VALTIOVARAINMINISTERIÖ

Julkishallinnon digitaalisen turvallisuuden arkkitehtuuri

Haukka-hanke

11.6.2021

Sisällys

TIIVISTELMÄ

Raportissa kuvataan julkisen hallinnon digitaalisen turvallisuuden arkkitehtuurin nykytila-arvio ja ehdotuksia sen kehittämiseksi. Raportin viitekehyksenä on valtioneuvoston periaatepäätös julkisen hallinnon digitaalisesta turvallisuudesta (VM 2020:23) ja sen toimeenpanosuunnitelma (VM 2020:33) (Haukka). Raportti perustuu selvityksiin, jotka on toteutettu osana Haukka-hankkeen toimenpidettä julkisen hallinnon digitaalisen infrastruktuurin suojaaminen.

Selvitystyö toteutettiin kahdessa eri typpisessä ohjattujen työpajojen sarjassa. Ensimmäisessä työpajasarjassa selvitettiin julkishallinnon digiturvallisuuden nykytilaa kypsyysarvioinnin avulla. Kypsyysarviointi toteutettiin käyttäen Yhdysvaltain energiaviraston kehittämää C2M2-mallia. Arviointi toteutettiin 25 organisaatiossa, joihin kuului ministeriöitä, niiden alaisia virastoja ja laitoksia, sekä kaupunkeja ja kuntia. Toisessa työpajasarjassa selvitettiin valtionhallinnon näkemyksiä digitaalisen turvallisuuden arkkitehtuurin määritelmästä ja sisällöstä. Toisessa työpajasarjassa oli kahdeksan työpajaa, joihin osallistui ministeriöiden ja niiden alaisten virastojen ja laitosten asiantuntijoita. Tässä raportissa on kuvattu työpajojen menetelmät ja tulokset sekä tavoitetilan kuvaus suositeltavine toimenpiteineen.

Selvityksen perusteella sekä digitaalisen turvallisuuden kypsyyden arviointi, että digitaalisen turvallisuuden arkkitehtuurin käsite ja toteuttaminen ovat haasteellisia. Digitalisaation nopea kehittyminen, digitaalisen turvallisuuden ja digitaalisen turvallisuuden arkkitehtuurin määritelmien kirjo sekä asiantuntijoiden niukkuus vaikuttavat digitaalisen turvallisuuden tilasta muodostuvaan kokonaiskuvaan. Digitallisen turvallisuuden ja digitaalisen turvallisuuden arkkitehtuurin käsitteitä ehdotettiin selkiytettäviksi. Yhteisesti hyväksytyt määritelmät luovat perustan yhteisesti käsiteltävien asioiden kehittämiselle ja tuottamiselle. Tämä määrittelytyö ehdotetaan sisällytettäväksi Digi- ja väestötietovirastossa jo käynnistyneeseen digitaalisen turvallisuuden riskienhallinnan sanastotyöhön. Digitaalisen turvallisuuden arkkitehtuurin sisällön suunnittelun tueksi ehdotetaan käytettäväksi laajasti tunnettua kriittisen infrastruktuurin kyberturvallisuuden parantamiseen tähtäävää *NIST Cybersecurity Framework* –viitekehystä. Julkisen hallinnon digitaalisen turvallisuuden kypsyyden arviointia tulee toteuttaa jatkossa säännöllisesti. Keskeisenä tavoitteena on jatkuvuuden hallinnan turvaaminen sekä riskien ja uhkien tunnistamisen hallinta. Kaikkien kuntien tulisi saavuttaa vähintään digitaalisen turvallisuuden kypsyystaso kolme vuoden 2023 lopussa.

Raportti on kirjoitettu työryhmässä, jossa toimivat erityisasiantuntija Mika Tuikkanen, erityisasiantuntija Niko Mäkilä ja tietohallintoneuvos Tuija Kuusisto valtiovarainministeriöstä, sekä KPMG:n konsultteja.

1 JOHDANTO

1.1 Selvityksen tausta

Työn taustalla olevassa valtioneuvoston periaatepäätöksessä julkisen hallinnon digitaalisesta turvallisuudesta (valtiovarainministeriön julkaisuja 2020:23) määritetään kehittämisen periaatteet ja keskeiset palvelut turvallisuuden edistämiseksi digitaalisessa toimintaympäristössä. Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelmassa 2020-2023 (Haukka) (VM 2020:33) kuvataan periaatepäätöksen toteuttaminen. Haukka-toimeenpanosuunnitelmaan on valittu 19 tehtävää, joiden avulla kehitetään keskeisiä julkisen hallinnon digitaalisen turvallisuuden palveluita. Toimeenpanosuunnitelmalla tuetaan myös kyberturvallisuusstrategian 2019 kehittämisohjelman valmistelua ja toteuttamista, sekä edistetään valtioneuvoston päätöstä huoltovarmuuden tavoitteista (1048/2018).

Tämä selvitys toteuttaa Haukka-hankkeen tehtävää julkisen hallinnon digitaalisen turvallisuuden arkkitehtuurin kehittämisestä. Selvitystyö aloitettiin lokakuussa 2020, jolloin päätettiin selvityksen tavoitteet ja menetelmät sen toteuttamiseksi. Työ jaettiin käytännössä kahden työpajasisällön selvitysmalliksi, joista toisessa keskityttiin selvittämään digiturvallisuus arkkitehtuurin käsitettä, viitekehystä ja strategista johtamista. Toisessa selvitettiin digiturvallisuuden kypsyyden nykytilaa julkishallinnossa. Työt tukevat toisiaan. Tehdyn selvityksen pohjalta voidaan myös täydentää Huoltovarmuusorganisaation tuottamaa selvitystä toimialojen kyberturvallisuuden kypsyydestä vuosina 2019-2020.

1.2 Selvityksen tavoite ja menetelmä

Digitaalisen turvallisuuden arkkitehtuurin kehittämiseksi selvitettiin sen nykytilaa ja mitä asioita julkisen hallinnon digitaalisen turvallisuuden arkkitehtuurissa tulisi ottaa huomioon. Lisäksi digitaalisen turvallisuuden käsitteen katsottiin tarvitsevan selkeyttämistä ja vahvistamista. Työn jatkon kannalta katsottiin tärkeäksi, että digitaalinen turvallisuus ja digitaalisen turvallisuuden arkkitehtuuri ymmärretään julkishallinnossa samalla tavalla.

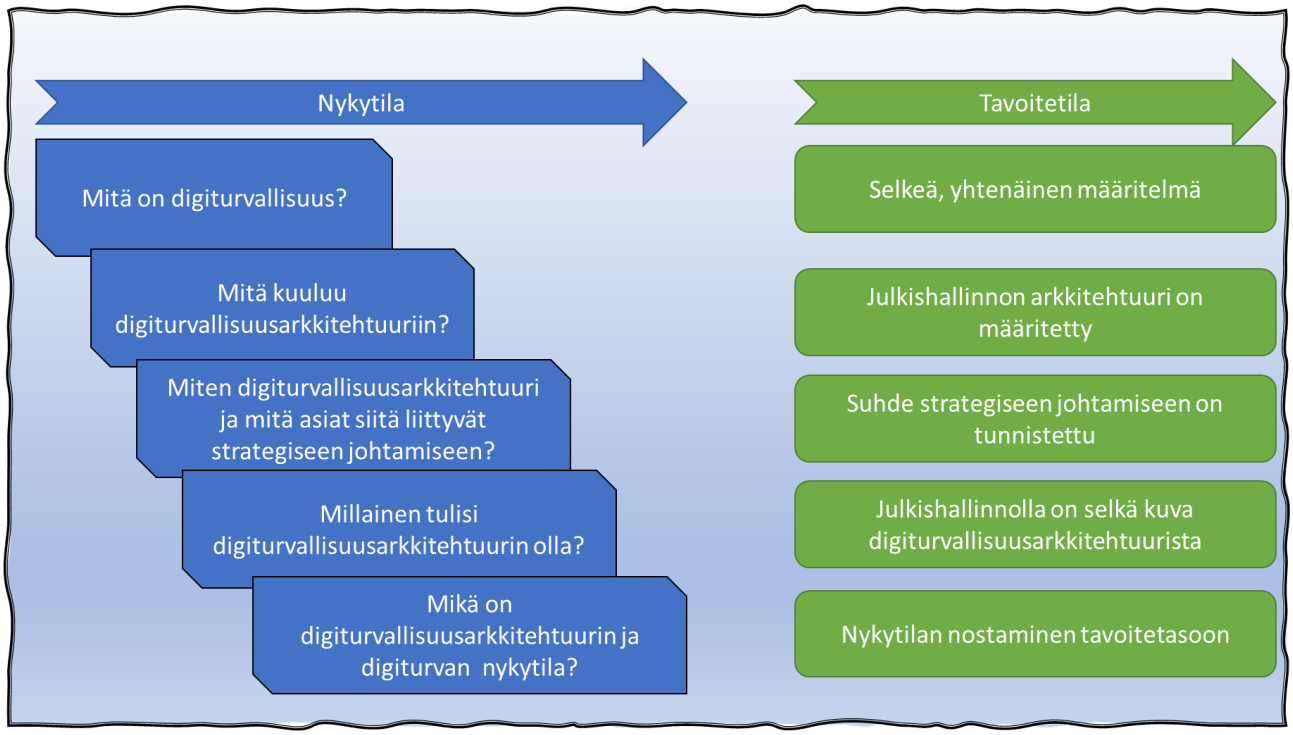
Nykytilan selvittäminen toteutettiin 11/2020 – 02/2021 välisenä aikana kahdella tavalla:

1. Digitaalisen turvallisuuden arkkitehtuurin ohjattuja työpajoja järjestettiin kahdeksan kappaletta. Työpajoihin osallistui eri ministeriöiden ja niiden alaisten virastojen edustajia.

2. Digitaalisen turvallisuustilanteen kypsyyden ohjattuja itsearviointityöpajoja järjestettiin 25 kappaletta. Työpajoihin osallistui organisaatioita sekä valtionhallinnosta että kuntasektorilta.

1.3 Rajaukset ja viitekehys

Tämä kartoitus sisältää analyysit työpajoista sekä suositukset jatkotoimista keskittyen digitaalisen turvallisuuden arkkitehtuurin viitekehyksen sisällä oleviin asioihin. Tämä viitekehys on esitetty alla olevassa kuvassa.



Kuva 1. Turvallisuusarkkitehtuurin viitekehys ja tämän selvityksen rajaus

Selvitystyön kannalta on keskeistä se, miten digiturvallisuus ymmärretään sekä luoda pohja digiturvaarkkitehtuurin yhteiselle ymmärtämiselle. Työn yhtenä tavoitteena nähtiin myös digitaalisen turvallisuuden arkkitehtuurin sisällön perusteiden etsiminen. Valtionhallinnon tavoitteena on luoda turvalliset keskitetyt palvelut eri virastoille, joten strategisen johtamisen osuus turvallisuudessa tai digiturvallisuudessa nähtiin tarpeelliseksi selvittää. Lopuksi koko digiturvallisuuden kypsyyden selvittämisellä nähtiin mahdolliseksi selvittää julkishallinnon tilannetta kypsyysarvioiden kautta.

Työn alkuvaiheessa asetettiin tehtäväksi kartoittaa, mitä valtiovarainministeriö, valtionhallinto, kuntasektori ja kukin organisaatio voisi tehdä mahdollisten esille nousevien kehityskohteiden hyväksi. Tavoitetilan sisältöä ja tasoa on kartoitettu työn perusteella ja tässä raportissa on esitetty joitain selvitystyön tuloksiin perustuvia suosituksia.

1.4 Määritelmät

Tämän työn keskeisin määritelmä on digitaalinen turvallisuus ja digitaalisen turvallisuuden arkkitehtuuri. Määritelmä on esitetty tarkemmin luvussa 2.1

Digiturvallisuuden määritelmää pidetiin työpajoissa uutena eikä se ollut monillekaan tuttu. Digitalisaatiosta on puhuttu jo useita vuosia ja digiturvallisuuden määrittelyyn on työpajoissa käytyjen keskusteluiden pohjalta tullut tarve, koska paremmin tunnetut termit, kuten tietoturvallisuus tai kyberturvallisuus eivät kata esim. taloudellisia tai sosiologisia asioita tai kuvaa eri osa-alueiden välisiä suhteita. Digiturvallisuus voidaan näin ymmärtää edellä mainittuja laajempana kokonaisuutena. Uudet teknologiat, kuten asioiden internet (IoT), tekoäly (AI) tai pilvipalvelut ovat laajentaneet perinteisesti tarkasteltua kokonaisuutta. Terminä kyberturvallisuus jakaa mielipiteitä: koskeeko se kaikkea toimintaa vai onko sillä vahva sotilaallista toimintaa koskeva painotus. Suomessa kyberpuolustus ja

vaikuttaminen ainakin nähdään enemmän sotilastoimintana. Toisaalta joissakin työpajoissa kyberturvallisuuden nähtiin koskettavan digitaalisia alustoja toiminnasta riippumatta.

Digiturvallisuuden arkkitehtuurin voidaan ymmärtää koskevan käsitteenä digitalisaation teknistä, rakenteellista ja toiminnallista johtamismallia tai prosessia. Tämän työn yhteydessä sen merkitys nähtiin monella tavalla. Yleensä arkkitehtuuriin panostetaan eniten jonkin asian suunnitteluvaiheessa, jolloin arkkitehtuurikuvauksen perusteella voidaan tunnistaa muun muassa riippuvuussuhteita, toimitusketjuja, turvallisuusratkaisuja, prosesseja, toteutusjärjestystä ja aikatauluja. Digiturvallisuuden arkkitehtuuri ei poikkea arkkitehtuurin perusasioista muutoin kuin arkkitehtuurin asettamisella digitaaliseen toimintaympäristöön niin, että huomioidaan kokonaisarkkitehtuurin tapaan käsiteltävä tieto, teknologia ja toiminnot.

Tietoturvallisuus ymmärretään kyberturvallisuuden sanaston mukaan järjestelyinä, joilla pyritään varmistamaan tiedon saatavuus, eheys ja käytettävyys. Kyberturvallisuus on samassa yhteydessä määritelty tavoitetilana, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. Tietosuoja taas ymmärretään järjestelyinä, joilla pyritään varmistamaan henkilötietojen asianmukainen käsittely ja niiden yksityisyyden säilyminen.

2 SELVITYSTYÖN LÄHTÖKOHDAT

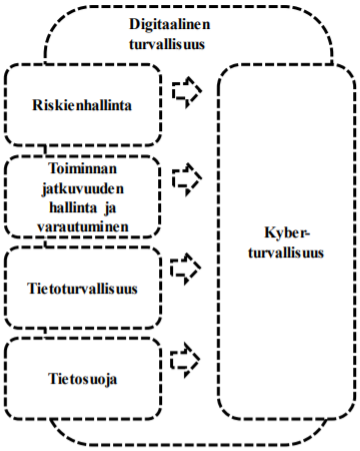
Digitaalisen arkkitehtuurityön työpajojen lähtökohdiksi valittiin kuvauksia eri kysymyksiin. Työpajat järjestettiin niin, että tämän luvun kohtia 2.1-2.4 käsiteltiin vain valtionhallinnon työryhmissä. Niihin kutsuttiin useita toimijoita ja asiantuntijoita yhtaikaa niin ministeriöistä kuin niiden alaisista virastoista.

Luvussa 2.5 kuvatut asiat ja niihin liittyvä kypsyysarviointi toteutettiin organisaatiokohtaisissa työpajoissa. Lisäksi osallistujien ja heidän organisaatioittensa nimet pseudokoodattiin ja muistiinpanot yleistettiin niin, että organisaatioita ja vastaajia ei niiden perusteella tunnistettaisi.

2.1 Digitaalisen turvallisuuden määritelmä

Työpajoja varten tuotetussa materiaalissa oli runsaasti esimerkkejä digitaalisen turvallisuutta koskevien määritelmien taustoista. Eri lähteisiin perustuneissa laajoissa selvityksissä oli hyvin vähän käsitelty digitaalista turvallisuutta yhtenäisenä käsitteenä. Useimmissa tapauksissa vahvimmin oli esillä tietoturva, kyberturva ja tietosuoja.

Digitaalisen turvallisuuden määrittelyn kannalta haluttiinkin eri tahojen näkemyksiä ja ajatuksia, kuinka he asian ymmärtävät.

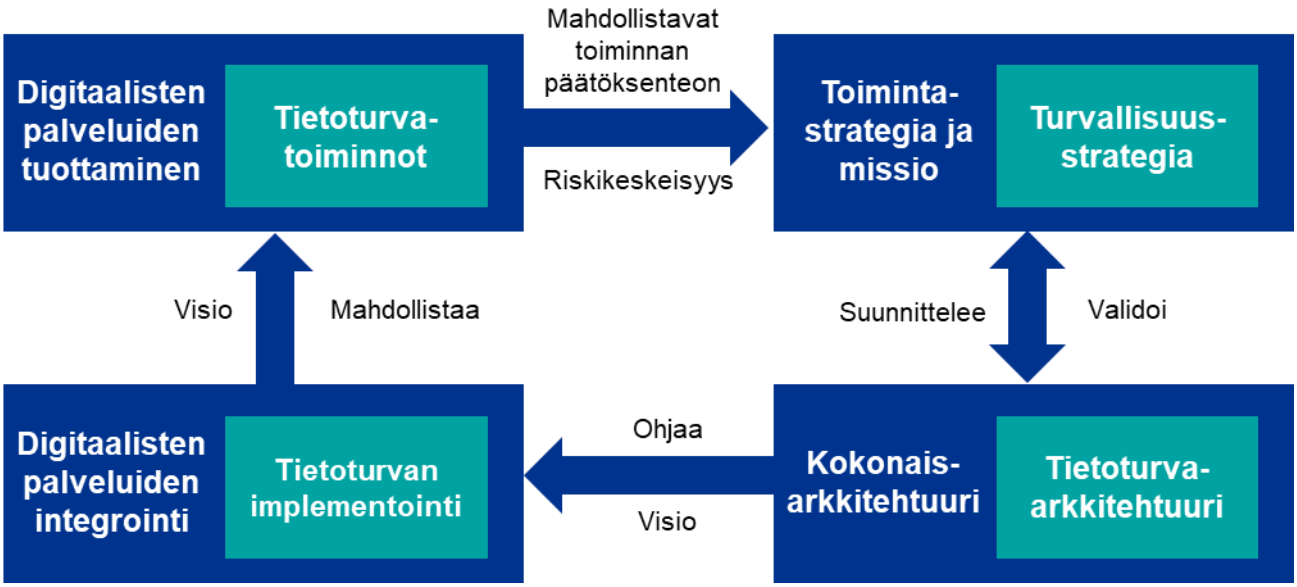


Kuva 2. Digitaalisen turvallisuuden määrittely Valtioneuvoston periaatepäätöksessä 8.4.2020 Julkisen hallinnon digitaalisesta turvallisuudesta

Valtioneuvoston peraatepäätöksessä 8.4.2020 Julkisen hallinnon digitaalisesta turvallisuudesta (VM 2020:23) todetaan että ”Digitaalisen turvallisuuden viitekehykseen sisältyy riskienhallintaan, toiminnan jatkuvuudenhallintaan ja varautumiseen sekä kyberturvallisuuteen, tietoturvallisuuteen ja tietosuojaan liittyviä asioita”. Jokaisessa mainitussa viidessä alueessa on asioita, joihin digitaalinen toiminta ei vaikuta tai tuota sisältöä. Silti on kuitenkin perusteltua sanoa, että digitaalisuudella on vahva sidonnaisuus kaikkiin edellä mainittuihin alueisiin.

2.2 Digitaalisen turvallisuuden arkkitehtuurin lähtökohta

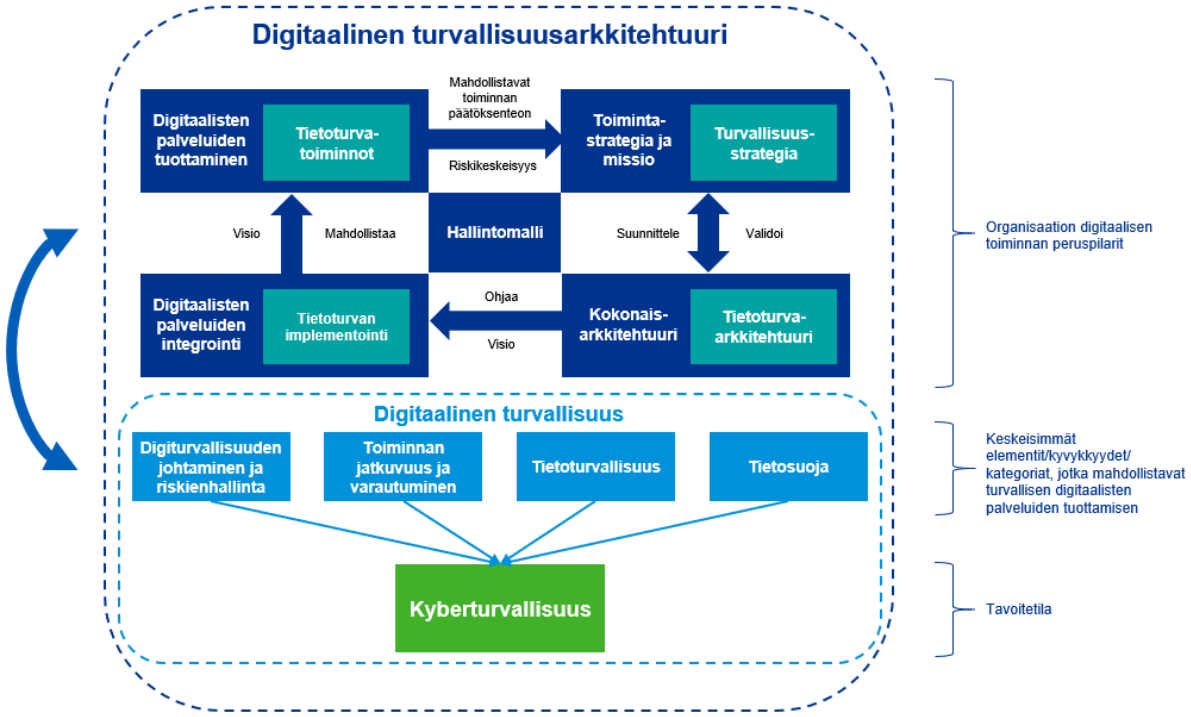
Digitaalisen turvallisuuden arkkitehtuuria voidaan tarkastella monella tavalla. Työpajatyöskentelyjen pohjaksi laadittiin turvallisuuden arkkitehtuurin nelikenttä. Nelikentän sisältöinä ovat toimintastrategia ja missio, kokonaisarkkitehtuuri, digitaalisten palveluiden integrointi sekä digitaalisten palveluiden tuottaminen.



Kuva 3. Turvallisuusarkkitehtuurin nelikenttä

Turvallisuusarkkitehtuuri voi olla esimerkiksi toimintalähtöinen tietoturvasuunnitelma, joka tukee ja toteuttaa organisaation tietoturvastrategiaa ja kohdennettua toimintamallia, joka vastaa liiketoiminnan tarpeita. Se voi sisältää mallin organisaation tietoturvaominaisuuksista ja teknologiakomponenteista sekä niiden suhteesta toisiinsa. Siinä voi myös olla malli, jolla varmennetaan toiminnan tarpeiden ymmärtäminen ja asetetaan suunta ja visio turvallisuustoimintojen tai -ominaisuuksien käyttöönotolle ja toiminnalle itselleen. Yleensä se on luotu linjassa kokonaisarkkitehtuurin kanssa sisältäen tarvittavat tietoturvakomponentit toiminnan tarpeiden tukemiseksi. Turvallisuusarkkitehtuurin tulisi mahdollistaa organisaation päätöksenteko riskikeskeisessä lähestymistavassa.

Turvallisuusarkkitehtuurilla voi olla erilaisia tavoitteita. Esimerkiksi organisaation turvallisuusarkkitehtuuri sisältää kokonaisvaltaisesti organisaation digitaalisen turvallisuussuunnittelun ja on yhdenmukainen kokonaisarkkitehtuurin kanssa. Tai toisaalta digitaalinen turvallisuuden arkkitehtuuri voi tukea turvallisuusratkaisujen kehittämistä niin, että ne soveltuvat muuhun turvallisuusympäristöön.

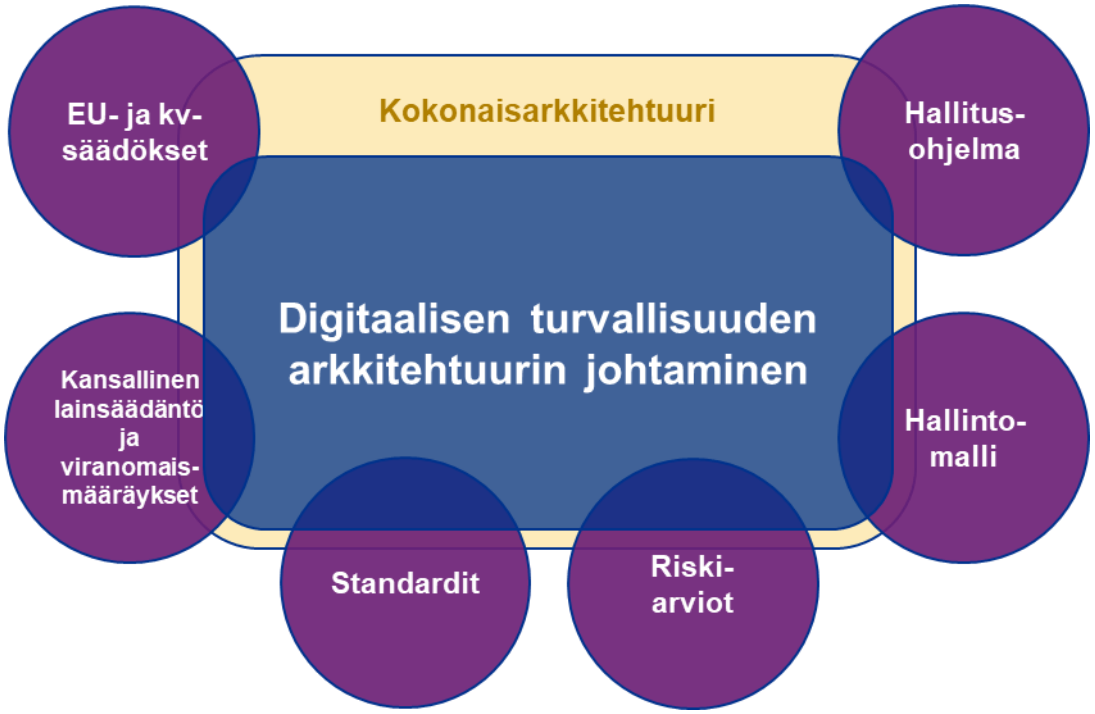


Kuva 4. Digitaalisen turvallisuuden arkkitehtuuri

Työpajoja varten valmisteltiin edeltävän kuvan 4. kehys digiturvallisuuskäsitteestä. Turvallisuusarkkitehtuurin nelikenttä tuottaisi digitaalisen turvallisuuden arkkitehtuuriin organisaation digitaalisen toiminnan turvallisuuden perusteet. Seuraava taso, johon kuuluvat muun muassa tietoturva ja tietosuoja, tuottaisi arkkitehtuuriin elementtejä, kyvykkyyksiä ja kategorioita turvallisten digitaalisten palveluiden tuottamiseksi.

2.3 Strategisen johtamisen lähtökohta

Kokonaisarkkitehtuuri voidaan nähdä perusteena johtamiselle. Rakennusalalla tehdyt arkkitehtuuripiirrokset ovat perusta esimerkiksi lupamenettelylle, tarjouksille, rakentamiselle ja tarkastuksille. Arkkitehtien toimintaa kuitenkin sitoo useat eri säädökset ja määräykset. Ne ovat enimmäkseen kansallisia, mutta usein taustalla on myös kansainväliset säädökset joko suoraan tai epäsuorasti.



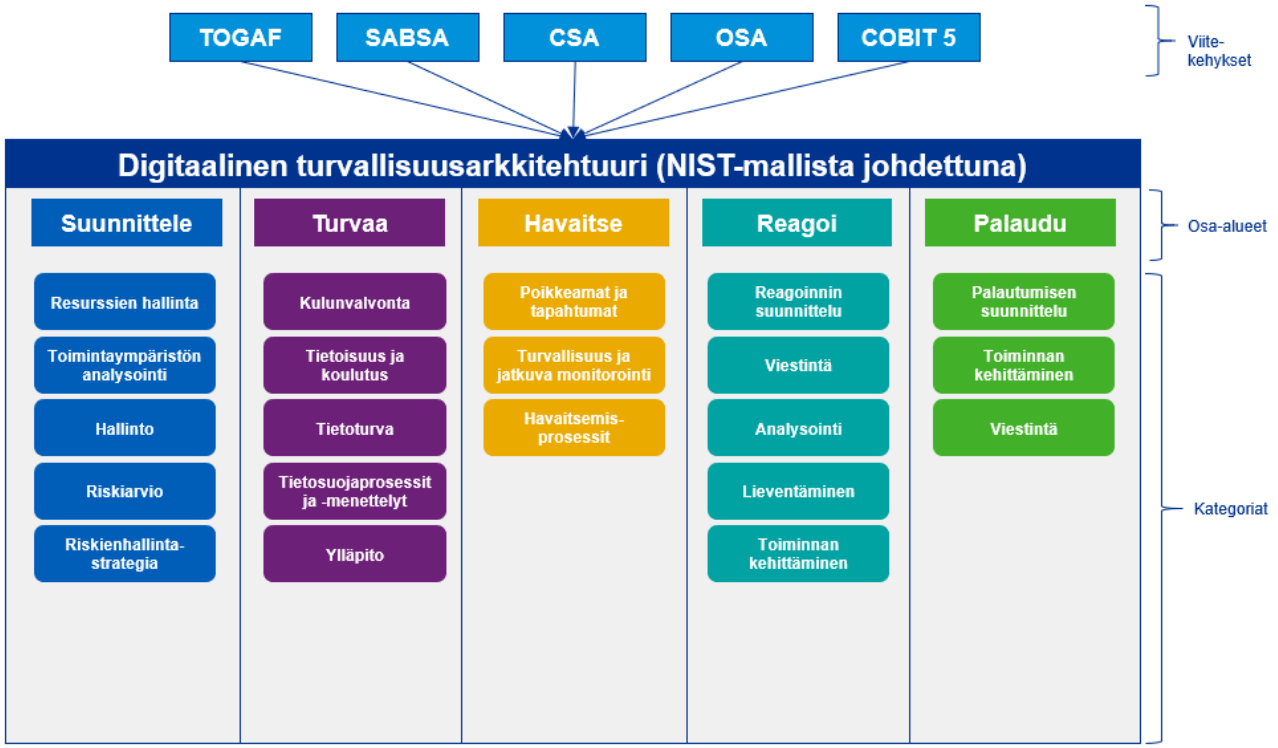
Kuva 5. Digitaalisen turvallisuuden johtaminen

Hyvän digitaalisen turvallisuuden arkkitehtuurin taustavoimina ovat myös alan standardit ja toimintaa koskevat riskiarviot. Organisaatioiden oma hallintomalli yleensä määrittää prosessit ja vastuut. Digitaalisen turvallisuuden arkkitehtuurin johtamiseen ja sisältöön voi vaikuttaa myös voimassa oleva kansallinen hallitusohjelma tai muu strategia säädösten lisäksi.

2.4 Digitaalisen turvallisuuden arkkitehtuurin standardipohjainen lähtökohta

Yhtenä lähtökohtana ja mahdollisena digitaalisen turvallisuuden arkkitehtuurin sisällön tarkastelupohjana työpajoissa käytiin keskustelua kuvasta, joka on johdettu kyberturvallisuuden turvallisuusarkkitehtuurista (NIST CSF-malli). Siinä eri viitekehyksiin kuuluvista kansainvälisistä standardeista on laadittu viisiosainen rakenne. Osa-alueet ovat suunnittelu, turvaaminen, havaitseminen, reagointi ja palautuminen. Niiden sisällä ovat tarkemmat kategoriat.

Kuvan 6. pohjalta voidaan yhdistää alan standardit ja viitekehykset ja parhaat käytännöt organisaation digitaalisen turvallisuuden parantamiseksi ja hallinnoimiseksi. Hahmotelman voidaan myös katsoa parantavan organisaation laajuisesti ymmärrystä turvallisuusarkkitehtuurin osa-alueista, organisaation kyvykkyyksistä ja turvallisuusriskeistä.



Kuva 6. NIST-standardin perusteella muodostettu digitaalisen turvallisuuden arkkitehtuurimalli

2.5 Digitaalisen turvallisuuden kypsyyskartoituksen (C2M2-mallin) lähtökohta

Julkishallinnon digitaalisen turvallisuuden arkkitehtuurin kypsyyttä arvioitiin organisaatiokohtaisissa työpajoissavaltionhallinnossa ja kuntasektorilla. Arviointipohjaksi sovittiin Huoltovarmuusorganisaatiolle tehdyn toimialojen kyberturvallisuuden tilannekuvaselvityksen kyselylomake. Koska alun perin määrittelyssä todettiin tarkastelun sisältävän sekä kyberturvallisuuden että muiden digiturvallisuuden osa-alueita, tarkennettiin kyselyyn kyberturvallisuuden tilalle digiturvallisuus. Arvioinnissa **arkkitehtuuria** koskeva kysymys on **tavoite 4.3**.

Digitaalisen turvallisuuden arkkitehtuurin kehittämiskohteita on mahdollista selvittää digitaalisen turvallisuuden osa-alueiden kautta. Kyselyä varten riskienhallinnan osa-aluetta täydennettiin lisäämällä siihen digiturvallisuuden johtaminen. Osa-alueet siis olivat digiturvallisuuden johtaminen ja riskienhallinta, toiminnan jatkuvuus ja varautuminen, tietoturva, kyberturvallisuus ja tietosuoja. Kyselyssä hyväksyttiin kypsyyttä arvioitaessa digitaalisen eri osa-alueiden tasoarvio ja se kirjattiin työpajan muistiinpanoihin. Osa-alueista erityinen mielenkiinto kohdistuu digiturvallisuuden johtamiseen ja riskienhallintaan sekä toiminnan jatkuvuuteen ja varautumiseen. Tietoturvan, kyberturvan ja tietosuojan toteutumista voidaan arvioida kokonaiskypsyyden perusteella, sillä useimmilla organisaatiolla ne otettiin jo määrittelyissä huomioon ja muodostivat siten vastauspohjan näiden kolmen digitaalisen turvallisuusalueen arvioinnille.

Digiturvallisuuden johtamista ja **riskienhallintaa** arvioitiin kahdessa osassa. Johdon tukea, sitoutumista tai asemaa käsitellään tavoitteessa:

Johdon tuki digiturvallisuuden hallintajärjestelmälle (4.2)

Riskien hallintaa taas arvioitiin erikseen. Sitä arvioitiin useissa kyselylomakkeen tavoitteissa. Erityisesti seuraavat otettiin huomioon:

Kriittisten palveluiden hallinta (1.2),
Digiturvallisuushäiriöiden vaikutusten minimointi kriittisille palveluille (1.3),
Riskien hallintastrategian määrittely (2.1)
Digiturvallisuusriskien hallinta (2.2),
Riippuvuusriskien hallinta (5.2),
Jatkuvuuden suunnittelu (7.4)
Uhkien tunnistaminen ja hallinta (10.1) sekä
Haavoittuvuuksien hallinta (10.2)

Toiminnan jatkuvuus ja varautuminen on huomioitu tavoitteessa 7.4. sekä uhkien tunnistaminen ja hallinta tavoitteessa 10.1.

3 DIGITAALISEN TURVALLISUUDEN ARKKITEHTUURIN NYKYTILA TYÖPAJOJEN TULOSTEN MUKAAN

Digitaalisen turvallisuuden aarkkitehtuurin kahdeksassa työpajassa käsiteltiin määritelmiä, strategisen tason digitaalisen turvallisuuden arkkitehtuurin viitekehystä sekä johtamista. Työpajan pohjaksi oli jaettu malleja arvioitaviksi sekä kehitettäväksi.

3.1 Digitaalisen turvallisuuden määritelmän tuloksia

Työpajojen alkuvaiheessa ilmeni, että digitaalinen turvallisuus koettiin uudeksi, ennalta määrittämättömäksi tai muutoin tuntemattomaksi asiaksi esitetyssä muodossa. Yleisesti tiedon käsittelyssä turvallisuutta on tarkasteltu tietoturvan, tietosuojan tai kyberturvallisuuden näkökulmista. Eräässä työpajassa käsitteiden evoluutiota tarkasteltiin siten, että ATK-aikana alettiin puhua tietoturvasta, ICT-aikakaudella tietoturvasta ja digitalisaation aikana digitaalisesta turvallisuudesta (tai digiturvallisuudesta). Tietosuoja on tullut vahvemmin esiin EU-direktiivien ja henkilötietojen turvaamisen tarpeesta muutaman vuoden sisällä.

Valtioneuvoston periaatepäätöksessä 8.4.2020 (VM 2020:23) kuvattu ja työpajan materiaalissa esitetty digitaalisen turvallisuuden OECD:n lähtökohtiin perustuva määritelmä sai enemmistön kannatuksen. Tärkeimmäksi asiaksi koettiin asian ymmärtäminen samalla tavalla. Merkittävimmät erot koskivat lähinnä esitetyn mallin suhteita toisiinsa. Lisäksi nähtiin hyvänä, jos asia ymmärrettäisiin myös kansainvälisesti yhteneväisellä tavalla.

Suomessa on käytössä useita eri tapoja hyväksyä termien määrittelyjä. Niitä voidaan hyväksyä osana säädöksi ja termipankkeja. Määritelmiä tyypillisesti myös käsitellään tutkimuksissa, hankeohjelmissa, selvityksissä. Työpajoissa esitettiin, että digiturvallisuutta ja digiturvallisuuden arkkitehtuuria koskevat määritelmät täydennettäisiin seuraavassa päivityskierroksessa esimerkiksi Sanastokeskuksen kanssa tuotettuun Kyberturvallisuuden sanastoon.

3.2 Digitaalisen turvallisuusuuden arkkitehtuuria ja sen sisältöä koskevia tuloksia

Valtionhallinnosta löytyy niukasti syvällistä osaamista turvallisuusarkkitehtuuriin liittyen. Lisäksi selvityksissä ilmeni, että useita digiturvallisuuden alueita arkkitehtuureineen oli käsitelty kyber-, tietoturva- ja tietosuojia käsittelevissä dokumenteissa (esimerkiksi strategia, politiikka, säännöstö, turvallisuusarkkitehtuurin). Työpajojen perusteella on kuitenkin havaittavissa, että alan arkkitehtejä on vähän, arkkitehtuurien taso on kirjava ja kokonaiskuvasta oli useimmilla työpajoihin osallistuneilla vain ylimalkainen käsitys, sillä digiturvallisuuden arkkitehtuurikuvauksia ei ole keskitetysti saatavilla eikä kokonaiskuvaa niiden perusteella ole muodostettu.

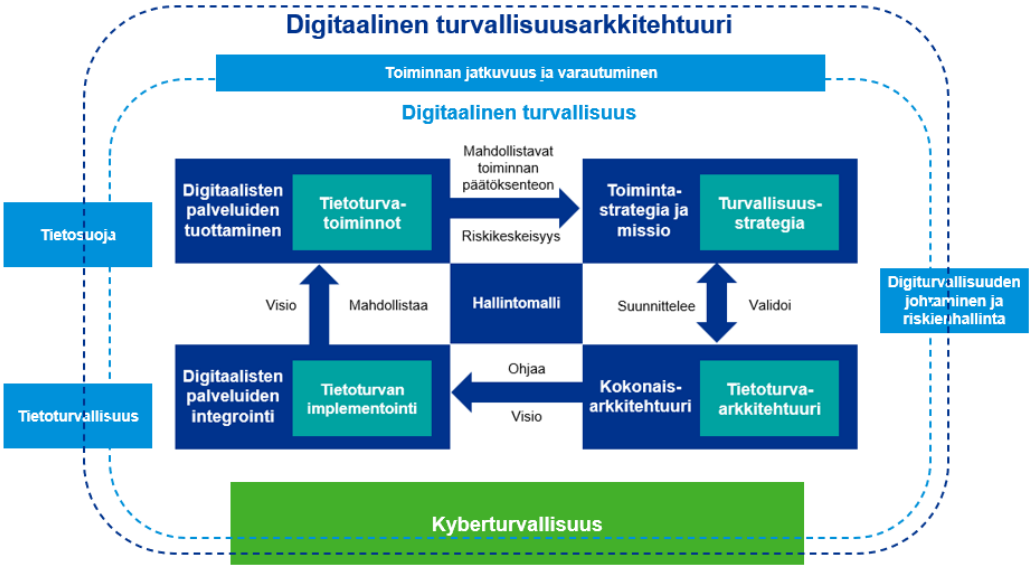
Työpajan taustaksi esitetty kuvassa 4. oleva digitaalisen turvallisuuden arkkitehtuurimalli sai runsaasti kommentteja ja kehittämisehdotuksia. Useimmat asettivat digiturvallisuuden arkkitehtuurin lähtökohdaksi tieto-omaisuuden ja siitä juontuvat tarpeet niin tekniselle toteutukselle kuin prosesseille. Lisäksi määrittelyyn toivottiin joustavuutta. Kunkin toimijan vastuu tunnistettiin lakiin julkisen hallinnon tiedonhallinnasta (906/2019) kirjatun vaatimuksen mukaisesti, jokaisen tiedonhallin-

tayksikön on ylläpidettävä sen toimintaympäristön tiedonhallintaa määrittelevää ja kuvaavaa tiedonhallintamallia. Toisaalta vaatimuksia ilmeni keskitettyjen palveluiden digiturvallisuusarkkitehtuurin ja tekniseen arkkitehtuurin läpinäkyvyyteen ja vaikutusmahdollisuuksiin. Tämä liittyy sekä valtiovarainministeriön tehtäviin huolehtia tiedonhallintakartan ylläpidosta että ministeriöiden tehtäviin omalla toimialallaan huolehtia julkisen hallinnon tiedonhallintakartan sisällön ajantasaisuudesta.

Työpajojen lähtökohdaksi tuotettu kuvassa 1. oleva viitekehys koettiin myös haasteelliseksi ymmärtää. Asian liityntäpintaa digitaalisen turvallisuuden arkkitehtuuriin hämmensi määritelmien tuoreus. Lisäksi valtionhallinnolla käytössä olleen JSH179 tilanteesta ja tulevaisuudesta oli epätietoisuutta. Kuvassa 7. näkyviä JHS179:n arkkitehtuurirakenteita pidettiin edelleen valideina.

Kuva 7. JHS 179:n arkkitehtuurirakenne

Mallin perusteella nähtiin tarpeelliseksi pilkkoa arkkitehtuuri pienempiin ja helpommin hallittaviin sekä hahmotettaviin osiin. Samalla kuitenkin asetettiin toiveita valtionhallinnon kokonaisturvallisuusarkkitehtuurin näkyvyyteen. Sitä kaivattiin joustavana ja yleisen tason ohjauksena, jotta organisaatiolla olisi yhtenäisempi käsitys valtionhallinnon tarpeista, joihin tulisi vastata.



Kuva 8. Esimerkki digitaalisen turvallisuuden arkkitehtuurin sisällöstä

Kuvassa on digitaalisen turvallisuuden arkkitehtuurin rakenne työpajojen pohjalta koottuna esimerkkinä. Siinä johtamiseen liittyvän mallin vaiheet/tehtävät on liitetty digitaalisen turvallisuuden määritelmän mukaisiin osa-alueisiin. Rakennetta voidaan käyttää pohdittaessa mitä asioita tulisi huomioida ja mikä on toteutusvastuu, kun organisaatiot ylläpitävät digitaalisen turvallisuuden arkkitehtuuria tiedonhallintamallin ylläpitoon liittyen. Organisaation tulisi laatia tämän alueen toimintasuunnitelma.

3.3 Strategisen johtamisen tuloksia

Työpajoissa käsiteltiin sitä, että mikä on digitaalisen turvallisuuden arkkitehtuurin rooli ja asiasisältö strategisen johtamisen näkökulmasta. Lisäksi pohdiskelua synnytti, millä tasolla strategista johtamista käsitellään. Taustamateriaalina jaettu kuva 5 herätti paljon uusia ajatuksia ja asioita, jotka on otettava huomioon digitaalisen turvallisuuden arkkitehtuurin strategisen tason johtamisessa.

Kansalliset ja kansainväliset säädökset ja määräykset sekä alan standardit ja toimintaa koskevat riskiarviot nähtiin relevantteina. Hallintomalli nähtiin myös tärkeäksi. Eniten pohdintaa synnytti hallitusohjelma, jonka tavoitteiden vaikutusaikaa (4 v) pidettiin osassa työpajoja strategisen tason johtamisnäkökulmana liian lyhyenä.

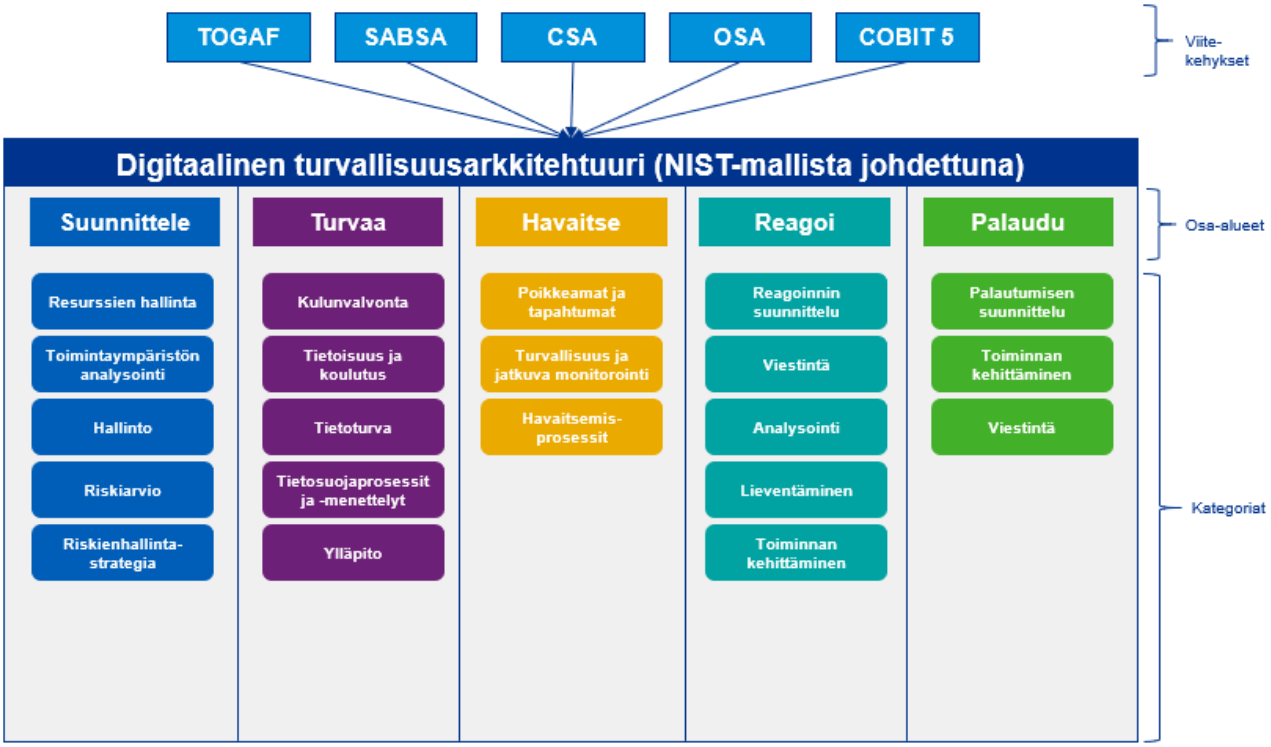
Uusia työpajoissa esiin nostettuja lisäyksiä olivat selonteot ja kansallinen uhka-arvio, visiot, periaatepäätökset, teknologian ja toiminnan kehitys sekä tiedonhallintamalli ja tiedonhallintakartta. Työpajoissa esitettiin myös asioiden ryhmittämistä uudelleen. Esitettyjen näkökulmien pohjalta digitaalisen turvallisuuden arkkitehtuurin johtamisen sisältöä voidaan täydentää ja tarkastella asiaa laajemmasta näkökulmasta kuvassa 9 esitetyllä tavalla..

Kuva 9. Digitaalisen turvallisuuden johtaminen työpajojen perusteella muokattuna

Työpajoissa uusina ulottuvuuksina esiin nostetut rakenteet on huomioitu kuvassa 8. Digiturvallisuuden arkkitehtuurin strategisen tason johtamista voisi kehittää eri arkkitehtuurien ja tieto-omaisuuden hallinnan kautta. Keskeisiä huomioitavia asioita ovat eri arkkitehtuuritasojen kytkökset tiedonhallintakarttaan sekä eri lähteistä tuleviin vaatimuksiin. Näitä vaatimuksia asettavat muun muassa eri lait ja asetukset sekä riskit ja uhka-arviot.

3.4 Tuloksia digitaalisen turvallisuuden arkkitehtuurin standardimallista

Kuvassa 6. oleva NIST-standardiin perustuva digitaalisen turvallisuuden arkkitehtuurimalli koettiin selkeimmäksi selvityksessä käytetyistä malleista. Malli nähtiin potentiaalisena pohjana digitaalisen turvallisuuden arkkitehtuurin sisällöksi etenkin viiteen osa-alueeseen jaettujen keskeisten tehtävien osalta. Tarkennuksia haluttiin erityisesti tehtäväalueiden sisälle kategorioihin, mutta kuitenkin niin, että kaikkien työpajojen ehdotuksia ei lisättäisi niihin sellaisenaan vaan jalostettuna.



Kuva 10. Esimerkki digitaalisen turvallisuusarkkitehtuurin sisällöstä

Kuvan 10. laajaan viitekehyksen ei ollut nähtävissä täydennystarvetta. Tehtäviä voisi tarkastella kuvan mukaisella tavalla. Ensimmäisen kohdan ”suunnittele”, voisi hyvinkin ymmärtää myös johtamisena. Tärkeintä on kuitenkin huomioida resurssit, toimintaympäristö, hallinnon prosessointi, riskit ja riskienhallintaa liittyvä strategia. Neljä seuraavaa tehtävää käsittävät toteuttamisen. Riskipohjainen tarkastelu ja suunnittelu loisi pohjan turvallisuuden kehittämiselle. Siinää voitaisiin huomioida pääsynhallintaa/kulunvalvontaa, tietoturvaa, tietosuojaa sekä niihin liittyviä ylläpitoprosesseja. Havainnoinnissa voisi keskittyä ensin havainnointiprosessin määrittelyyn ennen siinä tarvittavaa teknologiaa. Reagoinnissa ja palautumisessa korostuu kehittämisen lisäksi tiedottaminen.

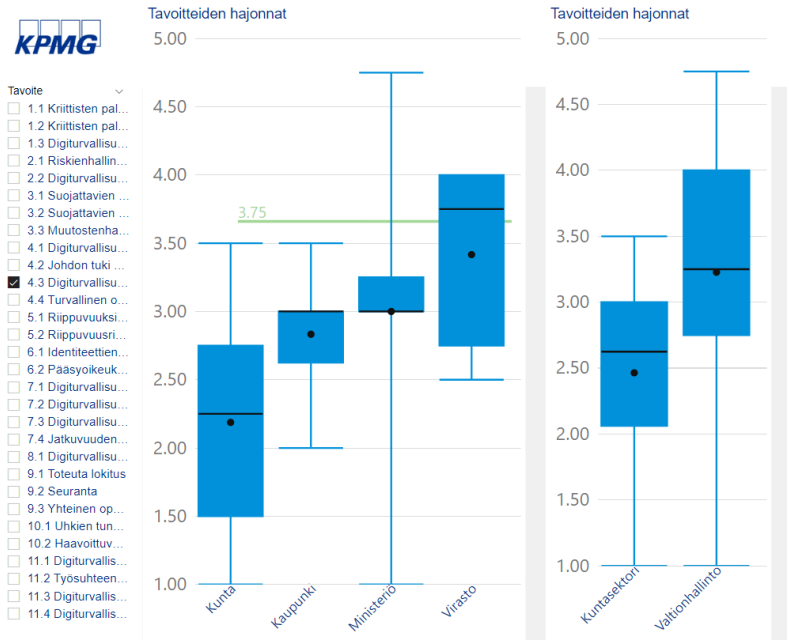
3.5 Digitaalisen turvallisuuden kypsyyskartoitus, julkishallinnon itsearvion, mukaan

Itsearvioinnin 30 kysymyksen (tavoitetila) joukossa kysyttiin digitaalisen arkkitehtuurin kypsyyttä. Työpajoissa ilmeni, että digitaalisen turvallisuuden arkkitehteja edusti hyvin pieni joukko. Julkishallinnossa arkkitehtuurin kypsyysarvio oli heikoin sekä valtionhallinnossa että kuntasektorilla. Merkittäväksi haasteeksi koettiin henkilöresurssit. Harvalla organisaatiolla oli omia digi-, kyber- tai tietoturva-arkkitehtejä. Joissakin tapauksissa ilmeni, että arkkitehtuuritöissä tukeuduttiin ulkopuolisiin ostopalveluihin. Kyselyssä tarkasteltiin myös uhkien- ja riskienhallinnan maturiteettia.

Digitaalisen turvallisuuden arkkitehtuurin kypsyydellä on riippuvuuksia kyselyn muihinkin osa-alueisiin. Kuten aiemmin jo todettiin, on arkkitehtuurin perusteella helpompi tunnistaa ja hallita esimerkiksi toimitusketjuja, niiden riippuvuusriskejä, digitaalista turvallisuutta, riskiarvioita sekä uhka-arvioita.

3.5.1 Digiturvallisuuden arkkitehtuuri (4.3)

Ohjatuissa työpajoissa suoritetun itsearvion perusteella digitaalisen turvallisuuden arkkitehtuurin taso on kehityskohde. Kuntasektorin keskiarvoa 2.46 selittää kuntien (2.19) ja kaupunkien (2.83) alhaiset tasot. Valtionhallinnossa tilanne on parempi. Valtionhallinnon keskiarvo on 3.23, ja tarkemmin ministeriöiden 3.00 ja virastojen 3.2. Lisäksi virastoja lukuun ottamatta on hajonta suurta. Kokonaisuudessaan tavoitteen taso oli julkishallinnon toiseksi alimmalla kypsyystasolla.



Kuva 11. Digitaalisen turvallisuusarkkitehtuurin (4.3) kypsyyden keskiarvot, keskiluvut ja hajonnat eri näkökulmista

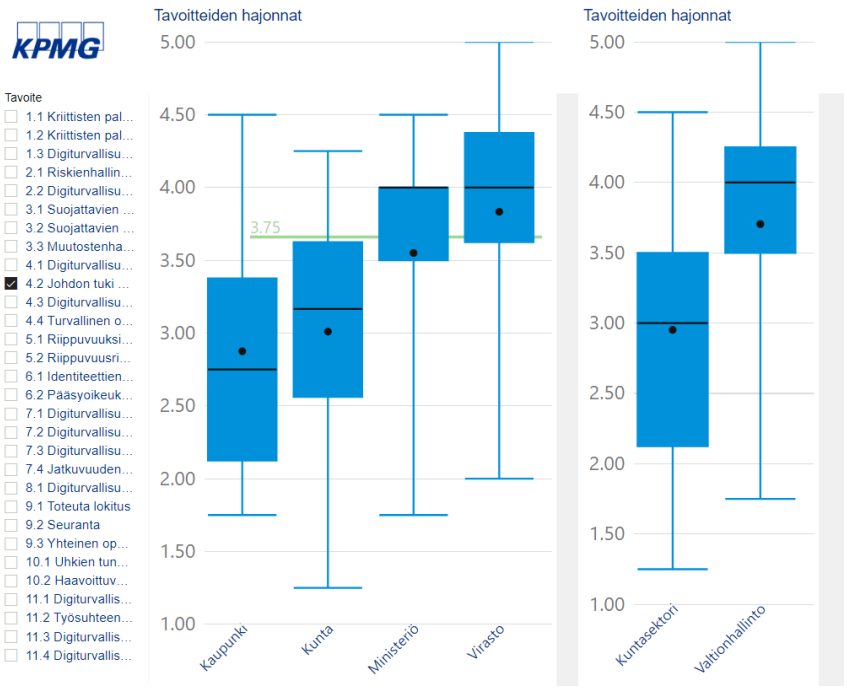
Kyselylomakkeen määritelmän mukaan ”digiturvallisuusarkkitehtuuri on olennainen osa kokonaisarkkitehtuuria. Sen avulla kuvataan organisaation turvallisuusprosessien, digiturvallisuusjärjestelmien ja henkilöstön rakenne sekä näiden suhde organisaation tavoitteeseen ja strategisiin suunnitelmiin. Tärkeä osa digiturvallisuusstrategiaa on IT- ja OT-ympäristöjen onnistunut eriyttäminen.”

Lisäksi digitaalisen turvallisuuden arkkitehtuurin merkitys korostuu toimitusketjujen ja niiden riippuvuusriskien tunnistamisessa ja hallinnassa. Arkkitehtuurin pohjalta digitaalinen turvallisuus, riskiarviot sekä uhka-arviot ovat varmemmin hallittavissa.

Työpajoissa oli lähtökohtana ympäristöjen eriyttäminen sekä segmentointi ja arvioinnissa keskityttiin pääsääntöisesti yhteisten palveluiden arkkitehtuuriin. Useimmissa työpajoissa näkymä arkkitehtuuriin koettiin heikoksi ja kytköksiä kokonaisarkkitehtuuriin ei tunnistettu olevan olemassa. Lisäksi vaikutusmahdollisuuden arkkitehtuuriin ja sen kautta digitaalisten palveluiden kehittämiseen olisi toivottu olevan suurempaa.

3.5.2 Digiturvallisuuden johtaminen ja riskien hallinta: Johdon tuki digiturvallisuuden hallintajärjestelmälle (4.2)

Johdon tuella on suuri merkitys digiturvallisuuden suunnittelulle, toteuttamiselle, ylläpidolle ja kehittämiselle. Kypsyysmittauksessa johtamiseen liittyviä kohtia oli useita, mutta pääpaino tässä tarkastelussa kohdistui tavoitteeseen 4.2. Tulosten perusteella valtionhallinnon keskiarvo on tavoitetasossa 3.75. Hajonta on kuitenkin melko suuri.



Kuva 12. Johdon tuki digiturvallisuuden hallintajärjestelmälle (4.2) keskiarvot, keskiluvut ja hajonnat eri näkökulmista

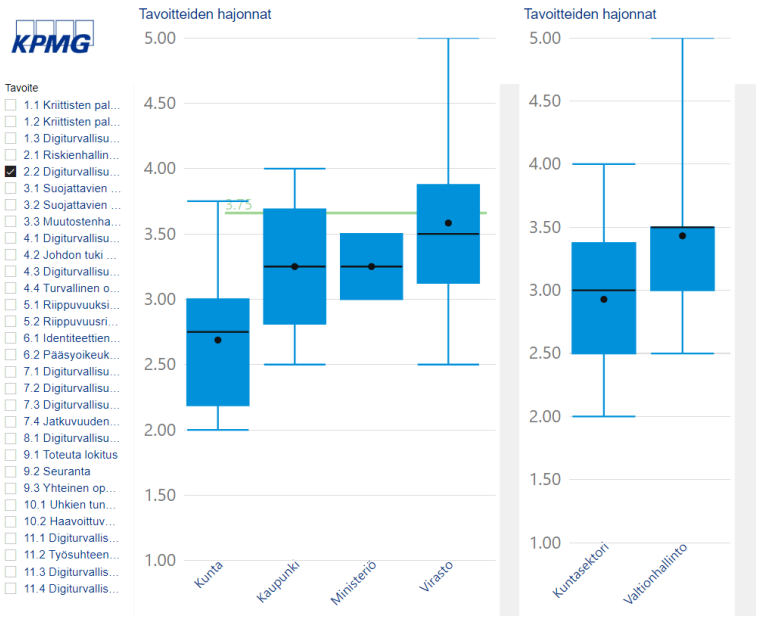
Keskeisin digiturvallisuuden dokumentti on digiturvallisuusstrategia. Sen tyypillisin ilmentymä oli tietoturva- ja tietosuojastrategia. Joissakin organisaatioissa sitä kutsuttiin politiikaksi. Digitaalisuuteen liittyvät strategiset linjaukset saattoivat sisältyä organisaation kokonaisturvallisuusstrategiaan. Keskeisintä selvitystyön kannalta oli, että digiturvallisuusstrategiaa vastaavat asiat oli huomioitu ja ne oli johto hyväksynyt.

Toisaalta kyselyssä haluttiin selvittää, onko strategialla johdon tuki. Esimerkiksi kyselylomakkeessa olevassa tavoitteessa 4.2 todetaan, että ”Johdon tuki on tärkeää digiturvallisuuden hallintajärjestelmän jalkauttamiselle digiturvallisuusstrategian mukaisesti. Perustasolla tuki sisältää riittävien resurssien mahdollistamisen (henkilöt, työkalut, rahoitus). Kehittyneempi tuki pitää sisällään ylimmän johdon näkyvän osallistumisen sekä vastuiden määrittelyn ja valtuutukset hallintajärjestelmälle. Edelleen, tuki pitää sisällään organisaatiotasoisen tuen poliitikkojen tai muiden organisaatiota velvoittavien ohjeistuksien määrittelylle ja ylläpitämiselle”.

Selvityksen aikana ilmeni, että organisaatiossa on johdon tuki hyvin vaihtelevaa. Kaikissa tapauksissa johdon tuen määrään ilmoitettiin vaikuttavan resurssien määrän. Myös julkisuuden paineella koettiin olevan vaikutusta johdon suhtautumiseen ja mielenkiintoon digiturvallisuutta kohtaan

3.5.3 Digiturvallisuuden johtaminen ja riskien hallinta: Digiturvallisuusriskien hallinta (2.2)

Riskienhallinnalla on suuri merkitys digiturvallisuuden suunnittelulle, toteuttamiselle, ylläpidolle ja kehittämiselle. Kypsyysmittauksessa riskeihin liittyviä kohtia oli useita. Tulosten esittelyn alussa pääpaino on tavoitteessa 2.2 Digiturvallisuusriskien hallinta. Toisessa vaiheessa tarkastellaan riskien hallintaa vaikuttavien neljän alueen kypsyyttä. Myös uhkien tunnistamista ja hallintaa tarkasteltiin.

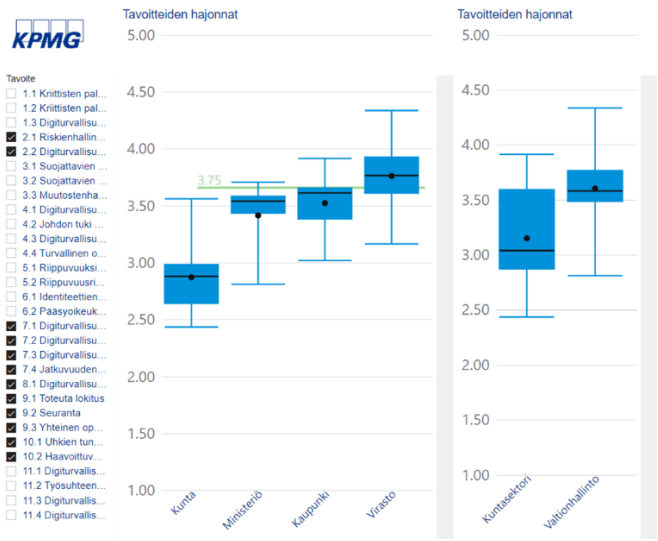


Kuva 13. Digiturvallisuusriskien hallinnan kypsyyden keskiarvot, keskiluvut ja hajonnat eri näkökulmista

Keskeisin riskienhallinnan dokumentti on riskienhallintastrategia. Sen tyypillisin ilmentymä oli tietoturva- ja tietosuojariskistrategia. Riskien hallintaan liittyvät strategiset linjaukset saattoivat sisältyä organisaation laajempaan riskienhallinta strategiaan. Keskeisintä selvitystyön kannalta oli, että riskienhallinta oli huomioitu ja johto oli dokumentit hyväksynyt.

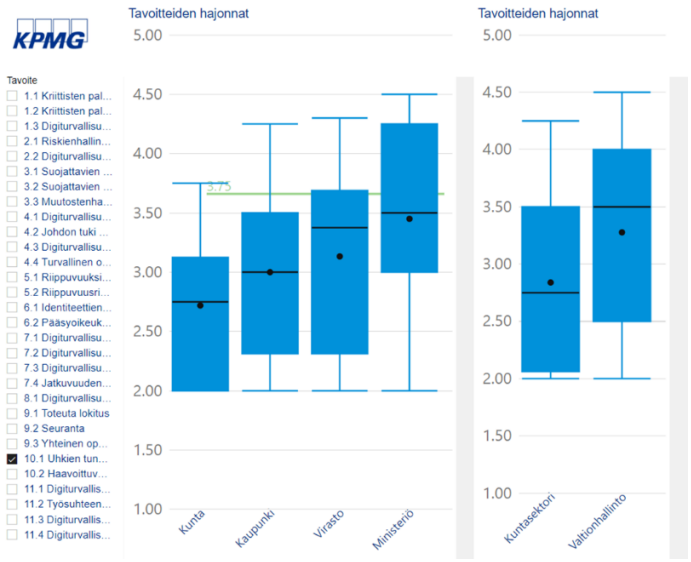
Kyselylomakkeessa olevassa tavoitteessa 2.2 todetaan, että ” Digiturvallisuusriskien hallinta sisältää riskien tunnistamisen, arvioinnin, käsittelyn (hyväksyminen, välttäminen, pienentäminen tai siirtäminen) ja seurannan tavalla, joka huomioi toiminnan tarpeet. Avainasemassa näiden aktiviteettien toteuttamiseen on organisaatiolaajuinen ymmärrys riskienhallintastrategiasta. Määritetyn riskiluokittelun avulla organisaation on mahdollista johdonmukaisesti käsitellä ja seurata riskejä. Riskirekisteri - lista tunnistetuista riskeistä ja riskeihin liittyvistä tiedoista - helpottaa tätä prosessia. Tämän osa-alueen muut kohdat (sisältäen Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus; Uhkien ja haavoittuvuuksien hallinta; Tilannekuva) viittaavat riskirekisteriin ja näyttävät miten tämän mallin käytännöt toimivat vahvemmin, kun ne ovat kytkettynä riskienhallintamalliin.”

Kun koostetaan yhteen edellä mainitut alueet, 7. Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus; 10. Uhkien ja haavoittuvuuksien hallinta; 9. Tilannekuva ja 2 Riskienhallinta, voidaan todeta hajonnan olevan pientä. Kypsyys on usealla organisaatiolla yli tavoitetaso, mutta turvallisuuden lisääminen nähtiin eri riskienhallintaa koskevien alueiden kehittämisen kautta mahdolliseksi. Lisäksi selvityksen aikana ilmeni, että riskilähtöinen tarkastelu koettiin merkittäväksi kehittämiskohteeksi.



Kuva 14. Digiturvallisuusriskien hallinnan alueiden keskiarvot, keskiluvut ja hajonnat eri näkökulmista

Kyselylomakkeen mukaan tavoitteessa 10.1 ”Uhkien tunnistaminen ja hallinta alkaa hyödyllisen uhkatiedon keräämisellä luotettavista lähteistä ja jatkuu tulkitsemalla kerättyä tietoa organisaation omaan kontekstiin sekä laatimalla toimenpiteitä uhkatekijöille, joilla on kyky, motivaatio ja mahdollisuus vaikuttaa häiritsevästi palveluiden tuottamiseen. Uhkaprofiilia voidaan käyttää tarkempien uhkien tunnistamiseen, riskianalyysiprosessiin (vrt. 2. Riskienhallinta) ja/tai tilannekuvan rakentamiseen.

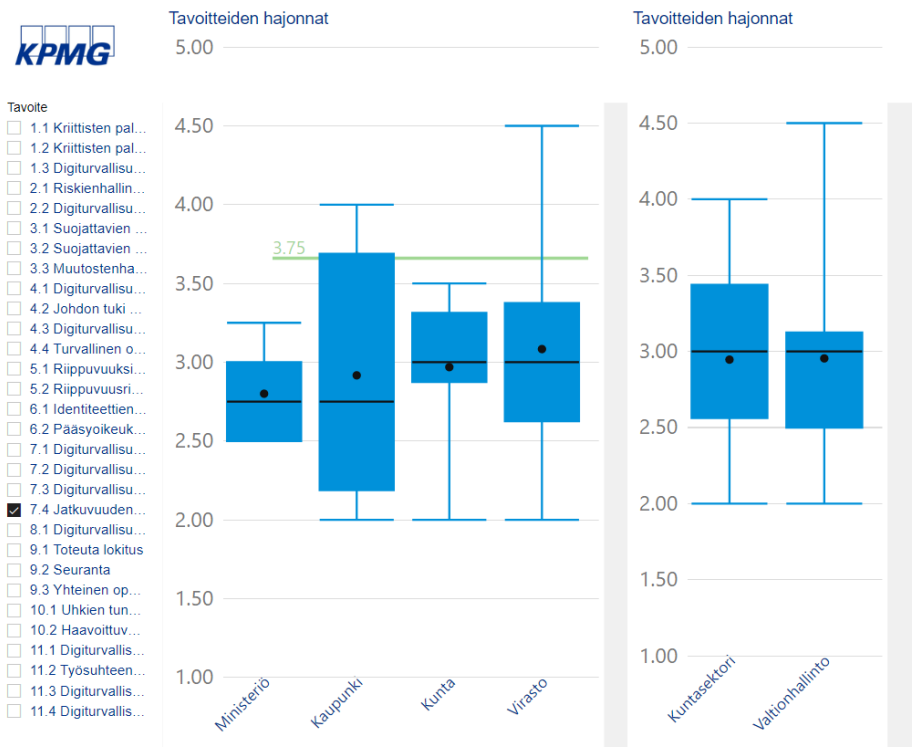


Kuva 15. Uhkien tunnistaminen ja hallinta 10.1 keskiarvot, keskiluvut ja hajonnat eri näkökulmista

Työpajoissa tämä tavoite nähtiin yhtenä julkishallinnon tärkeimmistä kehityskohteista.

3.5.4 Toiminnan jatkuvuus ja varautuminen: Jatkuvuuden turvaaminen

Kysellyn mukaan ”Jatkuvuuden suunnittelu sisältää tarvittavat toimenpiteet kriittistentoimintojen ylläpitämiseksi keskeytysten aikana, kuten esimerkiksi merkittävien digiturvallisuus poikkeamien tai onnettomuuksien aikana. Toiminnan vaikutusanalyysin avulla organisaation on mahdollista tunnistaa olennaisimmat suojattavat kohteet ja määritellä toipumistavoitteet. Jatkuvuussuunnitelmia tulisi testata ja päivittää testausten perusteella, jotta niiden ajantasaisuus ja käyttökelpoisuus voidaan varmistaa.”

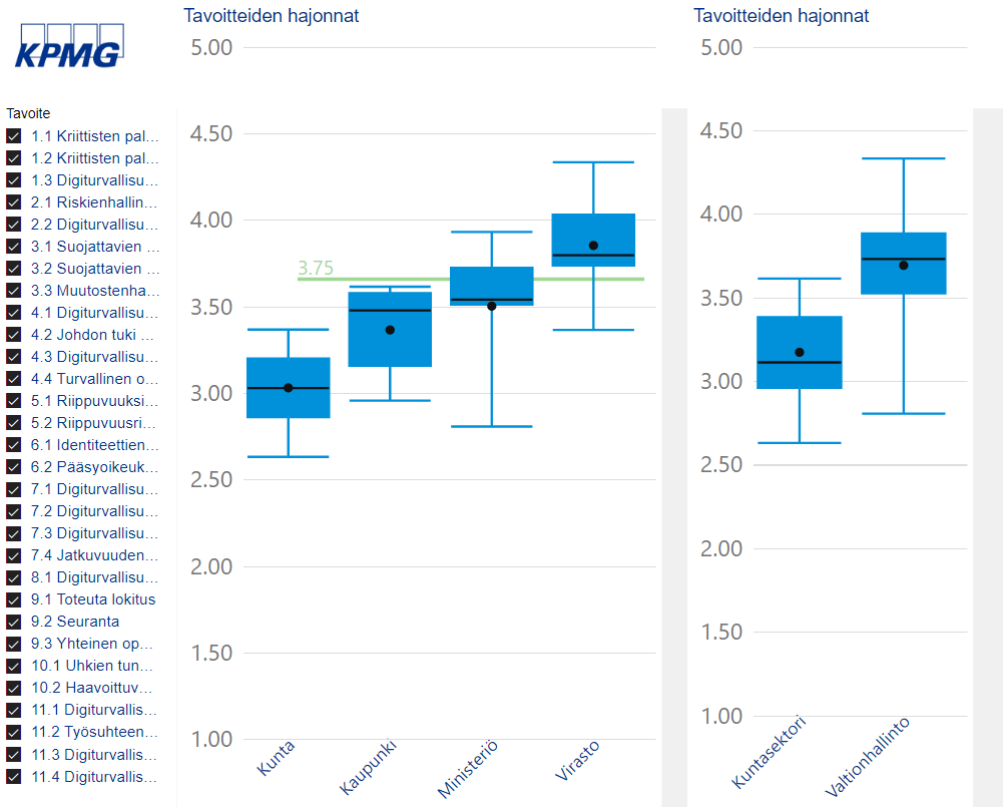


Kuva 16. Jatkuvuuden suunnittelu (7.4) keskiarvot, keskiluvut ja hajonnat eri näkökulmista

Tulosta voi pitää yllättävänä, sillä tämä oli koko julkishallinnon heikoin tavoitekohtainen kypsyysarvio. Työpajoissa kävi kuitenkin ilmi, että pandemian mukaan tuomien ilmiöiden huomioiminen on käynnistänyt koko varautumissuunnittelun päivityskierroksen ja se prosessi oli pääsääntöisesti vielä kesken. Toimintaa on kuitenkin tehostettu muilla johtamistoimilla. Tässä yhteydessä kaikki jatkuvuuden turvaamiseen liittyvien osa-alueiden, myös digiturvallisuuden, tarkastaminen ja päivittäminen nähtiin aiheelliseksi.

3.5.5 Tietoturvan, kyberturvan sekä tietosuojan tilanteesta

Muihin digiturvallisuuden alueisiin, kuten tietoturvaan, kyberturvaan ja tietosuojaan, ei kyselyssä erikseen kohdennettu omia kysymyksiä. Käytännössä nämä näkökulmat kuitenkin löytyvät kyselyn alakohdista eli tavoitteista Digiturvallisuuden osa-alueista parhaiten tunnistettiin tietoturva- ja tietosuoja. Erityisesti jälkimäiseen on viime aikoina panostettu tietosuoja-asetuksen velvoitteiden pohjalta. Edellä mainituin perustein tietoturvan, kyberturvan ja tietosuojan kypsyyttä ja tilannetta voidaan karkeasti arvioida kypsyysarvion kokonaistuloksen avulla.



Kuva 17. Digitaalisen turvallisuuden kypsyysarvion kokonaiskuva

Tulosten ja työpajojen perusteella valtionhallinnon digitaalisen turvallisuuden kypsyys oli jonkin verran kuntasektoria parempi. Valtionhallinnon keskimääräinen kypsyys ylitti tavoitetason 3,75, mutta hajonta oli kohtuullisen suurta ja osa valtionhallinnon organisaatioistakin jäi kokonaiskypsyydeltään selkeästi tavoitetason alapuolelle.

Kuntasektorilla tulosten hajonta oli selvästi valtionhallintoa pienempää ja isoilla kaupungeilla havaittiin kypsyyden olevan pieniä kuntia parempi. Kaikilla arvioinnissa mukana olleilla kunnilla digitaalisen turvallisuuden kokonaiskypsyys jäi kuitenkin tavoitetason alapuolelle.

4 DIGITAALISEN TURVALLISUUDEN ARKKITEHTUURIN TAVOITETILA

Tavoitetiloihin on tyypillistä edetä kahdessa vaiheessa. Ensimmäinen eli välitavoite on tarkoituksenmukaista asettaa alle kolmen vuoden päähän ja varsinainen tavoitetila viiden tai kuuden vuoden päähän. Tavoitetiloihin pääsyä kannattaa seurata esimerkiksi toistamalla kypsyysarvioinnit 2-3 vuoden välein.

4.1 Digiturvallisuuden määritelmien tavoitetilat

Digitaalisuutta käsittelevien tai siihen liittyvien määritelmien ymmärtäminen yhteisellä tavalla on perusta johdonmukaiselle toiminnalle. Ilman sitä on vaikea arvioida kypsyyttä, tuottaa tai kehittää arkkitehtuuria ja tuotantoa sekä johtaa toimintaa. Ensimmäisessä vaiheessa luodaan perusta kansallisiin määritelmiin ja valmistellaan kansainvälinen ulottuvuus. Toisessa vaiheessa määritelmät on valtaosin huomioitu eri dokumenteissa ja kansainvälinen viestintä on toteutettu.

4.1.1 Digiturvallisuuden ja digitaalisen turvallisuuden arkkitehtuurin määritelmien välitavoitetila vuonna 2024

Digiturvallisuuden, digitaalisen turvallisuuden määrittely on vakiintunut hankkeissa ja selvityksissä. Digitaalisen turvallisuusarkkitehtuurin määrittelyt on tehty, ja niitä aletaan ottaa huomioon vuoden 2024 jälkeen tuotettujen tai päivitettyjen eri dokumenttien sisällössä.

Digiturvallisuus ja digitaalinen turvallisuus ovat synonyymejä. Lisäksi digitaalisen turvallisuuden suhteet ja merkitys muihin turvallisuusmääritelmiin ymmärretään yhtenäisesti. Keskeisimpiä turvallisuuden alueita tässä tapauksessa ovat kokonaisturvallisuus, kyberturvallisuus, tietoturvallisuus sekä tietosuoja.

4.1.2 Digiturvallisuuden ja digitaalisen turvallisuuden arkkitehtuurin määritelmien tavoitetila vuonna 2026

Tavoitetilassa digitaalisen turvallisuuden ja digitaalisen turvallisuuden arkkitehtuurin määritelmät ovat yhteisesti ymmärrettynä käytössä koko julkishallinnossa. Määritelmät noudattavat soveltuvin osin yhtenäistä kansainvälistä linjaa. Ne löytyvät esimerkiksi termipankeista.

4.2 Digitaalisen turvallisuuden arkkitehtuurin tavoitetilat

4.2.1 Digitaalisen turvallisuuden arkkitehtuurin välitavoitetila vuonna 2024

Digitaalinen arkkitehtuuri perustuu kansainvälisiin standardeihin tai niitä hyvin läheisesti noudattavaan malliin. Arkkitehdit on perehdytetty standardien tuomiin mahdollisuuksiin ja niitä osataan hyödyntää täysipainoisesti arkkitehtuurityössä. Standardeihin perustuvat ratkaisut ovat kansallisesti ja kansainvälisesti yhteensopivia sekä tuottavat tiedon hallinnan tueksi turvallisuusluokiltaan eritasoisia, kustannustehokkaita ja toimivia ratkaisuja.

Standardeihin tukeutuva malli antaa perusteet laatia tai tarkentaa nykyinen julkisen hallinnon digitaalisen turvallisuuden arkkitehtuuri. Arkkitehtuurin perusta on tuotettu ja sen pohjalta voidaan tarkastaa, suunnitella ja toteuttaa digitaalisen turvallisuuden arkkitehtuurin täyttäviä ratkaisuja. Arkkitehtuuri on joustava, mutta huomioi riittävät perusteet yhteisille palveluille sekä organisaatioiden omille kohdearkkitehtuureille.

Digiturvallisuuden arkkitehtuuri on tunnistettu osana kokonaisarkkitehtuuria. Sen avulla on alustavasti kuvattu organisaation turvallisuusprosessien, digiturvallisuusjärjestelmien ja henkilöstön rakenne sekä näiden suhde organisaation tavoitteeseen ja strategisiin suunnitelmiin. Digiturvallisuuden C2M2-mallin pohjalta tuotetut kypsyys on välitavoitetilassa vähintään tasolla kolme eli digiturvallisuuden arkkitehtuuri on tehty koko organisaatiolle. Julkiselle hallinnolle on luotu yhteinen digitaalisen turvallisuuden arkkitehtuurin kehikko, joka tukee julkisen hallinnon organisaatioiden digitaalisen turvallisuuden arkkitehtuurin määrittelyn ja samalla yhtenäistää julkisen hallinnon arkkitehtuurin hallintaa osana tiedonhallintakartan ja tiedonhallintamallien ylläpitoa.

4.2.2 Digitaalisen turvallisuuden arkkitehtuurin tavoitetila vuonna 2026

Digiturvallisuuden standardeihin perustuva malli on päivitetty kokemusten perusteella. Digitaalisen turvallisuuden arkkitehtuuri on käytössä johtamisen apuvälineenä ja se on selkeä osa kokonaisturvallisuusarkkitehtuuria.

Yhteisten palveluiden osalta digiturvallisuusarkkitehtuuri on riittävässä laajuudessa jaettu käyttäjien turvallisuusvastaaville. Arkkitehtuuria kehitetään yhteistyössä asiakasfoorumeissa. Toteutukset vastaavat arkkitehtuuria.

Julkishallinnolla on käytössään yhteinen arkkitehtuurin kehikko. Organisaatioiden omalla vastuulla olevat kohdearkkitehtuurit on laadittu tai päivitetty, ja ne tukeutuvat yhteisen arkkitehtuurin rakenteeseen.

Digiturvallisuuden arkkitehtuuri on toteutettu osana kokonaisarkkitehtuuria siten että sen avulla on kuvattu organisaation turvallisuusprosessien, digiturvallisuusjärjestelmien ja henkilöstön rakenne sekä näiden suhde organisaation tavoitteeseen ja strategisiin suunnitelmiin. Digiturvallisuuden C2M2-mallin pohjalta tuotetut kypsyys on jokaisella organisaatiolla tavoitetilassa vähintään tasolla 3,75 eli digiturvallisuuden arkkitehtuuri on laadittu ja sen toteutumista seurataan kokonaisvaltaisesti.

4.3 Strategisen johtamisen tavoitetilat

Strategisen johtaminen perustuu tavoitetilassa selkeisiin, turvallisesti tuotettuihin ratkaisuihin. Digiturvallisuuden arkkitehtuurista vastaavat tai sitä ohjaavat henkilöt tunnistavat koko viitekehyksen ja muun muassa siinä toimivat tahot, riskit, uhat, teknologiat, prosessit, tarpeet, ohjauksen sekä säädöspohjaiset määräykset ja muut ohjeet. Strategisesta johtamisesta vastaavat tahot osaavat ottaa digitaalisen turvallisuuden arkkitehtuurin mahdollisuudet huomioon johtamisprosesseissaan. Ylin johto osallistuu digiturvallisuuden hallinnan tavoiteasetantaan ja seurantaan säännöllisesti ja aktiivisesti.

4.3.1 Digiturvallisuuden ja digitaalisen turvallisuuden arkkitehtuurin strategisen johtamisen tavoitetila vuonna 2024

Strategisen johtamisen tavoitetilan määrittelyssä on hyödynnetty C2M2-kypsyyskyselyssä esitettyjä alueita ja tavoitteita. Tavoitetilassa organisaation johto tukee riskienhallintastrategia, digiturvallisuusstrategiaa sekä jatkuvuuden suunnittelua.

Riskienhallinnan toteuttamisessa hyödynnetään Tiedonhallintalautakunnan suosituksia. Riskienhallintastrategia on määritetty ja se on johdon hyväksymä. Digiturvallisuusriskit on huomioitu joko osana yhteistä tai omana riskienhallintastrategiaa. Välitavoitetilassa C2M2-mallin mukainen kypsyys on jokaisella organisaatiolla vähintään tasolla kolme eli digiturvallisuusriskienhallintastrategia on tehty koko organisaatiolle.

Digiturvallisuusriskien hallintajärjestelmä on toteutettu. Johto on osoittanut riittävät resurssit ja seuraa digiturvallisuusriskien tilannetta. Välitavoitetilassa C2M2-mallin mukainen kypsyys on jokaisella organisaatiolla vähintään tasolla kolme eli digiturvallisuusriskien hallinta on määritelty koko organisaatiolle.

Digiturvallisuusstrategia on laadittu, sillä se on digiturvallisuusohjelman perusta. Digiturvallisuusstrategia pitää sisällään vähintään listan digiturvallisuuden tavoitteista ja suunnitelman niiden saavuttamiseksi. Välitavoitetilassa C2M2-mallin mukainen kypsyys on jokaisella organisaatiolla vähintään tasolla kolme eli digiturvallisuusstrategia on tehty koko organisaatiolle sisältäen priorisoinnin ja lähestymistavan osana organisaation strategisia tavoitteita.

Johto tukee digiturvallisuuden hallintajärjestelmän jalkauttamista digiturvallisuusstrategian mukaisesti. Perustasolla tuki sisältää riittävät resurssit eli henkilöt, työkalut ja rahoituksen. Johto tukee organisaatiotasoisten poliitikkojen tai muiden organisaatiota velvoittavien ohjeistuksien määrittelyä ja ylläpitoa. Välitavoitetilassa C2M2-mallin mukainen kypsyys on jokaisella organisaatiolla vähintään tasolla kolme eli digiturvallisuuden hallintajärjestelmä on koko johdon hyväksymä vahvistettuna digiturvallisuuspolitiikkojen selkeällä omistajuudella.

Toiminnan jatkuvuuteen ja varautumiseen on kiinnitetty huomiota. Jatkuvuuden suunnittelu sisältää tarvittavat toimenpiteet kriittistentoimintojen ylläpitämiseksi keskeytysten aikana, kuten esimerkiksi merkittävien digiturvallisuus poikkeamien tai onnettomuuksien aikana. Toiminnan vaikutusanalyysit on tuotettu, koska niiden avulla organisaation on mahdollista tunnistaa olennaisimmat suojattavat

kohteet ja määritellä toipumistavoitteet. Jatkuvuussuunnitelmat on testattu ja päivitetty testausten perusteella, jotta niiden ajantasaisuus ja käyttökelpoisuus voidaan varmistaa. Välitavoitetilassa C2M2-mallin mukainen kypsyys on jokaisella organisaatiolla vähintään tasolla kolme eli jatkuvuuden suunnittelu on määritelty koko organisaatiolle ja siinä on huomioitu vaikutusanalyysit ja toipumisaikatavoite sekä toipumispisteen määritys (RTO/RPO).

4.3.2 Digiturvallisuuden ja digitaalisen turvallisuuden arkkitehtuurin strategisen johtamisen tavoitetila vuonna 2026

Tavoitetilassa riskienhallintastrategia on määritetty ja se on johdon hyväksymä. Tavoitetilassa C2M2-mallin mukainen kypsyys on jokaisella organisaatiolla vähintään tasolla 3,75 eli digiturvallisuusriskienhallintastrategia on laadittu, toteutettu ja edistymistä seurataan koko organisaatiossa. Lisäksi olisi suotavaa, että sitä seurataan systemaattisesti ja päivitetään säännöllisesti

Digiturvallisuusriskien hallintajärjestelmä on toteutettu. Johto on varmistanut, että käytössä on riittävät resurssit ja johto on seurannut digiturvallisuusriskien tilannetta. Tavoitetilassa C2M2-mallin mukainen kypsyys on jokaisella organisaatiolla vähintään tasolla 3,75 eli digiturvallisuusriskejä hallitaan kokonaisvaltaisesti ottaen myös huomioon digiturvallisuuden arkkitehtuuri. Lisäksi olisi tavoiteltavaa, että digiturvallisuusriskien hallintaa seurataan systemaattisesti ja kehitetään jatkuvasti osana koko organisaation riskienhallintaa.

Digiturvallisuusstrategia on laadittu korkeammalle tasolle. Korkeammalla kypsyystasolla digiturvallisuusstrategia on laajempi ja laadukkaampi sisältäen prioriteetit, hallintamallin kuvauksen, digiturvallisuuden hallintaorganisaation rakenteen ja vastuut sekä ylimmän johdon sitoutumisen ja osallistumisen hallinnan suunnitteluun ja järjestämiseen. Tavoitetilassa C2M2-mallin mukainen kypsyys on jokaisella organisaatiolla vähintään tasolla 3,75 eli digiturvallisuusstrategia on laadittu, toteutettu ja edistymistä seurataan koko organisaatiossa sisältäen hallintajärjestelmän. Lisäksi olisi tavoiteltavaa, että digiturvallisuusstrategiaa seurataan systemaattisesti ja päivitetään säännöllisesti ympäristön ja uhkien muuttuessa.

Tavoitetilassa johto tukee digiturvallisuuden hallintajärjestelmän jalkauttamista digiturvallisuusstrategian mukaisesti. Perustasolla on toteutettu riittävät resurssit, kuten henkilöt, työkalut sekä rahoitus. Kehittyneempi tuki sisältää ylimmän johdon näkyvän osallistumisen sekä vastuiden määrittelyn ja valtuutukset hallintajärjestelmälle. Lisäksi johdon tuki sisältää organisaatiotasoisen tuen politiikkojen tai muiden organisaatiota velvoittavien ohjeistuksien määrittelylle ja ylläpidolle. Tavoitetilassa C2M2-mallin mukainen kypsyys on jokaisella organisaatiolla vähintään tasolla 3,75 eli digiturvallisuuden hallintajärjestelmällä on johdon hyväksyntä ja aktiivinen tuki koko organisaatiossa. Johto nostaa säännöllisesti esille digiturvallisuuden tärkeyden. Digiturvallisuudesta vastuullisella on tarvittavat valtuudet rooliinsa. Lisäksi olisi tavoiteltavaa, että digiturvallisuuden hallintajärjestelmä on johdon aktiivisesti tukema ja jatkuvan kehityksen kohteena osana koko organisaation vaatimuksienhallintaa, mittaamista ja tavoiteasetantaa.

Toiminnan jatkuvuus ja varautuminen on toteutettu. Jatkuvuuden suunnittelu sisältää testatut tarvittavat toimenpiteet kriittistentoimintojen ylläpitämiseksi keskeytysten aikana. Toiminnan vaikutusanalyysit on tuotettu ja testattu. Jatkuvuussuunnitelmat on testattu ja päivitetty testausten perusteella, jotta niiden ajantasaisuus ja käyttökelpoisuus voidaan varmistaa. Tavoitetilassa C2M2-mallin mukainen kypsyys on jokaisella organisaatiolla vähintään tasolla 3,75 eli jatkuvuuden suunnittelu on määritelty koko organisaatiolle ja siinä on huomioitu vaikutusanalyysit ja toipumisaikatavoite sekä toipumispisteen määritys (RTO/RPO). Edellä mainitun lisäksi jatkuvuuden suunnittelua tehdään johdonmukaisesti koko organisaatiossa sisältäen säännölliset harjoitukset. Lisäksi olisi tavoiteltavaa, että jatkuvuuden suunnittelua tehdään järjestelmällisesti ja kehitetään riskilähtöisesti. Toiminnassa korostuu säännöllinen päivitys, riskilähtöiset RTO/RPO sekä suojattavien kohteiden päivitys.

5 SUOSITUKSET, MAHDOLLISUUDET JA TAVAT TAVOITTEIDEN SAAVUTTAMISEKSI

Tässä luvussa on kuvattu suosituksia digitaalisen turvallisuuden parantamiseksi ja tavoitellun kypsyystason saavuttamiseksi.

5.1 Esityksiä digiturvallisuuden määritelmään liittyvien tavoitteiden saavuttamiseksi

5.1.1 Esityksiä digiturvallisuuden ja digitaalisen turvallisuuden arkkitehtuurin määritelmien välitavoitetilan saavuttamiseksi vuonna 2024

Määrittelyiden osalta suositellaan, että määrittelyt viedään asteittain asianmukaisiin sanastoihin ja säädöksiin. Tarvittaessa määritelmät voidaan viedä lausuntokierrokselle. Heti hyväksymisne jälkeen määritelmät otetaan käyttöön uusissa dokumenteissa.

Digiturvallisuus tai digitaalinen turvallisuus sekä muut turvallisuuden käsitteet, kuten kokonaisturvallisuus, kyberturvallisuus, tietoturvallisuus sekä tietosuoja, ymmärrettiin eri tavoin digitaalisen turvallisuusviitekehyksen osalta.

Yhtenä määritelmien julkaisualustana voisi olla Turvallisuuskomitean ylläpitämä kyberturvallisuuden käsitteistö. Sen osalta täydennys voitaisiin tehdä osana seuraavaa päivityskierrosta. Lisäksi määritelmiä tulisi markkinoida eri turvallisuusalan foorumeissa myös ulkomaille.

5.1.2 Esityksiä digiturvallisuuden ja digitaalisen turvallisuuden arkkitehtuurin määritelmien tavoitetila saavuttamiseksi vuonna 2026

Tavoitetilaan pääsy edellyttää välitavoitteen saavuttamista. Määrätietoisesti tuotetuilla määritelmärekistereillä on mahdollista saada digitaalisen turvallisuuden ja digitaalisen turvallisuuden arkkitehtuurin määritelmät yleisesti käyttöön koko julkishallinnossa. Määritelmät noudattavat soveltuvin osin yhtenäistä kansainvälistä linjaa. Määritelmien osalta voidaan järjestää myös verkkokoulutusta. Digiturvallisuuden seuraavien maturiteettikyselyiden perusteella voidaan arvioida, kuinka hyvin tavoitteeseen on päästy.

5.2 Esityksiä digitaalisen turvallisuuden arkkitehtuurin tavoitteiden saavuttamiseksi

5.2.1 Esityksiä digitaalisen turvallisuuden arkkitehtuurin tavoitetilan saavuttamiseksi vuonna 2024

Digitaalisen turvallisuuden arkkitehtuuri voidaan rakentaa NIST-mallin pohjalle. Arkkitehtuuriosaamisen laajentaminen on mahdollista kurssittamalla nykyistä henkilökuntaa tai tukeutumalla ostopalveluihin. Edellä mainittujen seikkojen pohjalta olisi mahdollista saavuttaa kansallisesti ja kansainvälisesti yhteensopivia sekä tuottavat tiedon hallinnan tueksi turvallisuusluokiltaan eritasoisia, kustannustehokkaita ja toimivia ratkaisuja.

Valtionhallinnolle tulisi tuottaa joustava arkkitehtuurikehikko. Tätä työtä voisi johtaa valtiovarainministeriö. Mallista olisi hyvä järjestää organisaatioiden arkkitehtuurin vastuuhenkilöille koulutusta. Mallin voisi myös valmistella yhteisissä työpajoissa tai käyttää sitä lausuntokierroksella ennen julkaisua. Tämän jälkeen organisaatioiden omille kohdearkkitehtuureille olisi paremmat edellytykset.

Digiturvallisuuden uudelleen arvioinnin voisi tehdä C2M2-mallin pohjalta kahden tai kolmen vuoden jälkeen edellisestä.

5.2.2 Esityksiä digitaalisen turvallisuuden arkkitehtuurin tavoitetilan saavuttamiseksi vuonna 2026

Digiturvallisuuden standardeihin perustuvan mallin käyttöönottoa tuetaan. Digitaalisen turvallisuuden arkkitehtuuri on tuotettu ymmärrettävään muotoon, jotta sen on käytettävissä johtamisen apuvälineenä. Lisäksi julkishallinnon kokonaisarkkitehtuurin sisältöön tuodaan selkeämmin digiturvallisuusnäkökulmat.

Yhteisten palveluiden osalta digiturvallisuusarkkiturvallisuuden arkkitehtuuri voidaan jakaa käyttäjien turvallisuusvastaaville esimerkiksi työpajojen kautta. Arkkitehtuurin kehittäminen yhteistyössä asiakasfoorumeissa edellyttäisi vetovastuun ottamista. Myös julkishallinnon yhteistä arkkitehtuurikehikkoa voitaisiin työstää työpaja tai julkishallinnon arkkitehtuuritiimin voimin. Organisaatioiden omalla vastuulla olevien kohdearkkitehtuurien laadintaan voisi osoittaa koulutuksen lisäksi asiantuntijatukea.

Digiturvallisuuden uudelleen arvioinnin voisi tehdä C2M2-mallin pohjalta toisen kerran kahden tai kolmen vuoden jälkeen edellisestä.

5.3 Esityksiä strategisen johtamisen tavoitetilan saavuttamiseksi

5.3.1 Esityksiä strategisen johtamisen tavoitetilan saavuttamiseksi vuonna 2024

Riskienhallintastrategiasta voisi olla tarkoituksenmukaista tuottaa valtionhallinnon yhteinen pohja. Lisäksi riskinottohalukkuudesta voisi käydä laajempaa keskustelua niin organisaatioiden omien palveluiden kuin keskitetyn palvelun suhteen. Julkishallinnon digiturvallisuusriskien analysointiin ja priorisointiin sekä riskiluokittelussa ja -rekisterissä voisi harkita yhteisten nimittäjien käyttämistä.

Riskienhallintajärjestelmän laatu riippuu sen päivittämisestä sekä huomioimisessa toiminnassa. Sen pohjalta voidaan paremmin laatia mm. toiminnan jatkuvuuden vaatimuksia. Varautumisen perusta luodaan nimenomaan riskien ymmärtämisen kautta. Riskiarvioiden tulisi perustua faktoihin.

Digiturvallisuusstrategiaan liittyvän lista digiturvallisuuden tavoitteista voisi olla myös yhdessä pohdittava asia. Digitalisaation laajuutta ja vaikuttavuutta ei johto saisi aliarvioida, joten käytännönläheisiä esimerkkejä ja tiedottamista voitaisiin käyttää enemmän. Johdon osaamista ja sitoutumista digiturvallisuuteen tulee lisätä, jolloin riittävät resurssit eli henkilöt, työkalut ja rahoitus, olisi saatavissa riskinottopohjan mukaisesti. Digiturvallisuusstrategian rungon voisi tuottaa NIST-standardin pohjalta. Sen sisältöä tulisi kuitenkin vielä hioa valtionhallintoon sopivaksi, mutta välitavoitteessa se olisi jo todennäköisesti hyväksytty.

Organisaatioiden johdon perehdyttämistä poliitikkojen tai muiden organisaatiota velvoittavien ohjeistuksien hyväksymiseksi tulisi kehittää. Digiturvallisuuden hallintajärjestelmä tulisi nähdä olennaisena osana johtamista, myös kriisitilanteissa.

Toiminnan jatkuvuus ja varautuminen edellyttäisi voimassa olevien tai juuri valmistuvien päivityskierrosten jälkeen testaamista harjoituksin. Suunnitelmia tulisi ensin testata organisaatiokohtaisesti, jonka lisäksi olisi laajempia harjoituksia. Julkisessa hallinnossa on olemassa valmiita harjoitusorganisaatioita.

Digiturvallisuuden uudelleen arvioinnin voisi tehdä C2M2-mallin pohjalta kahden tai kolmen vuoden jälkeen edellisestä.

5.3.2 Esityksiä strategisen johtamisen tavoitetilan saavuttamiseksi vuonna 2026

Riskienhallintastrategia ja digiturvallisuuden hallintajärjestelmää päivitetään ottamalla huomioon muuttunut toimintaympäristö. Lisäksi johto voisi suunnata tavoitteita toimitusketjujen arviointiin ja niissä olevien riskien tunnistamiseen ja hallintaan. Huomiota voisi myös kehittää tapahtumien ja poikkeamien hallintaan, toiminnan jatkuvuuteen, uhkien ja haavoittuvuuksien hallintaan sekä tilannekuvaan.

Digiturvallisuusstrategia on mahdollista saada laajempialaiseksi ja laadukkaammaksi, kun sen sisällössä huomioidaan prioriteetit, hallintamallin kuvauksen, digiturvallisuuden hallintaorganisaation ra-

kenteet ja vastuut sekä ylimmän johdon sitoutumisen ja osallistumisen hallinnan suunnittelu ja järjestäminen. Työssä voisi käyttää yhteistä pohjaa joko valtionhallinnon tuottamana tai ulkopuoliseen apuun turvautuen.

Harvan organisaation johto pystyy viemään digiturvallisuuden hallintajärjestelmän jalkauttamisen digiturvallisuusstrategian mukaisesti yksin. Työ vaatisi tiimityöskentelyä, jossa koko organisaatio, erityisesti turvallisuusvastaavat, otettaisiin mukaan työhön. Ylimmän johdon näkyvä osallistuminen sekä vastuiden määrittely ja valtuutukset hallintajärjestelmälle ovat tärkeitä toiminnan onnistumisen kannalta.

Toiminnan jatkuvuus ja varautuminen vaativat testaamista ja testeissä saatujen kokemusten hyödyntämistä. Vaikutusanalyysit voidaan tehdä ensin organisaatioiden sisäisissä harjoituksissa, mutta myös keskitettyjen palveluiden osalta yhteisharjoittelulla olisi perusteet. Yhteisharjoituksia voitaisiin käyttää myös näkyvyyden lisäämiseen.

Digiturvallisuuden uudelleen arvioinnin voisi tehdä C2M2-mallin pohjalta kahden tai kolmen vuoden jälkeen edellisestä. Myös Julkri-, Katakri-, ISO- tai muita vastaavia auditointeja voisi suositella tavaksi selvittää digiturvallisuuden tila ja hoitaa seuranta.