VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelma 2020–2023 (Haukka)

Julkisen hallinnon ICT

Valtiovarainministeriön julkaisuja – 2020:33

Valtiovarainministeriön julkaisuja 2020:33

Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelma 2020–2023 (Haukka)

Tuija Kuusisto (toim.)

Valtiovarainministeriö, Helsinki 2020

Valtiovarainministeriö

ISBN PDF: 978-952-367-289-5

Taitto: Valtioneuvoston hallintoyksikkö, Julkaisutuotanto

Helsinki 2020

Kuvailulehti

Julkaisija	Valtiovarainministeriö		22.4.2020
Tekijät	Tuija Kuusisto (toim.)		
Julkaisun nimi	Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelma 2020–2023 (Haukka)		
Julkaisusarjan nimi ja numero	Valtiovarainministeriön julkaisuja 2020:33		
Diaari/hankenumero	VN/1465/2020	**Teema**	Julkisen hallinnon ICT
ISBN PDF	978-952-367-289-5	**ISSN PDF**	1797-9714
URN-osoite	http://urn.fi/URN:ISBN:978-952-367-289-5		
Sivumäärä	34	**Kieli**	suomi
Asiasanat	Julkisen hallinnon ICT, tietopolitiikka, riskienhallinta, kyberturvallisuus, varautuminen, tietoturva, digitalisaatio		

Tiivistelmä

Valtioneuvoston periaatepäätöksessä julkisen hallinnon digitaalisesta turvallisuudesta (Valtiovarainministeriön julkaisuja 2020:23) 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. Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelmassa 2020-2023 (Haukka) kuvataan periaatepäätöksen toteuttaminen.

Haukka-toimeenpanosuunnitelmaan on valittu 19 tehtävää, joiden avulla kehitetään keskeisiä julkisen hallinnon digitaalisen turvallisuuden palveluita. Toimeenpanosuunnitelmalla tuetaan myös käynnistymässä olevaa kyberturvallisuusstrategian 2019 kehittämisohjelman valmistelua ja toteuttamista, sekä osaltaan pannaan täytäntöön valtioneuvoston päätöstä huoltovarmuuden tavoitteista (1048/2018).

Toimeenpanosuunnitelma valmisteltiin valtiovarainministeriön asettamassa poikkihallinnollisessa koordinaatioryhmässä. Sen toteuttamista ohjaa valtiovarainministeriö. Toteuttamisen kustannukset ovat valtiovarainministeriössä 600 000 euroa, Digi- ja väestötietovirastossa 2 280 000 euroa, sekä Liikenne- ja viestintävirastossa 780 000 euroa, yhteensä 3 660 000 euroa.

Kustantaja	Valtiovarainministeriö
Julkaisun jakaja/myynti	Sähköinen versio: julkaisut.valtioneuvosto.fi Julkaisumyynti: vnjulkaisumyynti.fi

Presentationsblad

Utgivare	Finansministeriet		22.4.2020
Författare	Tuija Kuusisto (redaktör)		
Publikationens titel	Genomförandeplanen för digital säkerhet inom den offentliga förvaltningen 2020–2023 (Haukka)		
Publikationsseriens namn och nummer	Finansministeriets publikationer 2020:33		
Diarie-/ projektnummer	VN/1465/2020	**Tema**	Offentliga förvaltningens ICT
ISBN PDF	978-952-367-289-5	**ISSN PDF**	1797-9714
URN-adress	http://urn.fi/URN:ISBN:978-952-367-289-5		
Sidantal	34	**Språk**	finska
Nyckelord	IKT inom den offentliga förvaltningen, informationspolitik, riskhantering, cybersäkerhet, beredskap, dataskydd, digitalisering		

Referat

I statsrådets principbeslut om digital säkerhet inom den offentliga förvaltningen (finansministeriets publikationer 2020:24) fastställs principerna för utvecklingsarbetet och de centrala tjänsterna med syftet att främja säkerhet i en digital verksamhetsmiljö. Målet är att inom referensramen 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. I genomförandeplanen för digital säkerhet inom den offentliga förvaltningen 2020-2023 (Haukka) beskrivs hur principbeslutet ska verkställas.

För Haukka-genomförandeplanen har man valt 19 uppgifter med vilka man ska utveckla de centrala tjänsterna för digital säkerhet inom den offentliga förvaltningen. Genomförandeplanen stöder också den beredning och det genomförande av utvecklingsprogrammet inom cybersäkerhetsstrategin 2019 som har inletts samt bidrar till verkställandet av statsrådets beslut om målen för försörjningsberedskapen (1048/2018).

Genomförandeplanen bereddes i en förvaltningsövergripande samordningsgrupp tillsatt av finansministeriet. Verkställandet sker under ledning av finansministeriet. Kostnaderna för genomförandet uppgår vid finansministeriet till 600 000 euro, vid Myndigheten för digitalisering och befolkningsdata till 2 280 000 euro och vid Transport- och kommunikationsverket till 780 000 euro, dvs. sammanlagt till 3 660 000 euro.

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

Description sheet

Published by	Ministry of Finance		22 April 2020
Authors	Tuija Kuusisto (Ed)		
Title of publication	Implementation plan for digital security in the public sector		
Series and publication number	Publications of the Ministry of Finance 2020:33		
Register number	VN/1465/2020	**Subject**	Public Sector ICT
ISBN PDF	978-952-367-289-5	**ISSN (PDF)**	1797-9714
Website address (URN)	http://urn.fi/URN:ISBN:978-952-367-289-5		
Pages	34	**Language**	Finnish
Keywords	public administration ICT, information policy, risk management, cyber security, preparedness, data security, digitalisation		

Abstract

The Government Resolution on digital security in the public sector (Publications of the Ministry of Finance 2020:24) defines the development principles 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. The implementation plan for digital security in public administration 2020–2023 (Haukka) describes how the resolution is to be put to practice.

The 19 tasks selected to the implementation plan aim to develop the key services in terms of digital security in the public sector. The implementation plan also supports the preparation and implementation of the development programme for the Cyber Security Strategy 2019 that is getting started, and contributes to the implementation of the Government Decision on the Objectives of Security of Supply (1048/2018).

The implementation plan was prepared in a cross-sectoral coordination group appointed by the Ministry of Finance, which will also lead the implementation process. The implementation costs at the Ministry of Finance will be EUR 600,000, at the Digital and Population Data Services Agency EUR 2,280,000, and at the Finnish Transport and Communications Agency EUR 780,000, which gives the grand total of EUR 3,660,000.

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

Sisältö

Johdanto 9

1 Julkisen hallinnon digitaalisen turvallisuuden kansallinen ja kansainvälinen yhteistoimintamalli 11
- 1.1 Julkisen hallinnon digitaalisen turvallisuuden strateginen johtoryhmä 11
- 1.2 Julkisen hallinnon digitaalisen turvallisuuden yhteistoiminta- ja hallintamalli 12
- 1.3 Julkisen hallinnon digitaalisen turvallisuuden toiminnallisen tason kehittäminen 13
- 1.4 Digitaalisen turvallisuuden kansainvälisen kentän julkisen hallinnon yhteistyö 14

2 Julkisen hallinnon digitaalisen turvallisuuden riskien hallinta 15
- 2.1 Julkisen hallinnon strategisen tason digitaalisen turvallisuuden riskianalyysi 15
- 2.2 Julkisen hallinnon digitaalisen turvallisuuden vaikuttavuus-/kustannusmalli. 16

3 Kunnille tarkoitetut yhteiset, digitaalista turvallisuutta edistävät palvelut 18
- 3.1 Kuntien käytössä olevien tietoverkkojen turvallisuus 18
- 3.2 Kuntien yhteiset digitaalisen turvallisuuden palvelut 19

4 Digitaalisen identiteetin hallinta 20

5 Kansalaisten ja henkilöstön osaamisen kehittäminen 21
- 5.1 Digitaalisen turvallisuuden koulutuspalvelut kansalaisille ja henkilöstölle 21
- 5.2 Digitaalisen turvallisuuden ajokortti kansalaisille ja henkilöstölle 22

6 Julkisen hallinnon digitaalisen turvallisuuden asiantuntijapalvelut 23
- 6.1 Digitaalisen turvallisuuden asiantuntijapalveluiden järjestäminen 23

7 Julkisen hallinnon palveluiden ja palvelutuotannon digitaalisten turvallisuuden arviointi 24
- 7.1 Tietoturvallisuuden arvioinnin säädökset 24
- 7.2 Digitaalisten palveluiden valmiuden ja varautumisen arvioinnin säädökset 25

8 Julkisen hallinnon tarvitseman digitaalisen infrastruktuurin suojaaminen 26
8.1 Julkisen hallinnon turvallisuusarkkitehtuuri 26
8.2 Julkisen hallinnon tarvitsema havainnointi, reagointi ja analysointi 28
8.3 Julkisen hallinnon pilvipalvelut 29

9 Julkisen hallinnon autonomisten ja oppivien järjestelmien sekä palveluiden turvallinen kehittäminen 30
9.1 Julkisen hallinnon autonomisten ja oppivien järjestelmien valvonta 30
9.2 Julkisen hallinnon turvallinen palvelukehitys 31

10 Yhteenveto kustannuksista 33

JOHDANTO

Valtioneuvoston periaatepäätöksessä julkisen hallinnon digitaalisesta turvallisuudesta on kuvattu julkisen hallinnon digitaalisen turvallisuuden kehittämisalueet ja kehittämisen periaatteet, sekä keskeisiä hallinnon toimintaa ja prosesseja tukevat digitaalisen turvallisuuden palvelut. Tässä toimeenpanosuunnitelmassa kuhunkin palveluun liittyen on valittu tehtäviä julkisen hallinnon digitaalisen turvallisuuden nykytilaselvityksen ja kansainvälisen vertailun perusteella. Tehtäville on asetettu tavoitteet ja aikataulu, sekä kuvattu tavoitteiden saavuttamiseksi tarvittavat toimenpiteet, niiden toteutumisen mittaaminen sekä arvioitu kustannuksia ja hyötyjä. Toimeenpanosuunnitelma tukee ja se on tarkoitettu myös syötteeksi Suomen kyberturvallisuusstrategian 2019 kehittämisohjelman valmistelulle. Toimeenpanosuunnitelmaa ylläpidetään tarvittaessa toimintaympäristön muutosten ja kyberturvallisuusstrategian 2019 kehittämisohjelman asettamien vaatimusten mukaisesti.

Valtiovarainministeriö asetti 29.8.2019 julkisen hallinnon digitaalisen turvallisuuden linjausten valmistelun koordinaatioryhmän 1.9.2019–28.2.2020 väliseksi ajaksi. Koordinaatioryhmä muodostui laajasti julkisen hallinnon eri toimijoista. Koordinaatioryhmä valmisteli julkisen hallinnon digitaalinen turvallisuus periaatepäätösluonnoksen liitteineen sekä tämän toimeenpanosuunnitelman vuosille 2020–2023. Ne olivat julkisesti lausuttavina lausuntopalvelussa 24.1.–19.2.2020 välisenä aikana. Lausuntopalautteen perusteella tämä toimeenpanosuunnitelma viimeisteltiin ensin koordinaatioryhmässä ja sen jälkeen valtiovarainministeriössä.

Toimeenpanosuunnitelman 2020-2023 vastuutahot ovat seuraavat:

Valtiovarainministeriö (VM)

- Julkisen hallinnon digitaalisen turvallisuuden strateginen ohjausryhmä, puheenjohtaja alivaltiosihteeri Päivi Nerg: Valvoo toimeenpanosuunnitelman ja kuntien digitaalisen turvallisuuden tiekartan toteuttamista.
- Julkisen hallinnon ICT-osasto; ICT-johtaja, ylijohtaja Anna-Maija Karjalainen: Ohjaa Haukka-toimeenpanosuunnitelman toteuttamista sekä ohjaa Digi- ja väestötietovirastoa.
- Haukka-hankepäällikkö Tuija Kuusisto: Johtaa Haukka-hankeen toimeenpanoa.

Digi- ja väestötietovirasto (DVV)

- Vahti-johtoryhmä: Tuottaa tilannekuvan ja riskiarvion perustan, ohjaa Vahti-asiantuntijaverkostoa.
- Toteuttaa Haukka-toimeenpanosuunnitelmassa DVV:lle nimetyt tehtävät pääsääntöisesti Julkisen hallinnon digitaalisen turvallisuuden (JUDO) kehittämisen hankkeessa, jolle DVV on asettanut ohjausryhmän.

Traficom/Kyberturvallisuuskeskus

- Toteuttaa Haukka-toimeenpanosuunnitelmassa Traficomille/Kyberturvallisuuskeskukselle nimetyt tehtävät osana DVV:n JUDO-hanketta.

Muut ministeriöt, Kuntaliitto ja kunnat

- Yhteistyössä VM:n kanssa toteuttavat Haukka-toimeenpanosuunnitelmassa kuvatut tehtävät.

1 Julkisen hallinnon digitaalisen turvallisuuden kansallinen ja kansainvälinen yhteistoimintamalli

Kansallisen ja kansainvälisen yhteistyön kautta tehostetaan digitaalisen turvallisuuden koordinointia ja vaikuttavuutta sekä edistetään Suomen kilpailukykyä. Ministeriöt hallinnonaloineen, kunnat ja yhteisöt vaikuttavat aktiivisesti digitaalisen turvallisuuden myönteiseen kehittymiseen Euroopan unionissa sekä keskeisissä kansainvälisissä järjestöissä kuten YK ja OECD.

1.1 Julkisen hallinnon digitaalisen turvallisuuden strateginen johtoryhmä

Tavoite: Digitalisoitumista ja digitaalista turvallisuutta edistetään tasapainoisesti.

Vastuu: Valtiovarainministeriö

Viestintä: Valtiovarainministeriö laatii viestintäsuunnitelman ja viestii digitaalisen turvallisuuden strategisen johtoryhmän toiminnasta.

Kohde: Julkinen hallinto

Aikataulu: 2020–2024

Toimenpiteet: Valtiovarainministeriö asettaa digitaalisen turvallisuuden strategisen johtoryhmän. Ryhmään kuuluvat valtioneuvoston kanslia, ulkoministeriö, sisäministeriö, puolustusministeriö, liikenne- ja viestintäministeriö, sosiaali- ja terveysministeriö, työ- ja elinkeinoministeriö, Turvallisuuskomitea, Kuntaliitto, kuntien edustaja, Huoltovarmuuskeskus, yliopistojen edustaja sekä asiantuntijana Digi- ja väestötietovirasto. Ryhmä koordinoi julkisen hallinnon digitaalisen turvallisuuden strategista riskiarviota, luo ja koordinoi digitaalisen turvallisuuden yhteistoimintamallia, sekä arvioi julkisen hallinnon strategista digitaalisen turvallisuuden tilannetta, ja keskeisiä kehitettäviä

digitaalisen turvallisuuden palveluita, linjaa keskeisiä digitaalisen turvallisuuden asioita kuten digitaalisen turvallisuuden tavoitteita, sekä valvoo tämän digitaalisen turvallisuuden toimeenpanosuunnitelman ja kuntien digitaalisen turvallisuuden tiekartan toteutumista.

Mittaaminen: Julkisen hallinnon digitaalisen turvallisuuden strateginen johtoryhmä on asetettu vuonna 2020 ja toiminnassa. Strategista riskiarviota on käsitelty ja resursseja on suunnattu sen perusteella vaikuttavimpiin kehittämiskohteisiin.

Kustannus/hyöty:

Julkisen hallinnon digitaalisen turvallisuuden strategisen johtoryhmän työ on virkatyötä. Ryhmän osallistujatahot vastaavat edustajiensa matka- ja muista kustannuksista. Ryhmä onnistuessaan vaikuttaa merkittävästi julkisen hallinnon digitaalisen turvallisuuden keskeisten strategisten riskien ennalta ehkäisemiseen, mikä vähentää hallinnon prosessien ja toimintojen laajoja katkoksia ja lamaantumista sekä niistä aiheutuvia haittoja yhteiskunnan toiminnan jatkuvuudelle. Vähentää mainehaittoja ja luottamuksen rapautumista sekä hallinnossa, yhteisöissä että kansalaisten keskuudessa. Ryhmän onnistunut toiminta myös edistää Suomen kilpailukykyä ja mahdollistaa innovaatioita ja kasvua.

1.2 Julkisen hallinnon digitaalisen turvallisuuden yhteistoiminta- ja hallintamalli

Tavoite: Valtiovarainministeriö yhdessä muiden ministeriöiden, kuntien ja yhteisöjen kanssa toimivat julkisen hallinnon digitaalista turvallisuutta tehostavan yhteistoiminta- ja hallintamallin mukaisesti.

Vastuu: Valtiovarainministeriö

Viestintä: Valtiovarainministeriö laatii viestintäsuunnitelman ja viestii digitaalisen turvallisuuden yhteistoiminta- ja hallintamallista julkisen hallinnon organisaatioille ja kansalaisille.

Kohde: Julkinen hallinto, kansalaiset

Aikataulu: 2021–2023

Toimenpiteet: Valtiovarainministeriö yhdessä muiden ministeriöiden, kuntien ja yhteisöjen kanssa sekä Vahti-toiminnan tukemana luo ja koordinoi toiminnan ja talouden sekä osaamisen kehittämisen kattavan kansallisen strategisen tason digitaalisen turvallisuuden yhteistoimintamallin. Yhteistoimintamallin valmistelussa käsitellään valtion, kuntayhtymien ja kuntien tehtäviä ja vastuita sekä julkisen hallinnon digitaalisen turvallisuuden palveluita kansalaisille, ja tutkimusyhteistyötä. Määritellään operatiivisen johtamisen vastuut ja järjestelyt, huomioiden

viranomaisten toimivaltuudet, sekä kehitetään kansallista kybertilannekuvaa huomioiden eri yhteiskunnan toimijoita sekä kansainvälisiä kumppaneita. Valtiovarainministeriö ja muut ministeriöt viestivät digitaalisen turvallisuuden tavoitteista ja sisällyttävät ne julkisen hallinnon toiminnallisiin tavoitteisiin.

Mittaaminen: Yhteistoimintamalli on kuvattu ja toiminnassa. Taloussuunnitelmiin sisältyy konkreettisia, digitaalisen turvallisuuden osa-alueita parantavia tavoitteita.

Kustannus/hyöty:
Yhteistoimintamallin selvitys 80 000 euroa. Toimeenpanon koordinointi on pääsääntöisesti virkatyötä. Toimeenpanon kustannukset arvioidaan tarkemmin selvitystyön yhteydessä. Hyötynä on edelleen parantuvan yhteistoiminnan mahdollistama digitaalisen turvallisuuden strategisen ja operatiivisen tason sekä osaamisen kehittäminen.

1.3 Julkisen hallinnon digitaalisen turvallisuuden toiminnallisen tason kehittäminen

Tavoite: VAHTI-johtoryhmä edistää ja kehittää koko julkisen hallinnon digitaalisen turvallisuuden toimeenpanon yhteistyötä ja koordinaatiota.

Vastuu: Digi- ja väestötietovirasto

Viestintä: Digi- ja väestötietovirasto laatii viestintäsuunnitelman ja viestii VAHTI-johtoryhmän toiminnasta.

Kohde: Julkinen hallinto, kansainvälinen yhteistyö

Aikataulu: 2020–2024

Toimenpiteet: Digi- ja väestötietovirasto asettaa VAHTI-johtoryhmän toiminnallisen tason poikkihallinnolliseksi ohjausryhmäksi. Uudistetun Vahti-johtoryhmän on suunniteltu muodostuvan keskusvirastojen ja keskeisten yhteisöjen ja toimielinten johdosta. Vahti-johtoryhmä edistää kansallista ja kansainvälistä osaamisen kehittämistä. Vahti-toiminnassa hyödynnetään useiden eri viranomaisten tuottamaa digitaalisen turvallisuuden tilannekuvaa.

Mittaaminen: Julkisen hallinnon toiminnallinen/VAHTI-johtoryhmä on asetettu ja toimii.

Kustannus/hyöty:
Vahti-johtoryhmän työ on virkatyötä. Ryhmän osallistujatahot vastaavat edustajiensa matka- ja muista kustannuksista. Ryhmä onnistuessaan vaikuttaa merkittävästi julkisen hallinnon digitaalisen turvallisuuden keskeisten operatiivisten riskien ennalta ehkäisemiseen, mikä vähentää häiriötilanteiden ja toteutuneiden tietoturvaloukkausten aiheuttamia kustannuksia sekä mainehaittoja ja luottamuksen rapautumista niin hallinnossa, yhteisöissä kuin kansalaisten keskuudessa.

1.4 Digitaalisen turvallisuuden kansainvälisen kentän julkisen hallinnon yhteistyö

Tavoite: EU-säädösten mukaisten teknologiaratkaisujen kehittyminen, sekä riittävien digitaalisen turvallisuuden vaatimusten toteutuminen julkisen hallinnon palveluissa. Tämä myös edistää Suomen kilpailukykyä kansainvälisen yhteistyön avulla.

Vastuu: Kukin ministeriö oman vastuualueensa osalta

Viestintä: Kukin ministeriö viestii digitaalisen turvallisuuden kansainvälisestä yhteistyöstään muille ministeriöille sekä yhteisöille.

Kohde: Kansainvälinen yhteistyö

Aikataulu: 2021-2023

Toimenpiteet: EU-asioissa valtioneuvoston kanslian ja muissa kansainvälisissä asioissa ulkoministeriön koordinoimana kukin ministeriö oman vastuualueensa osalta yhdessä muiden ministeriöiden kanssa edistävät EU-säädösten mukaisten teknologiaratkaisujen kehittymistä, sekä riittävien digitaalisen turvallisuuden vaatimusten toteutumista julkisen hallinnon palveluissa.

Valtiovarainministeriö käynnistää yhteistyössä muiden ministeriöiden ja toimijoiden kanssa selvitystyön kansainvälisten asioiden raportoinnin keskittämisestä siten, että Suomessa yksi toimija kokoaisi yhteen ja raportoisi Suomen tiedot digitaalisen turvallisuuden kansainvälisiin arviointeihin sekä eri kansainvälisiin yhteisöihin.

Valtiovarainministeriö yhdessä digi- ja väestötietoviraston Vahti-toiminnan kanssa vahvistavat julkisen hallinnon digitaalisen turvallisuuden yhteistyötä Baltian ja Pohjoismaiden kanssa. Yhteistyö koordinoidaan ulkoministeriön ja valtioneuvoston kanslian kansainvälisten digitaalisen turvallisuuden alueen toimien kanssa.

Mittaaminen: Julkisen hallinnon kansainväliselle yhteistyölle on asetettu tavoitteet, joita seurataan. Kansainvälisille yhteisöille raportoinnin keskittäminen on suunniteltu ja sitä toteutetaan. Valtiovarainministeriön sekä Baltian ja Pohjoismaiden välinen digitaalisen turvallisuuden yhteistyö tuottaa uutta tietoa päätöksenteon tueksi.

Kustannus/hyöty:

Kansainvälinen yhteistyö ja raportoinnin keskittämisen suunnittelu ovat virkatyötä. Osallistujatahot vastaavat edustajiensa matka- ja muista kustannuksista. Työ onnistuessaan vaikuttaa merkittävästi julkisen hallinnon digitaalisten palveluiden hankintamahdollisuuksiin ja tuotantomalleihin sekä palveluiden, infrastruktuurin ja tietojen turvallisuuden jatkuvaan paranemiseen, koska näitä ei ole mahdollista kehittää ainoastaan Suomessa tehtävillä toimenpiteillä.

Yhteensä kohdassa 1 selvitystyötä koskevat hankinnat 80 000 euroa.

2 Julkisen hallinnon digitaalisen turvallisuuden riskien hallinta

Digitaalisen turvallisuuden nykytila-arvion ja kokonaiskuvan perusteella tuotettavien riskianalyysien ja vaikutusarviointien avulla valitaan kehityskohteet, joihin suunnataan resursseja.

2.1 Julkisen hallinnon strategisen tason digitaalisen turvallisuuden riskianalyysi

Tavoite:	Digitaalisen turvallisuuden nykytila-arvioon ja strategisen tason kokonaiskuvaan perustuva riskianalyysi on käytettävissä.
Vastuu:	Valtiovarainministeriö, Digi- ja väestötietovirasto
Viestintä:	Valtiovarainministeriö viestii strategisesta riskiarviosta. Digi- ja väestötietovirasto laatii viestintäsuunnitelman ja viestii digitaalisen turvallisuuden riskienhallintaan liittyvistä palveluista julkisen hallinnon organisaatioille.
Kohde:	Julkinen hallinto
Aikataulu:	2020–2021
Toimenpiteet:	Digi- ja väestötietovirasto selvittää ja toteuttaa prosessin ja palvelut, joiden avulla se kokoaa keskitetysti tiedon organisaatioiden digitaalisen turvallisuuden uhkista, riskeistä ja kypsyystasosta, sekä jakaa digitaalisen turvallisuuden kehitystoimintaan tarvittavaa tietoa. Yhteistyötahoina ovat VN Controller-toiminto, sekä muu julkinen hallinto. Valtiovarainministeriö selvittää ja toteuttaa prosessin yhdessä Digi- ja väestötietoviraston kanssa, jonka avulla se ylläpitää digitaalisen turvallisuuden pitkän aikavälin strategista riskiarviota ja laatii pitkän aikavälin linjaukset kehitystoimintaa varten. Valtiovarainministeriö koordinoi linjauksia toteuttavaa Haukka-toimeenpano-ohjelmaa sekä arvioi säännöllisesti linjausten toteutumista.
Mittaaminen:	Kokonaiskuvaan perustuva riskiarvio on luotu, toteutettu ja saatavilla.

Kustannus/hyöty:

Selvitys koskien prosesseja riskien tunnistamiseen ja ylläpitoon 80 000 euroa sekä ensimmäinen riskianalyysi strategisten digiturvallisuuden uhkien osalta arviolta 60 000 euroa. Riskien ylläpito kokonaiskuvapalvelun yhteydessä arviolta 100 000 euroa. Toteutusten kustannukset arvioidaan tarkemmin selvityksen yhteydessä. Organisaatioiden sisäinen riskienhallinta toteutetaan virkatyönä. Hyödyt on kuvattu kohdassa 1.1.

2.2 Julkisen hallinnon digitaalisen turvallisuuden vaikuttavuus-/kustannusmalli

Tavoite: Digitaalisen turvallisuuden kustannusten ja vaikuttavuuden arviointimallien ja menettelyjen edistäminen julkisessa hallinnossa.

Vastuu: Valtiovarainministeriö

Viestintä: Valtiovarainministeriö laatii viestintäsuunnitelman ja viestii julkisen hallinnon organisaatioille vaikuttavuus-/kustannusmallin kehittämistä sekä mallin käytöstä ja hyödyntämisestä julkisessa hallinnossa. Digi- ja väestötietovirasto viestii mallin käytöstä osana kokonaiskuvapalvelua.

Kohde: Julkisen hallinnon organisaatiot

Aikataulu: 2020–2021

Toimenpiteet: Valtiovarainministeriö yhdessä digi- ja väestötietoviraston kanssa laatii digitaalisen turvallisuuden vaikuttavuus-/kustannusmallin ja prosessin. Suunnitellaan digitaalisen turvallisuuden hallinnan ja kehittämisen vaikuttavuuden ja kustannusten arviointi valtion hallinnossa ja kunnissa. Tavoite on se, että julkinen hallinto panostaisi digitaaliseen turvallisuuteen määrärahalla joka vastaa viittä prosenttia ICT-menoista. Mallia pilotoidaan ja pilotoinnin kokemusten perusteella päivitetty malli otetaan käyttöön vuonna 2021. Malli otetaan soveltuvin osin käyttöön osana digi- ja väestötietoviraston kokonaiskuvapalvelua.

Mittaaminen: Malli on luotu ja toteutettu. Vaikuttavuusarviointi on saatavilla.

Kustannus/hyöty:

Selvitys koskien mallin ja prosessin laadintaa 60 000 euroa. Toteutuksena osana kokonaiskuvapalvelua tiedonsiirron rajapintoja valtion toimijoille 50 000 euroa sekä käyttöliittymän tarjoaminen kunnille 50 000 euroa. Tämä arvio ei sisällä tuotantoympäristön ylläpitokustannuksia. Toteutuksen kustannukset sisältäen kunnissa tapahtuvan työn kustannukset tarkennetaan mallin ja prosessin laadinnan yhteydessä. Mallia ja prosessia tarvitaan, jotta digitaalisen turvallisuuden strateginen johtaminen voi perustua tietoon.

Digitaalisen turvallisuuden strategisen johtamisen hyötyjä on käsitelty kohdassa 1.1.

Yhteensä kohdassa 2 selvitystyötä koskevat hankinnat 140 000 euroa sekä toteutusta ja ylläpitoa koskevat hankinnat yhteensä 260 000 euroa.

3 Kunnille tarkoitetut yhteiset, digitaalista turvallisuutta edistävät palvelut

Kuntien digitaalisen turvallisuuden kehittämisen tiekarttaa ylläpidetään, ja sen toteutumista seurataan.

3.1 Kuntien käytössä olevien tietoverkkojen turvallisuus

Tavoite: Kuntien havainnointi- ja reagointikyvyn kasvattaminen.

Vastuu: Digi- ja väestötietovirasto, Kuntaliitto, kunnat

Viestintä: Digi- ja väestötietovirasto laatii viestintäsuunnitelman ja viestii kunnille havainnointi- ja reagointikyvyn kasvattamiseen liittyvistä toimenpiteistä.

Kohde: Kunnat

Aikataulu: 2020-2022

Toimenpiteet: Valtiovarainministeriön ohjauksessa digi- ja väestötietovirasto yhdessä Traficomin, Kuntaliiton ja kuntien kanssa kokoaa ryhmän selvittämään ja koordinoimaan kuntien havainnointi- ja reagointikyvyn kasvattamista. Yhtenä mahdollisena palveluna on Havaro-palvelun valmistelu kuntasektorille. Toimenpide liittyy kohtaan 8.2.

Mittaaminen: Havainnointi- ja reagointikykyä kasvattavia palveluita on kuntien käytettävissä.

Kustannus/hyöty: Selvitys 60 000 euroa, ja toteutus kuvattu kohdan 8.2 yhteydessä. Selvityksen aikana valitaan palveluita käyttävät kunnat sekä palvelut ja tarkennetaan toteutuksen kustannukset kunnissa. Palvelun käyttäjät vastaavat käyttöönottoon ja palvelun käyttöön liittyvistä kuluista sekä tarvittavista lisenssimaksuista. Nopeammalla reagoinnilla turvataan kansalaisten palveluiden jatkuvuus ja turvallisuus sekä pienennetään häiriötilanteiden ja toteutuneiden tietoturvaloukkausten aiheuttamia kustannuksia. Vähennetään mainehaittoja ja luottamuksen rapautumista sekä hallinnossa, yhteisöissä että kansalaisen keskuudessa.

3.2 Kuntien yhteiset digitaalisen turvallisuuden palvelut

Tavoite: Kuntien yhteistä digitaalisen turvallisuuden kehittämisen tiekarttaa ylläpidetään ja seurataan sen toteutumista.

Vastuu: Digi- ja väestötietovirasto, Kuntaliitto, kunnat

Viestintä: Digi- ja väestötietovirasto yhdessä Kuntaliiton kanssa laatii viestintäsuunnitelman ja viestii kunnille digitaalisen turvallisuuden kehittämisen tiekartan toteutumisesta sekä kuntien tehtävistä digitaalisen turvallisuuden kehittämiseksi.

Kohde: Kunnat

Aikataulu: 2021–2023

Toimenpiteet: Valtiovarainministeriön ohjauksessa digi- ja väestötietovirasto yhdessä Kuntaliiton ja kuntien kanssa kokoaa työryhmän selvittämään kuntien yhteisten digitaalisen turvallisuuden kehittämishankkeiden tarvetta ja toteutusta. Selvitys perustuu tähän toimeenpanosuunnitelmaan, joka muodostaa kuntien digitaalisen turvallisuuden kehittämisen tiekartan perustan. Selvitetään lisäksi digitaalisten toimintaympäristöjen valvomotoiminne (kuntien yhteinen kyber- ja tietoturvavalvomo). Valvomotoiminne olisi mahdollista toteuttaa yhteisesti saatavilla olevana valvomopalveluna ja siten, että varoitustiedot tulisivat kunnan johdon päätöksenteon tueksi.

Mittaaminen: Työryhmä on perustettu ja selvitykset laadittu. Kuntien digitaalisen turvallisuuden tiekarttaa ylläpidetään.

Kustannus/hyöty:
Selvitys 100 000 euroa. Selvityksen aikana tunnistetaan edellytykset, jotka palvelun on täytettävä, jotta se voisi liittyä palveluun, ja tarkennetaan toteutuksen kustannukset. Valittavien palveluiden tulee olla sellaisia, joissa kaikilla tai useilla kunnilla on samanlainen palvelutarve. Jos kunnat tekevät ja selvittävät palveluita erikseen, niin julkisia voimavaroja hukkaantuu.

Yhteensä kohdassa 3 selvitystyötä koskevat hankinnat 160 000 euroa.

4 Digitaalisen identiteetin hallinta

Edistetään Suomen kansalaisille ja kaikille Suomessa asuville mahdollisuutta sähköiseen tunnistautumiseen. Edistetään toimivien sähköisten tunnistusratkaisujen kehittymistä, jotka mahdollistavat erilaisten välineiden käytön.

Tavoite: Julkinen hallinto takaa jokaiselle kansalaiselle ja asukkaalle luotettavan, käytettävän sähköisen identiteetin. Valtio mahdollistaa kattavasti ja syrjimättömästi digitaalisen tunnistamisratkaisun kansalaisille ja asukkaille, ja takaa henkilöllisyyden todentamisen mahdollisuuden digitaalisessa maailmassa.

Vastuu: Valtiovarainministeriö

Viestintä: Valtiovarainministeriö laatii viestintäsuunnitelman ja viestii kansalaisille digitaalisen identiteetin hallinnan tilasta.

Kohde: Kansalaiset

Aikataulu: 2020–2023

Toimenpiteet: Valtiovarainministeriö koordinoi yhdessä muiden ministeriöiden kanssa tarvittavat lainsäädäntömuutokset ja Digi- ja väestötietovirastossa tarpeelliset tehtävät.

Mittaaminen: Lainsäädäntömuutokset on tehty ja tarvittavat tehtävät määritelty. Sähköisen asioinnin käytön lisääntyminen ml. toisen puolesta asiointi ja valtuudet (ts. niiden henkilöiden lukumäärän kehittyminen, joilla on mahdollisuus sähköiseen asiointiin)

Kustannus/hyöty: Palvelukokonaisuus toteutetaan omana hankkeena, jossa kustannukset ja hyödyt arvioidaan ja joka vastaa myös palvelukokonaisuuden rahoituksen järjestämisestä.

5 Kansalaisten ja henkilöstön osaamisen kehittäminen

Kehitetään julkisen hallinnon ja yhteisöjen kaikkien henkilöryhmien sekä yksityisten kansalaisten digitaalisen turvallisuuden taitoja ja tietoisuutta.

5.1 Digitaalisen turvallisuuden koulutuspalvelut kansalaisille ja henkilöstölle

Tavoite: Digitaaliseen turvallisuuteen liittyvän osaamisen kasvattaminen.

Vastuu: Digi- ja väestötietovirasto

Viestintä: Digi- ja väestötietovirasto laatii viestintäsuunnitelman ja viestii julkisen hallinnon organisaatioille ja kansalaisille käytettävissä olevista digitaalisen turvallisuuden koulutuksista.

Kohde: Kansalaiset, henkilöstö ja johto

Aikataulu: 2022–2023

Toimenpiteet: Digi- ja väestötietovirasto yhdessä opetus- ja kulttuuriministeriön kanssa tuotteistaa digitaalisen turvallisuuden koulutukset kansalaisille, valtion ja kuntien henkilöstölle ja johdolle. Jatketaan JUDO-hankkeessa vuosille 2019–2021 suunniteltua osaamisen kehittämistä. Huomioidaan harjoitukset yhtenä osaamisen kehittämisen keinona, sekä palveluasenteen kehittäminen. Opetus- ja kulttuuriministeriö kehittää kansalaisten digitaalisen turvallisuuden osaamista kattavasti osana suomalaista koulutusjärjestelmää.

Mittaaminen: Koulutuskokonaisuudet on laadittu ja jakelukanava on käytössä.

Kustannus/hyöty: Kustannukset arviolta 80 000 euroa vuodessa. Koulutusten jakelukanavana voidaan käyttää nykyisiä alustoja, joten lisenssi- ja käyttöönotosta syntyvät kustannukset ovat maltilliset. Kustannukset koostuvat uuden materiaalin tuottamisen sekä ylläpitämiseen liittyvistä kuluista, koulutusmateriaalien

lisensseistä ja palvelumaksuista sekä verkkosivuston ja palvelualustan lisenssikustannuksista (esim. Pilvipalvelualustan vuosikustannus). Osaamisen kehittämisellä turvataan hallinnon palveluiden turvallisuutta ja toimintavarmuutta sekä kansalaisten ja asukkaiden mahdollisuuksia käyttää hallinnon palveluita.

5.2 Digitaalisen turvallisuuden ajokortti kansalaisille ja henkilöstölle

Tavoite: Kansalaisten ja henkilöstön osaamisen tunnistamismenettelyn kehittäminen luottamuksen lisäämiseksi ja osaamisen tunnistamiseksi.

Vastuu: Digi- ja väestötietovirasto

Viestintä: Digi- ja väestötietovirasto laatii viestintäsuunnitelman ja viestii kansalaisille ja julkisen hallinnon henkilöstölle osaamisen tunnistamismenettelystä.

Kohde: Julkinen hallinto

Aikataulu: 2021–2022

Toimenpiteet: Digi- ja väestötietovirasto selvittää kansalaisten digitaalisen turvallisuuden osaamisen osoittamiseksi kehitettyjä menettelyjä kuten kansalaisen kyberturvallisuuden ajokortti, sekä henkilöstön digitaalisen turvallisuuden perustaitojen osaamisen osoittamiseksi kehitettyjä menettelyjä. Selvityksessä esitetään etenemisvaihtoehdot menettelyjen toteuttamiselle/laajentamiselle.

Mittaaminen: Selvitys digitaalisen turvallisuuden osaamisen osoittamisen menettelyistä on tehty. Selvityksen perusteella on ehdotettu toteutusmalleja, joita on tarpeen vaatiessa pilotoitu. Menettelyjen toteuttamisen edistäminen on suunniteltu.

Kustannus/hyöty:

Selvitys 40 000 euroa, ja toteutus arviolta 40 000 euroa. Kansalaiset ja julkisen hallinnon henkilöstö voivat osoittaa noudattavansa turvallisia toimintatapoja digitaalisessa toimintaympäristössä. Hyötynä digitaalisen turvallisuuden tietoisuuden kasvaminen kansalaisten ja julkisen hallinnon henkilöstön piirissä.

Yhteensä kohdassa 5 selvitystyötä koskevat hankinnat 40 000 euroa ja toteutusta koskevat hankinnat 40 000 euroa sekä 80 000 euroa vuodessa kahden vuoden ajan eli yhteensä 240 000 euroa.

6 Julkisen hallinnon digitaalisen turvallisuuden asiantuntijapalvelut

Digitaalisen turvallisuuden keskitettyjä asiantuntijapalveluita kehitetään ja tarjotaan laajasti koko julkisen hallinnon käyttöön.

6.1 Digitaalisen turvallisuuden asiantuntijapalveluiden järjestäminen

Tavoite: Yhteiset digitaalisen turvallisuuden asiantuntijapalvelut on järjestetty julkiselle hallinnolle.

Vastuu: Digi- ja väestötietovirasto

Viestintä: Digi- ja väestötietovirasto laatii viestintäsuunnitelman ja viestii julkisen hallinnon organisaatioille digitaalisen turvallisuuden asiantuntijapalveluiden käytöstä.

Kohde: Julkinen hallinto

Aikataulu: 2020–2021 valmistelu, 2022–23 palvelut käytettävissä

Toimenpiteet: Digi- ja väestötietovirasto yhdessä Hanselin kanssa selvittää ja kehittää edelleen julkisen hallinnon digitaalisen turvallisuuden konsultoinnin ja -auditoinnin palveluita ja niiden hankintamenettelyjä. Selvitys kattaa palveluntarjoajien yhtenäiset mahdollisuudet palveluiden tarjontaan, julkisen hallinnon organisaatioiden tarpeen digitaalisen turvallisuuden konsultointiin ja -auditointiin sekä asiantuntijapalvelun hankintaan liittyvät vaihtoehtoiset mallit.

Selvityksen perusteella Digi- ja väestötietovirasto rakentaa julkisen hallinnon digitaalisen turvallisuuden asiantuntijapalvelun sekä sitä tukevat työkalut.

Mittaaminen: Asiantuntijapalvelu ja työkalut ovat käytössä.

Kustannus/hyöty: Palveluiden järjestäminen toteutetaan virkatyönä. Palveluiden käyttäjätahot kustantavat palveluiden käytön. Hyötynä palveluiden saatavuus koko julkiselle hallinnolle.

7 Julkisen hallinnon palveluiden ja palvelutuotannon digitaalisten turvallisuuden arviointi

Edistetään normeihin ja standardeihin perustuvaa digitaalisten palveluiden ja palvelutuottajien arviointia ja varmentamista.

7.1 Tietoturvallisuuden arvioinnin säädökset

Tavoite: Lain viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1046/2011) sekä lain tietoturvallisuuden arviointilaitoksista (1045/2011) mahdolliset uudistamistarpeet selvitetään ja johtopäätösten perusteella toteutetaan mahdollinen säädösvalmistelu.

Vastuu: Valtiovarainministeriö

Viestintä: Valtiovarainministeriö viestii säädösvalmistelusta noudattaen säädösvalmistelun viestintäperiaatteita.

Kohde: Julkinen hallinto

Aikataulu: 2021–2022

Toimenpiteet: Valtiovarainministeriö yhdessä liikenne- ja viestintäministeriön sekä Traficomin ja muiden ministeriöiden ja mahdollisesti kuntien kanssa selvittävät nykytilan ja uudistamistarpeet vuonna 2021. Johtopäätösten perusteella lainvalmistelu 2021–2022. Mahdolliset uudet lakiehdotukset eduskuntaan alkusyksystä 2022.

Mittaaminen: Selvitykset on tehty. Selvitysten aiheuttamat jatkotoimenpiteet on toteutettu.

Kustannus/hyöty: Selvitykset ja mahdollinen säädösten valmistelu laaditaan virkatyönä. Valmisteluun sisältyy vaikuttavuusarviointi ja taloudellisten vaikutusten arviointi. Traficomin työ ei sisälly kustannusarvioon.

7.2 Digitaalisten palveluiden valmiuden ja varautumisen arvioinnin säädökset

Tavoite: Arvioidaan digitaalisten palveluiden ja infrastruktuurin varautumisen ja valmiuden vaatimuksiin ja niiden arviointimenettelyyn liittyvät säädöstarpeet ja toteutetaan mahdollinen säädösvalmistelu.

Vastuu: Valtiovarainministeriö

Viestintä: Valtiovarainministeriö viestii säädösvalmistelusta noudattaen säädösvalmistelun viestintäperiaatteita.

Kohde: Julkinen hallinto

Aikataulu: 2021–2022

Toimenpiteet: Valtiovarainministeriö yhdessä liikenne- ja viestintäministeriön sekä Traficomin ja muiden ministeriöiden ja mahdollisesti kuntien kanssa selvittävät nykytilan ja uudistamistarpeet vuonna 2021. Johtopäätösten perusteella lainvalmistelu 2021–2022. Mahdolliset uudet lakiehdotukset eduskuntaan alkusyksystä 2022.

Mittaaminen: Selvitykset on tehty. Selvitysten aiheuttamat jatkotoimenpiteet on toteutettu.

Kustannus/hyöty: Selvitykset ja mahdollinen säädösten valmistelu laaditaan virkatyönä. Valmisteluun sisältyy vaikuttavuusarviointi ja taloudellisten vaikutusten arviointi. Traficomin työ ei sisälly kustannusarvioon.

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.

8.1 Julkisen hallinnon turvallisuusarkkitehtuuri

Tavoite: Julkisen hallinnon turvallisuusarkkitehtuurilla ohjataan digitaalisen infrastruktuurin kehittämistä.

Vastuu: Digi- ja väestötietovirasto

Viestintä: Valtiovarainministeriö yhdessä digi- ja väestötietoviraston kanssa laativat viestintäsuunnitelman ja viestivät julkisen hallinnon organisaatioille turvallisuusarkkitehtuurin kehittämisestä sekä hyödyntämisestä.

Kohde: Julkinen hallinto

Aikataulu: Selvitys 2020–2021, toimeenpano 2021–2023

Toimenpiteet: Valtiovarainministeriön ohjauksessa digi- ja väestötietovirasto laatii Traficomin, Kelan, muiden valtion virastojen ja laitosten sekä kuntien kanssa julkisen hallinnon turvallisuusarkkitehtuurin. Työssä hyödynnetään Tiedonhallintalain toimeenpanon yhteydessä laadittavia tiedonhallintakarttoja ja -malleja sekä valtiovarainministeriön yhteentoimivuuden ohjausta. Tehtävässä toimitaan yhteistyössä kriittisen infrastruktuurin varautumista kehittävien, kriittisen infrastruktuurin keskeisiin osa-alueisiin keskittyvien ohjelmien, kuten Huoltovarmuuskeskuksen digitaalinen turvallisuus 2030 -ohjelman kanssa.

a. Kuvataan mille tasolle kansallinen kyvykkyys rakennetaan ja mitkä ovat sellaisia kriittisiä digitaalisia palveluita, tietoa ja infrastruktuuria, johon liittyy erityiset kansalliset hallinnan ja turvaamisen vaatimukset. Julkisesti saatavilla oleva tieto voi muodostaa riskin itsessään tai riski

muodostuu yksittäisten julkisten tietojen yhdistämisen kautta (tiedon kasautuvuus). Esimerkkeinä tällaisesta tiedosta voivat olla muun muassa sähköverkon kaaviot tai siltojen rakennepiirustukset. Kaiken julkisen tiedon ei ole perusteltua olla digitaalisesti saatavilla. Valmistellaan linjaukset siitä, 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.

b. Laaditaan ja otetaan käyttöön julkisen hallinnon palveluiden ja tietojärjestelmien kriittisyyden luokitusjärjestelmä sekä arvioidaan tietojärjestelmärekisterin tarve ja arvioidaan kriittisten palveluiden, tietojärjestelmien ja tietoliikenneratkaisuiden vaatimustenmukaisuuden nykytilanne.
c. Valmistellaan luettelo teknologioista, joiden käyttöä julkisen hallinnon digitaalisissa palveluissa suositellaan. Valmistellaan myös luettelo teknologioista, joiden käyttöä on vältettävä ja mahdollinen käyttö on arvioitava riskienhallinnan näkökulmasta, esimerkiksi vanhentunut teknologia.
d. Kohtaan 7 liittyen laaditaan suunnitelma palveluiden ja palveluverkkojen turvallisuuden tarkistamisen kehittämiseksi.

Toimenpiteet arkkitehtuurin noudattamiseksi:

e. Kootaan tietopohja yhteiskunnan kriittisten tietojärjestelmien, tietovarantojen sekä tietoverkkojen pitkän aikavälin kehittämistarpeista sekä laaditaan suunnitelma keskitetyllä rahoituksella toteutettavan kehittämisohjelman käynnistämiseksi. Tähän liittyen tarkastellaan erityisesti kriittisten vanhojen tietojärjestelmien haavoittuvuuksien kartoittamista ja elinkaaren suunnittelua.
f. Laaditaan pitkän aikavälin kehittämissuunnitelma kriittisten palveluiden, tietojärjestelmien ja tietoliikenneratkaisuiden vaatimustenmukaisuuden parantamiseksi ja olemassa olevan korjausvelan hallitsemiseksi.

Mittaaminen: Kohdat a–d on tehty. Kohdat e–f on toteutettu julkisen hallinnon tai valtion hallinnon yhteisten palvelujen osalta.

Kustannus/hyöty:

Selvitys nykytilanteesta ja puutteiden kartoitus 60 000 euroa. Turvallisuusarkkitehtuurin kehittämistarpeiden kuvaaminen/selvitys sisältäen kohtien a–d mukaiset asiat 100 000 euroa. Teknologisten linjausten laadinta 120 000 euroa. Teknologisten linjausten toteuttamisesta ja niiden mukaisen ympäristöjen rakentamisesta kohtien e–f osalta vastaa kukin viranomainen, ja

nämä kustannukset arvioidaan hankekohtaisesti. Turvallisuusarkkitehtuurin taso vaihtelee, jos jokainen viranomainen valmistelee erikseen turvallisuusarkkitehtuuriin kuuluvat asiat. Keskitetyllä koordinaatiolla on mahdollista vähentää kustannuksia ja parantaa suunnittelun tulosten yhdenmukaisuutta ja laatua sekä tuotettavien palvelujen ja niiden tuotantoympäristöjen turvallisuuta, valmiutta ja varautumista.

8.2 Julkisen hallinnon tarvitsema havainnointi, reagointi ja analysointi

Tavoite: Digitaalisen turvallisuuden häiriöiden käsittelyn nopeuttaminen ja haavoittuvuuksien tunnistaminen.

Vastuu: Digi- ja väestötietovirasto

Viestintä: Digi- ja väestötietovirasto yhdessä Traficomin kanssa laativat viestintäsuunnitelman ja viestivät julkisen hallinnon organisaatioille ja yhteisöille havainnointi- ja reagointikyvyn kasvattamiseen liittyvistä toimenpiteistä.

Kohde: Julkinen hallinto sekä yhteisöt

Aikataulu: 2021, suunnitelman toimeenpano 2022

Toimenpiteet: Digi- ja väestötietovirasto yhdessä Kyberturvallisuuskeskuksen kanssa laatii ohjeita ja suosituksia julkisen hallinnon palvelujen havainnointi- ja reagointikyvyn kehittämiseksi sekä VIRT-häiriötilanteiden hallintamallin parantamiseksi. Kuntien osalta toimenpiteeseen liittyvä selvitys tehdään kohdassa 3.1. Yhdessä kansallisen kyberturvallisuusstrategian täytäntöönpanon kanssa kehitetään kansallista kybertilannekuvaa huomioiden eri yhteiskunnan toimijoita sekä kansainvälisiä kumppaneita.

Digi- ja väestötietovirasto yhdessä Kyberturvallisuuskeskuksen kanssa suunnittelee julkisen hallinnon kriittisten tietojärjestelmien, tietoliikenneverkkojen ja IoT-laitteiden tunnistamisen. Suunnitelmassa käsitellään haavoittuvuustestausten toteutusta siten, että kriittiseksi tunnistettujen tietojärjestelmien, tietoliikenneverkkojen ja IoT-laitteiden omistajat laativat suunnitelman haavoittuvuuksien löytämiseksi. Suunnitellaan havaintojen kerääminen yhteen jaettavaksi kriittisten tietojärjestelmien, tietoliikenneverkkojen ja IoT-laitteiden käyttäjäorganisaatioille. Lisäksi suunnitellaan elinkaarensa loppupuolella olevien tietojärjestelmien haavoittuvuuksien kartoittaminen ja elinkaaren hallinta.

Cert-fi toimintaa kehitetään edelleen lisäämällä havainnointikykyä ja kokoamalla yhteen nykyisiä havaintotietoja. Havainnointiin tarvitaan teknisiä välineitä (esim. Havaro), skannauspalveluja ja tietoja kriittisten järjestelmien

haavoittuvuuksien määrien kehittymisestä. Suunnitellaan hankinnat ja käyttöönoton tukipalvelut ja toimeenpanovastuut kaikille suunnitelman tehtäville.

Mittaaminen: Ohjeet ja suositukset on laadittu ja tukipalvelu on käytössä. Haavoittuvuustestausten toteutuminen suunnitelmaa vasten.

Kustannus/hyöty:
Selvitys 60 000 euroa. Toteutus vaatii arviolta vuonna 2021 kaksi henkilötyövuotta, vuonna 2022 neljä henkilötyövuotta ja vuonna 2023 kuusi henkilötyövuotta Traficomissa. Toteutus ei sisälly kustannusarvioon. Nopeammalla reagoinnilla turvataan kansalaisten palvelujen jatkuvuus ja turvallisuus sekä pienennetään häiriötilanteiden ja toteutuneiden tietoturvaloukkausten aiheuttamia kustannuksia. Vähennetään mainehaittoja ja luottamuksen rapautumista sekä hallinnossa, yhteisöissä että kansalaisen keskuudessa.

8.3 Julkisen hallinnon pilvipalvelut

Tavoite: Julkisen hallinnon pilvipalveluiden käytön tukeminen.

Vastuu: Digi- ja väestötietovirasto

Viestintä: Digi- ja väestötietovirasto laatii viestintäsuunnitelman ja viestii julkisen hallinnon organisaatioille pilvipalveluiden käyttöön liittyvistä asioista.

Kohde: Julkinen hallinto

Aikataulu: 2021–2023

Toimenpiteet: Digi- ja väestötietovirasto yhdessä Valtorin kanssa valmistelevat sopimuslausekkeita, määrittelydokumentteja ja vaatimusmäärittelyjä pilvipalvelun vaihtamista tai käytön päättämistä varten (ns. pilvi-exit), jolloin palveluiden siirtäminen toiseen pilviympäristöön tulee myös mahdolliseksi. Suunnitellaan pilvipalveluiden käyttäminen palveluverkostojen varmentamisessa. Laaditaan analyysi vaihtoehdoista eri turvallisuustilanteissa, niihin liittyvä riskianalyysi sekä pilvipalveluiden käyttöön liittyvät suositukset.

Mittaaminen: Käyttötapaukset ja vähimmäisvaatimukset on kuvattu.

Kustannus/hyöty:
Määritysten valmistelu 80 000 euroa. Yhtenäisillä määrityksillä on mahdollista vähentää kustannuksia ja parantaa pilvipalveluiden turvallisuutta, valmiutta ja varautumista.

Yhteensä kohdassa 8 selvitystyötä koskevat hankinnat 300 000 euroa ja toteutustyötä koskevat hankinnat 120 000 euroa.

9 Julkisen hallinnon autonomisten ja oppivien järjestelmien sekä palveluiden turvallinen kehittäminen

Autonomisten ja oppivien järjestelmien sekä digitaalisten palveluiden turvallisuudesta huolehditaan riskienhallinnan avulla.

9.1 Julkisen hallinnon autonomisten ja oppivien järjestelmien valvonta

Tavoite:	Autonomisten ja oppivien järjestelmien valvonnasta huolehditaan. Autonomisten ja oppivien järjestelmien kehittämiseen ja valvontaan liittyvät turvallisuusperiaatteet ja kontrolliympäristö on määritetty ja sen toteutumista valvotaan.
Vastuu:	Valtiovarainministeriö
Viestintä:	Valtiovarainministeriö laatii viestintäsuunnitelman ja viestii julkisen hallinnon organisaatioille sekä yhteisöille autonomisten ja oppivien järjestelmien käyttöön liittyvistä soveltamisohjeista.
Kohde:	Julkinen hallinto sekä yhteisöt
Aikataulu:	2022–2023
Toimenpiteet:	Valtiovarainministeriö yhdessä digi- ja väestötietoviraston kanssa asettaa työryhmän selvittämään autonomisten ja oppivien järjestelmien turvallisuuteen liittyviä kontrolliympäristöjä. Ryhmässä luodaan yhteistä ymmärrystä säädöksistä, ja niiden mahdollisista kehittämistarpeista, sekä säädösten ja etiikan yhteisestä perustasta. Huomioidaan täysimääräisesti EU:n ohjeistus ja työkalut. Selvityksen perusteella laaditaan järjestelmien kehittämiseen ja valvontaan liittyvät periaatteet sekä kontrolliympäristö, joka ohjaa järjestelmien kehitystä ja ylläpitoa sekä viestintää myös kansalaisille.

Luottamuksen on säilyttävä palvelun sisältöön ja tuloksiin eri tilanteissa. Palvelun toiminta tulee läpinäkyvästi viestiä kansalaisille.

Autonomisten ja oppivien järjestelmien turvallisuusperiaatteiden ja kontrolliympäristön tulee ottaa kantaa kehitys- ja valvontavaatimuksiin seuraavilla osa-alueilla:

- oikeudenmukaisuus; mallien on oltava lainmukaisia ja niiden on käsiteltävä tietoa puolueettomasti
- eheys ja häiriönsieto; mallit toimivat johdonmukaisesti eri toiminta-ympäristöissä ja toimintatavat häiriötilanteissa on määritetty
- selitettävyys; mallien tapa oppia ja tehdä päätöksiä on tulkittavissa ja selitettävissä

Valtiovarainministeriö edistää aktiivisesti autonomisten ja oppivien järjestelmien eettisen säännöstön ja kontrolliympäristön kehittämistä kansainvälisessä yhteisössä.

Digi- ja väestötietovirasto laatii standardin mukaisen kansallisen soveltamisohjeen autonomisten ja oppivien järjestelmien kehittämiseen ja käyttöönottoon. Virasto kehittää asiantuntijapalvelun järjestelmien testaamiseen ja varmentamiseen.

Autonomisten ja oppivien järjestelmien kontrolliympäristö edellyttää uusien uhkaskenaarioiden ja riskien sekä niiden hallintaan sopivien kontrollien määrittelyä. Kontrolliviitekehyksen tai eettisen säännöstön ja kontrolliympäristön laatiminen koostuu riskianalyysistä, kontrollien määrittelytyöstä sekä soveltamisohjeen kirjoittamisesta. Lisäksi hankkeessa tulee tehdä pilotti, jossa testataan kontrollien sopivuutta julkisen sektorin organisaatioon.

Mittaaminen: Kansallinen soveltamisohje on valmisteltu.

Kustannus/hyöty:

Selvitys koskien riskianalyysiä, kontrollien määrittelyä sekä ohjeistoa ja sen pilotointia 100 000 euroa. Yhdenmukaisella ohjeistuksella turvataan oppien ja autonomisten järjestelmien turvallisuus ja jatkuvuus sekä pienennetään häiriötilanteiden ja toteutuneiden tietoturvaloukkausten aiheuttamia kustannuksia, ja mainehaittoja.

9.2 Julkisen hallinnon turvallinen palvelukehitys

Tavoite: Julkisen hallinnon palvelukehitysprosessissa huomioidaan jatkuvasti päivittyvät tietoturvallisuusvaatimukset riskienhallinnan avulla, erityisenä tavoitteena ovat oppiviin ja autonomisiin järjestelmiin liittyvät tarkennukset.

Vastuu: Digi- ja väestötietovirasto

Viestintä: Digi- ja väestötietovirasto laatii viestintäsuunnitelman ja viestii julkisen hallinnon organisaatioille turvallisen palvelukehityksen menetelmien käytöstä.

Kohde: Julkinen hallinto

Aikataulu: 2022–2023

Toimenpiteet: Digi- ja väestötietovirasto määrittää miten palvelukehityksessä asetetaan riskienhallinnan kautta jatkuvasti päivittyvät digitaalisen turvallisuuden vaatimukset, erityisesti koskien autonomisia ja oppivia järjestelmiä. Palvelukehitykseen liittyvien turvallisuusvaatimusten tulee kattaa eri sovelluskehitysmalleihin sopivat turvallisuuden varmistamiseen liittyvät toimenpiteet. Lisäksi Digi- ja väestövirasto laatii ohjeistuksen suositelluista menetelmistä, kuten DevSecOps-kehitysmenetelmä. Digi- ja väestötietovirasto tuotteistaa turvallisen palvelukehityksen koulutuksia julkishallinnon ja elinkeinoelämän käyttöön.

Mittaaminen: Vaatimusten muodostumisprosessi ja keskeisiä vaatimuksia on kuvattu ja niitä käytetään riskienhallinnan avulla autonomisia ja oppivia järjestelmiä koskevissa palvelukehityshankkeissa.

Kustannus/hyöty:

Selvitys koskien uhka- ja riskianalyysitietojen analysointiin tarvittavan mallin luomista 40 000 euroa. Testausmenetelmän ja sitä tukevien työkalujen määrittely 40 000 euroa. Koulutusten valmistelu ja toteutus 50 000 yhtenä vuonna. Mahdollisista keskitetyistä ohjelmistoista kuten testaustyökaluista päätetään erikseen. Yhdenmukaisella uhka- ja riskianalyysitietojen mallilla turvataan digitaalisten palveluiden turvallisuus ja jatkuvuus sekä pienennetään häiriötilanteiden ja toteutuneiden tietoturvaloukkausten aiheuttamia kustannuksia, ja mainehaittoja.

Yhteensä kohdassa 9 selvitystyötä koskevat hankinnat 180 000 euroa ja toteutusta koskevat hankinnat 50 000 euroa.

10 Yhteenveto kustannuksista

Yhteenveto selvityksiä ja toteutusta koskevista hankinnoista:

	Selvitys	Toteutus
Kohta 1	80 000 €	0 €
Kohta 2	140 000 €	260 000 €
Kohta 3	160 000 €	0 €
Kohta 4	0 €	0 €
Kohta 5	40 000 €	200 000 €
Kohta 6	0 €	0 €
Kohta 7	0 €	0 €
Kohta 8	300 000 €	120 000 €
Kohta 9	180 000 €	50 000 €
Yhteensä	**900 000 €**	**630 000 €**

Toimeenpanosuunnitelman toteuttamiseksi tarvittavat selvitystöitä koskevat hankinnat ovat arviolta 900 000 euroa ja toteutusta koskevat hankinnat arviolta 630 000 euroa, sekä lisäksi viestintään arviolta 80 000 euroa. Yhteensä 1 610 000 euroa.

Henkilötyöhön on varattu valtiovarainministeriössä arviolta 280 000 euroa, Digi- ja väestötietovirastossa arviolta 990 000 euroa sekä Liikenne- ja viestintävirastossa arviolta 780 000 euroa eli yhteensä 2 050 000 euroa.

Valtiovarainministeriössä yhteensä 600 000 euroa, Digi- ja väestötietovirastossa 2 280 000 euroa, sekä Liikenne- ja viestintävirastossa 780 000 euroa.

Yhteensä kustannukset ovat 3 660 000 euroa, momentilta 28.70.01.

Toimeenpanosuunnitelman toteuttamisesta ei aiheudu välttämätöntä pysyvää kustannusten kasvua.

Kustannusarvion ulkopuolelle on rajattu seuraavia asioita:

- Valtiovarainministeriön JulkiCT-osaston, digi- ja väestötietoviraston ja Traficomin ulkopuolinen valtion tai kuntien henkilöstön mahdollinen osallistuminen kehittämistehtäviin Vahti-verkostossa sekä tulosten käyttöönotto.
- Tähän kuuluu muun muassa valtiolla ja kunnissa tehtävän digitaalisen turvallisuuden riskien ja taloudellisen vaikuttavuuden arvioinnin kustannukset.
- Valtion ja kuntien havainnointi- ja reagointikyvyn kasvattamisen palveluiden käyttöönoton ja käytön kustannukset.
- Kuntien kyberhäiriöiden valvomotoiminteen kustannukset.
- Digitaalisen turvallisuuden asiantuntijapalveluiden käyttämisen kustannukset julkisessa hallinnossa.
- Teknologisia linjauksia vastaavien tieto- ja viestintäteknisten käyttö- ja tuotantoympäristöjen toteuttamisen kustannukset.
- Julkisen hallinnon infrastruktuurin ja palveluiden turvallisuuden tilan arvioinnin kustannukset.

VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

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

ISSN 1797-9714 (pdf)
ISBN 978-952-367-289-5 (pdf)

Huhtikuu 2020