VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Digital säkerhet inom den offentliga förvaltningen

Offentliga förvaltningens ICT

Finansministeriets publikationer – 2020:24

Finansministeriets publikationer 2020:24

Digital säkerhet inom den offentliga förvaltningen

Finansministeriet, Helsingfors 2020

Finansministeriet

ISBN PDF: 978-952-367-308-3

Layout: Statsrådets förvaltningsenhet, publikationsverksamheten

Helsingfors 2020

Presentationsblad

Utgivare	Finansministeriet		8.4.2020
Författare			
Publikationens titel	Digital säkerhet inom den offentliga förvaltningen		
Publikationsseriens namn och nummer	Finansministeriets publikationer 2020:24		
Diarie-/ projektnummer	VN/1465/2020	**Tema**	Offentliga förvaltningens ICT
ISBN PDF	978-952-367-308-3	**ISSN PDF**	1797-9714
URN-adress	http://urn.fi/URN:ISBN:978-952-367-308-3		
Sidantal	44	**Språk**	svenska
Nyckelord	offentliga förvaltningens IKT, informationspolitik, riskhantering, cybersäkerhet, beredskap, informations- och kommunikationsteknik		

Referat

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.

Principbeslutet och genomförandeplanen, som ska stödja riktlinjerna i det, bereddes i en förvaltnings-övergripande 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.

Tuija Kuusisto
informationsförvaltningsråd
beredningsgruppens ordförande

Förläggare	Finansministeriet
Distribution/ beställningar	Elektronisk version: julkaisut.valtioneuvosto.fi Beställningar: vnjulkaisumyynti.fi

Kuvailulehti

Julkaisija	Valtiovarainministeriö		8.4.2020
Tekijät			
Julkaisun nimi	Julkisen hallinnon digitaalinen turvallisuus		
Julkaisusarjan nimi ja numero	Valtiovarainministeriön julkaisuja 2020:24		
Diaari/hankenumero	VN/1465/2020	**Teema**	Julkisen hallinnon ICT
ISBN PDF	978-952-367-308-3	**ISSN PDF**	1797-9714
URN-osoite	http://urn.fi/URN:ISBN:978-952-367-308-3		
Sivumäärä	44	**Kieli**	ruotsi
Asiasanat	julkisen hallinnon ICT, tietopolitiikka, riskienhallinta, kyberturvallisuus, varautuminen, tieto- ja viestintätekniikka		

Tiivistelmä

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.

Periaatepäätös ja sen linjauksia edistävä toimeenpanosuunnitelma valmisteltiin valtiovarainministeriön asettamassa poikkihallinnollinesa 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.

Tietohallintoneuvos Tuija Kuusisto
Valmisteluryhmän puheenjohtaja

Kustantaja	Valtiovarainministeriö
Julkaisun jakaja/myynti	Sähköinen versio: julkaisut.valtioneuvosto.fi Julkaisumyynti: 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 2020:24		
Register number	VN/1465/2020	**Subject**	Public Sector ICT
ISBN PDF	978-952-367-308-3	**ISSN (PDF)**	1797-9714
Website address (URN)	http://urn.fi/URN:ISBN:978-952-367-308-3		
Pages	44	**Language**	Swedish
Keywords	public administration ICT, information policy, risk management, cybersecurity, preparedness, information and communications technologies		

Abstract

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.

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.

Tuija Kuusisto
Senior Ministerial Adviser
Chair of the preparation group

Publisher	Ministry of Finance
Distributed by/ Publication sales	Online version: julkaisut.valtioneuvosto.fi Publication sales: vnjulkaisumyynti.fi

Innehåll

Sammanfattning

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. De snabba framstegen i digitaliseringen, hoten mot olaglig användning av information och påverkan med felaktiga uppgifter samt det ökade nationella och internationella ömsesidiga beroendet ställer nya krav på hela den offentliga förvaltningens digitala säkerhet och styrningen av den. Därför är det motiverat att dra upp riktlinjer för utvecklandet av den digitala säkerheten inom den offentliga förvaltningen samt att planera och genomföra utvecklingsuppgifterna enligt riktlinjerna. På så vis preciseras cybersäkerhetsstrategin 2019 i fråga om den offentliga förvaltningen och stöds beredningen och genomförandet av det utvecklingsprogram för cybersäkerhetsstrategin som snart inleds.

Målet för den digitala säkerheten är att inom referensramen för den övergripande säkerheten skydda medborgarna, sammanslutningarna och samhället mot de risker och hot som kan riktas mot personuppgifter och medborgarnas tjänster samt mot samhällets och myndigheternas verksamhet, processer, tjänster och informationsmaterial i en digital miljö. Principerna för utveckling av den digitala säkerheten i den offentliga förvaltningen är följande:

- Vi leder säkerheten i det digitala samhället tillsammans utifrån lägesinformation och riskbedömning.
- Vi planerar och följer upp effekterna av och kostnaderna för den digitala säkerheten inom den offentliga förvaltningen.
- Vi utvecklar medborgarnas och de anställdas förståelse för konsekvenserna av och ansvaret för riskerna i digital säkerhet.
- Vi främjar den digitala säkerheten i samarbete mellan den offentliga förvaltningen, sammanslutningarna och medborgarna.
- Vi påverkar den digitala säkerheten på EU-nivå och internationellt och utnyttjar resultaten av samarbetet.
- Vi förutsätter en säker teknik och tjänsteproduktion.

De viktigaste digitala säkerhetstjänster som ska utvecklas till stöd för verksamhetsprocesserna och tjänsterna är följande: nationell och internationell samarbetsmodell för den digitala säkerheten inom den offentliga förvaltningen, gemensamma tjänster för kommunerna för främjande av digital säkerhet, hantering av digital identitet, utveckling av medborgarnas och de anställdas kunnande, sakkunnigtjänster för den digitala säkerheten inom den offentliga förvaltningen, bedömning av den digitala säkerheten i tjänster och tjänsteproduktion, skydd av den digitala infrastrukturen samt säker utveckling av autonoma och lärande system och tjänster inom den offentliga förvaltningen.

Samhällets verksamhet och tjänster samt samutnyttjandet av information baserar sig på ett ömsesidigt förtroende för säkerhetshanteringen. Säkerhetsproblem inom den offentliga förvaltningens digitala tjänster kan undergräva medborgarnas och sammanslutningarnas förtroende för myndigheterna. Samhället ska därför på ett balanserat sätt satsa på att trygga digitaliseringen samt digital verksamhet och tjänster. De mål som ställs för utvecklingsprojekten för digital säkerhet ska gagna samhället och nyttan av dem ska vara mätbar.

Principer och centrala tjänster för utvecklingen av den digitala säkerheten inom den offentliga förvaltningen

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. Utifrån internationella bedömningar av digitaliseringen är Finland känt som en föregångare både när det gäller förutsättningarna för digitaliseringen i samhället[1] och som tillhandahållare av digitala tjänster för medborgare och sammanslutningar[2]. I internationella bedömningar av hanteringen av cybersäkerheten och beredskapen för den[3] har Finland placerat sig nära de ledande staterna.

I strategin för cybersäkerheten i Finland 2019 ställs de viktigaste nationella målen upp för utvecklingen av cybermiljön och säkerställandet av de vitala funktioner som anknyter till den. Ofta med säkerhet i den digitala omvärlden, dvs. digital säkerhet, avses detsamma som med cybersäkerhet. I digital säkerhets referensram ingår frågor som gäller såväl cybersäkerhet som riskhantering, kontinuitetshantering i verksamheten och beredskap, informationssäkerhet och dataskydd. Målet för den digitala säkerheten är att inom referensramen för den övergripande säkerheten skydda medborgarna, sammanslutningarna och samhället mot de risker och hot som kan riktas mot personuppgifter och medborgarnas tjänster samt mot samhällets och myndigheternas verksamhet, processer, tjänster och informationsmaterial i en digital miljö. Riktlinjerna för den digitala säkerheten inom den offentliga förvaltningen tryggar hela den offentliga förvaltningen och fungerande offentliga tjänster utan att begränsa sig till tryggandet av samhällets vitala funktioner.

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)

De snabba framstegen i digitaliseringen, hoten mot olaglig användning av information och påverkan med felaktiga uppgifter samt det ökade nationella och internationella ömsesidiga beroendet ökar samhällets sårbarhet och ställer nya krav på hela den offentliga förvaltningens digitala säkerhet och styrningen av den. Behovet av samarbete och förståelse både nationellt och internationellt samt av att säkerhetsfaktorer beaktas i de ekosystem som utgörs av den offentliga förvaltningen, företag, organisationer och medborgare blir allt större. Därför är det motiverat att dra upp riktlinjer för utvecklandet av den digitala säkerheten inom den offentliga förvaltningen samt att planera och genomföra utvecklingsuppgifterna enligt riktlinjerna. Det kommer också att stödja beredningen och genomförandet av det utvecklingsprogram för cybersäkerhetsstrategin 2019 som snart inleds, samt verkställa statsrådets beslut om målen med försörjningsberedskapen (1048/2018). Digital säkerhet möjliggör också utveckling av nya tjänster och deras säkerhet.

I en internationell jämförelse bedömdes digital säkerhet i fråga om styrning, uppgifter, strukturer, risker och resurser i Nederländerna, Australien, Storbritannien, Israel, Sverige, Tyskland, Ryssland och Estland[4] jämfört med Finland. I jämförelsestaterna har målet varit att utveckla lagstiftningen så att den motsvarar de snabba förändringarna i den digitala miljön. Ledningen av den digitala säkerheten koncentreras och ämbetsverk sammanförs till större helheter. Jämförelsen ger vid handen att Finland ska utvärdera ledningsstrukturerna, ansvaret och rollerna för den digitala säkerheten samt förnya dem i enlighet med den internationella utvecklingen. I jämförelsestaterna betraktas den offentliga förvaltningen, näringslivet, högskolorna och forskningsinstituten samt medborgarna allmänt som aktiva aktörer inom den digitala säkerheten. Alla dessa ska ha en aktiv roll som aktörer inom den digitala säkerheten. Utvecklandet av färdigheterna i digital säkerhet ska vara en strategisk prioritering i hela samhället. Förvaltningen, medborgare och sammanslutningar ska tillhandahållas stöd för identifierade störningar i den digitala säkerheten. Finland ska tydligt beskriva hoten mot den digitala säkerheten i en sådan form som alla aktörer i samhället förstår. I jämförelsestaterna ses den digitala infrastrukturen som en del av servicestrukturerna och den digitala säkerheten som en del av servicehelheten. Tjänsteleverantören ska svara för kraven på digital säkerhet och garantera en säker användning av tjänsten. I Finland ska det systematiskt förutsättas att internationella standarder för digital säkerhet tillämpas.

Målet för den digitala säkerheten är att inom referensramen för den övergripande säkerheten skydda medborgarna, sammanslutningarna och samhället mot de risker och hot som kan riktas mot personuppgifter och medborgarnas tjänster samt mot samhällets och myndigheternas verksamhet, processer, tjänster och informationsmaterial i en digitaliserad miljö. På målnivå är den offentliga förvaltningens verksamhet, digitala tjänster och

4 Internationell jämförelse av digital säkerhet, KPMG, februari 2020, på finska

information samt den infrastruktur som behövs för dessa tillförlitliga, och tjänsternas och informationens konfidentialitet, integritet och tillgänglighet är tryggad.

Utifrån utredningen av nuläget för den digitala säkerheten inom den offentliga förvaltningen och en internationell jämförelse har man valt ut utvecklingsområden och principer för utvecklingen inom den offentliga förvaltningen samt centrala tjänster för den digitala säkerheten som stöder förvaltningens verksamhet och processer. De uppgifter som på ett centralt sätt främjar den offentliga förvaltningens tjänster för digital säkerhet beskrivs i genomförandeplanen för digital säkerhet inom den offentliga förvaltningen 2020–2023. Genomförandeplanen upprätthålls vid behov i enlighet med förändringarna i omvärlden och de krav som ställs i utvecklingsprogrammet för cybersäkerhetsstrategin 2019.

Utvecklingsområdena i samband med den digitala säkerheten inom den offentliga förvaltningen är: ledning och samarbete; digitalt samhälle; internationell verksamhet; ekonomi; teknik; medborgare, anställda och kompetens:

Principerna för utveckling av den digitala säkerheten i den offentliga förvaltningen med anknytning till utvecklingsområdena är följande:

- Vi leder säkerheten i det digitala samhället tillsammans utifrån **lägesinformation** och **riskbedömning**.
- Vi planerar och följer upp **effekterna av och kostnaderna för** den digitala säkerheten inom den offentliga förvaltningen.

- Vi utvecklar medborgarnas och de anställdas **förståelse** för konsekvenserna av och ansvaret för riskerna i digital säkerhet.
- Vi främjar den digitala säkerheten **i samarbete** mellan den offentliga förvaltningen, sammanslutningarna och medborgarna.
- Vi påverkar den digitala säkerheten **på EU-nivå och internationellt** och utnyttjar resultaten av samarbetet.
- Vi förutsätter en säker **teknik** och tjänsteproduktion.

De viktigaste **digitala säkerhetstjänster** som ska utvecklas till stöd för verksamhetsprocesserna och tjänsterna är följande:

1. Nationell och internationell samarbetsmodell för den digitala säkerheten inom den offentliga förvaltningen.
   Genom det nationella och internationella samarbetet effektiviseras samordningen av den digitala säkerheten och dess effektfullhet samt främjas Finlands konkurrenskraft.
2. Riskhantering i samband med den digitala säkerheten inom den offentliga förvaltningen
   Med hjälp av bedömningen av nuläget för den digitala säkerheten och de riskanalyser och konsekvensbedömningar som produceras utifrån helhetsbilden väljs utvecklingsobjekt som tilldelas resurser.
3. Gemensamma tjänster för kommunerna för främjande av digital säkerhet
   En färdplan för utveckling av den digitala säkerheten i kommunerna kommer att upprätthållas och genomförandet av färdplanen övervakas.
4. Hantering av digital identitet
   Finska medborgare och alla invånare i Finland ska ges möjlighet till elektronisk identifiering. Utveckling av fungerande elektroniska identifieringslösningar, som möjliggör användningen av olika slags verktyg, ska främjas.
5. Utveckling av medborgarnas och de anställdas kompetens
   Färdigheterna i och medvetenheten om digital säkerhet i alla persongrupper inom den offentliga förvaltningen och sammanslutningarna samt hos de enskilda medborgarna utvecklas.
6. Sakkunnigtjänster för den digitala säkerheten inom den offentliga förvaltningen
   De centraliserade sakkunnigtjänsterna inom digital säkerhet utvecklas och tillhandahålls i stor utsträckning för hela den offentliga förvaltningen.
7. Bedömning av den digitala säkerheten i tjänster och tjänsteproduktion inom den offentliga förvaltningen

Utvärdering och certifiering av digitala tjänster och tjänsteproducenter som baserar sig på normer och standarder främjas.

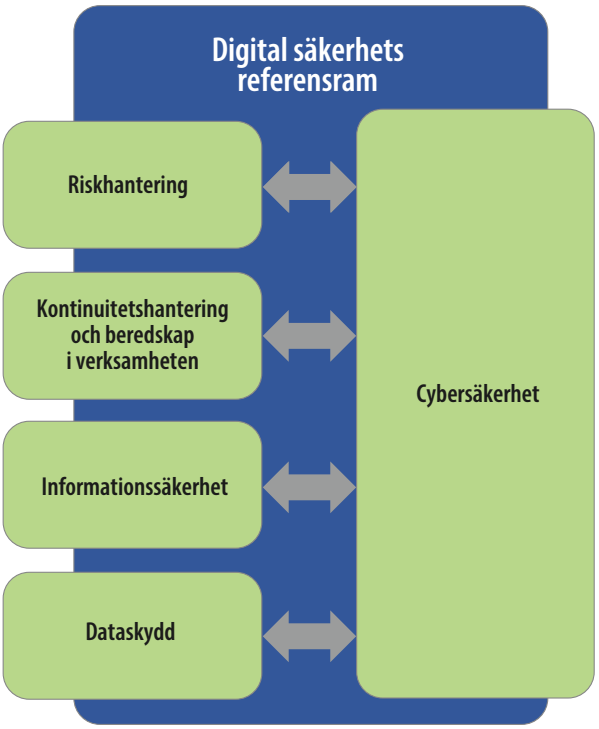
8. Skydd av den digitala infrastruktur som behövs för den offentliga förvaltningen
   Säkerheten i centrala gemensamma tekniker och tjänster främjas så att kontinuiteten och informationen i den offentliga förvaltningens verksamhet, processer och tjänster är tryggad.
9. Säker utveckling av autonoma och lärande system och tjänster inom den offentliga förvaltningen
   Säkerheten i de autonoma och lärande systemen samt de digitala tjänsterna säkerställs med hjälp av riskhantering.

Den förändring som eftersträvas genom principerna för utvecklingen av den digitala säkerheten i den offentliga förvaltningen är att stärka styrningen, samordningen och samarbetet i fråga om utvecklandet av den digitala säkerheten på strategisk och operativ nivå och att utvidga den till hela den offentliga förvaltningens område. Detta framgår av den nya styrgruppen på strategisk nivå för digital säkerhet inom den offentliga förvaltningen samt av stärkandet av styrningen av utvecklingen av den operativa nivån på den digitala säkerheten inom den offentliga förvaltningen och av styrningen av utvecklingen via färdplanen för den digitala säkerheten i kommunerna.

Utvecklingen möjliggörs genom att utöka medborgarnas och personalens kompetens och genom övningsverksamhet samt genom att förbättra tillgången till sakkunnigtjänster. Dessutom genomförs en kategorisering av kritiska tjänster, processer, infrastruktur och data i samband med beredningen av säkerhetsarkitekturen samt identifiering av kritiska utvecklingsobjekt, utarbetande och utvärdering av utvecklingsplaner. För att bedöma situationen i fråga om digital säkerhet inom den offentliga förvaltningen främjas hanteringen av utvärderingen av informationssäkerheten genom lagberedning och ökas kapaciteten inom den offentliga förvaltningen att analysera den digitala infrastrukturens och servicens tillstånd. De centrala genomförarna av genomförandeplanen för digital säkerhet inom den offentliga förvaltningen är finansministeriet, Myndigheten för digitalisering och befolkningsdata, och Transport- och kommunikationsverket samt de företag som producerar de tjänster som anskaffas.

Bilaga 1. Termer

Digital säkerhet Ofta synonym till cybersäkerhet. I digital säkerhets referensram ingår frågor som gäller riskhantering, kontinuitetshantering och beredskap i verksamheten samt cybersäkerhet, informationssäkerhet och dataskydd[5]. Termen är ny och inte etablerad. Det finns ingen internationell överenskommelse om termer.



Utvecklingen av den digitala säkerheten är riskhanteringsbaserad utveckling av säkerheten genom kontinuitet och beredskap i verksamheten, informationssäkerhet och dataskydd och samtidigt är den också utveckling av cybersäkerheten.

Cybersäkerheten omfattar i synnerhet i internationella sammanhang också sådana delområden som i stor utsträckning är föremål även för annat intresse än det som utgår från den digitala säkerheten. Dessa delområden är till exempel cyberdiplomati, cyberpåverkan, cyberresiliens och hybridpåverkan.

5 Pilkahduksia tulevaisuuteen, Tietopolitiikka, tekoäly ja robotisaatio hyvinvoinnin ja taloudellisen menestyksen mahdollistajana Suomessa (Glimtar av framtiden – Informationspolitik, artificiell intelligens och robotisering möjliggör Finlands välfärd och ekonomiska framgång), Finansministeriets publikationer 2019:22

Inom OECD används termen digital security[6], eftersom termen är enhetligare än cybersäkerhetstermerna digitalisering, digital transformation och digital ekonomi. Den digitala säkerheten liksom även cybersäkerheten påverkar också säkerheten i den fysiska världen på samma sätt som den digitala säkerheten påverkas via den fysiska världen.

Cybersäkerhet Ett måltillstånd där man kan lita på cybermiljön och där dess funktion tryggas. Där man med informationssäkerhet avser tillgång till information, integritet och konfidentialitet innebär cybersäkerhet säkerheten i ett digitalt och nätverksbaserat samhälle eller i en organisation och dess inverkan på deras funktioner.[7] Som synonym till cybermiljö kan användas termen digital miljö.

Informationssäkerhet
Arrangemang som syftar till att säkerställa sekretess, integritet och tillgänglighet[8].

Dataskydd Skydd för människors privatliv och skydd mot obehörig användning av uppgifter om individer vid behandling av personuppgifter[9].

Riskhantering Systematisk verksamhet som inbegriper riskanalys samt planering, genomförande, uppföljning och korrigerande åtgärder i fråga om behövliga åtgärder[10].

Kvarstående risk Risk som kvarstår efter att en risk har åtgärdats och som man inte kan eller inte vill eliminera. Kvarstående risker kan omfatta oidentifierade risker.[11]

Kontinuitetshantering
Organisationsprocess för att identifiera hot mot verksamheten och bedöma deras konsekvenser i organisationen och dess nätverk av aktörer och för att skapa en strategi för hantering av störningssituationer och kontinuitet i verksamheten under alla förhållanden[12].

Beredskap Åtgärder för att säkerställa att uppgifterna sköts så störningsfritt som möjligt och att eventuella behövliga åtgärder som avviker från det normala vidtas i störningssituationer och under undantagsförhållanden[13].

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

7 Terminologicentralen TSK TEPA-termbanken, Ordlista om cybersäkerhet (TSK 52, 2018)

8 Terminologicentralen TSK TEPA-termbanken, Ordlista om cybersäkerhet (TSK 52, 2018)

9 Terminologicentralen TSK TEPA-termbank, Vetenskapstermbanken 06.08.2019

10 Terminologicentralen TSK TEPA-termbanken, Ordlista om cybersäkerhet (TSK 50, 2017)

11 Finansministeriet, Anvisning för riskhantering, finansministeriets publikationer 22/2017, bilaga 1

12 Terminologicentralen TSK TEPA-termbanken, Ordlista om cybersäkerhet (TSK 52, 2018)

13 Terminologicentralen TSK TEPA-termbanken, Ordlista om cybersäkerhet (TSK 50, 2017)

Bilaga 2. Om nuläget för digital säkerhet

I enlighet med regeringsprogrammet för statsminister Sanna Marins regering effektiviseras den strategiska ledningen inom den offentliga förvaltningen, och det utarbetas riktlinjer för hur sådana data, datanät och informationssystem som är kritiska för tryggandet av samhällets funktioner ska utvecklas i den digitala verksamhetsmiljön. Statsrådets senaste principbeslut om utvecklingen av informationssäkerheten inom statsförvaltningen är från 2009. Sedan dess har såväl den offentliga förvaltningens strukturer och verksamhet som strategier, författningar och anvisningar förändrats avsevärt och hoten mot den digitala miljön har ökat. De största förändringarna är det ökade samarbetet och ömsesidiga beroendet mellan olika aktörer i samhället, en precisering av bestämmelserna inom den informations- och kommunikationstekniska sektorn, senast lagen om informationshantering inom den offentliga förvaltningen (906/2019), och Säkerhetsstrategin för samhället 2017, cybersäkerhetsstrategin från 2019 och centraliseringen av ICT-tjänsteproduktionen i kommunerna, samkommunerna och statsförvaltningen. Statens center för informations- och kommunikationsteknik, Valtori, grundades 2014 och Myndigheten för digitalisering och befolkningsdata 2020.

I strategin för cybersäkerheten i Finland 2019 ställs de viktigaste nationella målen upp för utvecklingen av cybermiljön och säkerställandet av de vitala funktioner som anknyter till den. Den baserar sig på de allmänna principerna i strategin för cybersäkerheten 2013. De tre strategiska riktlinjerna är: internationellt samarbete, bättre samordning av ledningen, planeringen och beredskapen inom cybersäkerheten samt utveckling av cybersäkerhetskompetensen. Avsikten är att dimensioneringen av resurser för cybersäkerheten och samarbetet ska förbättras av utvecklingsprogrammet för cybersäkerheten som sträcker sig över regeringsperioderna. Syftet med programmet är att konkretisera de nationella riktlinjerna och göra helhetsbilden av projekt, forskning och utvecklingsprogram tydligare. För samordning av den nationella utvecklingen av cybersäkerheten har en befattning som cybersäkerhetsdirektör inrättats vid kommunikationsministeriet.

På grund av förändringarna i samhället och för att precisera strategin för cybersäkerheten i Finland 2019 för den offentliga förvaltningens del behöver nuläget för den digitala säkerheten inom den offentliga förvaltningen ses över och utifrån utvärderingen dras upp riktlinjer för utvecklingen av den digitala säkerheten inom den offentliga förvaltningen. Syftet med riktlinjerna för den digitala säkerheten inom den offentliga förvaltningen är att säkerställa att hela den offentliga förvaltningen och dess tjänster fungerar, utan att det begränsas till tryggandet av samhällets vitala funktioner.

Det digitala samhället

Under de senaste åren har den digitala miljön och dess inverkan på samhället och den offentliga förvaltningen förändrats avsevärt. I takt med att digitaliseringen framskrider har information börjat användas i allt större utsträckning och mer effektivt med hjälp av ny teknik, såsom robotstyrd processautomation och artificiell intelligens. **Medborgarna** ska enligt planerna tillhandahållas människocentrerade tjänster som baserar sig på livssituationer och samfund tjänster som baserar sig på affärshändelser.

I internationella bedömningar[14] av hanteringen av och beredskapen för cybersäkerhet ligger Finland nära de ledande länderna. Inga omfattande dataläckage har förekommit i Finland. Den digitala säkerheten inom den offentliga förvaltningen utvecklas på ett decentraliserat sätt i olika förvaltningsorganisationer. I de flesta fall är förvaltningsorganisationernas interna ansvar för den digitala säkerheten tydligt. Den operativa ledningen av en situation med omfattande cyberkränkning har dock inte definierats och det finns skäl att förbättra bildandet av en operativ lägesbild av cybersäkerheten[15]. Det saknas riktlinjer för den digitala säkerheten i samhället som helhet, och ansvarsfördelningen behöver i vissa fall klargöras. Gemensamma riskhanteringsmetoder används inte fullt ut för att stödja beslutsfattandet.

Viktiga nationella och internationella aktörer inom digital säkerhet är ministerierna, myndigheter och samarbetsorgan som behandlar frågor som gäller digital säkerhet samt offentliga och privata tjänsteproducenter inom den digitala säkerheten[16] (bilaga 4). Främjandet av den digitala säkerheten i **samarbete mellan staten, kommunerna, den privata sektorn, forskningsvärlden, frivilligorganisationerna och medborgarna** kräver fortsatt utveckling jämfört med nuläget.

Internationell verksamhet

Frågor som gäller digital säkerhet och cybersäkerhet är i allt större utsträckning internationella politiska frågor som präglas av politiska konflikter. I det internationella samfundet har det under de senaste åren uppstått ett behov av att **stärka samarbetet** i säkerhetsfrågor som gäller den digitala miljön. Inom EU har det inrättats en ständig horisontell arbetsgrupp för cybersäkerhet vid Europeiska unionens råd och flera andra rådsarbetsgrupper tar upp cybersäkerhetsfrågor utifrån sina egna ansvarsområden. Verksamhetsfältet är inte

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

15 Statens revisionsverk, organisering av cyberskyddet, Revisionsberättelse 16/2017

16 Lehto, Limnéll, Kokkomäki, Pöyhönen, Salminen. Kyberturvallisuuden strateginen johtaminen Suomessa (Strategisk ledning av cybersäkerheten i Finland,) Publikationsserie för statsrådets utrednings- och forskningsverksamhet 28/2018

statiskt, utan de förändringar som ny teknik och artificiell intelligens medför återspeglas i debatten om internationella spelregler. Finland deltar i det internationella cybersäkerhetssamarbetet i syfte att stärka den lagstadgade internationella ordningen och främja demokrati, yttrandefrihet och rättsstatsprincipen.

Ledning och samarbete

Samarbetet inom den offentliga förvaltningen samt mellan den offentliga förvaltningen och sammanslutningar inom området för digital säkerhet är på en mycket god nivå i Finland. Utmaningen för **ledningen** av den offentliga förvaltningen är att djärvt främja ibruktagandet av nya digitala tjänster och samtidigt på ett ansvarsfullt sätt bedöma riskerna med dem samt hantera de kvarstående riskerna. Tillståndet inom den digitala säkerheten i den offentliga förvaltningen bedöms inte på ett heltäckande sätt. Det finns inga tydliga principer om vilka digitala tjänster och digitala säkerhetstjänster som det är motiverat att genomföra gemensamt.

Tekniska problem och störningar, naturfenomen samt olika former av påverkan kräver en fortlöpande och i fråga om kritiska funktioner centralt styrd utveckling av funktionssäkerheten. Den nuvarande sektorvisa utvecklingen inom den offentliga förvaltningen har inte lett till ett tillfredsställande slutresultat. Utvecklingen av informationsresurser, informationsnätverk och tjänster som är kritiska när det gäller samhällets funktion har inte styrts och tilldelats resurser centraliserat och det har inte ställts upp tydliga mål för utvecklingen.[17]

De flexibla **förutsättningar** och **samarbetsmodeller** under ständig utveckling som behövs i en snabbt föränderlig omvärld är inte tillräckligt tillgängliga för myndigheter och sammanslutningar. Till dessa hör gemensamma begrepp och strategier, kategorisering av allvarlighetsgraden för information och hantering av digitala tjänster samt ansvars- och beroendebeskrivningar.

I den offentliga förvaltningen saknas en organisation som ordnar **teknisk granskning** av informationssäkerhet och som till exempel skulle ansvara för en heltäckande skanning av kända sårbarheter. Säkerställandet av verksamhetsförutsättningarna för alla centrala sektorer för kontinuiteten i samhällets verksamhet, även i händelse av kränkningar av informationssäkerheten och cyberstörningar, är delvis otillräckligt.

17 Uudistuva, vakaa ja kestävä yhteiskunta (Ett förnybart, stabilt och hållbart samhälle, Finansministeriets tjänstemannainlägg) Finansministeriets publikationer 2019:11

Medborgare, personal och kompetens

Medborgarnas och invånarnas roll som producenter av digital säkerhet i samhället är bristfälligt identifierad och definierad. I digital säkerhet framhävs ofta tekniska lösningar i stället för kundorientering. Vid genomförandet söker man ännu förfaranden för att förena de delvis motstridiga målen för såväl säkerheten som integritetsskyddet.

Att förvärva och upprätthålla **kompetens** är betydande utmaningar i Finland. Det finns för få specialsakkunniga inom digital säkerhet och både den offentliga förvaltningen och privata tjänsteproducenter har rekryteringssvårigheter. Vid utläggning av tjänster överförs utvecklingen av organisationernas egen kompetens till tjänsteleverantörerna, vilket undergräver utvecklingen av den djupa kunskapen och överföringen av den tysta kunskapen inom organisationen. Utbildningsmaterial finns att tillgå för att utveckla kompetensen i digital säkerhet hos personalen inom den offentliga förvaltningen, men nivån på den systematiska kompetensutvecklingen varierar.

Ekonomi

Någon allmän **kostnads- och nyttomodell för investeringar** har inte fastställts för den digitala säkerheten i den offentliga förvaltningen och den digitala säkerhetens **effektivitet** är inte exakt känd. Detta beror delvis på att det är svårt att identifiera exakt hur stor del utvecklingen av den digitala säkerheten utgör av utvecklingen av den informations- och kommunikationstekniska infrastrukturen och de informations- och kommunikationstekniska tjänsterna. Därmed är det i nuläget svårt att bedöma om de ekonomiska resurser som anvisats för utveckling av den digitala säkerheten är tillräckliga. Säkerhetsincidenter som beror på bristfälliga resurser orsakar dock oftast mångdubbla kostnader jämfört med att risker kan förebyggas eller bekämpas på ett effektivt sätt. Det är svårt att mäta kostnaderna för kontinuiteten i förvaltningens verksamhet och ett förlorat förtroende i pengar.

Utvidgningen av digitaliseringen och koncentrationen av IKT-tjänsteproduktionen har medfört kostnadsbesparingar och utvecklat tjänsterna för kunderna, men samtidigt har det uppstått nya sårbarheter när det gäller tjänsternas kontinuitet samt uppgifternas tillförlitlighet, tillgänglighet och integritet. Angriparnas mångfald ökar och attackerna blir tekniskt alltmer avancerade, vilket innebär att organisationernas kapacitet att reagera effektivt på de ökande yttre hoten kan allvarligt försämras. I samband med digitaliseringen av tjänster har kostnadsbesparingarnas betydelse ökat när verksamheten förändras. **Riskhantering** har inte i tillräcklig utsträckning använts **vid bedömning av** den digitala säkerhetens **effektivitet** och för att uppnå balans mellan kostnadsbesparingar samt förbättrande av tjänsterna och deras säkerhet.

Tekniker

Utvecklingen av observationskapaciteten, **övervakningen** av systemen och hanteringen av sårbarheter samt den offentliga förvaltningens och företagens gemensamma genomförande av utvecklingen på basis av observationer ökar resursbehoven. De skapar också ett krav på att personalens arbetstid i allt högre grad ska inriktas på uppgifter inom den digitala säkerheten. **Proaktiv informationssäkerhet** och **automatisering** av den digitala säkerheten i rutinuppgifter utnyttjas inte i någon större utsträckning för att minska den arbetsinsats som behövs.

Molntjänster är både en möjlighet och ett hot ur ett digitalt säkerhetsperspektiv. Genom att stödja sig på molntjänster kan man öka funktionssäkerheten hos vissa offentliga förvaltningstjänster. Med hjälp av molntjänster kan man eventuellt också effektivt förebygga effekterna av överbelastningsattacker. Det finns inte tillräckligt med riktlinjer för en informationssäker användning av molntjänster samt för dataskydd och hantering av verksamhetens kontinuitet, vilket försvårar utnyttjandet av tjänsterna inom den offentliga förvaltningen. Digitaliseringen ökar ständigt efterfrågan på öppen och strukturerad information, och lokala och slutna informationssystem stöder inte denna utveckling. Det finns inte tillräckligt med informationssäkra databehandlingsmiljöer, såsom säkra offentliga och privata molntjänster eller lokala lösningar där data, algoritmer och förädlade data kan placeras. Utmaningar i fråga om molntjänster är ofta att olika stater har olika bestämmelser. Det innebär risker och osäkerhet för användarna om en tjänst tillhandahålls utanför Finland i enlighet med bestämmelserna i det landet.

Utnyttjandet av **artificiell intelligens** och **kvantteknik** är ny teknik som fortfarande är underutnyttjad. I samband med utvecklingen av artificiell intelligens diskuteras hur de data som används för att lära upp systemen påverkar den artificiella intelligensens funktion och hurdana etiska principer som bör beaktas. Det är svårt att bedöma hur snabbt kvantteknikenutvecklas och hur de risker som dess ibruktagande medför realiseras bl.a. vid avvecklingen av krypteringsalgoritmer.

Hotbedömningar

Ledningsgruppen för digital säkerhet inom den offentliga förvaltningen (VAHTI) publicerade 2019 en rapport om säkerheten i den digitala miljön. Enligt rapporten visar de största förändringarna i säkerhetsutmaningarna att organisationernas verksamhet för närvarande påverkas mest av olika – både små och omfattande – störningar i **IKT-tjänsteproduktionen**. I sådana situationer är det typiskt att tjänsterna inte fungerar, vilket samtidigt inverkar på tillgången till tjänsterna och den information som behandlas i dem. På så sätt kan störningar i tjänsteproduktionen ofta också leda till störningar i samband med den digitala säkerheten.

Lagstiftningsåtgärder har vidtagits för att säkerställa säkerheten i gemensamma, **centraliserade digitala tjänster** och serviceproduktionen i dem. En fullständig digital säkerhet är inte möjlig att genomföra, vilket understryker vikten av riskhantering som en del av ledningen av verksamheten. Utmaningen för organisationernas strategier på området digital säkerhet är strävan efter en kontinuerlig tjänst dygnet runt, vilket skulle kräva enhetligare verksamhetskulturer och t.ex. en tydligare hantering av störningssituationer. Även privatpersoner och sammanslutningar förväntar sig ofta att digitala tjänster är funktionssäkra dygnet runt, men inom statsförvaltningen finns inte en sådan centraliserad och kontinuerlig övervakningsfunktion (SOC) eller ett sådant servicehanteringssystem som skulle behövs för detta.

Att säkerställa säkerheten för de IKT-tjänster som produceras av utomstående **tjänsteproducenter** är en utmaning för organisationerna. Det görs försök att hantera denna utmaning genom avtal, men problemet är att få tillräckliga villkor i avtal med multinationella leverantörer. Utmaningarna i **produktionskedjorna** både utanför den offentliga förvaltningen och inom förvaltningen är risknivåer, informationssäkerhet, kompetens och produktionskapacitet. Hoten mot de gemensamma systemen är delade, men substansen och riskprofilerna är olika. I kommuner och samkommuner har de digitala säkerhetskoncepten inte förbättrats tillräckligt med de IKT-leverantörer som identifierats som centrala.

Upprepade kränkningar av informationssäkerheten i offentliga förvaltningsorganisationer och användningen av privatpersoners personliga utrustning för att genomföra dessa kränkningar visar att minimikraven på digital säkerhet inte till alla delar uppfylls. Utöver dataintrång undergräver också svårigheterna att använda autentiseringsförfaranden eller **identitetshantering** förtroendet för den offentliga förvaltningens digitala tjänster och äventyrar användarnas säkerhet och integritet. Den offentliga förvaltningen får inte överföra sina risker på dem som använder tjänsterna, och säkerhetskraven får inte vara ett hinder för användarna.[18]

För närvarande är den inbyggda informationssäkerheten hos olika slags **IoT-utrustning** ofta bristfällig, eftersom det vid tillverkningen eftersträvas så små kostnader som möjligt. Sådan utrustning kopplas dock i allt högre grad till industriella och andra automatiska lösningar. Cybersäkerhetscentrets cybersäkerhetsmärke, som visar att utrustningen uppfyller minst de grundläggande kraven på informationssäkerhet, är en betydande förbättring i detta avseende.

18 En utmaning ur serviceanvändarnas synvinkel är störningar i användningen av den offentliga förvaltningens digitala tjänster i situationer där det förutsätts att användarna iakttar vissa tidsfrister. Till exempel anmälan av inkomstuppgifter, ändring av skattesatsen eller anmälan till arbetskraftsbyrån kan visa sig vara utmanande inom utsatt tid, om den digitala tjänsten för detta ändamål inte är tillgänglig på grund av tekniska eller andra störningar. Det behövs klara riktlinjer för hur kunderna ska instrueras i händelse av långvariga störningar.

De gamla basinformationssystemen har ofta en bristfällig **arkitektur** och de tekniska lösningarna uppfyller inte de nuvarande kraven. I beställar-utförarmodellen försvåras lokaliseringen av problem av de utmaningar som vid hanteringen och övervakningen av helheten ofta uppstår i samband med den utlagda och centraliserade tjänsteproduktionen. Vid utveckling av delområdena inom digital säkerhet utnyttjas inte alltid internationella standarder i tillräcklig utsträckning. Det finns till exempel inte tillräckligt med riktlinjer för målet att använda certifieringar och certifierade produkter vid konkurrensutsättning av upphandling. Man sörjer inte för att de nationella referensramarna är internationellt kompatibla, kontrastera de kriterier för krav eller revision med avseende på informationssäkerheten som utarbetats i Finland.

Vid utvecklingen av nya innovationer och tekniska lösningar tas ofta inte tillräcklig hänsyn till ansvar och skapandet av etiska spelregler. Säkraverksamhetsmodeller har inte alltid integrerats i utvecklingsprocesser som syftar till att automatisera utveckling, testning och underhåll av programvara (DevOps).

Sammanfattning och slutsatser

Samhället måste avgöra vad som avses med genomförandet av säkerhet i en digital miljö. Vilka frågor ansvarar privatpersoner för vid hanteringen av den digitala säkerheten, vilka ansvarar sammanslutningar för, vilka ansvarar kommersiella producenter av t.ex. teknisk infrastruktur eller tjänster för och vilka frågor hör till kommunernas och samkommunernas eller de statliga myndigheternas ansvar? Ansvarsområdena ska vara tydliga och alla aktörer ska förstå dem på samma sätt.

Fenomenen och egenskaperna i den digitala miljön skiljer sig från den fysiska omvärlden, och därför bör **uppgifterna och ansvaret** förtydligas för att bättre återspegla den snabba förändring i omvärlden som digitaliseringen medför. Medborgarna, liksom också företag och olika sammanslutningar, måste kunna ansluta sig på ett säkert sätt till de normala digitala tjänster som förvaltningen tillhandahåller. Olika aktörer måste också kunna lita på att tjänsterna fungerar och i sista hand på myndigheternas hjälp i störningssituationer. På samma sätt måste kommunala aktörer kunna förlita sig på statliga aktörer i omfattande störningssituationer.

Den samhälleliga debatten om säkerheten i den digitala miljön och bekämpningen av de hot som den innebär har varit fokuserad på att utveckla verksamheten på operativ nivå för att hanterade de nuvarande kända hoten och störningarna. Särskild tonvikt har lagts vid utveckling av kapaciteten för observationer och hantering av störningar samt vid dataskydds- och informationssäkerhetsfrågor. Forskningen och styrningen av förvaltningen bör i högre grad inriktas på de **strategiskt** sett mest verkningsfulla frågorna på lång sikt. Riktlinjer som styr utvecklingen behövs för utnyttjande av nya servicelösningar, samarbete

mellan förvaltningen och företagen samt internationellt samarbete. Tydligare vägledning än för närvarande behövs för hur tjänster produceras och infrastrukturen byggs upp med nationella åtgärder och resurser, till vilka delar man stöder sig t.ex. på EU:s gemensamma utveckling eller annat internationellt samarbete och särskilt inom den offentliga förvaltningen på hur olika nya servicemodeller och tekniska möjligheter bör och kan utnyttjas vid produktion av offentliga digitala tjänster.[19]

Det är nödvändigt att **mäta** investeringarnas **produktivitet** för att de begränsade resurserna ska kunna fördelas så effektivt som möjligt. De mål som ställs för utvecklingsprojekten för digital säkerhet ska gagna samhället och vara mätbara. Både mätresultat och riskanalyser bör tillämpas vid planeringen av framtida investeringsprogram.

Leveranssäkerhet i fråga om datatrafik och elförsörjning är en grundläggande förutsättning för den digitala miljön. Säkerheten i informationsnätverk och leveranssäkerheten i elförsörjningen är för närvarande på en god nivå i Finland. Utvecklingen av den digitala miljön förutsätter att telekommunikationsoperatörerna och elnätsoperatörerna kontinuerligt förbättrar säkerheten, hanteringen och övervakningen. **Medborgarna** ska ha tillgång till en säker digital miljö där säkerheten motsvarar erfarenheten av säkerhet i den fysiska miljön. Detta innebär bl.a. bekämpning av attacker redan i datanätet, filtrering av sabotageprogram och förebyggande av överbelastningsattacker. Också myndigheternas befogenheter och organiseringen av tillsynsansvaret och tillsynsskyldigheterna i förhållande till tjänsteleverantörerna inom den digitala infrastrukturen ska bedömas.

Syftet med digitaliseringen är att väsentligt utveckla verksamhetsprocesserna och på samma sätt ska man förhålla sig till den digitala säkerheten med ett **innovativt** och nyskapande tänkande. Principerna om säkerhet som sådana ändras inte i samband med digitaliseringen, men de gamla säkerhetsåtgärderna kan förbigås om de upplevs vara faktorer som begränsar verksamheten. Säkerhetsmålen ska dock uppnås även i den nya verksamhetsmodellen, även om genomförandet förändras

19 Uudistuva, vakaa ja kestävä yhteiskunta (Ett förnybart, stabilt och hållbart samhälle, Finansministeriets tjänstemannainlägg) Finansministeriets publikationer 2019:11

Bilaga 3. Internationell jämförelse av digital säkerhet inom den offentliga förvaltningen

I en internationell jämförelse av digital säkerhet granskades styrning, uppgifter, strukturer, risker och resurser för digital säkerhet i jämförelsestaterna[20]. Jämförelsestaterna var Australien, Estland, Tyskland, Nederländerna, Israel, Storbritannien och Sverige. Jämförelseuppgifterna samlades in ur offentliga dokument i jämförelsestaterna på basis av frågor kring informationssökning som gällde lagstiftning, strategiska riktlinjer, organisering av verksamheten och resurser.

Termerna för digital säkerhet är varierande i jämförelsestaterna. Begreppen ”digital säkerhet”, ”cybersäkerhet” och ”informationssäkerhet” är inte heller helt etablerade i Finland och skillnaderna mellan begreppen ter sig delvis konstgjorda. I denna jämförelse består den digitala säkerheten av frågor som hör till informationssäkerhet, cybersäkerhet, kontinuitet och beredskap i verksamheten, riskhantering samt dataskydd. Bakgrundsmaterialet för jämförelsen består av material från alla delområden i varje jämförelsestat i den mån materialet fanns tillgängligt. Skillnaderna i begreppen och definitionerna syns också i bakgrundsmaterialet till utredningen: i jämförelsestaterna behandlades den digitala säkerheten i huvudsak i en cybersäkerhetsstrategi. I Sverige har riktlinjerna skrivits in i en informations- och cybersäkerhetshandlingsplan och i en digital agenda. I Nederländerna finns det utöver en cybersäkerhetsstrategi en separat digital agenda för samhället. I Tyskland och Storbritannien finns dessutom en separat digitaliseringsstrategi för förvaltningen. I bakgrundsmaterialet för jämförelsen användes dessutom nationella riskbedömningar samt dokument om skydd av kritisk infrastruktur och dataskydd och andra dokument som gäller digital säkerhet, när sådana fanns tillgängliga.

Lagstiftningen om digital säkerhet varierar, men EU:s allmänna dataskyddsförordning (GDPR) och direktivet om säkerhet i nätverk och informationssystem (NIS) förenhetligar praxis. Den nya EU-förordningen om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) 526/2013 (cybersäkerhetsakten) stärker EU:s gemensamma byrås (Enisa) roll som samordnare och rådgivare för cybersäkerheten och fastställer certifieringssystemet för processer, tjänster och produkter. Israel kräver personlig **certifiering** av personer som arbetar med cyberförsvar, intrångstest, utredning av kränkningar av informationssäkerheten, cybersäkerhetsmetoder eller cybersäkerhetsteknik. I Storbritannien kan Cyber Essentials-certifikatet skaffas av såväl företag och yrkespersoner som också

20 Internationell jämförelse av digital säkerhet, KPMG, februari 2020, på finska

privatpersoner. Finlands cybersäkerhetsmärke är ett exempel på en modell som kunde utnyttjas för certifiering av produkter och tjänster inom hela EU.

Digital infrastruktur behandlas inte som en separat helhet i jämförelsestaterna. Däremot anses den digitala infrastrukturen ingå i den fysiska världens strukturer, funktioner, tjänster och produkter och tryggandet av den är på motsvarande sätt en del av den allmänna beredskapen och kontinuitetshanteringen. Energiförsörjning och en fungerande datakommunikation ses som viktiga förutsättningar för ett digitaliserat samhälle.

I styrningen av den digitala säkerheten verkar trenden gå mot **centraliserade modeller** där det under ett ministerium har placerats en behörig myndighet som styr och samordnar, men också ger anvisningar och utbildar samt övervakar och reagerar. I en starkt decentraliserad modell kan kommunikationen mellan aktörerna och behörighetsfrågorna bli utmanande. Dataskyddsmyndigheten enligt GDPR ansvarar för dataskyddet i EU-staterna, men det finns dock stora skillnader i fråga om resurserna: I Finland har dataombudsmannens byrå tre fast anställda, i Estland 19, i Sverige 75 och i Tysklands federala myndighet 190. Israel och Australien har också en dataskyddsmyndighet med liknande uppgifter som EU-staternas myndigheter.

Risker i samband med den digitala säkerheten i jämförelsestaterna har behandlats i nationella riskbedömningar eller cybersäkerhetsstrategier. I dessa identifieras **fientlig påverkan** från främmande stater eller grupper som stöds av dem nästan undantagslöst som en strategisk risk. Cyberattacker betraktas som betydande hot bl.a. för att de anses kunna destabilisera samhället, t.ex. genom hybridpåverkan eller falska nyheter. Dessutom är den teknik som behövs för attacker lättillgänglig och risken för att angriparen ska bli fast är liten. För att förbättra säkerheten i den digitala miljön behövs det konkreta åtgärder som täcker olika samhällsområden och vars genomförande regelbundet följs upp, t.ex. med hjälp av cybersäkerhetsstrategin på samma sätt som i Storbritannien.

I jämförelseländerna betraktas den offentliga förvaltningen, näringslivet, högskolorna och forskningsinstituten samt medborgarna allmänt som aktiva aktörer inom den digitala säkerheten. **Samarbetet** mellan alla aktörer ger en mer heltäckande lägesbild av den digitala säkerheten. Utvecklingen av nya digitala produkter och tjänster kommer att leda till att hela cyberbranschen växer och ge nya exportmöjligheter. Israel och Nederländerna är exempel på stater där samhällsekonomisk nytta eftersträvas genom utveckling av branschen och forskningen.

I Finland har **medborgarnas** roll och ansvar som aktiva säkerhetsfaktorer i samhället inte definierats, till skillnad från i jämförelsestaterna. I dem är utveckling av kunnandet i hela samhället en strategisk prioritering och utveckling av färdigheterna och kunnandet i digital säkerhet ett strategiskt huvudmål.

Förändringar i den digitala miljön som utvecklas snabbt kräver en snabb och internationellt effektiv **observations- och reaktionskapacitet**. Cybermiljön och hoten mot den, såsom cyberspionage, cyberterrorism eller annan cyberbrottslighet, följer inte statsgränserna, så nya former av specialkompetens, informationsutbyte och samarbete mellan säkerhetsmyndigheterna är nödvändiga såväl nationellt som internationellt.

Slutsatser om den internationella jämförelsen

Den digitala infrastrukturen ska vara **en del av servicestrukturerna** och den digitala säkerheten en del av servicehelheten. Tjänsteleverantören ska svara mot kraven på digital säkerhet och garantera en säker användning av tjänsten. Finland ska systematiskt förutsätta att internationella **standarder** och kriterier för digital säkerhet tillämpas. De nationella kraven på den digitala säkerhetens delområden ska användas för att komplettera de internationella standarderna, inte för att ersätta dem.

Den digitala säkerhetens betydelse är allmänt erkänd och i många länder (bl.a. Sverige, Nederländerna, Tyskland, Estland) har man strävat efter att utveckla **lagstiftningen** så att den motsvarar de snabba förändringarna i den digitala miljön. Som konstateras ovan tas digitaliseringen av samhället i allmänhet upp i staternas cybersäkerhetsstrategier. I Tyskland har informationssäkerheten i myndighetssystemen och nätverk höjts till grundlagsnivå. Eftersom den digitala omvärlden överskrider de nationella gränserna måste lagstiftningen om den digitala säkerheten vara internationell, vilket förutsätter att Finland aktivt deltar i beredningen av EU:s lagstiftning: behovet av reglering i samhället ska följas upp och ändringsbehoven ska bemötas snabbt. Finland ska till exempel delta i arbetet med att utarbeta etiska principer för lärande system och anvisningar för övervakningen av användningen samt ta dem i bruk.

I jämförelsestaterna **centraliseras** ledningen av den digitala säkerheten och myndigheter slås samman till större helheter, och i Sverige bereds inrättandet av en ny centraliserad cybersäkerhetsmyndighet. Internationellt samarbete förutsätter tydliga ansvarsområden och roller. Finland ska utvärdera **ledningsstrukturerna, ansvaret och rollerna** för den digitala säkerheten samt förnya dem i enlighet med den internationella utvecklingen. Ansvaret för samordning och genomförande kan delas upp, men ansvarsområdena ska definieras tydligt för att säkerställa ett fungerande nationellt och internationellt samarbete. Behörighetsfrågorna får inte hindra utvecklandet av den digitala säkerheten. Finland bör öka samarbetet mellan alla aktörer inom den digitala säkerheten för att stärka ett tryggt digitalt samhälle.

Det är inte möjligt att bedöma investeringarna i den digitala säkerheten i jämförelsestaterna utifrån den information som samlats in. Målen för utvecklingsprojekten för säkerheten i den digitala omvärlden ska gagna samhället och nyttan ska kunna mätas.

Mätresultaten och riskanalyserna ska tillämpas vid planeringen av framtida investeringsprogram. Minimikrav för digital säkerhet ska fastställas för den teknik som används i samhällstjänster och genomförandet av dem ska övervakas. Minimikrav för personalens digitala säkerhetskompetens ska fastställas för de mest kritiska uppgifterna med tanke på säkerheten.

Utvecklingen av digital **säkerhetskompetens** är en del av strategierna i nästan alla jämförelsestater. Respektive myndighet i jämförelsestaterna (t.ex. i Sverige Myndigheten för samhällsskydd och beredskap, i Storbritannien National Cyber Security Centre och i Nederländerna Autoriteit Persoonsgegevens) ger anvisningar och utbildning för den offentliga förvaltningen, näringslivet och privatpersoner. Alla aktörer i det finländska samhället – förvaltningen, näringslivet, högskolorna och forskningsinstituten samt medborgarna – ska spela en aktiv roll i den digitala säkerheten. Utvecklandet av färdigheterna i digital säkerhet ska vara en strategisk prioritering i hela samhället. Till exempel medborgarnas bristfälliga säkerhetsfärdigheter och säkerhetslösningar i den digitala miljön öppnar ett brett anfallsområde mot produktionen av digitala tjänster. Sverige, Nederländerna och Estland har som mål att öka de digitala färdigheterna (bl.a. medieläskunnighet och cybersäkerhet) redan i läroplanerna på första och andra stadiet för att förbereda elevernas och studerandenas färdigheter. I Israel har genomförandet redan hunnit längre och cybersäkerheten är också en del av beväringstjänsten. I Storbritannien har man riktat olika cybersäkerhetskurser till tonåringar. Syftet med kurserna är förutom att öka de ungas färdigheter också att locka unga till cybersäkerhetsbranschen.

De hotanalyser som utförs i jämförelsestaterna liknar i regel varandra, men helheten är inte särskilt tydlig i en enda av de granskade staterna. Finland bör tydligt beskriva **hoten** mot den digitala säkerheten i en form som förstås av alla aktörer i samhället. Strategiska riktlinjer för att minska konsekvenserna av hot ska beskrivas som konkreta operativa uppgifter i genomförandeplanen. Ett nära samarbete mellan myndigheterna och näringslivet betonas i nästan alla jämförelsestater. Förvaltningen, medborgare och sammanslutningar ska **erbjudas stöd** för identifierade störningar i den digitala säkerheten. Storbritannien har till exempel inrättat en enhet som specialiserat sig på cyberbrottslighet vid alla lokala polisavdelningar.

Bilaga 4. Aktörer och uppgifter inom den offentliga förvaltningens digitala säkerhet

Den offentliga förvaltningen är långt digitaliserad, vilket innebär att alla aktörer inom den offentliga förvaltningen behöver digital säkerhet. Centrala aktörer när det gäller digital säkerhet inom den offentliga förvaltningen är för närvarande:

Riksdagen

Riksdagens kansli har till uppgift att skapa förutsättningar för riksdagen att sköta sina riksdagsuppgifter som statligt organ. Kansliets tjänster stöder också lagstiftningsarbetet, beslutsfattandet och det internationella samarbetet i anknytning till den digitala säkerheten. Riksdagen främjar öppenhet, tillgänglig information och demokrati.

Syftet med den digitala säkerheten i riksdagen är att säkerställa kontinuiteten i riksdagens verksamhet och att förebygga externa störningar. Eftersom riksdagen är det högsta statliga organet måste kontinuiteten i verksamheten säkerställas under alla omständigheter. En tillförlitlig kommunikation i rätt tid är en viktig del av den digitala säkerheten i riksdagen.

Statens revisionsverk

Statens revisionsverk granskar statens finanser och egendomsförvaltning samt övervakar finanspolitiken samt partifinansieringen och valfinansieringen. Genom sin verksamhet säkerställer Statens revisionsverk att statliga medel används i enlighet med lagen och på ett rationellt sätt till de objekt som riksdagen anvisar samt övervakar att finanspolitiken sköts på ett hållbart sätt. Statens revisionsverk bidrar också till att säkerställa principerna om rättsstat, demokrati och en hållbar ekonomi också inom Europeiska unionens ekonomiska förvaltning och i annat internationellt samarbete.

En rationell användning av medel när det gäller digital säkerhet innebär att digitala förvaltningstjänster är lättillgängliga, lätta och säkra att använda och dessutom produceras på ett ekonomiskt hållbart sätt. I sådana fall har hänsyn också tagits till en säkrad kontinuitet i tjänsterna. Statens revisionsverks mål är att stärka förtroendet för att den finländska statsförvaltningen fungerar öppet, resultatrikt och hållbart också digitalt.

Folkpensionsanstalten (FPA)

Folkpensionsanstalten (FPA) är en självständig offentligrättslig inrättning, vars förvaltning och verksamhet övervakas av fullmäktige som väljs av riksdagen. FPA har hand om den

sociala tryggheten i olika livssituationer för dem som bor i Finland och för många finländare som bor utomlands. Utöver sin självständiga ställning är Folkpensionsanstalten en betydande producent av riksomfattande informationssystemtjänster. Vid FPA:s it-tjänster arbetar över 700 it-experter, t.ex. apputvecklare, informationssäkerhetsarkitekter, webbtrafiks- och serverexperter. Informations- och cybersäkerheten i de informationssystem som FPA producerar är ytterst viktig med tanke på säkerställandet av tillgången till informationsinnehållet i de riksomfattande informationssystemen och de tjänster som tillhandahålls av FPA. I måltillståndet har kontinuiteten i FPA:s riksomfattande informationssystemstjänster säkerställts i alla situationer.

Finlands Bank

Ibruktagande och allmän övervakning av sådana infrastrukturer inom finanssektorn som är kritiska ur samhällets synvinkel, såsom principer och ramar som stöder cybersäkerheten i betalnings- och clearingsystem.

Finansinspektionen

Finansinspektionen har en central roll som övervakare av den digitala säkerheten inom finansbranschen. Finansinspektionen svarar för tillsynen över och kontrollen av operativa risker, cybersäkerhet och betalningssystem hos de aktörer som står under dess tillsyn. Dessutom meddelar Finansinspektionen föreskrifter och anvisningar inom ämnesområdet. Finansinspektionen deltar också i försörjningsberedskapsarbetet som medlem av pooler som lyder under finanssektorn. Dessutom har Finansinspektionen en stark roll när det gäller att skapa en lägesbild över den digitala säkerheten och cybersäkerheten inom finansbranschen under normala förhållanden och undantagsförhållanden genom uppföljning av de störnings- och incidentanmälningar som tillsynsobjekten sänder till Finansinspektionen.

Statsrådets kansli

Statsrådets kansli ansvarar under statsministerns ledning för tillsynen över genomförandet av regeringsprogrammet och biträder statsministern vid ledningen av statsrådets verksamhet. Kansliet tryggar statsministerns och regeringens verksamhetsförutsättningar under alla förhållanden. Till statsrådets kanslis ansvarsområde hör bl.a. statsrådets gemensamma lägesbild, beredskap och säkerhet, den allmänna samordningen av hanteringen av störningssituationer samt statsrådets och ministeriernas gemensamma informationsförvaltning och dokumentförvaltning.

Suomen Erillisverkot Oy

Suomen Erillisverkot Oy är ett bolag med specialuppgifter som ägs helt av finska staten. Det tryggar den kritiska ledningen av samhället och informationssamhällets tjänster under alla förhållanden. Bolaget erbjuder myndigheterna och kritiska aktörer med tanke på försörjningsberedskapen säkra och funktionssäkra IKT-tjänster. Bolaget utvecklar samhällets övergripande säkerhet och påverkar medborgarnas liv genom sin verksamhet.

Utrikesministeriet

Cybermiljön och cybersäkerheten har blivit en viktig del av Finlands utrikes- och säkerhetspolitik. Cyberhot känner inga statsgränser. För att stärka cybersäkerheten krävs ett alltmer fördjupat internationellt samarbete. Utrikesministeriet samordnar denna internationella verksamhet. Utrikesministeriet är också nationell säkerhetsmyndighet (National Security Authority, NSA). Den nationella säkerhetsmyndigheten har i enlighet med lagen om internationella förpliktelser som gäller informationssäkerhet till uppgift att styra och övervaka att den internationella säkerhetsklassificerade information som lämnats till Finland skyddas och behandlas på behörigt sätt. NSA styr den nationella verksamheten och ansvarar bland annat för beredningen av internationella överenskommelser om informationssäkerhet.

Dataombudsmannens byrå

Dataombudsmannen är en nationell tillsynsmyndighet som övervakar efterlevnaden av dataskyddslagstiftningen. Dataombudsmannen och de biträdande dataombudsmännen ska vara självständiga och oberoende i sin uppgift. Dataombudsmannen har till uppgift att främja tillgodoseendet av de kunskapsmässiga och andra grundläggande fri- och rättigheterna vid behandlingen av personuppgifter och skapandet av förtroende. Dataombudsmannen behandlar bland annat anmälningar om personuppgiftsincidenter, godkänner utfärdare av certifikat och utför kontroller av informationssystem. Dataombudsmannen får vid behov påföra administrativa sanktioner och utöva andra befogenheter. Dataombudsmannen företräder Finland i Europeiska dataskyddsstyrelsen.

Inrikesministeriet

Inrikesministeriet bereder lagstiftning som gäller polisen, räddningsväsendet, nödcentralsverksamheten, gränsbevakningen, sjöräddningen och invandringen.

Polisen

Polisen har till uppgift att förebygga, röja, utreda och föra brott till åtalsprövning. Cyberbrott undersöks vid polisinrättningarna i enlighet med territorialitetsprincipen.

Skyddspolisen

Skyddspolisen har till uppgift att förebygga och avvärja de allvarligaste hoten mot den nationella säkerheten, såsom terrorism och olaglig underrättelseinhämtning som främmande stater riktar mot Finland. Skyddspolisen utför dessa uppgifter också i den digitala miljön. Dessutom genomför skyddspolisen en proaktiv underrättelseanalys av fenomen som hotar den nationella säkerheten till stöd för statsledningens och andra myndigheters beslutsfattande.

Centralkriminalpolisen, Cyberbrottsbekämpningscentret

Centralkriminalpolisens cyberbrottsbekämpningscenter har följande huvudsakliga uppgifter i kampen mot cyberbrottslighet: undersökning av de allvarligaste datanätsbrotten, upprätthållande av en lägesbild över datanätsbrottsligheten, underrättelseinhämtning som avser internet och datanät, datateknisk undersökning samt sakkunnigtjänster för polisen och andra myndigheter i anslutning till förundersökningen.

Försvarsministeriet

Försvarsministeriet ansvarar som en del av statsrådet och som ledare för sitt förvaltningsområde för den nationella försvarspolitiken och säkerheten samt för det internationella försvarspolitiska samarbetet. Ministeriet svarar för det militära försvarets resurser och för försvarsmaktens verksamhetsbetingelser. Det ansvarar för Finlands deltagande i internationell krishantering och för att påverka Europas säkerhetsstrukturer i syfte att trygga nationella intressen. Försvarsministeriet svarar också för samordningen av totalförsvaret och för en hållbar försvarsvilja. Ministeriet ger andra myndigheter handräckning på begäran.

Säkerhetskommittén

Säkerhetskommittén bistår statsrådet och ministerierna i omfattande frågor som gäller den övergripande säkerheten. Kommittén följer utvecklingen i Finlands säkerhetsmiljö och samhälle samt samordnar den föregripande beredskapen i anslutning till den övergripande säkerheten. Den nya cybersäkerhetsstrategin 2019 baserar sig på de allmänna principerna i strategin för cybersäkerheten i Finland 2013. I enlighet med riktlinjerna i strategin (2013) följer och samordnar Säkerhetskommittén verkställandet av strategin. Målen med samordningen av cybersäkerheten är att undvika överlappande verksamhet, identifiera eventuella brister och försäkra sig om ansvariga parter. De egentliga besluten fattas av behörig myndighet i enlighet med vad som föreskrivs om saken.

Försvarsmakten

Försvarsmakten håller på att skapa en övergripande cyberförsvarskapacitet för sina lagstadgade uppgifter som en del av tryggandet av samhällets vitala funktioner. Med 'cyberförsvar' avses det försvarsområde av den nationella cybersäkerheten som bildas av kapaciteterna underrättelse, påverkan och skyddande. Med cyberförsvarets kapaciteter produceras underrättelseinformation till stöd för beslutsfattandet i statsledningen och försvarsmaktens ledning samt stöds försvarsmaktens insatser genom att skydda förutsättningarna för eget beslutsfattande.

Hoten mot cybermiljön har fått allt farligare konsekvenser för samhället. Attacker i cybermiljön kan användas som verktyg för politiska och ekonomiska påtryckningar och i en allvarlig kris som en påverkningsmetod vid sidan av traditionella militära maktmedel. Försvarssystemet är beroende av cybermiljöns tillgänglighet och med tanke på den militära verksamheten ska det också ses som en möjlighet och resurs.

Finansministeriet

Finansministeriet ansvarar som en del av statsrådet för den ekonomiska politik som stärker förutsättningarna för en stabil och hållbar tillväxt, för en god skötsel av statsfinanserna och för verksamhetsförutsättningarna för en hållbar kommunal ekonomi samt för en resultatrik offentlig förvaltning. I finansministeriets uppgifter ingår de allmänna grunderna för den offentliga förvaltningens informationspolitik, informationshantering och elektroniska tjänster. I samband med detta bereder finansministeriet allmänna grunder och krav för den offentliga förvaltningens IKT-infrastruktur, digitala tjänster och digital informationssäkerhet samt riktlinjer, författningar och utvecklingsprogram för den offentliga förvaltningens digitala säkerhet och styr genomförandet av dem samt tillsätter behövliga ledningsgrupper och samarbetsnätverk. Finansministeriet har tillsatt en strategisk ledningsgrupp för den digitala säkerheten inom den offentliga förvaltningen för att främja digitaliseringen och den digitala säkerheten på ett balanserat sätt.

Finanscontrollerfunktionen

Finanscontrollerfunktionen ska bland annat följa, utvärdera och utveckla organiseringen av den interna kontrollen och riskhanteringen inom statsförvaltningen. Funktionen kan lägga fram en rapport om sina iakttagelser till statsrådet och ministeriet samt statens ämbetsverk, inrättningar, affärsverk och fonder tillsammans med eventuella åtgärdsförslag.

Finanscontrollerfunktionen leder den delegation för intern kontroll och riskhantering som tillsatts av statsrådet. Delegationen följer och utvärderar metoderna för intern kontroll och riskhantering och den allmänna utvecklingen, den interna kontrollens funktion och användningen av förfarandena vid styrningen och ledningen av ekonomin och

verksamheten samt tar initiativ för att utveckla den interna kontrollen och dess riskhantering.

Informationshanteringsnämnden

En av informationshanteringsnämndens uppgifter är att främja förfarandena för informationshantering och informationssäkerhet samt uppfyllandet av kraven. Informationshanteringsnämnden kan tillsätta tillfälliga sektioner samt publicera rekommendationer och ordna seminarier och andra evenemang.

Myndigheten för digitalisering och befolkningsdata

Myndigheten för digitalisering och befolkningsdata ska främja digitaliseringen av samhället, trygga uppgifternas tillgänglighet och tillhandahålla tjänster för olika händelser i kundernas liv. Myndigheten ansvarar för flera servicehelheter vars störningsfria, säkra och smidiga funktion är viktig för att samhället ska fungera. Högklassiga befolkningsuppgifter, certifieringstjänster och stödtjänster för e-tjänster bidrar till att skapa de förutsättningar som digitaliseringen kan byggas på. Myndigheten har till uppgift att garantera funktionssäkerheten och säkerheten i fråga om dessa tjänster. Myndigheten ansvarar för experttjänsterna inom digital säkerhet och bereder rekommendationer och anvisningar. Myndigheten svarar också för verksamheten i ledningsgruppen för digital säkerhet inom den offentliga förvaltningen (Vahti). Myndigheten har tillsatt ett utvecklingsprogram för digital säkerhet inom den offentliga förvaltningen (JUDO-programmet) för åren 2019–2021.

Statens informations- och kommunikationstekniska center Valtori

Valtori producerar icke branschspecifika IKT-tjänster inom statsförvaltningen samt informations- och kommunikationstekniska tjänster och integrationstjänster som uppfyller kraven på hög beredskap och säkerhet. Valtori har till uppgift att säkerställa att informations- och cybersäkerheten i fråga om de tjänster som centret ansvarar för samt hanteringen av kontinuiteten och beredskapen uppfyller de fastställda kraven i en snabbt föränderlig omvärld. För att uppfylla kraven skapar och vidareutvecklar Valtori i fråga om cybersäkerheten en heltäckande lägesbild och observationskapacitet. Dessa möjliggör snabba reaktioner på it-händelser och störningssituationer. Observationskapaciteten förverkligas i myndighetssamarbete vid cyberoperationscentret (CSOC) som täcker Valtoris båda affärsmiljöer. När det gäller informationssäkerhet och digital säkerhet finns det en formbunden modell för hantering av informationssäkerheten som säkerställer gemensamma verksamhetsprocesser och möjliggör en affärscentrerad risk- och incidenthantering.

Undervisnings- och kulturministeriet

Undervisnings- och kulturministeriet svarar för utvecklingen av utbildnings-, vetenskaps-, kultur-, idrotts- och ungdomspolitiken och för det internationella samarbetet. Undervisnings- och kulturministeriets uppgifter i anknytning till digital säkerhet omfattar bland annat att upprätthålla utbildnings- och forskningssystemet samt kompetensen, trygga förutsättningarna för upprätthållande av biblioteks- och andra kulturtjänster och skydda kulturegendom.

Undervisnings- och kulturministeriet styr flera digitala tjänster och register inom utbildning. Ministeriets ansvarsområde ansvarar för tillgången på tillräcklig yrkeskunnig arbetskraft samt för utvecklandet av de färdigheter och den kompetens som krävs i medborgarnas digitala miljöer, t.ex. mediekompetens, på alla utbildningsnivåer. Kompetensutveckling kommer att stärka medborgarnas förtroende och delaktighet i ett digitaliserat samhälle. Aktörerna inom undervisnings- och kulturministeriets ansvarsområde ansvarar också för att utveckla specialkompetens och forskning inom området digital säkerhet. Dessutom har ministeriets förvaltningsområde till uppgift att på lång sikt eller permanent och i en begriplig form bevara det digitala informationsmaterial som uppstår inom statsförvaltningen och det centrala kulturarvet i digital form. Ministeriet styr övriga aktörer inom den offentliga förvaltningen i ärendet.

Kommunikationsministeriet

Kommunikationsministeriet svarar för utvecklingen av informationssäkerheten i fråga om elektroniska kommunikationstjänster och kommunikationsnät. Detta innebär t.ex. utveckling av bestämmelserna om informationssäkerhet i fråga om elektroniska kommunikationstjänster eller elektroniska kommunikationsnät, strategiarbete eller annan allmän styrning. Under kommunikationsministeriet finns Transport- och kommunikationsverket, som bildades vid ingången av 2019. Cybersäkerhetscentret, som också är internationellt erkänt, är en del av Transport- och kommunikationsverket.

Cybersäkerhetscentret vid Transport- och kommunikationsverket

Cybersäkerhetscentret vid Transport- och kommunikationsverket spelar en viktig roll i beredskapen i det digitala samhället. Centret ska genom sin verksamhet sörja för att samhället fungerar också vid störningar under normala förhållanden och under undantagsförhållanden, bland annat genom att säkerställa funktionen och säkerheten i allmänna kommunikationsnät och kommunikationstjänster och andra kommunikationsnät och kommunikationstjänster som är knutna till dem liksom för tillgång till frekvenser och krypteringstekniskt material, till exempel för säkerhetsmyndigheternas behov. Dessutom ansvarar centret för Finlands nationella toppdomän .fi och driver fi-namnservrar och övervakar registratorer.

Centret främjar konfidentialiteten i kommunikationen och övervakar i enlighet med bestämmelserna integritetsskyddet inom telekommunikationen. CERT-funktionen (Computer Emergency Response Team) vid Cybersäkerhetscentret sköter centrets lagstadgade uppgifter i samband med förebyggande och utredning av samt information om kränkningar av informationssäkerheten samt upprätthåller och distribuerar en lägesbild över cybersäkerheten. CERT-funktionen producerar och upprätthåller en lägesbild över cybersäkerheten tillsammans med betrodda inhemska och utländska samarbetspartner och motparter. Cybersäkerhetscentret CERT är en känd och betrodd samarbetspartner i flera internationella nätverk som har byggts upp under de 19 år som gått sedan CERT-funktionen inrättades.

Social- och hälsovårdsministeriet

Social- och hälsovårdsministeriet styr flera uppgifter som är viktiga för samhället. Den sociala tryggheten ansvarar för alla sociala förmåner och bland annat för försäkringar och pensioner. Social- och hälsotjänsterna svarar åter för tjänsterna inom socialvården samt hälso- och sjukvården. Området omfattar dessutom bland annat miljö- och hälsoskyddet. Utöver den egentliga verksamheten styr ministeriet också säkerhetsfrågor i relation till dessa. Det bör noteras att aktörerna på dessa områden inte bara är offentliga förvaltningsmyndigheter, utan omfattar många privata aktörer och även tredje sektorn. Säkerhetskraven kan gälla patientsäkerhet, där informationens tillgänglighet och korrekthet spelar en viktig roll, förordningen om medicintekniska produkter, som säkerställer säker drift av medicintekniska produkter som för närvarande ofta är nätanslutna datorer, eller dataskyddsförordningen, eftersom många känsliga personuppgifter behandlas inom sektorn. Utöver dessa krav omfattas system som är kopplade till nationella elektroniska tjänster av en mängd säkerhetskrav och måste certifieras. Ministeriet styr verksamheten och ansvarar för lagstiftningen medan myndigheterna i den underlydande förvaltningen (i synnerhet Institutet för hälsa och välfärd, Fimea och Valvira) ansvarar för verkställandet.

Tillståndsmyndigheten Findata

Findata är en tjänst för sekundär användning av social- och hälsovårdsdata. Myndigheten beviljar tillstånd till sekundär användning av personuppgifter inom social- och hälsovården när data från flera registeransvariga samkörs, registeruppgifterna härstammar från privata serviceanordnare inom social- och hälsovården eller när det är fråga om data som lagrats i hälsoarkivstjänsterna. Findata finns i anslutning till Institutet för hälsa och välfärd, avskilt från Institutet för hälsa och välfärds övriga verksamhet.

Jord- och skogsbruksministeriet

Jord- och skogsbruksministeriet styr, främjar och övervakar den digitala säkerheten inom sitt ansvarsområde. Viktiga uppgifter med tanke på den digitala säkerheten är att upprätthålla fastighetsdatasystemet och terrängdatasystemet och trygga kontinuiteten i systemen i alla säkerhetssituationer, trygga tillgången till statistiska uppgifter och genomföra det utbetalande organets uppgifter i enlighet med ISO27001-certifikatet. NIS-direktivet förpliktar företag som är kritiska med tanke på försörjningsberedskapen och centrala leverantörer av digitala tjänster att rapportera incidenter i informationssäkerheten till tillsynsmyndigheten inom sin sektor. Inom jord- och skogsbruksministeriets ansvarsområde gäller NIS-anmälningsskyldigheten vattentjänstverk som levererar minst 5 000 kubikmeter vatten per dygn eller tar emot avloppsvatten.

Lantmäteriverket

Till Lantmäteriverkets verksamhetsområde hör verksamhet i anslutning till register som behövs för att trygga ägandet av fastigheter och aktielägenheter, besittningen av fastigheter och andra registerenheter, krediteringssystemet och lokaliseringen, främjande av interoperabiliteten för och användningen av geografisk information samt forskning inom området för geografisk information och fastighetsbranschen. Dessutom sörjer Lantmäteriverket för grunderna för lokalisering och produktionen av grundläggande geografisk information samt producerar sakkunnigtjänster för samhället

Livsmedelsverket

Livsmedelsverket svarar för uppgifterna som utbetalande organ i Finland i enlighet med kommissionens krav. Kravet är att det utbetalande organet har ett certifierat ledningssystem enligt ISO/IEC 27001 och, när det gäller det utbetalande organets delegerade uppgifter, att informationssäkerhet säkerställs enligt ISO/IEC 27001 och 27002 standarder i överensstämmelse med det utbetalande organets verksamhet. Det utbetalande organets delegerade uppgifter har överförts till närings-, trafik- och miljöcentralerna, samarbetsområdena, Tullen och Åland.

Arbets- och näringsministeriet

Arbets- och näringsministeriet styr och svarar för informationssäkerheten i fråga om förvaltningsområdets funktioner och datalager samt för den lagstiftning som styr uppgifterna och funktionerna. Ämbetsverken och inrättningarna inom förvaltningsområdet ansvarar för verkställandet av tjänsterna. Centrala funktioner som ska tryggas är basregister i företag och sammanslutningar och deras verksamhet (riktighet och tillgänglighet), arbetskraftsverksamheten som helhet (dataskydd och tillgänglighet), säkerställande av

energiförsörjningen samt finansiella tjänster som innehåller affärshemligheter och riktar sig till näringslivet (processäkerhet).

Försörjningsberedskapscentralen

Försörjningsberedskapscentralen är en inrättning inom arbets- och näringsministeriets förvaltningsområde som har till uppgift att planera och bedriva operativ verksamhet i samband med upprätthållandet och utvecklandet av försörjningsberedskapen i landet. I samarbete med andra myndigheter och näringslivet säkerställer Försörjningsberedskapscentralen att de system som är mest kritiska för samhället fungerar i alla situationer. Försörjningsberedskapscentralen leder och finansierar programmet som gäller den digitala säkerheten 2030 och som förbättrar säkerheten i cyberinfrastrukturen och den digitala infrastrukturen med inriktning på behoven i näringslivet.

Teknologiska forskningscentralen VTT Ab

Teknologiska forskningscentralen VTT Ab är ett icke-vinstdrivande bolag som helt och hållet ägs av staten och som utför en specialuppgift. VTT tillhandahåller tjänster för digital säkerhet för företag och den offentliga förvaltningen.

Miljöministeriet

Miljöministeriets vision är ”en bättre miljö för kommande generationer”. Ministeriet har tre strategiska effektmål som alla överskrider förvaltningsgränserna: 1. En god miljö och biologisk mångfald, 2. Ett koldioxidneutralt kretsloppssamhälle och 3. En hållbar stadsutveckling. Miljöministeriet ansvarar tillsammans med Finlands miljöcentral för den digitala säkerheten och tillgängligheten i miljöinformationssystemen samt styr och främjar den digitala säkerheten i informationssystemen för den byggda miljön. Under ledning av miljöministeriet inleddes hösten 2019 ett arbete för att utveckla en informationsplattform för den byggda miljön i samarbete med andra ministerier. Arbetet inbegriper omfattande datahelheter i fråga om både cybersäkerhet och dataskyddsfrågor. Miljöministeriet tar å sin sida hänsyn till kraven på digital säkerhet vid byggandet och användningen av informationsplattformen.

Kommuner och samkommuner

Kommunerna tillhandahåller sina invånare tjänster, varav största delen anges som kommunernas uppgifter i lag. Kommunernas verksamhet är sektorsövergripande, vilket ställer utmaningar för den digitala säkerheten. Kommunstyrelsen har till uppgift att sörja för ordnandet av riskhanteringen. Enligt Kommunförbundets utredning sköts grundläggande informationsteknik, informationssäkerhet, upphandling och konkurrensutsättning

av informationsteknik, utveckling och underhåll i kommuner och samkommuner i stor utsträckning som eget arbete. Det finns skillnader mellan kommunerna och samkommunerna och kommunstorleken har betydelse för hur dessa ordnas. Via de bolag som ägs av kommuner och samkommuner sköts informationssäkerheten av uppskattningsvis cirka en tredjedel, och köpta tjänster används av uppskattningsvis cirka en femtedel.[21] Kommunerna har ålagts att före utgången av 2023 uppfylla de minimikrav på informationssäkerhet som anges i informationshanteringslagen.

Kommunförbundet

Kommunförbundet har till uppgift att främja tillämpningen av metoder och praxis för digital säkerhet och interoperabilitet på kommunfältet, i samarbete med kommunala aktörer. Definitionerna av digital säkerhet ska anpassas till de kommunala aktörernas verksamhet, och interoperabilitetens centrala uppgift är att säkerställa fungerande servicehelheter. Praxis för digital säkerhet ska bidra till att uppnå interoperabilitet. Med tanke på att e-tjänster blir allt viktigare i fråga om servicehelheter är tillhandahållandet av säkra och kvalitativa tjänster en del av kommuninvånarnas vardag, en del av säkerheten i vardagen. När definitionerna och praxisen genomförs ska det vara möjligt att anvisa användarna behövligt stöd, med beaktande av de kommunala aktörernas storleksklass.

Organisationer

Organisationerna har en viktig roll när det gäller att utveckla kompetensen i digital säkerhet samt vid beredskapen inför olika störningssituationer i samhället och hanteringen av olyckor. Organisationerna har erfarenhet av att ordna frivilligverksamhet tillsammans med medborgare och invånare.

21 Hyvärinen & Parviainen, Kommunernas it-kartläggning 2018, Kommunförbundet

Bilaga 5. Beredningsgruppen

I den arbetsgrupp som tillsattes för att samordna beredningen av principerna för utvecklingen av den digitala säkerheten inom den offentliga förvaltningen och genomförandeplanen 2020–2023 för perioden 1.9.2019–28.2.2020 ingick:

- *Tuija Kuusisto*, informationsförvaltningsråd, finansministeriet, ordförande
- *Mika Tuikkanen*, specialsakkunnig, finansministeriet, vice ordförande, tjänstledig 1.9.2019 -
- *Jaakko Poikonen*, specialsakkunnig, t.o.m. 31.12.2019, finansministeriet
- *Petri Puhakainen*, konsultativ tjänsteman, statsrådets kansli
- *Ari Uusikartano*, informationsförvaltningsdirektör, ersättare *Antti Savolainen*, datasäkerhetschef, utrikesministeriet
- *Ismo Parviainen*, ledande sakkunnig, ersättare *Kari Santalahti*, säkerhetschef, inrikesministeriet
- *Harri Mäntylä*, datasäkerhetschef, försvarsministeriet
- *Liisi Hakalisto*, specialsakkunnig, undervisnings- och kulturministeriet
- *Ari Huvinen*, direktör, Lantmäteriverket, ersättare *Jaana Merta*, ledande dataförvaltningsexpert, jord- och skogsbruksministeriet
- *Olli Lehtilä*, konsultativ tjänsteman, ersättare *Maija Rekola*, specialsakkunnig, kommunikationsministeriet
- *Teemupekka Virtanen*, specialsakkunnig, social- och hälsovårdsministeriet
- *Kari Klemm*, regeringsråd, ersättare *Jaakko Jokela*, utvecklingschef; *Petteri Ohvo*, utvecklingschef, t.o.m. 31.1.2020, ersättare *Sirpa Alitalo*, industriråd, arbets- och näringsministeriet
- *Roni Kiviharju*, överinspektör, *Tomi Marjamäki*, specialsakkunnig, miljöministeriet
- *Outi Juntura*, specialsakkunnig, datasäkerhetsansvarig, Riksdagen

– *Antti Sillanpää*, specialforskare, Säkerhetskommittén, fr.o.m. 21.1.2020

– *Mika Susi*, ledande sakkunnig, Finlands näringsliv t.o.m. 31.10.2019

– *Mika Susi*, verksamhetsledare, FISC ry, fr.o.m. 1.11.2019

– *Markku Raitio*, informationsförvaltningsdirektör, t.o.m. 17.12.2019, ersättare *Aaro Hallikainen*, informationssäkerhetsexpert, Helsingfors stad

– *Kari Perälä*, informationsdirektör, ersättare *Petri Hiirsalmi*, dataadministrationschef och datasäkerhetsansvarig, Imatra stad

– *Kalle Luukkainen*, beredskapschef, fr.o.m. 1.1.2020 *Jarna Hartikainen*, beredskapschef, Försörjningsberedskapscentralen

– *Jari Ylikoski*, specialsakkunnig, Kommunförbundet

– *Henri Burtsov*, enhetschef, ersättare *Jonna Ylikauppila*, informationssäkerhetsexpert, FPA

– *Kari Nykänen*, datasäkerhetschef, Uleåborgs stad

– *Juha Tallinen*, informationssäkerhetschef, ersättare *Pasi Koljonen*, dataadministrationschef, ersättare *Pertti Pyysing*, dataadministrationschef, Försvarsmakten

– *Pasi Hänninen*, datasäkerhetschef, Finlands Bank

– *Sami Niinikorpi*, datasäkerhetschef, *Otto Kolsi*, ersättare, Skyddspolisen

– *Rauli Paananen*, avdelningschef, Traficom

– *Mika Kuronen*, säkerhetschef, ersättare *Pyry Heikkinen*, IKT-säkerhetschef, ersättare tullöverinspektör *Antti Mielonen*, Tullen

– *Olli Joronen*, enhetschef, fr.o.m. 17.12.2019 *Hannu Naumanen*, säkerhetsdirektör, ersättare *Virpi Mäkinen*, enhetschef, ersättare *Sonja Marjamäki-Ruuskanen*, Statens informations- och kommunikationstekniska center Valtori

– *Samuli Bergström*, direktör, ersättare Mikko Hakuli, datasäkerhetschef, Skatteförvaltningen

– *Kimmo Rousku*, ledande specialsakkunnig, ersättare *Kirsi Janhunen*, ledande sakkunnig, t.o.m. 14.9.2019, ersättare *Erja Kinnunen*, ledande sakkunnig; *Pekka Ristimäki*, datasäkerhetschef, ersättare *Jarmo Pietikäinen*, specialsakkunnig, fr.o.m. 21.1.2020 *Antti Ahokas*, specialsakkunnig, Befolkningsregistercentralen, fr.o.m. 1.1.2020 Myndigheten

VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

FINANSMINISTERIET
Snellmansgatan 1 A
PB 28, 00023 STATSRÅDET
Telefon 0295 160 01
finansministeriet.fi

ISSN 1797-9714 (pdf)
ISBN 978-952-367-308-3 (pdf)

April 2020