutkija *Antti Sillanpää*, Turvallisuuskomitea, 21.1.2020 alkaen
- johtava asiantuntija *Mika Susi*, Elinkeinoelämän keskusliitto 31.10.2019 saakka
- toiminnanjohtaja *Mika Susi* FISC ry, 1.11.2019 alkaen
- tietohallintojohtaja *Markku Raitio* 17.12.2019 saakka, varajäsen tietoturva-asiantuntija *Aaro Hallikainen*, Helsingin kaupunki
- tietujohtaja *Kari Perälä*, varajäsen tietohallintopäällikkö ja tietoturvavastaava *Petri Hiirsalmi*, Imatran kaupunki
- varautumispäällikkö *Kalle Luukkainen*, 1.1.2020 alkaen varautumispäällikkö *Jarna Hartikainen*, Huoltovarmuuskeskus
- erityisasiantuntija *Jari Ylikoski*, Kuntaliitto
- yksikön päällikkö *Henri Burtsov*, varajäsen tietoturva-asiantuntija *Jonna Ylikauppila*, KELA
- tietoturvapäällikkö *Kari Nykänen*, Oulun kaupunki
- tietoturvallisuusjohtaja *Juha Tallinen*, varajäsen tietohallintopäällikkö *Pasi Koljonen*, varajäsen tietohallintopäällikkö *Pertti Pyysing*, Puolustusvoimat
- tietoturvapäällikkö *Pasi Hänninen*, Suomen Pankki
- tietoturvapäällikkö *Sami Niinikorpi*, varajäsen Otto Kolsi, Suojelupoliisi
- osastopäällikkö *Rauli Paananen*, Traficom
- turvallisuuspäällikkö *Mika Kuronen*, varajäsen ICT-tietoturvapäällikkö *Pyry Heikkinen*, varajäsen tullilylitarkastaja *Antti Mielonen*, Tulli
- yksikön päällikkö *Olli Joronen*, 17.12.2019 alkaen turvallisuusjohtaja *Hannu Naumanen*, varajäsen yksikön päällikkö *Virpi Mäkinen*, varajäsen *Sonja Marjamäki-Ruuskanen*, Valtion tieto- ja viestintätekniikkakeskus Valtori
- johtaja *Samuli Bergström*, varajäsen tietoturvapäällikkö *Mikko Hakuli*, Vero

- johtava erityisasiantuntija *Kimmo Rousku*, varajäsen johtava asiantuntija *Kirsi Janhunen* 14.9.2019 saakka, varajäsen johtava asiantuntija *Erja Kinnunen*; tietoturvapäällikkö *Pekka Ristimäki*, varajäsen erityisasiantuntija *Jarmo Pietikäinen*, 21.1.2020 alkaen erityisasiantuntija *Antti Ahokas*, Väestörekisterikeskus, 1.1.2020 alkaen Digi- ja väestötietovirasto



VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

VALTIOVARAINMINISTERIÖ
Snellmaninkatu 1 A
PL 28, 00023 VALTIONEUVOSTO
Puhelin 0295 160 01
vm.fi

ISSN 1797-9714 (pdf)
ISBN 978-952-287-857-1 (pdf)

Huhtikuu 2020