Valtiovarainministeriö x/2018

Julkisen hallinnon digitaalisen turvallisuuden kehittämisohjelma vuosille 2018-2021

Valtiovarainministeriö, Helsinki 2018

Valtiovarainministeriö

ISBN PDF:
Kuvat: Xxxxxxxxx Xxxx
Taitto: Xxxxxxx Xxxxxxx

Helsinki 2018

Kuvailulehti

Julkaisija	Valtiovarainministeriö		xx.xx.2018
Tekijät	Kimmo Rousku (toimittaja)		
Julkaisun nimi	Julkisen hallinnon digitaalisen turvallisuuden kehittämisohjelma		
Julkaisusarjan nimi ja numero	Valtiovarainministeriön julkaisuja xx/2018		
Diaari/hankenumero	xxxxx xxxxxxx	**Teema**	xxxxxxxxxxx
ISBN PDF	xxxx-xxx	**ISSN PDF**	xxxx-xxx
URN-osoite	http://urn.fi/URN:ISBN:		
Sivumäärä	32	**Kieli**	suomi
Asiasanat	VAHTI, riskienhallinta, tietoturva, tietosuoja, kyberturvallisuus, jatkuvuudenhallinta, digitaalinen turvallisuus		

Valtiovarainministeriön tehtävänä on julkisen hallinnon tietoturvallisuuden yleinen kehittäminen ja valtionhallinnon tietoturvallisuuden ohjaus. Osana tätä ohjaustyötä valtiovarainministeriö kerää julkisen hallinnon organisaatioilta tietoa niin organisaatioiden turvallisuuden toteutumisesta kuin havaituista tai toteutuneista uhkista. Hallinnollisen tiedon ohella kerätään tietoa henkilöstön ja johdon ohjeistuksesta, koulutuksesta, osaamisesta ja asenteista. Tätä kokonaiskuvaa täydennetään organisaatioiden kriittisten palveluiden toimintaa ja turvallisuuden toteutumista mittaavilla tiedoilla.

Tämän tietopohjan, toimintaympäristössä havaittujen muutosten, ennustettavan uhkatilanteiden muutoksen sekä viimeisten vuosien aikana julkaistujen muiden raporttien ja ohjausasiakirjojen sekä ennakoiden tulevia lainsäädäntömuutoksia valtiovarainministeriö on tunnistanut tarpeen julkisen hallinnon digitaalisen turvallisuuden kehittämisohjelmalle. Kehittämisohjelman tavoitteena on varmistaa, että julkishallinnon digitaaliset palvelut toimivat ja että niihin luotetaan. Kehittämisohjelmaan on valittu tavoitteen mahdollistamiseksi kolme painoaluetta, jotka ovat 1) Digiturvallisuuden johtamisen ja riskienhallinnan kehittäminen, 2) Osaava henkilöstö sekä 3) Uuden teknologian hyödyntäminen palveluiden ja turvallisuuden toteuttamisessa. Nämä edellä olevat osa-alueet tulee ottaa huomioon myös tietoturvallisuuteen liittyvää arkkitehtuurityötä kehitettäessä ja sitä hyödynnettäessä.

Kolmen valitun painoalueen kehittämiseksi valtiovarainministeriö toteuttaa julkisen hallinnon digitaalisen turvallisuuden toimenpideohjelman vuosille 2018-2021. Toimenpideohjelma koostuu viidestä toimenpiteestä, joiden avulla varmistetaan painoalueiden kehittyminen ja kehittämisohjelman tavoitteiden saavuttaminen. Valtiovarainministeriö voi tarjota organisaatioille uusia toimenpiteitä vuosittaisen kehittämisohjelman arvioinnin yhteydessä. Kehittämis- ja toimenpideohjelman laatimisesta ja ohjaamisesta vastaa valtiovarainministeriö. Väestörekisterikeskus vastaa kehittämisohjelman toimenpiteiden operatiivisesta tuottamisesta julkisen hallinnon käyttöön sekä niiden toteutumisen raportoinnista valtiovarainministeriöön ja VAHTIlle. Julkisen hallinnon organisaatiot vastaavat omalta osaltaan toimenpiteiden toteuttamisesta omassa toiminnassaan. Kehittämisohjelman avulla tuetaan myös Suomen Kyberturvallisuusstrategian ja sen toimeenpano-ohjelman toteutumista.

Kustantaja	valtiovarainministeriö
Julkaisun myynti/jakaja	Sähköinen versio: julkaisut.valtioneuvosto.fi Julkaisumyynti: julkaisutilaukset.valtioneuvosto.fi

Presentationsblad

Utgivare	xxx		xx.xx.2018
Författare	Etunimi Sukunimi (toimittaja)		
Publikationens titel	Publikation (även den finska titeln) xxx		
Publikationsseriens namn och nummer	xxx xx/2018		
Diarie-/projektnummer	xxxxx xxxxxxx	**Tema**	xxxxxxxxxx
ISBN PDF	xxxx-xxx	**ISSN PDF**	xxxx-xxx
URN-adress	http://urn.fi/URN:ISBN:		
Sidantal	xxx	**Språk**	xxx
Nyckelord	xxx, xxx, xxx		
Referat			
Förläggare	xxx ministeriet		
Beställningar/ distribution	Elektronisk version: julkaisut.valtioneuvosto.fi Beställningar: julkaisutilaukset.valtioneuvosto.fi		

Description sheet

Published by	xxx		xx.xx.2018
Authors	Etunimi Sukunimi (toimittaja)		
Title of publication	Tälle riville tulee julkaisun pääotsikko Mahdollinen alatotsikko		
Series and publication number	xxx xx/2018		
Register number	xxxxx xxxxxxx	**Subject**	xxxxxxxxxxx
ISBN PDF	xxxx-xxx	**ISSN PDF**	xxxx-xxx
Website address (URN)	http://urn.fi/URN:ISBN:		
Pages	xxx	**Language**	xxx
Keywords	avainsana, avainsana, avainsana		
Abstract			
Publisher	Ministry of XXX		
Publication sales/ Distributed by	Online version: julkaisut.valtioneuvosto.fi Publication sales: julkaisutilaukset.valtioneuvosto.fi		

Sisältö

LUKIJALLE

Valtiovarainministeriön tehtävänä on julkisen hallinnon tietoturvallisuuden yleinen kehittäminen ja valtionhallinnon tietoturvallisuuden ohjaus. Tämän julkisen hallinnon digitaalisen turvallisuuden kehittämisohjelman avulla valtiovarainministeriö varmistaa, että Suomi vahvistaa asemaansa digitaalisen turvallisuuden, kyberturvallisuuden kärkijoukoissa sekä pystyy tarjoamaan jatkossakin yhteiskunnan ja kansalaisten käyttöön turvallisia ja luotettavia palveluita. Lisäksi digitaalisen turvallisuuden avulla mahdollistetaan uuden teknologian turvallinen käyttöönotto ja hyödyntäminen.

Tällä julkisen hallinnon digitaalisen turvallisuuden kehittämisohjelmalla valtiovarainministeriö ohjaa julkista hallintoa toteuttamaan digitaalista turvallisuutta kiinteänä, tärkeänä osana johtamista, riskienhallintaa, osaamisen kehittämistä sekä hallinnon kehittämistä ja toimintaa. Digitaalisen turvallisuuden kehittäminen on edellytys yhteiskuntamme toimintojen ja palveluiden laadulle ja turvallisuudelle, tehokkuudella ja avoimuudelle, sidosryhmien ja kansalaisten luottamukselle hallinnon toimintaan sekä kansalaisten ja yhteisöjen eduille ja oikeuksille.

Tämä kehittämisohjelma on tarkoitettu kaikille julkisen hallinnon organisaatioille ja sen toimeenpano organisaatiossa on organisaation johdon vastuulla. Kehittämisohjelma on osoitettu organisaation johdolle, jonka vastuulla on digitaalisen turvallisuuden eri osa-alueiden kokonaisvastuu. Johdon tehtävänä on delegoida näiden osa-alueiden vastuu organisaatiossa sekä antaa käyttöön tarvittavat resurssit sekä seurata kokonaisuuden etenemistä. Tämä koskee myös tätä kehittämisohjelman toteuttamista.

Jokaisen julkisen hallinnon organisaation tulee huolehtia siitä, että sen toiminnan kriittisyyden ja sille muuten asetettujen tavoitteiden mukainen digitaalinen turvallisuus sekä henkilötietojen suoja toteutuvat organisaatiossa, sen tuottamissa ja käyttämissä palveluissa sekä yhteistyössä sidosryhmien kanssa ja hankittaessa palveluita organisaation ulkopuolelta. Tällöin kehittämisessä tulee huolehtia toimenpiteistä, joilla pyritään ennakoivasti estämään tietoturvaloukkausten todennäköisyyttä ja vaikutusta, mutta kuitenkin samalla kehittää myös suunnitelmia ja prosesseja, joilla tällaisten tapahtumien ilmetessä, organisaatiolla on kyky palautua normaaliin toimintaan.

Turvallisuuden toteuttaminen on esimerkiksi toiminnan johtamista, viestintää, henkilöstön osaamista, toimittajaketjujen hallintaa sekä teknologiaratkaisuja. Osaava henkilöstö toimii organisaation keskeisenä voimavarana ja turvallisuuden mahdollistajana. Henkilöstön osaaminen ja sitä kautta syntyvä turvallisuuskulttuuri ja –asenne ovat merkittävässä roolissa turvallisuuden toteuttamisessa ja luottamuksen rakentamisessa organisaatiossa ja sen sidosryhmissä. Tässä organisaation johdolla on keskeinen merkitys näiden muodostumisessa ja omalta osaltaan esimerkkinä toimimisessa.

Kehittämisohjelman tueksi on laadittu toimenpide-ohjelma, joka sisältää yhteensä viisi toimenpidettä, joihin organisaation tulee osallistua vuosien 2019-2021 aikana omaan aikatauluunsa ne sovittaen. Tämän kehittämisohjelman etenemisen seuranta ja vaikutusten mittaaminen sekä raportointi sisällytetään osaksi valtiovarainministeriön suorittamia julkisen hallinnon digitaalisen turvallisuuden kokonaiskuvan keräämistä.

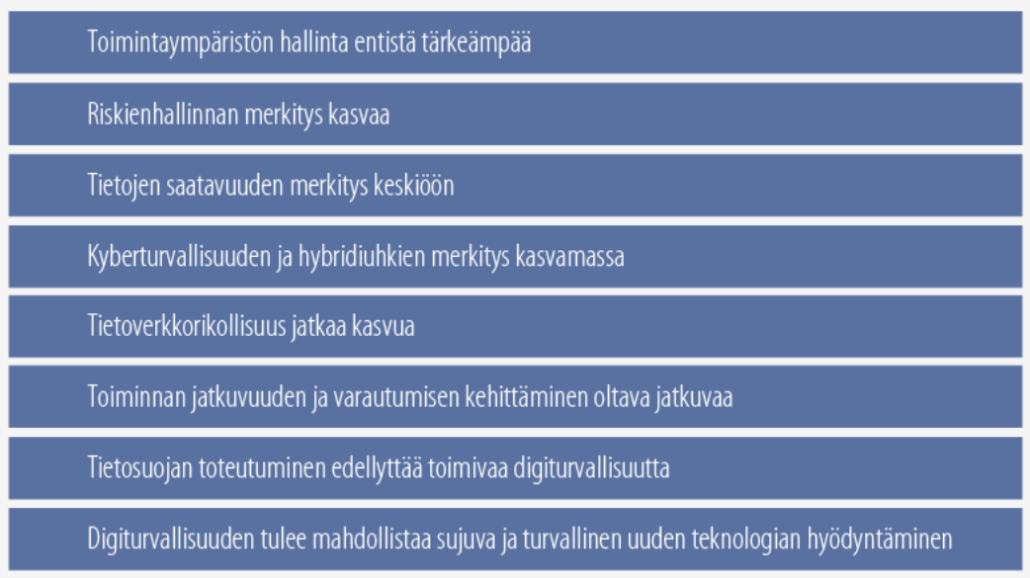
x.10.2018

Anu Vehviläinen
Kunta- ja uudistusministeri

Anna-Maija Karjalainen
VAHTIn puheenjohtaja
ICT-johtaja, ylijohtaja

1 Digitaalinen toimintaympäristö muutoksessa

Valtiovarainministeriö kerää julkisen hallinnon organisaatioilta tietoa niin organisaatioiden turvallisuuden toteutumisesta kuin havaituista tai toteutuneista uhkista. Hallinnollisen tiedon ohella kerätään tietoa henkilöstön ja johdon ohjeistuksesta, koulutuksesta, osaamisesta ja asenteista. Tätä kokonaiskuvaa täydennetään organisaatioiden kriittisten palveluiden toimintaa ja turvallisuuden toteutumista mittaavilla tiedoilla. Tämän tietopohjan, toimintaympäristössä havaittujen muutosten, ennustettavan uhkatilanteiden muutoksen sekä viimeisten vuosien aikana julkaistujen muiden raporttien ja ohjausasiakirjojen avulla valtiovarainministeriö on tunnistanut muun muassa seuraavia keskeisiä digitaalisen toimintaympäristöön ja sen turvallisuuteen vaikuttavia tekijöitä:



Kuva 1. Kehittämisohjelman laatimisessa on valtiovarainministeriön toteuttamien kyselyiden ja mittareiden perusteella sekä asiantuntijaryhmän avulla tunnistettu kahdeksan osa-aluetta, jotka on otettu huomioon sen laatimisessa. Digitaalinen toimintaympäristö, uudet teknologiat ja palvelut tarjoavat valtavia mahdollisuuksia, mutta samassa yhteydessä niihin liittyvien uhkien tunnistaminen ja riskienhallinta on edellytys näiden uusien mahdollisuuksien valjastamiselle.

1.1 Toimintaympäristön hallinta entistä tärkeämpää

Toimimme verkostoituneessa yhteiskunnassa osana globalisoituvaa maailmaa. Yksittäisten tietojärjestelmien tilalle palveluiden taustalla toimivat yhä laajemmat digitaalisten palveluiden ekosysteemit, jotka muodostava entistä laajempia palveluketjuja ja –alustoja. Laajan palvelukokonaisuuden toteuttamisessa saatetaan tarvita kymmeniä alihankkijoita.

Julkisessa hallinnossa on palveluita, joihin kohdistuu erityisiä turvallisuusvaatimuksia, kuten häiriönsieto vakavissa kriisitilanteissa. Lisäksi tiettyjen tietojen käsittelyn suojaamiseen liittyy kansallisia ja kansainvälisiä erityisvaatimuksia. Tietojenkäsittelyn ja toimintojen muuttuessa verkottuneemmaksi, tietojenkäsittely-ympäristöt edellyttävät laajempaa kokonaissuunnittelua. Suunnittelussa tulee pystyä huomioimaan eri toimijoiden tarpeet varmistaen ratkaisujen yhteensopivuus ja kustannustehokkuus.

Nopeassa muutoksessa oleva toimintaympäristö edellyttää aktiivista uhkien seurantaa ja riskienhallintaa, joiden avulla organisaatio pystyy varmistamaan tarkoituksenmukaisen turvallisuuden kehittämisen osana sen jokapäiväistä toimintaa. Tässä mallissa entistä tärkeämmäksi nousevat verkostossa toimivien tahojen välinen luottamus, yhteistyö sekä vastuunjaosta sopiminen.

Julkisessa hallinnossa on tapahtunut 2010-luvulla useita merkittäviä hallinnollisia rakennemuutoksia, joiden johdosta sekä ICT-palveluiden tuottaminen sekä julkisen hallinnon käyttöön tarkoitetut palvelut ovat uudistuneet merkittävästi. Uudet tai osin vielä kehitteillä olevat palvelukeskukset tai muu toimijat vastaavat keskitettyjen palveluiden tuottamisesta käyttäen joko omaa palvelutuotantoa ja henkilöstöä tai hyödyntäen markkinoilta saatavia palveluita ja alihankkijoita. Samanaikaisesti julkisessa hallinnossa, koko yhteiskunnassa on käynnissä merkittävä toimintatapojen uudistus rakentamalla ja muotoilemalla palveluita uudelleen asiakaslähtöisesti hyödyntäen uuden teknologian tarjoamia mahdollisuuksia.

Palveluiden hyödyntäessä yhä enemmän teknologioita, niiden muutosvauhti kasvaa. Julkisia palveluita tarjotaan yhä enemmän yhteistyössä eri toimijoiden kanssa. Palvelut voivat olla keskenään riippuvaisia ja palvelutuotanto voi koostua hankinta- ja tuotantoverkostoista. Yhteisissä palveluissa muutosten ja häiriöiden vaikutusten arviointi edellyttää riittävää kokonaiskuvaa. Palvelut voivat edellyttää myös yhteisiä toiminta- ja käyttösääntöjä turvallisuuden varmistamiseksi. Samalla tulisi kuitenkin voida varmistaa kustannustehokas toiminta.

1.2 Riskienhallinnan merkitys kasvaa

Valtiovarainministeriö julkaisi OECD:n laatiman ”Digitaaliseen turvallisuuteen kohdistuvien riskien hallinta taloudellisen ja yhteiskunnallisen hyvinvoinnin edistämiseksi” [1] suosituksen syksyllä 2016. Tässä suosituksessa nostetaan esille digitaalisen toimintaympäristön mukanaan tuomat haasteet.

Suosituksen mukaan ”Digitaaliseen turvallisuuteen kohdistuvien uhkien ja poikkeamien määrä on kasvanut viime vuosina sekä johtanut merkittäviin taloudellisiin ja sosiaalisiin seurauksiin niin julkisille ja yksityisille organisaatioille kuin yksilöillekin. Tällaisia ovat esim. toiminnan keskeytyminen (palvelunestohyökkäyksen tai sabotaasin seurauksena), välittömät taloudelliset tappiot, oikeusjutut, maineelle aiheutuva vahinko, kilpailukyvyn menettäminen, (esim. liikesalaisuuksien anastuksen yhteydessä) sekä asiakkaiden luottamuksen menetys.”

Samoin riskienhallinnan merkitys on noussut sekä EU:n yleisen tietosuoja-asetuksen johdotsa. Lisäksi valtiovarainministeriössä valmistelussa olevassa tiedonhallintalaissa edellytetään riskienhallinnan kehittämistä ja etenkin organisaatioilta kyvykkyyttä jäännösriskien käsittelyyn. Mikään organisaatio ei pysty digitaalisessa toimintaympäristössä toteuttamaan 100% turvallisuutta, joten toimiva riskienhallinta on nykyaikana välttämättömyys.

1.3 Tietojen saatavuuden merkitys keskiöön

Toiminnan aluksi sähköistyessä ja nyt uusia toimintamalleja digitalisoimalla tiedon saatavuuden merkitys on kasvanut. Keskeinen muutostekijä tässä on lisäksi tiedon määrän kasvaminen sekä tarve hyödyntää eri toimijoiden keräämiä ja tietoja entistä tehokkaammin. Koska kansalaisten, asiakkaiden ja muiden sidosryhmien tapa asioida on myös muuttunut 2010 luvulla uuden teknologian (uudenlaiset palvelut, mobiilit tietoliikenneyhteydet, päätelaitteet) ansiosta ajasta ja paikasta riippumattomaksi, palveluiden täytyy olla saatavilla käytännössä 24/7, vaikka organisaation ei alun perin tällaista palveluvelvoitetta ole tunnistanut. Tiedon saatavuuden mahdollistaminen edellyttää samalla sen eheydestä ja salassa pidettävien tietojen osalta niiden luottamuksellisuuden huolehtimisesta.

[1] http://julkaisut.valtioneuvosto.fi/handle/10024/75412

1.4 Kyberturvallisuuden ja hybridiuhkien merkitys kasvamassa

Perinteisen, vakiintuneen tietoturvallisuuden rinnalle on 2010-luvulla noussut kyberturvallisuuteen liittyvä käsite, joka kuvastaa samalla hyvin toimintaympäristöön kohdistuvissa uhkissa tapahtunutta muutosta. Kyberturvallisuuden avulla pyritään huolehtimaan sähköisen, digitaalisen toimintaympäristön kokonaisturvallisuudesta. Tämä kattaa digitaalisessa toimintaympäristössä olevien tietojen ja palveluiden tietoturvallisuuden ohella myös tarvittavan muun, etenkin kriittisen infrastruktuurin (esimerkiksi energian tuotanto ja jakelu, tietoyhteiskunnan palvelut, logistiikka sekä finanssiala) toiminnan mukaan luettuna toiminnassa tarvittavan henkilöstön.

Muutaman viimeisen vuoden aikana esille ovat nousseet myös hybridivaikuttaminen sekä hybridiuhat uutena kyberturvallisuutta sivuavana kokonaisuutena. Hybridivaikuttamisessa yhdistyvät perinteiset ja uudet vaikuttamisen keinot, esimerkiksi tässä yhteydessä voidaan käyttää erilaisia psykologisia, poliittisia, taloudellisia, teknisiä, humanitaarisia ja sotilaallisia keinoja. Keskeistä hybridivaikuttamiselle on avainhenkilöihin kohdistuva psykologinen vaikuttaminen sekä informaatiovaikuttaminen. Erityisesti informaatiovaikuttaminen voi sisältää mm. suoria kyberhyökkäyksiä tai tarkoituksellisesti harhaanjohtavan tiedon levittämistä käyttäen erilaisia digitaalisia toimintaympäristön tarjoamia palveluita.

1.5 Tietoverkkorikollisuus jatkaa kasvua

[2]Tutkimusten mukaan kyberrikollisuuden vaikutus talouteen viisinkertaistui vuosien 2013 ja 2017 välillä, ja se voi edelleen nelinkertaistua vuoteen 2019 mennessä. Tietoverkko- ja kyberrikollisuus sekä muut ryhmät hakevat koko ajan uusia keinoja saavuttaa taloudellista hyötyä. Tätä varten luodaan uusia hyökkäys- ja väärinkäyttö- sekä huijauskeinoja, joita kohdistetaan kaikkiin organisaatioihin ja käyttäjiin. Suomi tai meillä toimivat yritykset, julkisen hallinnon organisaatiot, käyttäjät tai kansalaiset ovat kohteina tässä globaalissa tietoverkko- ja kyberrikollisten verkostossa.

Käytännössä emme voi itse juuri vaikuttaa siihen, olemmeko miten erilaisten hyökkäys- tai huijauskampanjoiden kohteita, sen sijaan voimme vaikuttaa siihen, kuinka hyvin pystymme niitä omassa digitaalisessa toimintaympäristössä havainnoimaan ja

[2] http://europa.eu/rapid/press-release_IP-17-3193_fi.htm

sen jälkeen niihin reagoimaan. Erityisesti havainnointikyvyn kehittäminen on keskeinen kyvykkyys, jonka avulla organisaatio saa paremman kokonaiskuvan oman organisaation turvallisuuden tilanteesta.

1.6 Toiminnan jatkuvuuden ja varautumisen kehittäminen oltava jatkuvaa

Turvallinen yhteiskunta edellyttää, että julkisen hallinnon toiminta on turvallista ja digitaalisten palveluiden käyttö luotettavaa. Vaikka Suomessa havaitaan suhteellisen harvoin merkittäviä tietoturvaloukkauksia tai muita yhteiskunnan toimintaa häiritseviä tapauksia, tulee turvallisuuden eri osa-alueisiin panostaa. Hallinnon toimintojen ja palvelujen digitalisaation myötä erilaisten toiminnallisten sekä häiriötapausten hallinnan tarve on korostunut. Kyberuhkien kasvu ja monimuotoistuminen on muuttanut kehittämisen painopistettä.

Valtiovarainministeriön keräämä aineisto osoittaa sen, että digitaaliseen toimintaympäristöön kohdistuvat niin tekniset häiriöt kuin tieto- ja kyberturvallisuuteen vaikuttavat poikkeamat tulevat yleistymään ja niiden vaikutus laajentumaan. Tällaisten häiriö- ja vikatilanteiden hallintaa tulee kehittää organisaatiotasolla sen toiminnan kriittisyys huomioiden.

Tämä tapahtuu sekä ennakoivasti, mahdollisia uhkia tunnistamalla ja estämällä niiden syntyminen ennen kuin ne pääsevät vaikuttamaan toimintaan sekä kehittämällä varautumista ja valmiutta reagoida tällaisiin tilanteisiin toiminnan kriittisyyden edellyttämällä tavalla.

1.7 Tietosuojan toteutuminen edellyttää toimivaa digiturvallisuutta

Valtaosa useimpien viranomaisten tietojenkäsittelyä liittyy henkilötietoihin. On olemassa viranomaisia, jotka eivät käsittele niitä muuta kuin oman organisaation henkilöstön osalta, mutta tällöinkin tällainen organisaatio saa käyttöönsä osana muuta yhteistyötä muiden osapuolien esimerkiksi asiakas- tai muita yritystietoja. Käytännössä henkilötietojen, siten tietosuojan merkitys on kasvussa myös 2020-luvulla.

EU:n yleinen tietosuoja-asetus sekä kansallinen lainsäädäntö muuttavat henkilötietojenkäsittelyyn liittyvää sääntelyä. Myös tässä yhteydessä digiturvallisuudella on keskeinen rooli; se toimii henkilöstötietojen turvallisen käsittelyn mahdollistajana.

1.8 Digiturvallisuuden tulee mahdollistaa sujuva ja turvallinen uuden teknologian hyödyntäminen

Teknologian kehittyminen on nopeutunut erityisesti 2010-luvulla. Tämä koskee niin palveluiden tuotantomalleja, käytettävissä olevia päätelaitteita sekä tietoliikenneyhteyksiä. Yhteiskunnassa sekä globaalissa toimintaympäristössämme on meneillään teknologian tarjoamien mahdollisuuksien myötä yhä nopeutuva mahdollisuus uudistaa ja kehittää toimintaa disruptiivisella tavalla. Tämä korostuu uusia ekosysteemejä, alustoja luovassa ja hyödyntävässä sekä automatisaatiota, robotisaatiota ja tekoälyä entistä tehokkaammin käyttöönottavassa yhteiskunnassa. Muutoksessa on keskeistä pyrkiä ymmärtämään ja tarvittaessa ennakoimaan vaikutuksia.

Tästä hyvä esimerkki on käyttöpalveluiden ja muiden ICT-palveluiden ulkoistaminen ja siirtyminen käyttämään uudenlaisia palvelutuotantomalleja, esimerkiksi jaettua kapasiteettia hyödyntäviä malleja tai vielä laajamuotoisempia ns. ”pilvipalveluita”.

Päätelaitteiden muuttuminen tulee jatkumaan kiihtyvällä vauhdilla; mobiililaitteista on tullut yhä suorituskykyisempiä ja samoin niiden käytössä olevat tietoliikenneverkot tarjoavat yhä suurempia siirtonopeuksia, tosin vaihteluväli on hyvin suuri alueellisesti ja suorituskyky riippuu muutenkin verkon kuormituksesta.

Tietojenkäsittelykyvyn ja tietoliikenneyhteyksien tuominen tapahtuu osaksi kaikkia laitteita, jotka toimivat sähköllä. Jatkossa yhä useampi, jossain vaiheessa kaikki sähkölaitteet ovat kytkettynä tietoliikenneverkkoihin. Tällaisten esineiden-Internet-verkon (IoT, Internet of Things) laitteiden avulla saamme kerättyä jatkossa yhä enemmän tietoa sellaisista toiminnoista, joista se ei ole ollut aikaisemmin mahdollista tai taloudellisesti kannattavaa. Näiden IoT-laitteiden osalta keskeisenä uhkana pidetään niiden tietoturvattomuutta.

2 Julkisen hallinnon digitaalisen turvallisuuden kehittämisohjelma

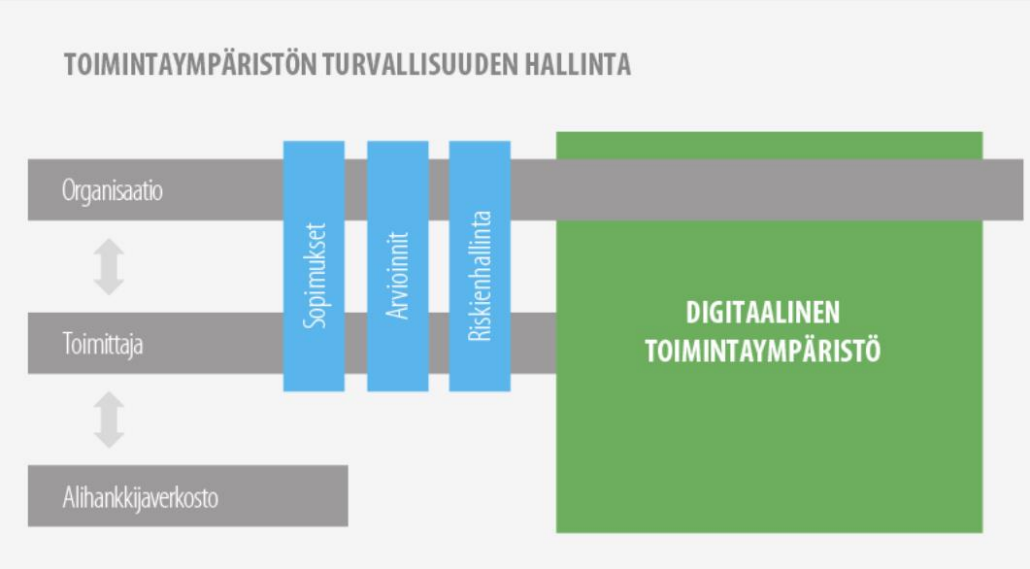
2.1 Ohjelman lähtökohdat

Julkisen hallinnon kehittämisohjelman laatimisesta on vastannut VAHTI-johtoryhmän jäsenistä sekä VAHTI-asiantuntijajaoston alaisuudessa toimivien viiden asiantuntijaryhmän puheenjohtajistosta koostuva ryhmä. Lisäksi tässä on huomioitu VAHTI-johtoryhmän ja sen alaisen asiantuntijajaoston jäsenten antamat kommentit kehittämisohjelman laatimisen eri vaiheissa.

Kehittämisohjelma on laadittu ottaen huomioon muun muassa seuraavat kokonaisuuteen vaikuttavat tekijät:

- Valtiovarainministeriön toteuttamat digitaalisen turvallisuuden kyselyt ja barometrit sekä näistä tehdyt havainnot sekä kehittämistoimenpide-ehdotukset
- Julkisen hallinnon digitaalisen turvallisuuden kokonaiskuva-raportoinnin kautta havaitut kehittämiskohteet
- Säädökset, muu regulaatio sekä laaditut selvitykset ja tarkastuskertomukset koskien digitaalisen turvallisuuden osa-alueita
- Toimintaympäristössä tapahtuvat tähän kokonaisuuteen liittyvät muutokset, tähän tehty kysely VAHTI-toimintaan osallistuville henkilöille
- Digitaalisen turvallisuuden tulevaisuuden ennakointi sen eri osa-alueiden näkökulmasta
- Kansainvälinen kehitys

Toimintaympäristöjen ja palveluiden muutokset edellyttävät myös riskienhallinnan jatkuvaa kehittämistä. Esimerkiksi yhteiskäyttöiset, globaalit pilvipalvelut, keinoälyn ja automatisaation hyödyntäminen luovat valtavia mahdollisuuksia, mutta samalla tuovat uusia uhkia, jotka pitää tunnistaa ja ottaa hallintaan.



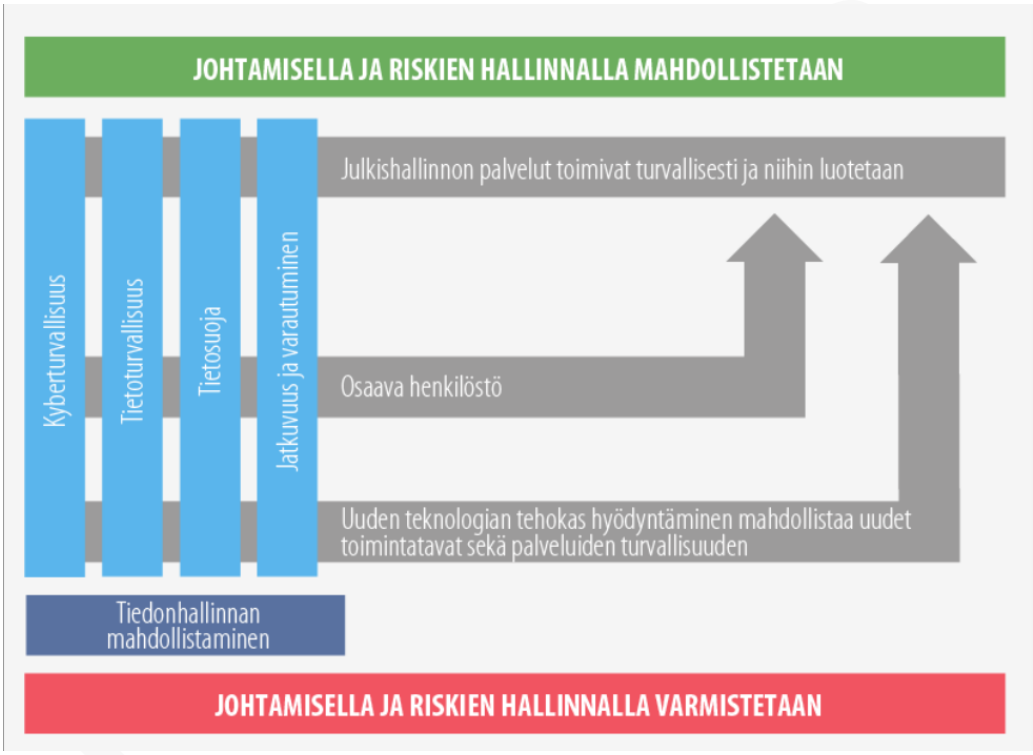
Kuva 2. Organisaation tulee varmistaa toimintaympäristön turvallisuus, jossa keskeisessä roolissa on palveluiden hankinta ja kilpailuttaminen tai oma kehittäminen, missä yhteydessä sovitaan myös turvallisuuden toteutumisen vaatimuksista.

Palveluiden tuottamisessa tulee huolehtia myös siihen liittyvän tietoturva-arkkitehtuurin huomioimisesta, joka mahdollistaa kustannustehokkaiden, yhteensopivien turvallisten palveluiden tuottamisen, joka on myös edellytys organisaatioiden väliselle tietojenvaihdolle.

2.2 Ohjelman tavoitteena varmistaa toimivat ja luotettavat digitaaliset palvelut

Kehittämisohjelman tavoitteena on varmistaa, että julkishallinnon digitaaliset palvelut toimivat ja että niihin luotetaan. Digitaalisten palveluiden tuottamisessa on tapahtunut merkittävä muutos viimeisen kymmenen vuoden aikana. Palvelutuotantoon liittyy usein eri palvelutoimittajia ja asiakkaita. Palvelut voivat olla riippuvaisia toisistaan ja niitä tuotetaan verkostomaisesti. Tietoja ja palveluja hyödynnetään eri tarpeisiin. Verkostomainen toiminta mahdollistaa entistä skaalautuvammat, kustannustehokkaat ja joustavammat ICT-palvelut. Tämä muutos on edellyttää myös jatkuvaa turvallisuuden johtamisen ja hallinnan kehittämistä.

Tällä kehittämisohjelmalla tuetaan ja mahdollistetaan digitalisaation toteuttaminen turvallisesti julkishallinnon palveluissa ja muussa sen toiminnassa. Tämä vahvistaa samalla palveluiden käyttäjien, niin kansalaisten, julkisen hallinnon henkilöstön, yritysten kuin muiden sidosryhmien luottamusta käytettäviin palveluihin ja toimintaan. Tämä tapahtuu kehittämisohjelmassa priorisoitujen osa-alueiden avulla.



Kuva 3. Kehittämisohjelman keskeiset osa-alueet liittyvät johtamiseen ja riskienhallintaan, osaavaan henkilöstöön sekä uuden teknologian tehokkaaseen hyödyntämiseen palveluiden ja turvallisuuden toteuttamisessa.

Rakentamalla turvallisia palveluita, käsittelemällä palveluissa olevia tietoja vaatimustenmukaisesti sekä huolehtimalla myös häiriötilanteissa tarvittavasta viestinnästä saavutetaan asiakkaiden, kansalaisten ja muiden sidosryhmien luottamus. Tämä on samalla edellytys myös uuden teknologian käyttöönottamiselle palveluiden kehittämisessä.

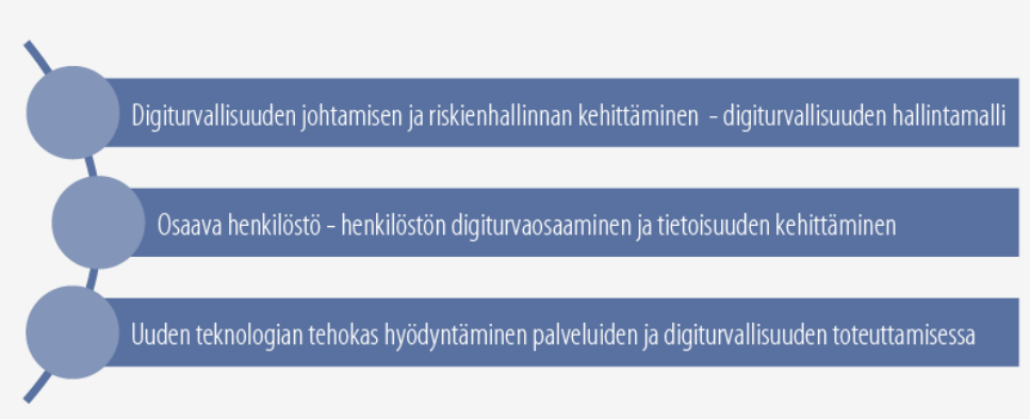
2.3 Kehittämisohjelman kattavuus

Kehittämisohjelma on tarkoitettu kattamaan koko julkinen hallinto. Kehittämisohjelman osa-alueet vaikuttavat välillisesti myös julkiselle hallinnolle palveluita tuottavien alihankkijoiden ja muiden sidosryhmien turvallisuuden parantumiseen.

Kuva 4. Kehittämisohjelma on tarkoitettu julkisen hallinnon organisaatioille.

2.4 Kehittämisohjelman painoalueet

Valtiovarainministeriö on ottanut huomioon painoalueita valitessaan toimintaympäristöön liittyvät muutostekijät (liite 1) sekä kehittämisohjelmalle asetetut tavoitteet. Tavoitteiden saavuttamisen mahdollistamiseksi on valittu seuraavat kolme osa-aluetta, joiden avulla varmistetaan digitaalisen turvallisuuden laaja-alainen ja tarkoituksenmukainen kehittäminen julkisessa hallinnossa.



Kuva 5. Kehittämisohjelman kolme painoaluetta keskittyvät digitaalisen turvallisuuden keskeisin rakenteisiin, niin toimintaympäristön turvallisuuden johtamisen ja riskienhallinnan, henkilöstön kuin teknologian näkökulmasta. Painoalueiden kehittämistä tuetaan toimenpide-ohjelmalla.

2.4.1 Digiturvallisuuden johtamisen ja riskienhallinnan kehittäminen

Digitaalisen turvallisuuden johtamisen kehittäminen on valittu yhdeksi kehittämisen osa-alueeksi sen takia, että mitä nopeammin ja kattavammin uutta teknologiaa sekä uusia palveluita otetaan käyttöön, sitä enemmän se edellyttää digitaalisen turvallisuuden sovittamista osaksi organisaation toimintaan, etenkin johtamisen näkökulmasta. Samalla tämä varmistaa myös olemassa olevien palveluiden ja toiminnan turvaamisen. Organisaation käyttöönottamissa digitaalisissa palveluissa ja niiden tuotantotavoissa sekä alihankintaverkostoissa tapahtuu muutoksia kiihtyvällä vauhdilla. Tämän tulee heijastua myös organisaation johdon toimintaan turvallisuuden johtamisen kehittämisen näkökulmasta.

Johtamisen, kuten digiturvallisuuden keskeisenä työkaluna toimii **riskienhallinta**. Organisaatio pystyy kehittämään omaa toimintaa tehokkaammin ja kustannustehokkaammin, kun sillä on toimiva riskienhallintaprosessi osana sen toimintaa, jossa on määritetty ne raamit, jonka sisällä se pystyy ottamaan riskejä (riskinottokyky) ja myös niitä käytännössä ottaa (riskinottohalukkuus). Osa toimivaa riskienhallintaa on kyky käsitellä ja hyväksyä sekä hallita jäännösriskejä; nykyaikana ei ole mahdollista toimia ilman jäännösriskiä.

Digitaalisen turvallisuuden johtaminen edellyttää

- riskilähtöistä toimintamallia organisaation ja digitaalisen turvallisuuden johtamisessa - riskienhallinta varmistaa, mutta myös mahdollistaa organisaation tavoitteiden saavuttamisen, jatkuvan toiminnan sekä toiminnan kehittymisen esimerkiksi uudenlaisten, turvallisten digitaalisten palveluiden avulla

- turvallisuuden eri osa-alueiden ymmärtämistä ja niiden tärkeyden tunnistamista osana organisaation toimintaa sekä koko toimintaverkostossa

- arkkitehtuurien hyödyntämistä yhteentoimivuuden ja tietojen sujuvan jakamisen mahdollistamiseksi

- toimintaverkoston hallintaa; sopimuksissa ja vaatimuksissa kuvattujen velvoitteiden seuranta osana sekä tarvittavien arviointien toteuttaminen

- vastuiden kuvaamista ja määrittämistä niin organisaation sisällä kuin sen keskeisten toimittajien ja sidosryhmien kesken

- tarvittavia resursseja käytännön tasolla toteuttaa digitaalisen turvallisuuden eri osa-alueilta edellytettäviä vaatimuksia

- kokonaisuuden raportointia ja seurantaa johdon tasolla, mutta myös organisaatiolle tuottavien alihankkijoiden osalta

Osana tämän kehittämisohjelman toimenpideohjelmaa luodaan johtamisen ja riskienhallinnan tueksi uusia toimintamalleja sekä toteutetaan yhteishanke julkisen hallinnon organisaatioille tämän osa-alueen kehittämiseksi.

Kuva 6. Riskienhallinnan tulee olla dynaamista ja huomioida toiminnan luonne, kriittisyys sekä toimintaympäristön muutokset. Organisaation johdon tehtävä on asettaa puitteet riskienhallinnan toteuttamiselle sekä huolehtia kokonaisuuden toiminnasta. Riskinottokyky ja halu pitää vaihdella arvioitavan toiminnon / kohteen mukaisesti, mitä suurempi mahdollinen vahinko on kyseessä, sitä tärkeämpää on kiinnittää huomiota riskienhallinnan toimivuuteen ja tunnistettujen riskien hallintaan.

Organisaation johdon tulee varmistaa, että se on liittänyt digitaalisen turvallisuuden johtamisen ja sen vaatiman osaamisen osaksi sen johtamisjärjestelmää.

Kuva 7. Organisaation johdon vastuuna on huolehtia digitaalisen turvallisuuden toteutumisesta sen toiminnassa sekä omassa organisaatiossa, että sille tuotettujen palveluiden ja toimintojen osalta.

Käytännössä tämä tapahtuu kokonaisuuden vastuuhenkilöiden toteuttamana siten, että kokonaisuutta varten luodaan digitaalisen turvallisuuden johtamisen ja hallinnan malli, jonka avulla organisaatio varmistaa vaatimustenmukaisuuden toteutumisen sen toiminnassa. Kuten kaikessa toiminnassa, myös digitaalisessa turvallisuudessa henkilöstön rooli on keskeinen, minkä johdosta henkilöstön osaamisen kehittäminen on yksi tämän kehittämisohjelman painoalueita. Organisaation tulee huolehtia ja kehittää myös heidän ydin/liiketoiminnan kehittämiseen liittyvän toimittajaverkoston asiantuntijoiden tarvitsemasta osaamisesta ja turvallisuustietoisuudesta heidän tuottaessa organisaatiolle palveluita.

Valtionhallinnossa osana toimenpide-ohjelman toteuttamista tulee varmistaa, miten tätä kehittämisohjelmaa voidaan toteuttaa tehokkaasti esimerkiksi valtioneuvostossa ja ministeriöiden hallinnonaloilla.

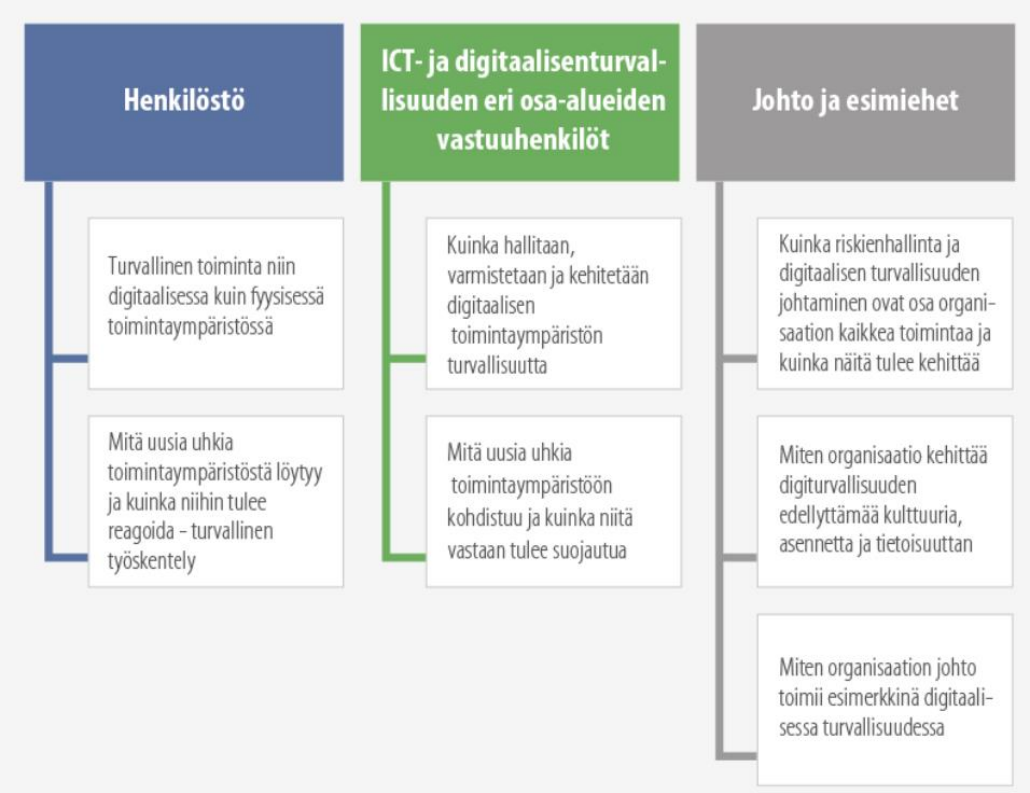
2.4.2 Osaava henkilöstö - henkilöstön digiturvaosaaminen ja tietoisuuden kehittäminen

Tässä kehittämisohjelmassa on aikaisemmin nostettu esille henkilöstön keskeinen, kriittinen rooli digitaalisen turvallisuuden toteuttamisessa organisaatiossa. Tämän kehittämisalueen avulla varmistamme, että julkisen hallinnon henkilöstö toimii jatkossa entistä turvallisemmin nopeasti muuttuvassa digitaalisessa toimintaympäristössä.

Tämä edellyttää uudenlaista digitaalisen turvallisuuden eri osa-alueiden koulutuksen kehittämistä ja toteuttamista. Kertaluonteinen tai vuosittainen koulutus ei enää riitä; digitaalisessa toimintaympäristössä tapahtuvat julkista hallintoa kohtaavat uhkakuvat kehittyvät entistä nopeammin. Tämän johdosta tarvitaan säännöllistä, paremmin toimintaympäristön muutokset ja nopeasti kehittyvät uhkakuvat huomioivaa koulutusta ja aktiivista viestintää. Tämä ei ole mahdollista ja taloudellista toteuttaa esimerkiksi pienten organisaatioiden osalta tarvittavalla tasolla, joten tämän tulee tapahtua jatkossa myös keskitetysti.

Valtiovarainministeriön valmistelema tiedonhallintalaki vaikuttaa astuessaan voimaan merkittävästi julkisen hallinnon digitaaliseen turvallisuuteen, joka tulee ottaa huomioon henkilöstön koulutuksessa ja ohjeistuksessa. Laki sinällään ei vaikuta tai muuta tämän kokonaisuuden henkilöstön ohjeistamiseen ja koulutukseen liittyviä perusperiaatteita, ainoastaan tarkentaa niitä esimerkiksi tietoaineistojen luokittelun osalta.

Jatkossa tarvitaan paremmin sovitettua ja suunnattua koulutusta ja viestintää hyödyntäen uuden teknologian tarjoamia mahdollisuuksia, esimerkiksi seuraaville kohderyhmille käsitellen alla mainittuja osa-alueita:



Kuva 8. Osaamista tulee kehittää keskitetysti eri kohderyhmille varmistaen koulutuksen ja tiedottamisen laadun, säännöllisyyden ja kustannustehokkuuden.

Osa koulutuksesta tulee toteuttaa siten, että julkisen hallinnon henkilöstön osalta tulee asettaa koulutuksien ja niihin liittyvien testien suorittaminen pakolliseksi, esimerkiksi osaksi palveluissa edellytettävien käyttöoikeuksien saamista.

Perinteisten koulutusten rinnalle tulee luoda uudenlaisia malleja osaamisen ja uhkatietoisuuden parantamiseksi hyödyntäen esimerkiksi pelillistämisen tarjoamia mahdollisuuksia.

2.4.3 Uuden teknologian tehokas hyödyntäminen palveluiden ja digiturvallisuuden toteuttamisessa

Valtiovarainministeriön keräämä kokonaiskuva osoittaa ja ennustaa, että tulemme jatkossa kokemaan yhä useammin erilaisia ICT-palvelutuotantoon, tieto- ja kyberturvallisuuteen sekä tietosuojaan liittyviä poikkeamia ja häiriöitä. Suomi etenee julkisen hallinnon digitalisoinnoin osalta globaalisti kärkijoukoissa, jolloin myös edelläkävijät joutuvat kokemaan ensimmäisten joukossa siihen liittyviä uhkia. Täten uuden teknologian käyttöönotto on uhka, mutta ennen kaikkea valtava mahdollisuus, jossa Suomi on toistaiseksi menestynyt loistavasti.

Julkiselle hallinnolle tuotettavien palveluiden yhteyteen tulee kasvattaa nykyistä tehokkaampaa havainnointikykyä ja sen mukaista reagointia meidän toimintaa uhkaavien riskien osalta. Uhkakuvien kasvaessa mahdollisesti tulevaisuudessa eksponentiaalisesti, tämä edellyttää sekä keinoälypohjaisen ja sen tuottaman tiedon asiantuntijavoimin tapahtuvan analysointikyvyn kehittämistä. Kuten useissa muissa tässä kehittämisohjelmassa esille nostetuissa kohteissa, tätä tulisi keskittää toiminnan laadun, tiedonvälityksen, yhteistyön sekä kustannustehokkuuden varmistamiseksi.

Kaikista tässä kehittämisohjelmassa esitettävistä toimenpiteistä huolimatta tulemme kokemaan jatkossa yhä enemmän toimintaamme kohdistuvia uhkia. Tämä johtuu siitä, että tietoverkko- ja kyberrikollisuus tulee entisestään laajentumaan ja globalisoitumaan.

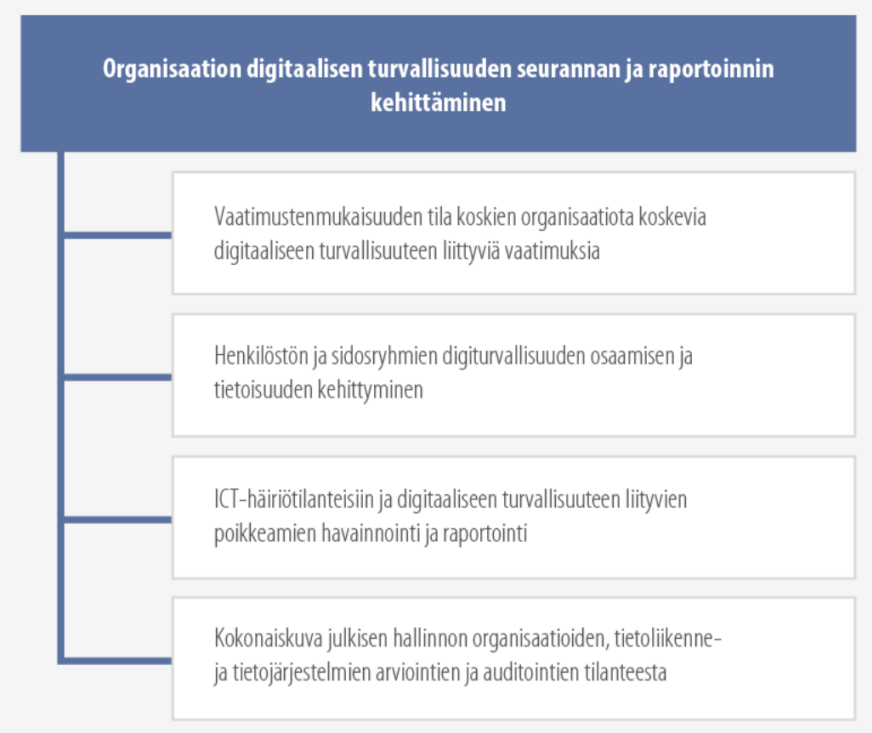
Eräs syy tähän on se, että internet-verkko ja digitaaliset palvelut eivät ole vielä kaikkialla maailmassa läheskään samalla tasolla kuin pitempään näitä hyödyntäneissä, teknologiaan ja uusiin palveluihin panostaneissa valtioissa. Tällöin nämä nopeasti kehittyvät markkinat houkuttelevat rikollisia entisestään kehittämään keinoja taloudellisen edun saavuttamiseksi uusien käyttäjien ja digitaalisten palveluiden avulla. Tästä kehityksestä myös Suomi saa osansa, vaikka emme välttämättä ole tällaisen toiminnan aktiivinen kohde, mutta globaalin tietoverkko- ja kyberrikollisuuden kehittyminen heijastuu myös tällä tavalla Suomalaiseen yhteiskuntaan. Se, että Suomi on maailman johtavia maita uuden teknologian käyttöönottamisessa, altistaa meidät myös ensimmäisten joukossa siihen kohdistuville uhille. Me emme voi vaikuttaa suoraan siihen, kuinka paljon meitä vastaan hyökätään, mutta me voimme vaikuttaa tällaisten hyökkäysten havaitsemiseen sekä reagointikykyyn ja sitä kautta toiminnan palauttamiseen sen kriittisyydelle määritettyjen vaatimusten mukaisesti.

Edellä kuvatun toiminnan ohella toinen, ei tietoisesti meitä vastaan kohdistuva uhka liittyy ICT-palveluiden ja niiden tuottamiseen liittyviin häiriöihin. Uuden teknologian

käyttöönotto tulee tapahtumaan kiihtyvällä vauhdilla, joka aiheuttaa haasteita sen luotettavan ja turvallisen toiminnan testaamiseen. Julkisen hallinnon ICT-palveluiden keskittäminen kasvattaa laajavaikutteisten häiriöiden mahdollisuutta, aikaisemmin organisaation itse tuottaman palvelun häiriön vain organisaatiokohtainen vaikutus tulee laajentumaan jopa koko yhteiskunnan tasolle keskitetyn palvelutuotannon häiriintyessä. Tällöin myös häiriötilanteiden hallinnassa tulee hyödyntää uutta teknologiaa, esimerkiksi automatisaatiota ja keinoälyä.

Tässä kehittämisohjelman kolmannessa osa-alueessa kehitetään organisaation omia digitaalista turvallisuutta kehittäviä toimintoja seurannan ja raportoinnin näkökulmasta. Kun organisaatio pystyy paremmin tunnistamaan sen oman digitaalisen turvallisuuden toiminnan tason, sen avulla organisaatio pystyy myös paremmin kehittämään omaa turvallisuutta muodostettavan kokonaiskuvan avulla. Vastaavasti valtiovarainministeriö pystyy tämän avulla muodostamaan koko julkisen hallinnon digitaalisen turvallisuuden kokonaiskuvan ja sen avulla vaikuttamaan esimerkiksi tunnistettujen erityistä tukea tai toimenpiteitä tarvitsevien osa-alueiden kehittämiseen.

Keskeisiä, toimenpideohjelmassa kehitettäviä osa-alueita ovat esimerkiksi:



Kuva 9. Digiturvallisuudessa tulee huolehtia laajasti turvallisuuden eri osa-alueiden kehittämisestä. Jokaisen organisaation tulisi entistä paremmin pystyä havainnoimaan, seuraamaan ja mittamaan oman organisaation digitaalisen turvallisuuden tilannetta.

2.5 Kokonaisarkkitehtuurin kehittämisellä mahdollistetaan turvallinen digitalisaation edistäminen

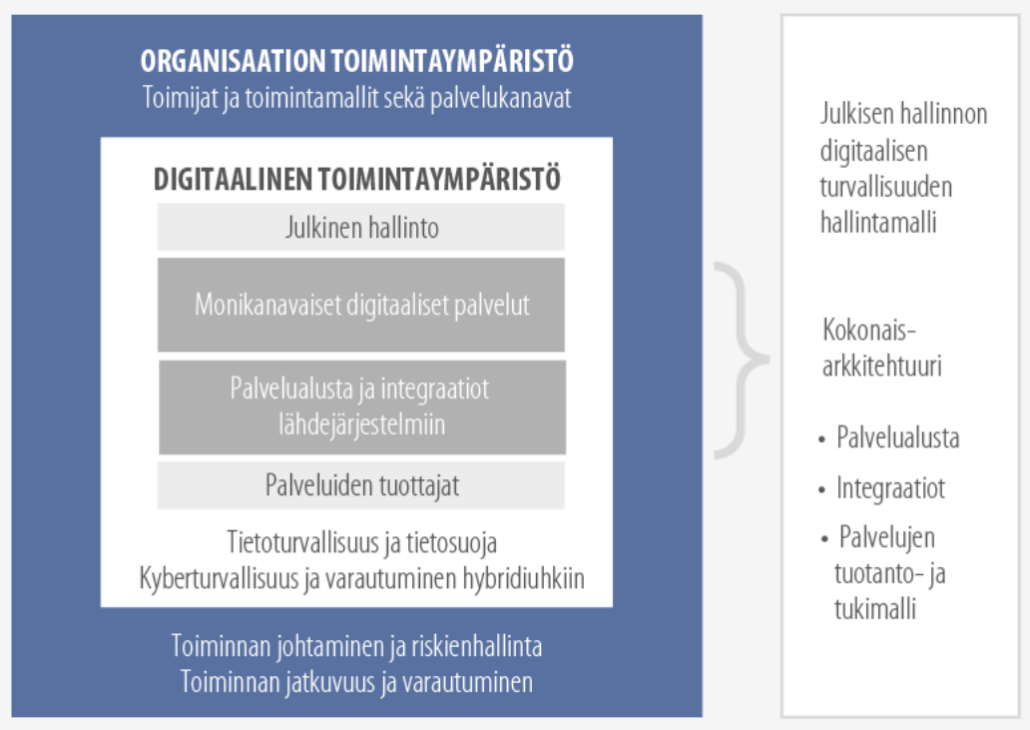
Yhteiskunnassa tapahtuva toimintatapojen muutos digitalisoimalla julkisen hallinnon palveluita edellyttää uudella tavalla digiturvallisuuden johtamista ja toteuttamista. Tällä myös mahdollistetaan, että julkisen hallinnon toimintatavat ja digitaaliset palvelut ovat tehokkaita sekä yhteensopivia vastaten asiakkaiden tarpeisiin.

Kuva 10. Kuvassa keskeisiä julkisten palveluiden digitalisoimisessa huomioitavia osa-alueita, jotka yhdessä ovat osa digitalisaation hallintamallia.

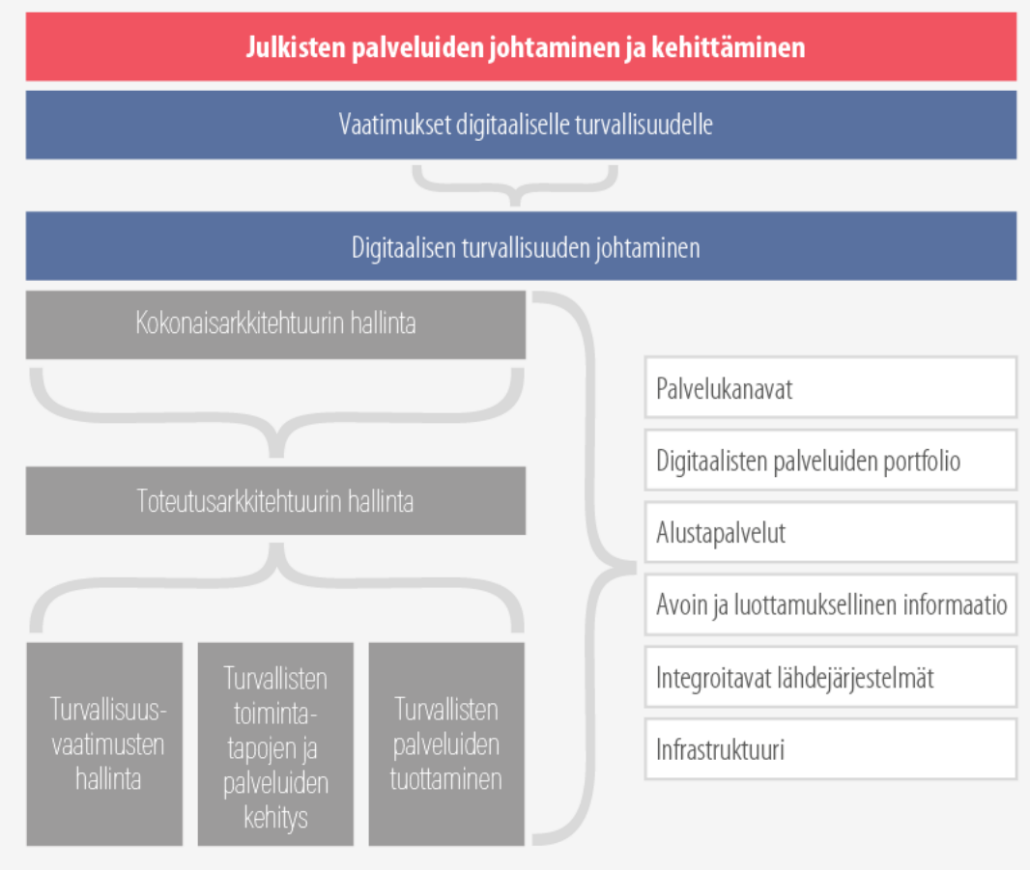
Tässä keskeinen rooli on kokonaisarkkitehtuurilla, joka mahdollistaa uusien työtapojen kytkeytymisen niitä tukeviin digitaalisiin palveluihin. Digitaalisten palveluiden kehittäminen edellyttää puolestaan modernia palveluympäristöä, joka hyödyntää yhteiskäyttöisiä tietoja turvallisesti sekä liittää järjestelmät ja infrastruktuurit hallituiksi kokonaisuuksiksi.

Julkisten palveluiden turvallinen digitalisaatio on henkisten ja taloudellisten resurssien, toimintatapojen sekä -rakenteiden muutosta. Turvallinen digitalisaatio parantaa toimintaa ja luo mahdollisuuksia esimerkiksi erilaisille ekosysteemeille.

Tiedon jakaminen ja yhteiskäyttö ovat toimivan moniviranomaisyhteistyön perusedellytys. Digitaalisen turvallisuuden kehittäminen tapahtuu aseittain osana nykyisten toimintatapojen ja palveluisen kehittämistä sekä uutena kehittämistyönä.



Kuva 11. Organisaation toimintaympäristön ja digitaalisen toimintaympäristön kehittämisessä tarvittavat rajapinnat sekä sovittaminen kokonaisarkkitehtuuriin ja tiettyihin digiturvallisuuden osa-alueisiin.

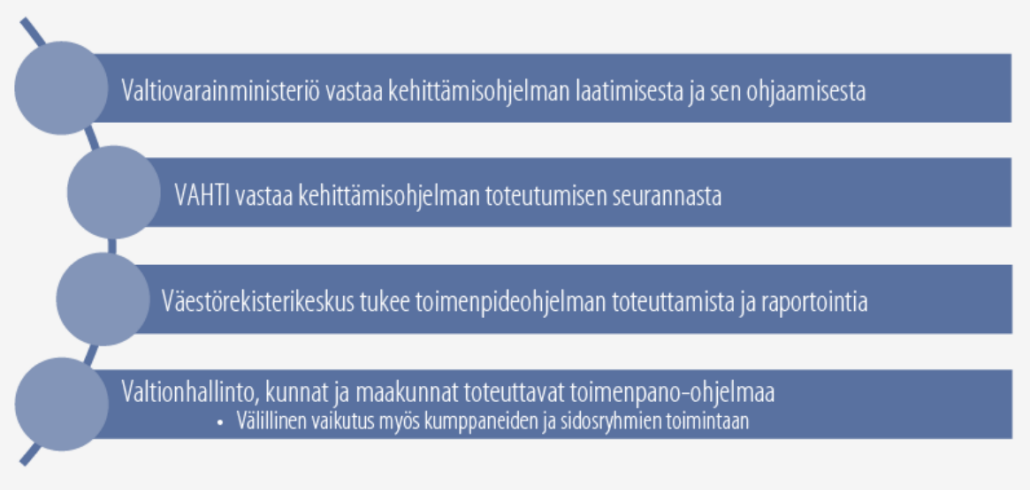


Kuva 12. Digiturvallisuuden kehittämisessä, erityisesti organisaatioiden välisen luottamuksen, tietojenvälittämisen ja yhteensopivuuden mahdollistamiseksi tarvitaan yhä enemmän yhteistyötä, jossa pitää hyödyntää enemmän KA-arkkitehtuurimalleja.

2.6 Kehittämisohjelman osapuolten vastuut

Kehittämisohjelman laatimisesta on vastannut valtiovarainministeriö ja se vastaa myös toimeenpano-ohjelman ohjaamisesta. Kehittämisohjelman ja toimeenpano-ohjelman toteutumisen seurannasta vastaa julkisen hallinnon digitaalisen turvallisuuden johtoryhmä. Väestörekisterikeskuksen vastuulla on kehittämisohjelman toimenpide-ohjelman toimenpiteiden tarjoaminen julkiselle hallinnolle ja raportointi toimenpiteiden etenemisestä valtiovarainministeriölle sekä VAHTIlle.

Valtionhallinto, kunnat ja maakunnat osallistuvat toimenpide-ohjelman toteuttamiseen kehittämisohjelmalle asetettujen tavoitteiden saavuttamiseksi.



Kuva 13. Kehittämisohjelman ja toimenpide-ohjelman vastuut.

2.7 Julkisen hallinnon digitaalisen turvallisuuden toimenpideohjelma

Tämän kehittämisohjelman tueksi on laadittu toimenpide-ohjelma vuosille 2018-2021. Valtaosa tässä kehittämisohjelmassa esille nostetuista tehtävistä ovat sellaisia, joita organisaation tulisi kehittää normaalisti osana turvallisuuden ylläpitoa ja kehittämistä. Toimeenpano-ohjelmalla halutaan priorisoida, osin keskittää ja yhteensovittaa kehittämistä koko julkisen hallinnon näkökulmasta.

Jokaiseen kehittämisohjelman keskeiseen kohtaan on luotu useampi toimenpide, joiden avulla kyseistä osa-aluetta voidaan kehittää sille asetettujen tavoitteiden saavuttamiseksi. Näistä toimenpiteistä on luotu kehittämisohjelman toimenpide-ohjelma. Sen ohjauksesta vastaa valtiovarainministeriö ja sen toteuttamisesta ja raportoinnista Väestörekisterikeskus. Toimeenpano-ohjelma kohdistetaan julkisen hallinnon organisaatioihin.

Kehittämistoimenpiteiden määrän sijaan priorisoidaan niiden laatua tunnistamalla sellaisia toimenpiteitä, joiden avulla voidaan laaja-alaisesti kehittää koko julkisen hallinnon digitaalista turvallisuutta kehittämisohjelman painotusten perusteella

Jokaiselle toimenpiteelle on

- luotu selkeä tavoite
-asetettu sen toimeenpanon toteuttamisesta vastaava organisaatio
-budjetti sen toteuttamiseksi
-vuosittaiset seurantamittarit
-seuranta ja raportointi toimenpiteiden etenemisestä

Toimeenpano-ohjelma kytketään tulevan tiedonhallintalain toimeenpanoon.

Toimenpideohjelma on erikseen julkaistava Liite 1. Tämä mahdollistaa myös sen, että toimenpideohjelmaan voidaan tuoda uusia toimenpiteitä kehittämisohjelman kuluessa osana valtiovarainministeriön vuosittaista kehittämisohjelman etenemisen tarkastelua.

3 Kehittämisohjelman odotettu vaikuttavuus ja mittarit

Valtiovarainministeriö tulee seuraamaan ja arvioimaan kehittämisohjelman vaikuttavuutta erilaisten mittareiden avulla. Jokaiselle toimenpiteelle luodaan omat mittarit, mutta myös kokonaisuutta seurataan omien mittareiden avulla.

3.1 Digitaalisen turvallisuuden johtamisen ja riskienhallinnan kehittäminen

Digitaalisia palveluita ja toimintaa johtaessa yhteensovitetaan organisaation tarpeita, sidosryhmien odotuksia ja erilaisia vaatimuksia. Kehittämisohjelma pyrkii parantamaan organisaatioiden kykyä johtaa digiturvallisuutta nykyaikaisin menetelmin sekä soveltaa riskienhallinnan menettelyjä johtamisessa.

Riskienhallinnan avulla organisaatio varmistaa sen tavoitteiden saavuttamiseksi lisäksi erilaisten vaatimusten ja sitoumusten toteuttamisen sekä sen toiminnan jatkuvuuden. Jatkossa riskienhallinta on yhä keskeisempi osa esimerkiksi tietosuojaa ja rekisteröityjen oikeuksien varmistamista.

Riskienhallinta on organisaation yksi keskeinen johtamisen työkalu ja se tulisi nähdä keskeisenä organisaation johtamisjärjestelmän osana. Riskienhallinnan avulla turvallisuustoimet voidaan mitoittaa organisaation riskinottohalukkuuden ja sille asetettujen velvoitteiden mukaisesti.

Tavoite (vaikuttavuus)	Mittari
Tiedonhallintalain avulla voidaan kehittää koko julkisen hallinnon digiturvallisuutta	Suoritetaan lähtötason mittaus ennen lainsäädännön voimaan astumista sekä säännöllisesti vuosittain sen astuttua voimaan.
Organisaatiossa on toimiva tiedonhallintalain vaatimuksia toteuttava digiturvallisuuden hallintamalli	Mittaaminen viedään osaksi uutta kokonaiskuvapalvelua
Riskienhallinta on osa organisaatioiden johtamisjärjestelmää	Mittaaminen viedään osaksi uutta kokonaiskuvapalvelua
Ohjelman puitteissa kehitetyt mallit tukevat organisaatioiden digitaalisten palveluiden kehittämistä	Mittaaminen viedään osaksi uutta kokonaiskuvapalvelua

3.2 Osaamisen kehittyminen

Julkisen hallinnon digitaalisten palveluiden turvallisuus ja luotettavuus perustuvat henkilöstön osaamiseen ja oikeanlaisen turvallisuuskulttuurin ja asenteen kehittymiseen.

Henkilöstön rooli turvallisuuden toteuttamisessa on keskiössä. Eri tutkimusten perusteella on arvioitu, että noin 95 prosenttia kyberturvallisuuspoikkeamista väitetään olevan sellaisia, jotka on mahdollistanut jonkinlainen – tarkoituksellinen tai tahaton – inhimillinen virhe[3].

Tavoite (vaikuttavuus)	Mittari
Digiturvallisuuden koulutuksen määrän ja tietoisuuden kehittyminen organisaatioissa	Koulutusten lukumäärä/organisaatio vuosittain Mittaaminen viedään osaksi uutta kokonaiskuvapalvelua
Henkilöstön digiturvallisuuteen liittyvän osaamisen parantuminen	Vastaajien oma arvio (toteutetaan kyselynä) Organisaatioiden arvio Mittaaminen viedään osaksi uutta kokonaiskuvapalvelua
Henkilöstön ja johdon asenteen ja toimintakulttuurin kehittyminen organisaatiossa	Vastaajien oma arvio (toteutetaan kyselynä) Organisaatioiden arvio Mittaaminen viedään osaksi uutta kokonaiskuvapalvelua

3.3 Uuden teknologian tehokas hyödyntäminen palveluiden ja digiturvallisuuden toteuttamisessa

Uusia digitaalisia palveluita kehitettäessä tulee huomioida tarpeet toimintatapojen muutoksille. Uudet teknologiat luovat mahdollisuuksia toteutuksille, mutta samalla niiden riskit tulee ottaa huomioon. Teknologia sellaisenaan ei kehitä merkittävästi toimintaa vaan palvelut tulee tarkastella kokonaisuutena. Palvelut toimivat ja vaikuttavat yhä

[3] http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:52017JC0450&from=EN

useammin samanaikaisesti sekä vapaa-ajan ja yksityiselämän kuin myös työelämän ja työtehtävien hoitamiseen.

Tavoite (vaikuttavuus)	Mittari
Julkisen hallinnon ICT-häiriöiden ja digiturvallisuuden poikkeamista saadaan tuotettua ajantasainen kokonaiskuva	Mittaaminen viedään osaksi uutta, luotavaa kokonaiskuvapalvelua, joka mahdollistaa myös muiden kehittämisohjelman toimenpiteiden seurannan
ICT-häiriöiden ja digiturvallisuuden poikkeamien määrä ei kasva nopeammin kuin palveluiden ja toiminnan digitalisointi keskimäärin	Mittaaminen viedään osaksi uutta kokonaiskuvapalvelua, mittarin avulla voidaan seurata ICT-häiriöiden ja digiturvallisuuden kehittymistä julkisessa hallinnossa
Häiriötilanteiden hallinnan kehittyminen digitaalisissa palveluissa	Organisaatioiden arvio Mittaaminen viedään osaksi uutta kokonaiskuvapalvelua

Liite 1. Julkisen hallinnon digitaalisen turvallisuuden toimenpideohjelma vuosille 2018-2021

Tässä luvussa on kuvattu 5 toimenpidettä, joiden avulla kehittämisohjelman kolmea painoaluetta edistetään. Jokaisesta toimenpiteestä tuotetaan yksityiskohtainen projektisuunnitelma.

Toimenpide 1 Digitaalisen turvallisuuden johtamisen ja riskienhallinnan kehittäminen

Kohderyhmä:	Organisaation johto sekä ICT- ja tietoturvallisuudesta sekä tietosuojasta vastaavat asiantuntijat, arkkitehdit. Organisaation ylimmän johdon vastuuhenkilö sekä muut asiantuntijat osallistuvat koulutuksiin ja yhteishankkeeseen.
Tavoite:	Kehittämishankkeen avulla organisaatio saa varmistettua, että sillä on tarvittava osaaminen digitaalisen turvallisuuden johtamiseksi, kehittämiseksi ja hallitsemiseksi muuttuvassa toimintaympäristössä. Tässä hyödynnetään tätä varten luotua digiturvariskien hallintamallia. Yhteishankkeessa jalkautetaan luotu JHKA 2.0- pohjainen arkkitehtuurin kuvausmalli.
Aikataulu:	xx/201x – 12/2021
Toteutusvastuu:	VRK rakentaa ohjelman yhdessä käyttäen VAHTI-asiantuntijajaostoa sekä VAHTI-toiminnassa olevien organisaatioiden asiantuntemusta hyödyntäen
Mittari:	Osallistuvien organisaatioiden määrä Osallistuneiden henkilöiden määrä Asiakastyytyväisyys Mittarit digiturvallisuuden johtamisen toteutumisen osalta ennen ja jälkeen yhteishankkeen Mittarit digiturvariskien hallinnan toteutumisen osalta ennen ja jälkeen yhteishankkeen
Muuta:	Osana koulutusta toteutetaan myös riskienhallinnan kehittämiseen liittyvät toimenpiteet ja osaamisen kehittäminen, jota esimerkiksi tiedonhallintalaki tulee edellyttämään.

Toimenpide 2 Digitaalisen turvallisuuden vaatimus- ja arviointikehikon toteuttaminen

Kohderyhmä: ICT- ja turvallisuuden vastuuhenkilöt

Tavoite:

Valtionhallinnossa voimassa olevat tietoturvallisuutta koskevat ohjeet pohjautuvat vuonna 2010 voimaan astuneeseen tietoturvallisuusasetukseen. Nyt tämä malli korvataan uudella digitaalisen turvallisuuden vaatimus- ja arviointikehikolla, joka samalla tukee ja toimii sekä tiedonhallinta-lain toimeenpanoa edistävänä hankkeena, että kehittää julkisen hallinnon digitaalisen turvallisuuden johtamista ja käytännön tason toteuttamista.

Hankkeessa toteutetaan uusi lainsäädäntöä tukeva digitaalisen turvallisuuden vaatimuskehikko, joka sisältää valtiovarainministeriön asettamat vaatimukset tiedonhallintalain toteuttamiseksi sekä tarvittavat arviointikriteerit eri osa-alueiden (organisaatio, ICT-palvelukokonaisuus, hankinnat) vaatimustenmukaisuuden arvioimiseksi. Arviointi, kuten vaatimukset voivat kohdistua esimerkiksi organisaatioon, tietoliikenne- tai tietojärjestelmään, hankintaan. Samassa yhteydessä luodaan prosessit vaatimustenmukaisuuden raportoimiseksi osaksi organisaation digitaalisen turvallisuuden kokonaiskuvan toteuttamista. Tällä korvataan aikaisemmin erikseen toteutetut VAHTI-organisaatiokyselyt.

Aikataulu: xx/201x – 12/2021

Toteutusvastuu: VRK rakentaa vaatimus- ja arviointikehikon yhdessä keskeisten yhteistyötahojen kanssa ja pilotoi sitä eri kokoisten kohderyhmien kanssa ennen sen toteuttamista.

Mittari: Hallintajärjestelmän käyttöönottaneiden organisaatioiden määrä
Asiakastyytyväisyys

Muuta:

Näiden jalkauttaminen toteutetaan yhteishankkeiden avulla. Yhteishankkeet pohjautuvat niitä varten luotuun käsikirjaan, jonka avulla organisaatio saa käyttöönsä digiturvallisuuden hallintajärjestelmämallin. Hallintajärjestelmästä luodaan kaksi mallia, vähimmäistason malli, joka on tarkoitettu ja soveltuu pienemmille organisaatioille sekä kehittyneempi malli, joka on tarkoitettu sellaisille organisaatioille, joiden turvallisuuden hallinta edellyttää kehittyneempää hallintamallia.

Toimenpide 3 Julkisen hallinnon digitaalisen turvallisuuden koulutusjärjestelmä sekä digiturvasovellus

Kohderyhmä:	Kolme eri kohderyhmää; julkisen hallinnon henkilöstö, ICT-, tietoturva ja tietosuojahenkilöstö sekä johto ja esimiehet, osa kehitettävistä palveluista voidaan mahdollisesti tuotteistaa tarjottavaksi myös kansalaisille.
Tavoite:	Julkisen hallinnon organisaatioiden käytössä on keskitetty digitaalisen turvallisuuden koulutusjärjestelmä. Organisaation henkilöstö osallistuu sille tarkoitettuihin velvoittaviin koulutuksiin ja ajankohtaiskatsauksiin. Koulutusten läpikäynti ja osallistuminen ajankohtaiskatsauksiin on edellytys käyttöoikeuksien saamiselle ja säilyttämiselle organisaatiossa.
Aikataulu:	xx/201x – 12/2021
Toteutusvastuu:	VRK toteuttaa koulutusjärjestelmän yhdessä eOppivan ja Valtorin kanssa varmistaen, että palvelu on käytettävissä koko julkisessa hallinnossa. Digiturvasovellus toteutetaan käyttäen VRK:n käytössä olevia sovelluskehitystoimittajia.
Mittari:	Osallistuvien organisaatioiden määrä Osallistuneiden henkilöiden määrä Koulutusten läpäisyprosentti Digiturvasovelluksen latausmäärä ja käytön yleistyminen Asiakastyytyväisyys
Muuta:	Organisaatio voi saada vastaavat materiaalit käyttöön omaan koulutusjärjestelmään. Osaksi kokonaisuutta toteutetaan myös digitaalisen turvallisuuden työkalupakki, joka sisältää materiaalipankin sekä muita sellaisia työkaluja, ohjeita ja materiaaleja, joita organisaatio voi hyödyntää oman toiminnan kehittämisessä. Materiaalipankin materiaalit julkaistaan avoimena datana.

Toimenpide 4 Julkisen hallinnon digitaalisen turvallisuuden kokonaiskuvan raportoinnin kehittäminen

Kohderyhmä: Julkisen hallinnon organisaatiot, niiden tietohallinto ja turvallisuuden vastuuhenkilöt, henkilöstö ja johto

Tavoite: Hankkeen avulla digitalisoidaan ja uudistetaan nykyaikaisen digiturvallisuuden kehittämisessä tarvittavien mittareiden kerääminen ja julkaiseminen. Hankkeen avulla siirrytään perinteisestä, kertaluonteisesti vuosittain toteutetuista kyselyistä ja raportoinneista ajantasaisesti tehtäviin sähköistä palvelua käyttävään raportointialustaan.

Aikataulu: xx/201x – 12/2021

Toteutusvastuu: VRK toteuttaa palvelun suunnittelun ja toteuttamisen.

Mittari: Kokonaiskuvaan kuuluvien mittareiden lukumäärä
Palvelun käyttöönottaneiden organisaatioiden lukumäärä
Asiakastyytyväisyys

Muuta:

Tämän hankkeen tarkoituksena on digitalisoida nämä edellä olevat yksittäiset kyselyt ja toimin-not yhtenäiseksi, ajantasaiseksi palveluksi, jonka avulla julkisen hallinnon organisaatioista saadaan selville:

- organisaation ja tietojärjestelmien vaatimustenmukaisuuden tila verrattuna uusiin, tiedonhallintalain edellyttämiin vaatimuksiin (vaatimustenmukaisuuden tila)
- henkilöstön ja johdon asenne ja toimintakulttuurin tila ei kertaluonteisesti vaan siten, että henkilöstö voi vastata tähän periaatteessa jatkuvasti sen hetkisen tilanteen ja tunteen mukaisesti
- ICT- ja digitaalisen turvallisuuden osa-alueisiin liittyvät häiriöt ja poikkeamat sitä mukaa kun organisaatiossa niitä tapahtuu
- toteutetut tietoturva-arvioinnit ja auditoinnit metatietojen osalta
- itse toteutetut ja osallistuminen digitaalisen turvallisuuden harjoituksiin (osa tieto- ja kyberturvallisuusharjoitussuunnitelman seurantaa)

Toimenpide 5 Digitaalisen turvallisuuden harjoitussuunnitelma ja sen perusteella laadittava harjoitusohjelma vuosille 2018-2021

Kohderyhmä:	Julkisen hallinnon organisaatiot ja niiden alihankkijat ja mahdolliset sidosryhmät
Tavoite:	Valtiovarainministeriö vastaa julkisen hallinnon digitaalisen turvallisuuden harjoitussuunnitelman toteuttamisesta, jonka laatimisesta ja operatiivisesta toteuttamisesta vastaa Väestörekisterikeskus. Harjoitussuunnitelman avulla kuvataan julkisen hallinnon tarve sekä käytettävät menetelmät koskien digitaalista turvallisuutta edistävää harjoitustoimintaa. Tämän perusteella laaditaan vuositasolle tarkoitettu harjoitusohjelma, jossa kuvataan tarkemmin lähivuosien aikana toteutettavaksi tarkoitetut keskeiset harjoitukset sekä ylläpidetään tähän liittyvää harjoituskalenteria. Harjoitusohjelmaa aletaan toteuttaa vuonna 2019, jonka perusteella julkisen hallinnon organisaatiot voivat osallistua suunniteltaviin harjoituksiin. Harjoitusten avulla varmistetaan vuosittain harjoituksille asetettujen tavoitteiden saavuttaminen, pääosin kyvykkyys selviytyä erilaisista organisaation digitaaliseen toimintaympäristöön liittyvistä häiriöistä ja loukkauksista.
Aikataulu:	xx/201x – 12/2021
Toteutusvastuu:	VRK toteuttaa harjoitusmallin yhteistyössä keskeisten sidosryhmien, esimerkiksi Huoltovarmuuskeskuksen, Puolustusvoimien, tietosuojavaltuutetun toimiston, Turvallisuuskomitean ja Viestintäviraston Kyberturvallisuuskeskuksen kanssa.
Mittari:	Harjoituksiin osallistuneiden organisaatioiden määrä Muiden valtiovarainministeriön keräämien mittareiden tulokset Asiakastyytyväisyys
Muuta:	-

Liite 2 Lähteet

OECD - Digitaaliseen turvallisuuteen kohdistuvien riskien hallinta taloudellisen ja yhteiskunnallisen hyvinvoinnin edistämiseksi

Linkki:
http://julkaisut.valtioneuvosto.fi/handle/10024/75412

Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä (7/2009)

Linkki:
https://vm.fi/documents/10623/307681/VAHTI+periaatep%C3%A4%C3%A4t%C3%B6s+2009/24355a33-4042-42fb-9dba-981e6398ee7a/VAHTI+periaatep%C3%A4%C3%A4t%C3%B6s+2009.pdf

Luonnos hallituksen esitykseksi eduskunnalle laiksi julkisen hallinnon tiedonhallinnasta sekä eräiksi siihen liittyviksi laeiksi

Linkki:
https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=3010f613-2ede-40c1-a59f-e75c23cddbb5

Valtiovarainministeriön julkisen hallinnon digitaalisen turvallisuuden kokonaiskuva – ST IV

Euroopan Unionin yhteinen tiedonanto Euroopan parlamentille ja neuvostolle - Resilienssi, pelote ja puolustus: vahvan kyberturvallisuuden rakentaminen EU:lle

Linkki:
https://publications.europa.eu/fi/publication-detail/-/publication/15499d93-794f-11e3-b889-01aa75ed71a1/language-fi

Tuleva EU-kyberturvallisuussääntely
Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication

Linkki:
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017PC0477

Suomen Kyberturvallisuusstrategia sekä toimeenpano-ohjelma vuosille 2017 – 2020

Linkki:
https://www.turvallisuuskomitea.fi/index.php/fi/mcdc/14-suomen-kyberturvallisuusstrategia

https://www.turvallisuuskomitea.fi/index.php/fi/component/k2/126-suomen-kyberturvallisuusstrategian-toimeenpano-ohjelma-2017-2020

Valtiontalouden tarkastusviraston tarkastuskertomus - Kybersuojauksen järjestäminen

Linkki:
https://www.vtv.fi/files/5862/16_2017_Kybersuojauksen_jarjestaminen.pdf

Valtioneuvoston selvitys- ja tutkimustoiminta - Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi

Linkki:
http://tietokayttoon.fi/hankkeet/hanke-esittely/-/asset_publisher/suomen-kyberturvallisuuden-nykytila-tavoitetila-ja-tarvittavat-toimenpiteet-tavoitetilan-saavuttamiseksi

Valtioneuvoston selvitys- ja tutkimustoiminta - Kyberturvallisuuden strateginen johtaminen Suomessa

Linkki:
http://tietokayttoon.fi/hankkeet/hanke-esittely/-/asset_publisher/kyberturvallisuuden-strateginen-johtaminen-suomessa

EU:n yleinen tietosuoja-asetus

Linkki:
http://eur-lex.europa.eu/legal-content/FI/TXT/?uri=OJ%3AL%3A2016%3A119%3ATOC

YTS 2017

Linkki:
https://www.turvallisuuskomitea.fi/index.php/fi/yhteiskunnan-turvallisuusstrategia-yts

Valtiontalouden tarkastusviraston tarkastuskertomus - Sähköisten palvelujen toimintavarmuuden ohjaus

Linkki:

https://www.vtv.fi/files/5863/15_2017_Sahkoisten_palvelujen_toimintavarmuuden_ohjaus.pdf

Valtioneuvoston periaatepäätös huoltovarmuuden periaatteista (luonnos, 2018) https://api.hankeikkuna.fi/asiakirjat/76b0aa83-9729-4df1-84a7-60ba6a1bbfdf/855b8073-5c37-4f5b-9628-6934edd01566/KIRJE_20180620091000.PDF