DIGI- JA VÄESTÖTIETO-VIRASTO

Organisaation Digiturva-kysely

Raportti ja kehittämiskohteet

18.8.2021

Puh. **0295 536 000** (vaihde) | Yhteystiedot, katso **www.dvv.fi**

VAHTI / Rousku Kimmo (DVV) 18.8.2021

Sisällysluettelo

VAHTI / Rousku Kimmo (DVV)
18.8.2021

Organisaation Digiturvakysely

Digi- ja väestötietoviraston (jäljempänä DVV) tehtävänä on edistää julkisen hallinnon organisaatioiden tietoturvallisuuden, sekä laajemmin digitaalisen turvallisuuden, kehittämistä. Osana tätä tehtävää se vastaa Julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI) ja viiden VAHTI-asiantuntijaryhmän toiminnasta. Tässä toiminnassa on mukana yli 300 johdon edustajaa ja alan asiantuntijaa. Tämän lisäksi DVV vastaa JUDO-hankkeen (Julkisen hallinnon digitaalisen turvallisuuden kehittämisohjelma) toteuttamisesta. Hanke käynnistyi vuonna 2019, ja se jatkuu vuoden 2023 loppuun saakka.

VAHTI-johtoryhmä on koonnut tietoa valtionhallinnon tietoturvallisuudesta jo 2000-luvun alusta alkaen, ja vuodesta 2017 tietoa on kerätty laajemmin koko julkisen hallinnon tietoturvallisuudesta. Vuodesta 2019 lähtien digitaalisen turvallisuuden tilannetietoa on koottu ja tarkasteltu hallinnollisesta näkökulmasta.

Toteutettujen kyselyiden avulla on voitu selvittää, miten lainsäädäntö – esimerkiksi tietoturvallisuusasetus vuonna 2010, EU:n yleinen tietosuoja-asetus vuonna 2018 sekä tiedonhallintalaki vuonna 2020 – ovat vaikuttaneet organisaatioiden digitaalisen turvallisuuden osa-alueiden kehittymiseen. Kyselytuloksia on hyödynnetty VAHTI-työryhmien toiminnassa sekä JUDO-hankkeen eri projekteissa, muun muassa toteutettaessa henkilöstön osaamisen kehittämiseen liittyviä koulutuksia sekä tukimateriaaleja.

Organisaation Digiturvakyselyn ohella DVV on toteuttanut Henkilöstön Digiturvabarometria syyskuusta 2020 alkaen. Organisaation Digiturvakyselyn avulla pystymme seuraamaan, miten organisaatioiden hallinnollinen digiturvallisuus kehittyy, ja Henkilöstön Digiturvabarometrin avulla seuraamme digitaaliseen toimintaympäristöön liittyvää henkilöstön osaamista, koulutustarpeita, toteutuneita uhkia, luottamusta eri toimijoihin sekä mm. koronaviruspandemian vaikutusta työtehtävien hoitamiseen. Seuraavat barometritulokset julkaistaan lokakuun loppupuolella osana 25.–29.10.2021 järjestettävää Digiturvaviikkoa. Toivomme, että organisaatiot sijoittavat Digiturvabarometrin henkilöstön vastattavaksi esimerkiksi intranet-sivustoilleen. Linkki barometrikyselyyn löytyy täältä ja kesäkuussa julkaistut barometrin tulokset täältä.

DVV kehittää parhaillaan verkkopalvelua, jonka avulla voimme jatkossa toteuttaa organisaation digiturvakyselyn sekä muita vastaavia kyselyitä. Sen avulla vastaajaorganisaatioiden on mahdollista saada entistä ajantasaisempi kuva digitaalisen turvallisuutensa tilanteesta ja kehityksestä.

Lisätietoja kyselystä antaa:

VAHTI-pääsihteeri Kimmo Rousku, puh. 0295 53 5120, kimmo.rousku@dvv.fi

VAHTI / Rousku Kimmo (DVV) 18.8.2021

Johdon tiivistelmä ja suositus kehittämistoimenpiteistä

Kesäkuussa 2021 Digi- ja väestötietovirasto toteutti Organisaation Digiturvakyselyn, johon saatiin 128 vastausta julkisen hallinnon organisaatioilta.

Digitaalisen turvallisuuden osa-alueissa on tapahtunut kehittymistä

Digi- ja väestötietoviraston vastuulla oleva Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä (VAHTI) on toteuttanut vuodesta 2019 alkaen digitaaliseen turvallisuuteen liittyviä vuosikyselyitä. Digitaalinen turvallisuus kattaa riskienhallinnan, toiminnan jatkuvuuden ja varautumisen, tietoturvan, tietosuojan ja kyberturvallisuuden, joiden kaikkien tasapainoista kehittämistä tarvitaan digitaalisen ja fyysisen toimintaympäristön suojaamiseksi.

Vaikka tuoreinta kyselyä onkin päivitetty, se sisältää osin samoja kysymyksiä ja teemoja kuin edellinen vuoden 2019 Digiturvakysely. Tulosten perusteella voidaan todeta, että organisaatioiden hallinnollinen turvallisuus on kehittynyt jonkin verran parempaan suuntaan viime vuosina. Tätä ovat edesauttaneet esimerkiksi lainsäädännön kehittyminen, erityisesti EU:n yleinen tietosuoja-asetus 25.5.2018 ja tiedonhallintalaki 1.1.2020 ovat edellyttäneet laaja-alaista turvallisuuden kehittämistä. Lisäksi keväällä 2020 käynnistynyt koronaviruspandemia aiheutti merkittävän muutoksen julkisen hallinnon organisaatioiden toimintatavoissa, mikä on vastaavasti edellyttänyt digiturvan uudenlaista huomioimista. Viime vuoden puolella Digi- ja väestötietovirasto julkaisi aiheesta erillisen raportin Koronaviruspandemian vaikutukset digitaaliseen turvallisuuteen (linkki).

Suomi on ollut yksi globaaleista edelläkävijöistä etätyön ja digitaalisten palveluiden hyödyntämisessä koronaviruspandemian aikana. Tämä on ollut mahdollista korkean ICT-palvelujen hyödyntämistasomme ansiosta. Käytössä oleva tekninen infrastruktuuri sisältää luotettavat ja toimivat tietoliikenneyhteydet sekä päätelaitteet, minkä lisäksi digitaalisessa muodossa olevaa tietoa on saatavilla ja käyttäjät kykenevät hyödyntämään sitä korkean osaamistasonsa myötä. Vaikka globaalisti digitaaliseen toimintaympäristöön kohdistuvat hyökkäykset ovat merkittävästi kasvaneet – etenkin viimeisen 1,5 vuoden aikana – ne eivät ole muutamaa poikkeusta lukuun ottamatta aiheuttaneet Suomen julkisessa hallinnossa niin merkittäviä ongelmia kuin muissa valtioissa. Kyselyssä on kuitenkin selvästi havaittavissa, että vastaajat ovat tunnistaneet näitä erilaisia hyökkäyskeinoja.

Taulukko 1. Digiturvan osa-alueiden kehittyminen vuosien 2019 ja 2021 kyselyissä

	2019	2021
Riskienhallinta ja johtaminen	0,73	(0,67)
Johtaminen	-	0,65
Riskienhallinta	-	0,68
Toiminnan jatkuvuus	0,62	0,68
Tietoturvallisuus	0,70	0,78
Tietosuoja	0,70	0,81
Kyberturvallisuus	0,61	0,59
Keskiarvo	**0,68**	**0,70**

Mitä lähempänä arvoa 1, sitä paremmin organisaatio on itse arvioinut suoriutuneensa kyselyyn kuuluvissa väittämissä. Erityisesti toiminnan jatkuvuuden ja varautumisen (0,06 parannus), tietoturvallisuuden (0,08) ja tietosuojan (0,11) kehittyminen on edennyt toivotulla tavalla, mutta kysely osoittaa myös sen, että noin neljäsosalla organisaatioista on vielä selvästi kehitettävää.

Taulukon osalta tulee huomata, että vuoden 2019 kyselyssä riskienhallintaan ja johtamiseen liittyvät kysymykset olivat samassa osiossa, minkä lisäksi niiden sisältöä on oleellisesti muutettu. Myös kaikki kyberturvallisuuteen liittyvät kysymykset on uudistettu, ja muidenkin osa-alueiden kysymyksiä päivitetty jossain määrin.

Toimintaympäristön uhat alkaneet konkretisoitua vahvemmin

Digiturvan osa-alueiden lisäksi kyselyssä selvitettiin, miten erilaiset häiriöt, hyökkäykset, loukkaukset tai muut digimaailman poikkeamat ovat vaikuttaneet organisaatioiden toimintaan. Vuonna 2021 kolme eniten havainnoitua riskitilannetta olivat seuraavat:

1. Organisaation käyttämissä kriittisissä palveluissa on ollut tekninen häiriö, joka on *jonkin verran* haitannut organisaation toimintaa.

2. Organisaation käyttämissä kriittisissä palveluissa on ollut tekninen häiriö, joka on *merkittävästi* haitannut organisaation toimintaa.

3. Organisaation käytössä olevaan palveluun on kohdistunut henkilötietojen tietoturvaloukkaus, joka on edellyttänyt ilmoitusta valvontaviranomaiselle.

Tuloksista havaitaan, että onnistuneet hyökkäykset tai muut digi- ja kyberturvallisuuteen liittyvät riskit eivät ole suurin ongelmien aiheuttaja, vaan yleisimmin kohdataan erilaisia ICT-palveluiden toimintaan ja saatavuuteen liittyviä, pääosin teknisiä häiriöitä. Jotta näiltä voitaisiin välttyä jatkossa paremmin, meidän tulee kyetä toteuttamaan entistä vikasietoisempia palveluita siten, että priorisoimme yhteiskunnan ja organisaation toiminnan kannalta kriittisiä palveluita.

Luonnollisesti myös kyberuhat ovat nousussa. Eräs yllättävä, fyysisen maailman uhka on erilaisten päätelaitteiden (tietokoneet ja älylaitteet) varkaudet, joita 33 % vastaajaorganisaatioista on raportoinut, ja osalla niitä oli jopa yli 10 tapauksen verran. Koska jokainen laitevarkaus saattaa aiheuttaa henkilötietojen tietoturvaloukkauksen, niiden ennaltaehkäisyyn tulisi kiinnittää enemmän huomiota.

Muita keskeisiä kyselytuloksista tehtyjä havaintoja ovat (havainnot koskevat vuotta 2020 ja alkuvuotta 2021):

- 33 prosenttia organisaatioista ilmoittaa kohdanneensa vähintään yhden kriittisen tietoturvapoikkeaman, ja 72 prosenttia on ylipäätään kohdannut tietoturvapoikkeamia. Positiivisena havaintona voidaan silti todeta, että 28 prosenttia vastaajista ei ole raportoinut poikkeamista.

- 62 prosentille vastaajista erilaiset poikkeamat, hyökkäykset ja loukkaukset ovat aiheuttaneet välittömiä kustannuksia; 27 prosentilla summa jää alle 1000 euroon, mutta 23 prosentilla kulut vaihtelevat 1000–10 000 eurossa ja 10 prosentilla 10 000–100 000 eurossa. Näiden lukujen perusteella kyselyyn vastanneiden suorien kulujen kokoluokka voidaan arvioida vastausten keskiarvoista noin 2,3 miljoonan euron tietämille. Lukuun sisältyy kuitenkin epävarmuuksia, sillä 2 prosenttia vastaajista ilmoitti mittavista, jopa miljoonaluokan kuluista, ja näiden muutaman tapauksen summat voivat vaikuttaa merkittävästi laskentaan. Vastaajien suorien kustannusten arvioiden perusteella näyttäisi, että kustannukset on onnistuttu pitämään julkishallinnossa maltillisina. Laskelmissa ei kuitenkaan ole huomioitu välillisiä kustannuksia, eritasoisia resursseja uhkiin vastaamiseksi, ennakoivia panostuksia digiturvaan tai riskien erityispiirteitä. Merkille pantavaa on, että kunnat arvioivat poikkeamiin reagoimisen keskimäärin aiheuttaneen huomattavasti alhaisemmat kustannukset kuin muissa vastaajaryhmissä.

- 40 prosentilla organisaatioista salassa pidettäviä tietoja tai henkilötietoja on käsitelty luvattomilla laitteilla tai luvattomissa palveluissa, ja 2 prosentilla ohjeiden vastaiset käsittelykerrat ovat huomattavia ylittäen 30 tapauksen määrän.

- 91 prosenttia vastaajista on välttänyt haittaohjelmien pääsyn päätelaitteisiinsa. Loput 9 prosenttia raportoivat, että niiden päätelaitteisiin on päässyt haittaohjelma korkeintaan 5 kertaa. Voidaankin todeta, että päätelaitteiden suojaamisessa on onnistuttu varsin kattavasti, vaikka jokainen onnistunut hyökkäys voi johtaa laajamittaisiin vaikutuksiin.

- Palveluiden käytön estävät haittaohjelmat eivät ole kovin yleisiä; 89 prosenttia on välttynyt niiltä kokonaan. Lisäksi 10 prosenttia vastaajista on ilmoittanut 1–5 tapauksesta, ja loput (1 %) raportoivat 6–10 tapauksesta.

- Valtaosa vastaajaorganisaatioista on kokonaan välttynyt palvelunestohyökkäysten aiheuttamalta haitalta, jonkinasteista haittaa on kokenut 34 prosenttia ja merkittävää 13 prosenttia. Koronaviruspandemian aikana on globaalisti raportoitu palvelunestohyökkäysten määrän kasvamisesta.

- Kriittisiltä tietoturvahaavoittuvuuksilta on välttynyt 48 prosenttia vastaajista, ja yhtä suuri joukko (48 %) on kohdannut niitä 1–5 kertaa. Lisäksi 1 prosentti organisaatioista ilmoitti 6–10 tapauksesta ja 2 prosenttia raportoi, että kriittisiä

tietoturvahaavoittuvuuksia on ollut jopa 11–30 kertaa. Haavoittuvuuksien hallinta, eli niiden tunnistaminen ja korjaaminen, onkin jatkossa entistä kriittisempi prosessi, sillä erilaisten haavoittuvuuksien hyödyntäminen yleistyy koko ajan.

- 64 prosenttia vastaajista ei ole joutunut kielteisten vaikuttamisyritysten kohteeksi.
- 85 prosenttia on onnistunut välttymään räätälöidyiltä hyökkäyksiltä.

Kysely vahvistaa myös mediasta havaittua ilmiötä; kaikkia kyselyssä esille nostettuja uhkia on koettu ja osa organisaatioista on ollut selvästi muita laajamittaisemmin niiden kohteena. Tuloksista on havaittavissa myös se, että koronaviruspandemian aikana erityisesti sote-toimijoita on koeteltu erilaisten hyökkäysyritysten muodossa. Muillakin toimialoilla yksittäiset organisaatiot ovat saattaneet joutua erilaisten kampanjoiden ja vaikuttamisyritysten kohteeksi.

Keskeiset kehittämiskohteet

Kyselyn 15 taustakysymyksen ja 97 väittämän perusteella olemme nimenneet yhden yleisen sekä 18 yksilöityä kehittämiskohdetta. Alle on poimittu niistä keskeisimmät:

Yleinen kehittämiskohde

Koko organisaation läpäisevä riskienhallintaprosessi. Useimmat digitaalisen turvallisuuden osa-alueet ovat selkeästi kehittyneet kuluneen kahden vuoden aikana, lukuun ottamatta riskienhallintaa ja johtamista. Digitaalisen turvallisuuden johtaminen on kuitenkin avainasemassa kaiken turvallisuustyön toteuttamisessa ja kehittämisessä. Toimiakseen se edellyttää koko organisaation läpäisevää riskienhallintaprosessia ja menettelyitä aina johtoryhmästä henkilöstöön saakka. Kaikkien on osallistuttava jokapäiväisen toiminnan uhkien tunnistamiseen ja havaituista riskeistä ilmoittamiseen.

I. **Raportin kehittämiskohde 1**

Henkilöstön osaamisen ja koulutustarpeiden kartoittaminen. Jokaisella organisaatiolla tulisi olla selkeä suunnitelma siitä, mistä aiheista koulutetaan ja mistä muistutetaan esimerkiksi sisäisellä viestinnällä. Asioiden omaksumista ja muistamista edistää se, että niitä käsitellään pitkin vuotta. Asiantuntijoiden osaamistarpeet voivat poiketa muun henkilökunnan tarpeista. Suosittelemme osallistumaan Digiturvaviikkoon 25.–29.10.2021 (linkki), hyödyntämään Digiturvallinen elämä -verkkokoulutuksia tai -mobiilipeliä (linkki) sekä seuraamaan Digi- ja väestötietoviraston tuottamia verkkotilaisuuksia (linkki tapahtumakalenteriin).

II. **Raportin kehittämiskohde 2**

Harjoitustoiminnan kehittäminen. Mikäli organisaatio ei ole osallistunut yhteenkään TAISTO-harjoitukseen, se voi osallistua siihen joko marraskuussa 2021 varsinaisena harjoituspäivänä tai suorittaa digitalisoidun TAISTOmaatti-harjoituksen. Organisaation johdolla on kriittinen rooli erilaisten kriittisten häiriötilanteiden, hyökkäysten ja loukkausten hallinnan johtamisessa, ja siksi johdon ja asiantuntijoiden tulisi harjoitella yhdessä.

III. **Raportin kehittämiskohde 4**

Säännöllinen digitaalisen turvallisuuden tilanneraportointi organisaation johdolle sovitusti, kuitenkin vähintään vuosittain käyttäen tarkoitukseen sopivia mittareita. Osana mittaristoa ja vertailupohjaa voidaan hyödyntää esimerkiksi tämän kyselyn

tuloksia. Tarkastelussa tulee huomioida myös organisaation taloudelliset resurssit, käytettävissä oleva henkilöstö sekä osaaminen.

IV. **Raportin kehittämiskohde 7**
Etäkäyttöön liittyvien riskien arviointi sekä kattava VPN-yhteyksien ja monivaiheisen tunnistautumisen käyttöönotto.

V. **Raportin kehittämiskohde 8**
Toimiva varmuuskopiointi, jonka merkitys on kasvanut sitä mukaa kun lunnashaittaohjelmahyökkäykset ovat yleistyneet. Organisaation tulisi varmistaa säännöllisesti tehtävällä palautusharjoituksella kriittisten palveluiden ja niissä olevien tietojen saatavuus ja eheys – unohtamatta ulkoistettuja palveluja.

VI. **Raportin kehittämiskohde 9**
Kattavat lokitiedot ja niiden käytettävyys. Lokitietojen tärkeys on noussut useasta eri syystä; niiden avulla voidaan tunnistaa ja ennakoida organisaatioon kohdistuvia hyökkäyksiä, selvittää toteutuneita hyökkäyksiä ja varmistaa tietojen asianmukainen käyttö eri tietojärjestelmissä.

VII. **Raportin kehittämiskohde 14**
Uhkatilanteen seuranta ja siihen liittyvien riskien hallinta. Organisaatioiden toimintaympäristö on kaikilta osin muuttumassa nopeammin kuin koskaan aikaisemmin, ja lisäksi vauhti tuntuu kiihtyvän jatkuvasti. Tämä tarjoaa uudenlaisia teknologisia mahdollisuuksia kehittää organisaation toimintaa, mutta myös organisaatioon kohdistuvat uhat ovat merkittävässä muutoksessa. Jotta organisaatio voi hyödyntää mahdollisuuksia, tunnistaa uhat ja hallita niihin liittyvät riskit, sen tulee kyetä seuraamaan ja arvioimaan toimintaympäristönsä muutoksien vaikutuksia säännöllisesti. Tämän kyvykkyyden kehitystä voidaan työstää kokonaisuutena, jossa linkittyvät eri osa-alueista sekä kyberturvallisuus, että johtamisen tarpeet, kuin myös riskienhallinnan seurantatarpeet.

VIII. **Raportin kehittämiskohde 16**
Palveluiden vikasietoisuuden parantaminen. Eriasteiset tekniset häiriöt ovat keskeinen organisaation, sen asiakkaiden ja sidosryhmien toimintaa haittaava ongelma. Mitä enemmän toimintaa digitalisoidaan ja uutta teknologiaa otetaan käyttöön, sitä paremmin on huolehdittava palveluiden saatavuudesta ja varmistettava niiden vikasietoisuuden toteutuminen palveluiden kriittisyydelle annettujen vaatimusten mukaisesti. Tähän liittyy oleellisesti myös toimiva riskienhallinta ja ajan tasalla olevat jatkuvuus- ja valmiussuunnitelmat.

Koko raportti on luettavissa täältä (linkki). Raportin liitteeseen 1 on koottu kaikki kehittämistoimenpiteet.

1 Yhteenveto kyselytuloksista

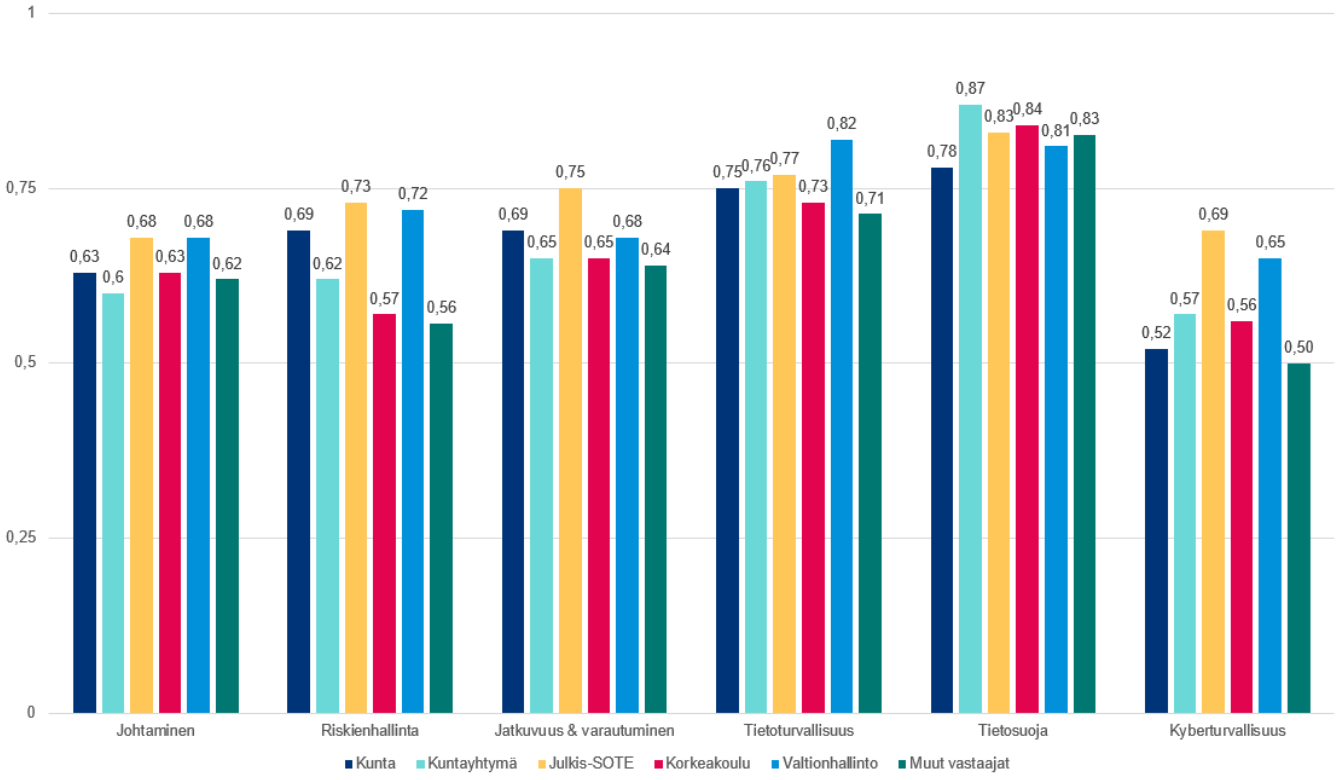
Tämä yhteenveto sisältää Digiturvakyselyn eri osa-alueiden keskiarvotulokset, keskeiset toimiala- ja osa-aluekohtaiset havainnot sekä tulosten perusteella esille nostetut 18 kehittämiskohdetta.

Digiturvakyselyssä 2021 oli 15 taustakysymystä sekä 97 varsinaista kysymystä, joiden avulla pyrittiin kartoittamaan vastaajaorganisaatioiden digitaalisen turvallisuuden tilannekuvaa. Rakenteeltaan Digiturvakysely jakautui seuraaviin osa-alueisiin: taustatiedot, johtaminen, riskienhallinta, toiminnan jatkuvuus ja varautuminen, tietoturvallisuus, tietosuoja, kyberturvallisuus ja havainnointi. Alla oleviin kaavioihin ja taulukoihin on koottu osa-alue- ja kysymyskohtaiset keskiarvot.

1.1 Osa-alueiden keskiarvot

Kuviossa 1 esitetään Digiturvakyselyn eri osioiden – *johtaminen, riskienhallinta, toiminnan jatkuvuus ja varautuminen, tietoturvallisuus, tietosuoja* ja *kyberturvallisuus* – vastausten keskiarvot asteikolla 0–1. Organisaatiot vastasivat annettuihin väittämiin neliportaisella asteikolla ja vastaukset on pisteytetty seuraavasti:

- kyllä (1)
- osittain (0,5)
- ei (0)
- ei koske meitä (vastausta ei huomioitu)



Kuvio 1. Digiturvakyselyn eri osioiden keskiarvot vastaajaryhmittäin

Vastaajaryhmät on muodostettu kyselyyn osallistuneiden organisaatioiden (yht. 128 organisaatiota) toimialajaottelun perusteella, ja ne ovat seuraavat:

- kunta (39 vastaajaa),
- kuntayhtymä (9 vastaajaa),
- julkishallinnon omistama sote-toimija (8 vastaajaa; taulukoissa ”Julkis-SOTE”),
- korkeakoulu (yliopisto/AMK; 11 vastaajaa),
- valtionhallinto (57 vastaajaa),
- välillinen julkishallinto (1 vastaaja),
- valtio- tai kuntaomisteinen yritys (1 vastaaja) ja
- joku muu (2 vastaajaa).

Kuviossa 1 kolme pienintä vastaajaryhmää eli välillinen julkishallinto (1 vastaaja), valtio- tai kuntaomisteinen yritys (1) ja jokin muu organisaatio (itsenäinen julkisoikeudellinen laitos ja rekisteröity yhdistys) on yhdistetty ”Muut vastaajat” -kuvaajan alaisuuteen selkeyden vuoksi. Kuitenkin raportin taulukoissa kolmen pienimmän vastaajaryhmän tulokset esitellään vain osana kaikkien vastausten kokonaiskeskiarvoa.

Kuvion 1 tiedot on esitetty alla taulukkomuodossa (taulukko 1). Lisäksi taulukkoon on sisällytetty yhteenlasketut, toimialakohtaiset keskiarvotilastot koko kyselyn osalta.

Taulukko 1. Digiturvakyselyn eri osioiden keskiarvot vastaajaryhmittäin

	128 KAIKKI	39 Kunta	9 Kunta-yhtymä	8 Julkis-SOTE	11 Korkea-koulu	57 Valtion-hallinto
Johtaminen	**0,65**	0,63	0,60	0,68	0,63	0,68
Riskienhallinta	**0,68**	0,69	0,62	0,73	0,57	0,72
Jatkuvuus & varautuminen	**0,68**	0,69	0,65	0,75	0,65	0,68
Tietoturvallisuus	**0,78**	0,75	0,76	0,77	0,73	0,82
Tietosuoja	**0,81**	0,78	0,87	0,83	0,84	0,81
Kyberturvallisuus	**0,59**	0,52	0,57	0,69	0,56	0,65
Keskiarvot	**0,70**	**0,68**	**0,68**	**0,74**	**0,66**	**0,73**

Voidaan havaita, että korkeimmat vastauskeskiarvot saavutettiin tietosuojan (kaikkien vastausten keskiarvo 0,81) ja matalimmat kyberturvallisuuden (0,59) alueilla. Välimaastoon asettuvat tietoturvallisuus (0,78), riskienhallinta (0,68), toiminnan jatkuvuus ja varautuminen (0,68) sekä johtaminen (0,65).

Kaikkien vastaajien osalta kyselyn keskiarvotulos on 0,70. Korkein vastauskeskiarvo on julkishallinnon omistamilla sosiaali- ja terveysalan toimijoilla (0,74), jota seuraa kyselyn suurin vastaajaryhmä eli valtionhallinto (0,73). Muut vastaajat jäävät hieman yhteiskeskiarvon alapuolelle: kunnat ja kuntayhtymät saavuttavat kumpikin saman tuloksen (0,68), ja viimeisenä ovat korkeakoulut (0,66). Tulos on hyvin samansuuntainen aikaisempina vuosina saatujen tulosten kanssa, mutta yleishavaintona voidaan todeta, että tilanne on viimeisten vuosien aikana jonkin verran parantunut.

Koska Digiturvakyselyn viimeinen osio poikkeaa vastausrakenteeltaan muista, sen tuloksia eli vastaajaorganisaatioiden havainnoimia ja raportoimia digiturvauhkia analysoidaan erikseen luvussa 1.2.7.

1.2 Kysymyskohtaiset keskiarvot

Taulukoissa 2–8 eritellään Digiturvakyselyn osa-alueiden – *johtaminen, riskienhallinta, jatkuvuus ja varautuminen, tietoturvallisuus, tietosuoja, kyberturvallisuus* ja *havainnointi* – kysymyskohtaiset vastauskeskiarvot sekä kaikkien vastaajien osalta että toimialakohtaisesti. Taulukot on lajiteltu siten, että korkeimmat yhteispisteet ovat aina ylimpinä. Asteikko ja vastaajaryhmittely noudattelevat edellisessä osiossa kuvattuja periaatteita. Tyhjät kentät ilmoittavat tilanteesta, jossa vastaaja on valinnut vaihtoehdon ”Ei koske meitä”. Vertailtavuuden parantamiseksi toimialakohtaiset vastausmäärät on toistettu kunkin taulukon otsikkorivillä.

1.2.1 Johtaminen

Taulukossa 2 esitetään johtamisosion 13 väittämän vastauskeskiarvot. Keskitymme tuloksissa vain kuntien, kuntayhtymien, julkis-soten, korkeakoulujen sekä valtionhallinnon tulosten arviointiin, koska muilta toimialoilta saatiin vain muutama yksittäinen vastaus.

Taulukko 2. Johtaminen – kysymyskohtaiset keskiarvot

		128 KAIKKI	39 Kunta	9 Kunta-yhtymä	8 Julkis-SOTE	11 Korkea-koulu	57 Valtion-hallinto
4.11	Organisaatiolla on olemassa prosessi väärinkäytöksiin reagoimiseksi	0,82	0,83	0,78	0,88	0,91	0,80
4.3	Organisaatio on kartoittanut sen digitaalista turvallisuutta ohjaavan lainsäädännön ja tunnistanut siitä aiheutuvat velvoitteet	0,82	0,78	0,83	0,81	0,82	0,85
4.7	Organisaation johto on sitoutunut digitaalisen turvallisuuden kehittämiseen	0,79	0,78	0,72	0,88	0,73	0,80
4.2	Organisaation tehtävät ja vastuut on tunnistettu ja kuvattu selkeästi	0,78	0,74	0,56	0,81	0,82	0,82
4.13	Digitaalisen turvallisuuden tilaa seurataan jatkuvasti	0,72	0,73	0,72	0,69	0,82	0,71
4.9	Henkilöstölle on olemassa riittävä ohjeistus digitaalisesta turvallisuudesta	0,72	0,69	0,67	0,69	0,77	0,74
4.14	Digitaalisen turvallisuuden kokonaistilanteesta raportoidaan säännöllisesti organisaation johdolle	0,70	0,67	0,56	0,75	0,55	0,77
4.10	Henkilöstölle annetaan säännöllisesti koulutusta digitaalisesta turvallisuudesta	0,66	0,64	0,56	0,69	0,50	0,75
4.4	Organisaatio on kartoittanut keskeiset sidos- ja asiakasryhmät sekä niiltä tulevat digiturvavaatimukset	0,66	0,54	0,67	0,81	0,68	0,71
4.8	Organisaation digitaalisen turvallisuuden osa-alueita kehitetään järjestelmällisesti hyödyntäen yhtä tai useampaa selkeää prosessia tai hallintamallia	0,54	0,55	0,56	0,44	0,41	0,56
4.6	Organisaatiolla on riittävä budjetti digiturvallisuuden ylläpitoon ja kehittämiseen	0,50	0,46	0,50	0,56	0,41	0,54
4.5	Organisaatiossa on riittävästi osaavaa henkilöstä kehittämässä digiturvallisuuden eri osa-alueita	0,46	0,44	0,50	0,44	0,45	0,48
4.12	Digitaaliseen turvallisuuteen liittyvät mittarit, joiden avulla organisaatio voi seurata osa-alueiden kehittymistä on määritelty	0,31	0,32	0,22	0,44	0,36	0,30
	YHTEENSÄ	**0,65**	**0,63**	**0,60**	**0,68**	**0,63**	**0,68**

Parhaimmat kysymyskohtaiset keskiarvot ovat kysymyksissä 4.11 sekä 4.3 (KA 0,82); vastaajilla on prosessit väärinkäytöksiin reagoimiseksi, ja digitaalista turvallisuutta ohjaavan lainsäädännön velvoitteet on tunnistettu. Heikointa suoriutuminen on kysymyksessä 4.12 (KA 0,31), eli vain harvalla on mittaristo digitaalisen turvallisuuden kehittymisen seurantaan. Lisäksi kysymykset 4.5 ”Organisaatiolla on riittävä budjetti digiturvallisuuden ylläpitoon ja kehittämiseen” ja 4.6 ”Organisaatiossa on riittävästi osaavaa henkilöstä kehittämässä digiturvallisuuden eri osa-alueita” osoittavat, että resurssien kanssa tuskaillaan useassa eri organisaatiossa.

Osa-alueen kokonaiskeskiarvo (0,65) on digiturvallisuuden viidestä osa-alueesta toiseksi matalin, ja erot toimialojen kesken ovat pienimmät: Julkis-SOTE (0,68) ja valtionhallinto (0,68) saavuttavat korkeimmat keskiarvot, seuraavina tulevat kunta (0,65) ja korkeakoulu (0,63). Matalin keskiarvo on kuntayhtymillä (0,60).

1.2.1.1 Johtamisen kehittämiskohteet

- **Kehittämiskohde 1**
  Henkilöstön osaamisen ja koulutustarpeiden kartoittaminen. Jokaisella organisaatiolla tulisi olla selkeä suunnitelma siitä, mistä aiheista koulutetaan ja mistä muistutetaan esimerkiksi sisäisellä viestinnällä. Asioiden omaksumista ja muistamista edistää se, että niitä käsitellään pitkin vuotta. Asiantuntijoiden osaamistarpeet voivat poiketa muun henkilökunnan tarpeista. Suosittelemme osallistumaan Digiturvaviikkoon 25.–29.10.2021 (linkki), hyödyntämään Digiturvallinen elämä -verkkokoulutuksia tai -mobiilipeliä (linkki) sekä seuraamaan Digi- ja väestötietoviraston tuottamia verkkotilaisuuksia (linkki tapahtumakalenteriin).

- **Kehittämiskohde 2**
  Harjoitustoiminnan kehittäminen. Mikäli organisaatio ei ole osallistunut yhteenkään TAISTO-harjoitukseen, se voi osallistua siihen joko marraskuussa 2021 varsinaisena harjoituspäivänä tai suorittaa digitalisoidun TAISTOmaatti-harjoituksen. Organisaation johdolla on kriittinen rooli erilaisten kriittisten häiriötilanteiden, hyökkäysten ja loukkausten hallinnan johtamisessa, ja siksi johdon ja asiantuntijoiden tulisi harjoitella yhdessä.

- **Kehittämiskohde 3**
  Prosessit kuntoon. Tärkeimpien prosessien kuvaaminen, jalkauttaminen ja harjoittelu sekä harjoittelun perusteella tapahtuva prosessien kehittäminen kaikilla digitaalisen turvallisuuden osa-alueilla.

- **Kehittämiskohde 4**
  Säännöllinen digitaalisen turvallisuuden tilanneraportointi organisaation johdolle sovitusti, kuitenkin vähintään vuosittain käyttäen tarkoitukseen sopivia mittareita. Osana mittaristoa ja vertailupohjaa voidaan hyödyntää esimerkiksi tämän kyselyn tuloksia. Tarkastelussa tulee huomioida myös organisaation taloudelliset resurssit, käytettävissä oleva henkilöstö sekä osaaminen.

1.2.1.2 Kehitys Digiturvakyselyyn 2019 verrattuna

Vuoden 2019 Digiturvakyselyn riskienhallinta ja johtaminen osa-alueella toiseksi huonoin tulos (0,57) saavutettiin väittämässä ”Organisaation käytössä ovat digiturvallisuuden eri osa-alueiden toteuttamisessa tarvittavat talous- ja henkilöstöresurssit”.

Myös vuoden 2021 tulosten perusteella sekä taloudelliset resurssit että henkilöstön osaaminen tulee ottaa huomioon vuosisuunnittelussa ja raportoinnissa.

Digiturvakyselyssä 2021 on erilliset kysymykset jatkuvuudenhallinnan (6.8), tietosuojan (8.12) sekä kyberturvallisuuden (9.6 ja 9.9) riskienhallinnasta. Näissäkin tulokset ovat alhaiset (keskiarvot 0,51–0,61), mutta oletettavasti sääntelyn vaatimuksista johtuen tietosuojan osa-alue on hieman parempi kuin muut. Myös nämä riskit ovat osa organisaation riskienhallinnan kokonaisuutta, ja ne tulee ottaa huomioon seurannassa, raportoinnissa ja riskien käsittelytoimissa. Kohdennettuja arviointeja voidaan tehdä vastaavasti myös muihin osa-alueisiin. Useimpiin kyselyn kysymyksiin liittyy jokin riski ja etenkin niihin liittyvien uhkien tulisi näkyä organisaatioiden omissa riskiarvioissa.

1.2.2 Riskienhallinta

Taulukossa 3 esitetään riskienhallinnan kahdeksan väittämän vastauskeskiarvot.

Taulukko 3. Riskienhallinta – kysymyskohtaiset keskiarvot

		128 KAIKKI	39 Kunta	9 Kunta-yhtymä	8 Julkis-SOTE	11 Korkea-koulu	57 Valtion-hallinto
5.5	Kriittisistä, organisaation toimintaa uhkaavista riskeistä raportoidaan johdolle välittömästi	0,90	0,91	0,89	0,94	0,73	0,93
5.1	Organisaatiolla on johdon hyväksymät, toimintaan sovitetut riskienhallinnan linjaukset, vastuut ja prosessi	0,75	0,72	0,78	0,63	0,64	0,84
5.3	Organisaatiossa viestitään digiturvallisuuden riskitilanteesta ja uusista riskeistä koko organisaation laajuisesti	0,75	0,78	0,78	0,69	0,64	0,76
5.8	Organisaatiossa kehitetään riskienhallintaprosessia riskienhallinnan tavoitteiden ja saatujen kokemusten perusteella	0,73	0,76	0,61	0,88	0,68	0,73
5.4	Organisaatiossa raportoidaan riskitilanteesta johdolle säännöllisesti	0,69	0,65	0,50	0,88	0,55	0,75
5.6	Organisaatio seuraa riskien ja niiden hallintatoimenpiteiden tilannetta säännöllisesti	0,62	0,65	0,50	0,69	0,59	0,63
5.2	Organisaatio tekee digiturvallisuuteen liittyvää säännöllistä riskienarviointia, jossa huomioidaan uudet ilmiöt, toimintaympäristön muutokset ja oman toiminnan vaikutukset sidosryhmien ja asiakkaiden tilanteeseen	0,52	0,53	0,39	0,63	0,50	0,53
5.7	Organisaatiossa arvioidaan jäännösriskejä riskienhallintatoimenpiteiden toteuttamisen jälkeen ja jäännösriskit käsitellään asianmukaisella tasolla	0,52	0,54	0,50	0,50	0,27	0,54
	YHTEENSÄ	**0,68**	**0,69**	**0,62**	**0,73**	**0,57**	**0,72**

Korkein kysymyskohtainen keskiarvo saavutettiin kohdassa 5.5 (KA 0,90), eli vastaajat raportoivat kriittisistä riskeistä johdolle välittömästi. Heikoimmaksi tulos jää kysymyksessä 5.7 (0,52) eli organisaatioilla on kehitettävää jäännösriskien arvioinnissa ja käsittelyssä sekä 5.2 (0,52) Organisaatio tekee digiturvallisuuteen liittyvää säännöllistä riskienarviointia, jossa huomioidaan uudet ilmiöt, toimintaympäristön muutokset ja oman toiminnan vaikutukset sidosryhmien ja asiakkaiden tilanteeseen.

Osa-alueen keskiarvo on 0,68. Toimialakohtaisesti erot ovat kohtalaisen suuret, sillä korkein keskiarvo on julkisomisteisilla sote-toimijoilla (0,73) ja matalin korkeakouluilla (0,57). Muut toimialakohtaiset keskiarvot asemoituivat seuraavasti: valtionhallinto (0,72), kunta (0,69) ja kuntayhtymä (0,62).

1.2.2.1 Riskienhallinnan kehittämiskohteet

- **Kehittämiskohde 5**
  Digitaalisen toimintaympäristön riskienhallinnan kokonaisvaltainen kehittäminen ja ulottaminen erilaisiin toimijoihin. Riskien arviointia toteutetaan järjestelmällisesti kaikissa keskeisissä muutoksissa, häiriöissä ja poikkeamissa – niin sisäisissä kuin ulkoisissa. Vähintäänkin tulee arvioida, onko laajempi analyysi tarpeen. Vain kerran vuodessa tehtävästä riskien arvioinnista on syytä päästä useammin toteutettavaan muutosarviointiin ja uusien riskien tunnistamiseen. Prosessiin voidaan yhdistää seurantatoimet ja jäännösriskien tarkastelu. Tiheämpi toistuvuus tukee osaamisen kehittymistä, pitää kuormituksen pienempänä sekä tukee johtamista paremmalla tilannetietoisuudella. Muutosten ja riskitasojen seurannan raportointia ja mittarointia voi kehittää osana johtamisen kehittämiskohdetta 4.

1.2.2.2 Kehitys Digiturvakyselyyn 2019 verrattuna

Kyselyn tulos on verrannollinen vuoden 2019 Digiturvakyselyyn, jossa riskienhallintaa ja johtamista tarkasteltiin yhtenä kokonaisuutena. Toimialakohtaiset keskiarvot olivat silloin seuraavat:

Sairaanhoitopiirit	0,83
Valtionhallinto	0,79
Kunnat	0,67
Yliopistot	0,63
Keskiarvo	**0,73**

Vaikka tulokset ovat samansuuntaiset, tulee huomata, että kyselyiden väittämät ja vastaajien ryhmittely eroavat jonkin verran toisistaan.

Vuoden 2019 Digiturvakyselyn huonoin tulos (KA 0,55) saavutettiin kysymyksessä ”Riskienarvioinnin tuloksia hyödynnetään johtamisessa ja päätöksenteossa, jäännösriskien käsittely on toimivaa”. Kun riskienhallintaa kehitetään kokonaisvaltaisesti, tulee samalla huolehtia mahdollisista prosessiin liittyvien puutteiden korjaamisesta käytettyjen menetelmien, jäännösriskien hallinnan ja raportoinnin osalta.

1.2.3 Toiminnan jatkuvuus ja varautuminen

Taulukossa 4 esitetään toiminnan jatkuvuus ja varautuminen -osion 16 väittämän vastauskeskiarvot.

Osion kaikkien vastausten keskiarvo on 0,68. Korkeimmat kysymyskohtaiset keskiarvot ovat kohdissa 6.11 ja 6.14 (KA 0,88), eli vastaajilla on viestintäsuunnitelma häiriö- ja kriisitilanteiden varalle ja organisaatiot myös kykenevät ilmoittamaan viranomaisille mahdollisista häiriö- ja kriisitilanteista. Matalin keskiarvo on kohdassa 6.8 (KA 0,53), joka koskee jatkuvuuteen liittyvien riskien ja niiden muutosten seurantaa.

Toimialoittain korkeimpaan keskiarvoon yltävät julkisomisteiset SOTE-toimijat (0,75), seuraavina tulevat kunta (0,69) ja valtionhallinto (0,68), kun taas kuntayhtymä (0,65) ja korkeakoulu (0,65) saavat matalimmat keskiarvot.

Taulukko 4. Toiminnan jatkuvuus ja varautuminen – kysymyskohtaiset keskiarvot

		128 KAIKKI	39 Kunta	9 Kunta-yhtymä	8 Julkis-SOTE	11 Korkea-koulu	57 Valtion-hallinto
6.11	Organisaatiolla on häiriö- ja kriisitilanteiden viestintäsuunnitelma	0,88	0,91	0,78	0,94	0,95	0,85
6.14	Organisaatiolla on olemassa menettely sen toimintaan kohdistuvien häiriöiden, hyökkäysten ja loukkausten ilmoittamiseksi keskeisille viranomaisille	0,88	0,92	0,89	0,88	0,86	0,83
6.1	Organisaation tehtävät ja vastuut ovat selkeät myös poikkeustilanteissa ja -oloissa	0,77	0,79	0,67	0,94	0,82	0,77
6.5	Organisaatio on tunnistanut sen toiminnan kannalta kriittiset toiminnot, palvelut, tiedot, tietovarannot ja tietojärjestelmät	0,77	0,78	0,83	0,75	0,68	0,79
6.2	Organisaatiolla on prosessi ja valmiudet nopeaan ja tehokkaaseen digiturvallisuuden häiriöiden, uhkien ja poikkeamien käsittelyyn	0,74	0,78	0,72	0,88	0,73	0,71
6.13	Organisaatiossa on luotu yhteydet ja verkostot tarvittavien sidosryhmien väliseen viestintään poikkeamatilanteissa	0,69	0,71	0,61	0,69	0,68	0,70
6.16	Jatkuvuus-, toipumis- ja viestintäsuunnitelmia päivitetään harjoitusten tai toteutuneiden häiriötilanteiden perusteella	0,66	0,72	0,61	0,63	0,55	0,66
6.12	Suunnitelmien sisältö on koulutettu häiriötilanteiden hallintaan osallistuville henkilöille	0,66	0,68	0,56	0,69	0,73	0,64
6.7	Toiminnan jatkuvuuden edellyttämät palvelutasovaatimukset ovat osa hankintavaatimuksia ja sopimuksia.	0,66	0,60	0,78	0,81	0,68	0,68
6.4	Organisaatio on tunnistanut ja dokumentoinut suojattavat kohteet	0,66	0,69	0,61	0,63	0,64	0,67
6.3	Organisaatio on kuvannut jatkuvuuden hallinnan periaatteet, tavoitteet, organisoinnin ja vastuut	0,64	0,67	0,56	0,75	0,59	0,63
6.10	Kriittisille tietojärjestelmille on laadittu toipumissuunnitelmat	0,61	0,58	0,56	0,75	0,55	0,64
6.15	Organisaatio harjoittelee säännöllisesti sen toimintaan kohdistuvien häiriöiden, poikkeamien ja hyökkäysten havainnointia, reagointia ja johtamista	0,59	0,55	0,44	0,50	0,64	0,62
6.6	Organisaatio on määritellyt, kuinka pitkiä toimintakatkoksia kriittiset toiminnot sietävät organisaation toiminnan häiriintymättä	0,55	0,59	0,61	0,75	0,50	0,52
6.9	Organisaatiolle ja sen kriittisille toiminnoille/palveluille on laadittu jatkuvuussuunnitelmat, jotka perustuvat tunnistettuihin riskeihin	0,55	0,51	0,61	0,56	0,45	0,59
6.8	Jatkuvuuteen liittyviä riskejä ja riskitilanteen muutosta arvioidaan säännöllisesti	0,53	0,58	0,50	0,81	0,32	0,53
	YHTEENSÄ	**0,68**	**0,69**	**0,65**	**0,75**	**0,65**	**0,68**

1.2.3.1 Toiminnan jatkuvuuden ja varautumisen kehittämiskohteet

- **Kehittämiskohde 6**
  Harjoitustoiminnan kehittäminen ja ylläpito. Vastaajista 24 % ei harjoittele säännöllisesti, eikä 14 % päivitä harjoitusten perusteella olemassa olevia suunnitelmiaan. Koska erilaisten häiriöiden, hyökkäysten ja loukkausten määrä tulee tulevaisuudessa kasvamaan ja vaikutus laajentumaan, harjoittelemalla varautuminen on entistäkin tärkeämpää.

- **Kehittämiskohde 16**
  Palveluiden vikasietoisuuden parantaminen. Eriasteiset tekniset häiriöt ovat keskeinen organisaation, sen asiakkaiden ja sidosryhmien toimintaa haittaava

ongelma. Mitä enemmän toimintaa digitalisoidaan ja uutta teknologiaa otetaan käyttöön, sitä paremmin on huolehdittava palveluiden saatavuudesta ja varmistettava niiden vikasietoisuuden toteutuminen palveluiden kriittisyydelle annettujen vaatimusten mukaisesti. Tähän liittyy oleellisesti myös toimiva riskienhallinta ja ajan tasalla olevat jatkuvuus- ja valmiussuunnitelmat.

1.2.3.2 Kehitys Digiturvakyselyyn 2019 verrattuna

Vuoden 2019 Digiturvakyselyssä osa-alueen keskiarvot olivat:

Sairaanhoitopiirit	0,79
Valtionhallinto	0,65
Kunnat	0,60
Yliopistot	0,42
Keskiarvo	**0,62**

Vuoden 2019 tuloksiin verrattuna on syytä huomata, että etenkin yliopistot ovat selvästi nostaneet keskiarvoaan. Vuoden 2021 kyselyssä yliopistotoimiala on kuitenkin laajennettu korkeakouluksi, jolloin mukaan on laskettu myös ammattikorkeakoulut. Sairaanhoitopiirit (nyk. julkis-SOTE) ovat säilyttäneet pienen etumatkan muihin toimialoihin, mikä on ymmärrettävää, kun otetaan huomioon toimialan kriittinen merkitys koko yhteiskunnalle.

Vuoden 2019 Digiturvakyselyn toiminnan jatkuvuus ja varautuminen osa-alueella huonoin tulos (KA 0,27) saatiin väittämässä ”Organisaation toiminnalle kriittisten järjestelmien toipumissuunnitelmia on harjoiteltu kahden viime vuoden aikana”. Tältä osin voidaankin havaita merkittävä parannus, sillä väittämän 6.15 ”Organisaatio harjoittelee säännöllisesti sen toimintaan kohdistuvien häiriöiden, poikkeamien ja hyökkäysten havainnointia, reagointia ja johtamista” keskiarvo on 0,59.

Näin merkittävää parantumista (0,27 vs. 0,59) voidaan selittää muun muassa vuonna 2018 käynnistyneillä TAISTO-harjoituksilla, joihin on osallistunut yli 300 julkisen hallinnon organisaatiota. Kannustamme kaikkia organisaatioita, myös yrityksiä, harkitsemaan osallistumista vuosittaisiin TAISTO-harjoituspäiviin tai digitalisoituun TAISTO-maatti-harjoitukseen.

1.2.4 Tietoturvallisuus

Osion 16 väittämän vastauskeskiarvot esitetään taulukossa 5. Kyselyn osa-alueista tietoturvallisuus yltää kokonaiskeskiarvollaan (0,78) toiseksi korkeimmalle sijalle tietosuojan (0,81) jälkeen. Hyvää tulosta selittää se, että kaikista digiturvallisuuden osa-alueista tietoturvallisuutta on kehitetty pisimpään ja sitä koskeva lainsäädäntö on laajentunut koskemaan koko julkista hallintoa vuoden 2020 alussa.

Kysymyksistä paras kokonaiskeskiarvo on kohdassa 7.10 (0,95) eli lähes jokainen organisaatio varmuuskopioi tietonsa säännöllisesti. Vaatimattomin tulos on sen sijaan kohdassa 7.11 (0,55); varmuuskopioinnista huolimatta niiden palautusten testaaminen ei ole yhtä yleistä. Lisäksi 7.14 ”Tietoturvallisuuteen ja tietojärjestelmiin liittyviä auditointeja tehdään säännöllisesti” (0,56) on ollut pitkään selkeä kehittämiskohde.

Toimialoista korkein keskiarvo on valtionhallinnolla (0,82), jota seuraavat julkis-SOTE (0,77), kuntayhtymä (0,76), kunta (0,75) ja korkeakoulu (0,73). Toimialojen väliset keskiarvoerot ovat toiseksi pienimmät.

Taulukko 5. Tietoturvallisuus – kysymyskohtaiset keskiarvot

		128 KAIKKI	39 Kunta	9 Kunta-yhtymä	8 Julkis-SOTE	11 Korkea-koulu	57 Valtion-hallinto
7.10	Organisaation tiedoista ja järjestelmistä otetaan säännöllisesti varmuuskopiot	0,95	0,97	1,00	0,94	0,91	0,93
7.1	Organisaatiolla on johdon hyväksymä tietoturvapolitiikka tai vastaava tietoturvallisuuden toteuttamista ohjaava asiakirja	0,93	0,95	0,83	0,94	1,00	0,92
7.9	Organisaatiolla on olemassa tarvittavat tekniset ratkaisut ja menettelyt haittaohjelmien tunnistamiseen ja torjuntaan	0,92	0,90	0,94	0,88	0,91	0,96
7.13	Käytössä olevien tietojärjestelmien teknisiin haavoittuvuuksiin liittyviä tiedotteita seurataan ja niihin reagoidaan	0,89	0,86	0,94	0,94	0,95	0,88
7.6	Organisaation tietojärjestelmät ja laitteet ovat kattavasti järjestelmänhallinnan piirissä	0,88	0,87	0,89	0,75	0,91	0,91
7.16	Tietoturva- ja tietosuojavaatimukset otetaan huomioon myös järjestelmien ja palveluiden kehittämisessä sekä ylläpidossa	0,85	0,85	0,89	0,81	0,86	0,84
7.15	Tietoturva- ja tietosuojavaatimukset ovat osa hankintavaatimuksia ja sopimuksia.	0,85	0,78	0,89	0,81	0,86	0,91
7.8	Toimitilojen ulkopuolella työskenneltäessä yhteydet organisaation ICT-palveluihin sallitaan vain VPN-yhteydellä	0,83	0,91	0,67	0,69	0,77	0,83
7.3	Organisaatiolla on olemassa käyttövaltuuspolitiikka ja prosessi käyttövaltuuksien hallintaan	0,75	0,73	0,72	0,88	0,95	0,74
7.7	Organisaatiolla on käytössä monivaiheinen tunnistus etäkäytössä	0,74	0,62	0,61	0,63	0,45	0,92
7.5	Organisaatio on määrittänyt fyysisesti suojatut turvallisuusalueet asiakirjojen käsittelyn ja tietojärjestelmien suojaamiseksi	0,73	0,67	0,67	0,75	0,65	0,81
7.12	Tietojärjestelmien käytöstä ja tietojen luovutuksista kerätään riittävät lokitiedot	0,68	0,69	0,56	0,81	0,59	0,70
7.4	Käyttövaltuuksien ajantasaisuus varmistetaan säännöllisesti	0,66	0,65	0,72	0,69	0,68	0,68
7.2	Organisaatiolla on olemassa henkilöiden taustatarkistuksiin liittyvä menettely, joka kattaa oman ja palvelutoimittajien henkilöstön	0,62	0,38	0,50	0,63	0,19	0,88
7.14	Tietoturvallisuuteen ja tietojärjestelmiin liittyviä auditointeja tehdään säännöllisesti	0,56	0,49	0,61	0,69	0,36	0,63
7.11	Varmuuskopioiden palautusta testataan säännöllisesti	0,55	0,68	0,61	0,50	0,41	0,49
	YHTEENSÄ	**0,78**	**0,75**	**0,76**	**0,77**	**0,73**	**0,82**

1.2.4.1 Tietoturvallisuuden kehittämiskohteet

- **Kehittämiskohde 7**
  Etäkäyttöön liittyvien riskien arviointi sekä kattava VPN-yhteyksien ja monivaiheisen tunnistautumisen käyttöönotto.

- **Kehittämiskohde 8**
  Toimiva varmuuskopiointi, jonka merkitys on kasvanut sitä mukaa kun

lunnashaittaohjelmahyökkäykset ovat yleistyneet. Organisaation tulisi varmistaa säännöllisesti tehtävällä palautusharjoituksella kriittisten palveluiden ja niissä olevien tietojen saatavuus ja eheys – unohtamatta ulkoistettuja palveluja.

- **Kehittämiskohde 9**
  Kattava lokitiedot ja niiden käytettävyys. Lokitietojen tärkeys on noussut useasta eri syystä; niiden avulla voidaan tunnistaa ja ennakoida organisaatioon kohdistuvia hyökkäyksiä, selvittää toteutuneita hyökkäyksiä ja varmistaa tietojen asianmukainen käyttö eri tietojärjestelmissä.

- **Kehittämiskohde 10**
  Haavoittuvuuksien hallinnan ja auditointitoiminnan kehittäminen. Vuosien 2020–2021 aikana yhä useampi tietomurto ja henkilötietojen tietoturvaloukkaus on syntynyt ICT-palveluista löytyneen ohjelmistollisen haavoittuvuuden takia. Tietoverkkorikolliset ja kybervakoilijat käyttävät entistä aggressiivisemmin ja nopeammin hyödykseen haavoittuvuuksia, etenkin ns. nollapäivähaavoittuvuuksia. Tietojärjestelmissä piilevien haavoittuvuuksien tunnistaminen edellyttää sekä haavoittuvuuksien hallinnan kehittämistä että säännöllisesti suoritettavia tietoturva-auditointeja tai -tarkastuksia kriittisimmissä järjestelmissä.

- **Kehittämiskohde 15**
  Salassa pidettävien ja henkilötietojen suojaaminen. Jokainen tilanne, jossa organisaation salassa pidettäviä tai henkilötietoja käsitellään ohjeiden vastaisesti, voi aiheuttaa merkittävää haittaa tai vahinkoa. Tämä on selkeä kehittämiskohde, joka tulee ottaa huomioon niin henkilöstön osaamisen kehittämiseen liittyvissä ohjeistuksissa ja koulutuksissa kuin tietojärjestelmien suunnittelussa.

- **Kehittämiskohde 17**
  Päätelaitteiden suojaaminen. Vastaajista 33 % prosenttia ilmoittaa, että organisaation hallinnassa oleva päätelaite on varastettu. Tämä on valitettavan korkea lukema. Henkilöstölle tuleekin korostaa turvallista päätelaitteiden kuljettamista ja säilyttämistä osana digiturvallisuuden osaamisen kehittämistä. Vastaavasti joka kerta kun päätelaite varastetaan, laitteen tietojen tulisi olla salakirjoitettuja. Näin laitteessa olevien salassa pidettävien tietojen tai henkilötietojen luottamuksellisuus eivät vaarannu. Etenkin mobiililaitteiden järjestelmänhallintatuotteilla voidaan yrittää paikallistaa ja tuhota tietoja sekä muilla keinoilla vaikuttaa siihen, että tietoja ei voida väärinkäyttää (mm. ilmoitukset teleoperaattorille).

- **Kehittämiskohde 18**
  Ohjeistuksen kehittäminen. Vaikka vain 37 % organisaatioista raportoi, että niiden nimissä on lähetetty erilaisia huijausviestejä, tulisi jokaisella organisaatiolla olla selkeä ohjeistus ja prosessi tällaisissa tilanteissa toimimiseen ja niistä viestimiseen.

1.2.4.2 Kehitys Digiturvakyselyyn 2019 verrattuna

Vuoden 2019 Digiturvakyselyssä osa-alueen keskiarvot olivat seuraavat:

Valtionhallinto	0,83
Sairaanhoitopiirit	0,75
Kunnat	0,63

Yliopistot	0,58
Keskiarvo	**0,70**

Jälleen voidaan havaita, että yliopistot (nyk. korkeakoulu) ja kunnat (nyk. kunnat ja kuntayhtymät) ovat nostaneet keskiarvojaan. Vaikka vain osa kysymyksistä on samoja, voidaan todeta, että näillä toimialoilla tietoturvallisuuden toteuttaminen on kehittynyt merkittävästi. Selittävinä tekijöinä voidaan pitää 1.1.2020 voimaan astunutta tiedonhallintalakia sekä digitaalisessa toimintaympäristössä tapahtunutta uhkatilanteen muutosta, joka on edellyttänyt tietoturvan kehittämistä. Valtionhallinnon pieneen etumatkaan vaikuttaa jo vuonna 2010 käynnistynyt tietoturva-asetuksen toimeenpano.

Vuoden 2019 Digiturvakyselyn tietoturvallisuuden osa-alueella huonoin tulos (KA 0,37) saatiin kysymyksessä ”Organisaation käytössä olevien kriittisten tai muuten tärkeiden tietojärjestelmien tietoturvallisuus on arvioitu (tehty ulkopuolinen arviointi tai auditointi) viimeisen kahden vuoden aikana”. Tämä on edelleen selkeä kehittämiskohde, mutta kahdessa vuodessa on tapahtunut positiivista kehitystä; keskiarvo noussut 0,37 → 0,56.

1.2.5 Tietosuoja

Taulukossa 6 esitetään tietosuojaosion 15 väittämän vastauskeskiarvot, ja osion kokonaiskeskiarvo (0,81) on koko kyselyn korkein.

Korkeimmat kysymyskohtaiset keskiarvot ovat kohdissa 8.1 ja 8.2 (KA 0,95): lähes jokainen organisaatio tuntee käsittelemänsä henkilötietotyypit ja on tunnistanut niiden käsittelyn oikeusperusteet. Sen sijaan suurin haaste on väittämä 8.10 (KA 0,46) eli rakenteettoman tiedon tunnistaminen ja hallinta.

Toimialojen väliset erot ovat pienet. Korkein keskiarvo on kuntayhtymillä (0,87). Seuraavina tulevat korkeakoulu (0,84), julkis-SOTE (0,83), valtionhallinto (0,81) ja kunta (0,78).

Taulukko 6. Tietosuoja – kysymyskohtaiset keskiarvot

		128 KAIKKI	39 Kunta	9 Kunta-yhtymä	8 Julkis-SOTE	11 Korkea-koulu	57 Valtion-hallinto
8.1	Organisaatiolla on tiedossa, millaisia henkilötietoja se käsittelee (TsA 4 art. 1 kohta)	0,95	0,96	1,00	0,94	0,91	0,95
8.2	Henkilötietojen käsittelyn oikeusperusteet on tunnistettu (TsA 6, 9 ja 10 art. TsL 6 ja 29 §, TtsL 2, 3, 5 ja 6 luku)	0,95	0,96	1,00	0,94	1,00	0,92
8.7	Tietosuojavastaavan asema ja rooli on määritelty (TsA 37–39 art.)	0,94	0,95	0,94	0,94	0,95	0,95
8.3	Organisaatio on tunnistanut, milloin se toimii rekisterinpitäjänä ja milloin käsittelijänä (TsA 4 art. 7–8 kohta)	0,93	0,96	1,00	0,88	1,00	0,89
8.13	Organisaatiolla on olemassa henkilötietojen tietoturvaloukkausten hallintaprosessi (TsA 33–34 art.)	0,91	0,88	1,00	0,94	0,95	0,89
8.9	Organisaatiolla on tiedossa, missä tietojärjestelmissä henkilötietoja käsitellään	0,90	0,92	1,00	0,88	0,86	0,87
8.6	Henkilötietojen käsittelyyn liittyvät oman organisaation sisäiset roolit ja vastuut on tunnistettu ja vahvistettu (TihL 4.2.§, TsA 37 art.)	0,88	0,88	0,89	0,94	0,86	0,87
8.8	Seloste käsittelytoimista on laadittu (TsA 30 art.)	0,84	0,73	0,94	0,81	0,82	0,89
8.11	Informointikäytännöt on määritelty ja niitä noudatetaan (TsA 12–14 art. Laki digitaalisten palveluiden tarjoamisesta 306/2019)	0,79	0,74	0,78	0,81	0,91	0,80
8.4	Sopimukset henkilötietojen käsittelystä on tehty ja sopimusten hallinta on kunnossa (TsA 28 art.)	0,78	0,72	0,89	0,88	0,77	0,78
8.14	Jos henkilötietoja siirretään kolmansiin maihin, organisaatio on selvittänyt siirron edellytykset (TsA 5 luku)	0,76	0,59	1,00	0,88	0,86	0,79
8.5	Yhteisrekisterinpitäjyystilanteet tunnistetaan ja yhteisrekisterinpitäjyyttä koskevista vastuista on sovittu (TsA 26 art., huom. EDPB:n ohje)	0,74	0,67	0,93	0,67	0,91	0,75
8.15	Organisaatiossa tietosuojasta huolehtiminen on muuttunut toiminnaksi, kulttuuriksi ja asenteeksi (TsA 5 art.)	0,66	0,68	0,67	0,69	0,64	0,65
8.12	Organisaatiolla on olemassa prosessi vaikutustenarvioinnin tarpeen tunnistamiseksi (TsA 35 1 art.)	0,61	0,57	0,56	0,69	0,82	0,59
8.10	Rakenteeton tieto on tunnistettu ja sen hallinta kuvattu	0,46	0,45	0,56	0,50	0,35	0,46
	YHTEENSÄ	**0,81**	**0,78**	**0,87**	**0,83**	**0,84**	**0,81**

1.2.5.1 Tietosuojan kehittämiskohteet

- **Kehittämiskohde 11**
  Tietosuojan vaikutustenarviointi. Kysymykseen kielteisesti vastanneiden (17 %) tulisi varmistaa, että kokonaisuus saadaan osaksi organisaation toimintaa.

1.2.5.2 Kehitys Digiturvakyselyyn 2019 verrattuna

Vuoden 2019 Digiturvakyselyssä osa-alueen keskiarvot olivat seuraavat:

Sairaanhoitopiirit	0,74
Yliopistot	0,69
Valtionhallinto	0,68
Kunnat	0,68
Keskiarvo	**0,70**

Tuloksista voidaan havaita, että tietosuojan kehittäminen on selkeästi edistynyt kuluneen kahden vuoden aikana.

Vuoden 2019 Digiturvakyselyn tietosuojan osa-alueella heikoin tulos (KA 0,48) saatiin kysymyksessä ”Miten edellä olevat kohdat ovat muuttuneet toiminnaksi, kulttuuriksi ja asenteeksi organisaatiossa”. Uusissa tuloksissa keskiarvo (0,66) on kohonnut eli kehitystä on selkeästi tapahtunut.

Sen sijaan vuoden 2021 kyselyssä selvästi heikoimmaksi kohdaksi on jäänyt väittämä ”Rakenteeton tieto on tunnistettu ja sen hallinta kuvattu”. Jokaisen organisaation tulisikin tunnistaa kattavammin sen tuottama ja käyttämä tieto. Viime vuosien aikana on pääosin saatu hallintaan organisaation prosesseissa ja tietojärjestelmissä syntyvä tieto sekä siihen liittyvät kuvaukset ja metatiedot. Kuitenkin useissa organisaatiossa saattaa olla vielä paljon sellaista tietoa, jota ei ole riittävän hyvin tunnistettu ja saatu hallintaan.

1.2.6 Kyberturvallisuus

Taulukossa 7 esitetään kyberturvallisuusosion 9 väittämän vastauskeskiarvot. Osion kokonaiskeskiarvo (0,59) on koko kyselyn alhaisin.

Taulukko 7. Kyberturvallisuus – kysymyskohtaiset keskiarvot

		128 KAIKKI	39 Kunta	9 Kuntayhtymä	8 Julkis-SOTE	11 Korkeakoulu	57 Valtionhallinto
9.4	Organisaatiossa on tunnistettu ne kriittiset palvelut, joilla on merkittävä vaikutus toisten organisaatioiden tai yhteiskunnan toimintaan	0,79	0,71	0,67	0,94	0,73	0,86
9.5	Organisaatiossa on kattavasti tunnistettu kriittisten palveluiden riippuvuudet ulkoisista palvelutoimittajista	0,75	0,73	0,75	0,88	0,68	0,76
9.1	Organisaatio on huomioinut digitaalisen turvallisuuden osana kokonaisarkkitehtuuria	0,72	0,68	0,83	0,69	0,82	0,71
9.3	Organisaatio on tunnistanut oman roolinsa YTS:n mukaisissa tehtävissä sekä globaalissa näkökulmassa	0,67	0,55	0,50	0,81	0,50	0,77
9.7	Kriittisten toimittajien ja alihankkijoiden kanssa käsitellään digiturvallisuutta säännöllisesti toimittaja/palvelunhallintakokouksissa	0,55	0,47	0,56	0,75	0,41	0,62
9.9	Organisaatiolla on menettely, jolla se seuraa toimintaympäristössä tapahtuvia ilmiöitä ja arvioi niiden vaikutusta organisaation toimintaan	0,54	0,43	0,44	0,63	0,45	0,63
9.6	Organisaation kriittisiin palveluihin liittyviä riskejä arvioidaan ja hallitaan säännöllisesti ja kattavasti yhteistyössä palvelutoimittajien kanssa	0,51	0,45	0,50	0,63	0,50	0,57
9.8	Organisaatio on varautunut ja laatinut suunnitelman siihen kohdistuvan mustamaalaus- tai vaikuttamiskampanjan varalta	0,41	0,32	0,39	0,38	0,50	0,50
9.2	Organisaatiolla on riittävät resurssit ja osaaminen digitaalisen turvallisuuden kehittämiseen osana kokonaisarkkitehtuuria	0,41	0,36	0,50	0,56	0,41	0,40
	YHTEENSÄ	**0,59**	**0,52**	**0,57**	**0,69**	**0,56**	**0,65**

Korkein kysymyskohtainen keskiarvo on kohdassa 9.4 (KA 0,79), joka koskee organisaatioiden valmiuksia tunnistaa sellaiset kriittiset palvelut, jotka vaikuttavat myös muiden tahojen toimintaan. Heikoin tulos on puolestaan kohdassa 9.2 (KA 0,41) eli digitaalisen turvallisuuden arkkitehtuurin kehittämisen riittävässä resursoinnissa.

Toimialoista korkein keskiarvo on julkisomisteisilla sote-toimijoilla (0,69), ja seuraavina tulevat valtionhallinto (0,65), kuntayhtymä (0,57), korkeakoulu (0,56) ja kunta (0,52).

1.2.6.1 Kyberturvallisuuden kehittämiskohteet

- **Kehittämiskohde 5**
  Digitaalisen toimintaympäristön riskienhallinnan kokonaisvaltainen kehittäminen ja ulottaminen erilaisiin toimijoihin. Riskien arviointia toteutetaan järjestelmällisesti kaikissa keskeisissä muutoksissa, häiriöissä ja poikkeamissa – niin sisäisissä kuin ulkoisissa. Vähintäänkin tulee arvioida, onko laajempi analyysi tarpeen. Vain kerran vuodessa tehtävästä riskien arvioinnista on syytä päästä useammin toteutettavaan muutosarviointiin ja uusien riskien tunnistamiseen. Prosessiin voidaan yhdistää seurantatoimet ja jäännösriskien tarkastelu. Tiheämpi toistuvuus tukee osaamisen kehittymistä, pitää kuormituksen pienempänä sekä tukee johtamista paremmalla tilannetietoisuudella. Muutosten ja riskitasojen seurannan raportointia ja mittarointia voi kehittää osana johtamisen kehittämiskohdetta 4.

- **Kehittämiskohde 12**
  JUDO-hankkeen arkkitehtuurityön hyödyntäminen. Digi- ja väestötietovirasto kehittää digitaalisen turvallisuuden kokonaisuutta JUDO-hankkeen projekteissa, joissa tehdään myös tietoturva-arkkitehtuuriin liittyvää kehittämistä. Suosittelemme tutustumaan JUDO-hankkeeseen osoitteessa: https://www.dvv.fi/judo.

- **Kehittämiskohde 13**
  Digitaalisen turvallisuuden kehittäminen yhteistyössä palvelutuottajien kanssa. Organisaation tulisi kehittää digiturvallisuuden eri osa-alueita yhteistyössä palvelutuottajiensa kanssa joko aloittamalla palvelutoimittajatapaamiset tai lisäämällä digiturvallisuusteemat nykyisten tapaamisten agendalle.

- **Kehittämiskohde 14**
  Uhkatilanteen seuranta ja siihen liittyvien riskien hallinta. Organisaatioiden toimintaympäristö on kaikilta osin muuttumassa nopeammin kuin koskaan aikaisemmin, ja lisäksi vauhti tuntuu kiihtyvän jatkuvasti. Tämä tarjoaa uudenlaisia teknologisia mahdollisuuksia kehittää organisaation toimintaa, mutta myös organisaatioon kohdistuvat uhat ovat merkittävässä muutoksessa. Jotta organisaatio voi hyödyntää mahdollisuuksia, tunnistaa uhat ja hallita niihin liittyvät riskit, sen tulee kyetä seuraamaan ja arvioimaan toimintaympäristönsä muutoksien vaikutuksia säännöllisesti. Tämän kyvykkyyden kehitystä voidaan työstää kokonaisuutena, jossa linkittyvät eri osa-alueista sekä kyberturvallisuus, että johtamisen tarpeet, kuin myös riskienhallinnan seurantatarpeet.

1.2.6.2 Kehitys Digiturvakyselyyn 2019 verrattuna

Vuoden 2019 Digiturvakyselyssä osa-alueen keskiarvot olivat seuraavat:

Sairaanhoitopiirit	0,67
Valtionhallinto	0,65
Kunnat	0,53
Yliopistot	0,48
Keskiarvo	**0,61**

Vaikka kärjen järjestys ei ole muuttunut, on huomattava, että vuonna 2019 kyselyosiossa oli täysin erilaiset kysymykset kuin tällä kerralla. Keskiarvoaan ovat

merkittävästi parantaneet kunnat (nyk. kunta ja kuntayhtymä) sekä yliopistot (nyk. korkeakoulu).

Vuoden 2019 Digiturvakyselyn toiminnan jatkuvuus ja varautuminen osa-alueella kysymyksessä ”Organisaatio on tunnistanut sen omalle tai sidosryhmien toiminnalle kriittiset palvelut sen toiminnalle asetettujen vaatimusten perusteella” saatiin keskiarvo 0,75. Nyt lähinnä vastaavan kohdan 9.4 ”Organisaatiossa on tunnistettu ne kriittiset palvelut, joilla on merkittävä vaikutus toisten organisaatioiden tai yhteiskunnan toimintaan” keskiarvo on 0,79. Vaikka muutos on kokonaistasolla pieni, merkittävää parannusta on tapahtunut SOTE-toimijoissa (aiemmin sairaanhoitopiirit, nousu 0,81 → 0,94) ja valtionhallinnossa (nousu 0,80 → 0,86). Kuntien ja kuntayhtymien tulos oli 0,63 vuonna 2019, ja nyt se on kunnilla 0,71 ja kuntayhtymillä 0,67. Sen sijaan yliopistojen (nyk. korkeakoulu, lasku 0,75 → 0,73) tulos on heikentynyt.

Yksi mahdollinen syy moniin parantuneisiin tuloksiin voi olla koronaviruspandemia, joka on edellyttänyt kaikkien digiturvallisuuden osa-alueiden huomioimista ja kehittämistä.

1.2.7 Havainnointi

Taulukossa 8 esitetään havainnointiosion 20 väittämän vastauskeskiarvot.

Osio eroaa edeltävistä; siinä organisaatiot ovat raportoineet kuinka eri uhat ovat toteutuneet niiden toiminnassa vuosina 2020–2021 (kyselyhetkeen saakka). Vastausvaihtoehdot ovat *0, 1–5, 6–10, 11–30* ja *yli 30 kertaa*, ja vaihtoehdot on pisteytetty keskiarvotilastoa varten seuraavasti:

- 0 (0)
- 1 – 5 (0,25)
- 6–10 (0,5)
- 11–30 (0,75)
- yli 30 kertaa (1)

Alhaiset keskiarvot osoittavat, että valtaosalla vastaajista uhat eivät ole realisoituneet. Eniten vastaajat raportoivat kriittisissä palveluissa ilmenneistä teknisistä häiriöistä, jotka ovat jonkin verran haitanneet organisaation toimintaa (kohta 10.7; KA 0,38). Vähiten mainintoja sai puolestaan kohta 10.16 (KA 0,01), eli organisaatioiden kriittisiä tietoja ei juuri ole korruptoitunut tai tuhoutunut pysyvästi.

Taulukko 8. Havainnointi – kysymyskohtaiset keskiarvot

		128 KAIKKI	39 Kunta	9 Kunta-yhtymä	8 Julkis-SOTE	11 Korkea-koulu	57 Valtion-hallinto
10.7	Organisaation käyttämissä kriittisissä palveluissa on ollut tekninen häiriö, joka on jonkin verran haitannut organisaation toimintaa	0,38	0,25	0,31	0,50	0,25	0,48
10.8	Organisaation käyttämissä kriittisissä palveluissa on ollut tekninen häiriö, joka on merkittävästi haitannut organisaation toimintaa	0,21	0,16	0,11	0,34	0,11	0,27
10.5	Organisaation käytössä olevaan palveluun on kohdistunut henkilötietojen tietoturvaloukkaus, joka on edellyttänyt ilmoitusta valvontaviranomaiselle	0,21	0,21	0,19	0,50	0,25	0,14
10.17	Organisaation nimissä on lähetetty huijausviestejä, joissa yritetään urkkia asiakkaiden tai muiden henkilöiden tietoja	0,18	0,17	0,17	0,25	0,41	0,14
10.6	Organisaation käytössä olevaan palveluun on kohdistunut henkilötietojen tietoturvaloukkaus, joka on edellyttänyt ilmoitusta rekisteröidyille	0,17	0,17	0,17	0,38	0,23	0,12
10.20	Organisaation henkilöstöön tai organisaation toimintaan on yritetty vaikuttaa kielteisillä keinoilla	0,15	0,12	0,03	0,28	0,09	0,18
10.14	Organisaation julkiseen verkkoon näkyvässä tietojärjestelmässä tai verkossa on ollut kriittinen ja hyödynnettävissä ollut tietoturvahaavoittuvuus	0,14	0,11	0,14	0,25	0,20	0,13
10.3	Organisaatio on vastaanottanut ICT-palvelutoimittajilta ilmoituksen hyökkäyksestä, joka on aiheuttanut tietomurron, tietovuodon tai henkilötietojen tietoturvaloukkauksen, joka koskee ainakin osittain organisaatiota	0,13	0,12	0,11	0,22	0,14	0,13
10.4	Organisaation salassa pidettäviä tietoja tai henkilötietoja on käsitelty ohjeiden vastaisesti luvattomilla laitteilla tai luvattomissa palveluissa	0,11	0,10	0,06	0,31	0,09	0,11
10.18	Organisaation palveluita tuottava toimittaja, alihankkija tai kumppani on toiminut vastoin sovittuja tietoturva- tai tietosuojakäytäntöjä	0,09	0,06	0,11	0,16	0,05	0,12
10.13	Organisaation hallinnassa oleva päätelaite on varastettu	0,09	0,10	0,14	0,31	0,14	0,03
10.11	Organisaation käytössä olleeseen palveluun on kohdistunut palvelunestohyökkäys, joka on jonkin verran haitannut organisaation toimintaa	0,09	0,12	0,19	0,06	0,07	0,07
10.2	Organisaation itse tuottamiin palveluihin on kohdistunut onnistunut hyökkäys, joka on aiheuttanut tietomurron, tietovuodon tai henkilötietojen tietoturvaloukkauksen	0,06	0,06	0,11	0,06	0,25	0,03
10.19	Organisaation web- tai sosiaalisen median kanaviin on ulkopuolisten tahojen toimesta yritetty vaikuttaa bottien, trollitilien tai vastaavien avulla tai muilla keinoilla	0,06	0,01	0,08	0,06	0,02	0,09
10.15	Organisaation työntekijä on tietoisesti luvattomasti käsitellyt salassa pidettäviä tietoja tai henkilötietoja	0,06	0,10	0,06	0,31	0,02	0,01
10.21	Organisaatio on ollut räätälöidyn, kohdistetun tietoturva- tai kyberhyökkäyksen kohteena	0,05	0,04	0,00	0,03	0,14	0,05
10.12	Organisaation käytössä olleeseen palveluun on kohdistunut palvelunestohyökkäys, joka on merkittävästi haitannut organisaation toimintaa	0,04	0,04	0,08	0,09	0,00	0,02
10.10	Organisaation käytössä olevaan palveluun on päässyt haittaohjelma, joka on esim. estänyt palvelun käytön tai aiheuttanut tietovuodon	0,03	0,03	0,06	0,03	0,05	0,02
10.9	Organisaation käytössä olevaan päätelaitteeseen on päässyt haittaohjelma, joka on esim. lukinnut päätelaitteen salaamalla tai aiheuttanut tietovuodon	0,02	0,03	0,00	0,03	0,07	0,01
10.16	Organisaation kriittisiä tai lakisääteisesti säilytettäviä tietoja on korruptoitunut tai tuhoutunut lopullisesti	0,01	0,02	0,00	0,03	0,00	0,01
	YHTEENSÄ	**0,11**	**0,10**	**0,11**	**0,21**	**0,13**	**0,11**

Osion kokonaiskeskiarvo on 0,11, ja eniten uhkia ovat tunnistaneet julkisomisteiset sote-toimijat (0,21). Muilla keskiarvot olivat: korkeakoulut (0,13), valtionhallinto (0,11) kuntayhtymät (0,11) ja kunnat (0,10). Tämä vahvistaa sitä käsitystä, että koronaviruspandemian aikana verkkorikolliset ja muut vihamieliset toimijat ovat kohdistaneet kampanjoitaan ja hyökkäyksiään erityisesti sote-toimialan organisaatioita vastaan.

1.2.7.1 Havainnoinnin kehittämiskohteet

- **Kehittämiskohde 15**
  Salassa pidettävien ja henkilötietojen suojaaminen. Jokainen tilanne, jossa organisaation salassa pidettäviä tai henkilötietoja käsitellään ohjeiden vastaisesti, voi aiheuttaa merkittävää haittaa tai vahinkoa. Tämä on selkeä kehittämiskohde, joka tulee ottaa huomioon niin henkilöstön osaamisen kehittämiseen liittyvissä ohjeistuksissa ja koulutuksissa kuin tietojärjestelmien suunnittelussa.

- **Kehittämiskohde 16**
  Palveluiden vikasietoisuuden parantaminen. Eriasteiset tekniset häiriöt ovat keskeinen organisaation, sen asiakkaiden ja sidosryhmien toimintaa haittaava ongelma. Mitä enemmän toimintaa digitalisoidaan ja uutta teknologiaa otetaan käyttöön, sitä paremmin on huolehdittava palveluiden saatavuudesta ja varmistettava niiden vikasietoisuuden toteutuminen palveluiden kriittisyydelle annettujen vaatimusten mukaisesti. Tähän liittyy oleellisesti myös toimiva riskienhallinta ja ajan tasalla olevat jatkuvuus- ja valmiussuunnitelmat.

- **Kehittämiskohde 17**
  Päätelaitteiden suojaaminen. Vastaajista 33 % prosenttia ilmoittaa, että organisaation hallinnassa oleva päätelaite on varastettu. Tämä on valitettavan korkea lukema. Henkilöstölle tuleekin korostaa turvallista päätelaitteiden kuljettamista ja säilyttämistä osana digiturvallisuuden osaamisen kehittämistä. Vastaavasti joka kerta kun päätelaite varastetaan, laitteen tietojen tulisi olla salakirjoitettuja. Näin laitteessa olevien salassa pidettävien tietojen tai henkilötietojen luottamuksellisuus eivät vaarannu. Etenkin mobiililaitteiden järjestelmänhallintatuotteilla voidaan yrittää paikallistaa ja tuhota tietoja sekä muilla keinoilla vaikuttaa siihen, että tietoja ei voida väärinkäyttää (mm. ilmoitukset teleoperaattorille).

- **Kehittämiskohde 18**
  Ohjeistuksen kehittäminen. Vaikka vain 37 % organisaatioista raportoi, että niiden nimissä on lähetetty erilaisia huijausviestejä, tulisi jokaisella organisaatiolla olla selkeä ohjeistus ja prosessi tällaisissa tilanteissa toimimiseen ja niistä viestimiseen.

1.2.7.2 Kehitys Digiturvakyselyyn 2019 verrattuna

Vuoden 2019 Digiturvakyselyssä kolme eniten havaittua uhkaa olivat:

1. Käyttämissämme palveluissa on ollut teknisiä (ei tieto- tai kyberturvallisuuteen liittyviä) häiriöitä, jotka ovat jonkin verran haitanneet palveluiden toimintaa ja sitä kautta vaikuttaneet organisaatiomme toimintaan.

2. Käyttämissämme palveluissa on ollut teknisiä (ei tieto- tai kyberturvallisuuteen liittyviä) häiriöitä, jotka ovat merkittävästi haitanneet palveluiden toimintaa ja sitä kautta vaikuttaneet organisaatiomme toimintaan.
3. Organisaation nimissä on lähetetty huijausviestejä, jossa yritetään urkkia asiakkaiden tietoja, esimerkiksi käyttäjätunnuksia, salasanoja, pankki- tai muihin palveluihin liittyviä tietoja?

Vuoden 2021 kyselyssä havaittujen ja toteutuneiden uhkien kärkisijat ovat pysyneet pitkälti samankaltaisina. Tälläkin kertaa ensimmäisellä ja toisella sijalla ovat organisaation toimintaa haitanneet tekniset häiriöt. Kolmannelle sijalle nousee kuitenkin henkilötietojen tietoturvaloukkaukset, joista organisaatiot ovat joutuneet tekemään ilmoituksen valvontaviranomaiselle. Huijausviestien määrä ei ole kuitenkaan vähentynyt, sillä tänä vuonna väittämä on sijalla neljä. Viimeisen parin vuoden aikana on yhä useammin lähetetty kalastelu- ja huijausviestejä joko kansainvälisesti tunnettujen ICT-toimijoiden, kansallisten posti- ja pankkipalveluyritysten tai tunnettujen viranomaisten nimissä. Tähän jokaisen julkisen hallinnon organisaation tulisi olla valmistautunut ohjeistuksen ja prosessien muodossa.

VAHTI / Rousku Kimmo (DVV)
18.8.2021

Liite 1 – Tulosten perusteella valitut kehittämiskohteet

Organisaation Digiturvakyselyn 2021 tulosten perusteella keskeisiksi digitaalisen turvallisuuden kehittämiskohteiksi nousevat seuraavat:

Yleinen kehittämiskohde

Koko organisaation läpäisevä riskienhallintaprosessi. Useimmat digitaalisen turvallisuuden osa-alueet ovat selkeästi kehittyneet kuluneen kahden vuoden aikana, lukuun ottamatta riskienhallintaa ja johtamista. Digitaalisen turvallisuuden johtaminen on kuitenkin avainasemassa kaiken turvallisuustyön toteuttamisessa ja kehittämisessä. Toimiakseen se edellyttää koko organisaation läpäisevää riskienhallintaprosessia ja menettelyitä aina johtoryhmästä henkilöstöön saakka. Kaikkien on osallistuttava jokapäiväisen toiminnan uhkien tunnistamiseen ja havaituista riskeistä ilmoittamiseen.

I. Henkilöstön osaamisen ja koulutustarpeiden kartoittaminen. Jokaisella organisaatiolla tulisi olla selkeä suunnitelma siitä, mistä aiheista koulutetaan ja mistä muistutetaan esimerkiksi sisäisellä viestinnällä. Asioiden omaksumista ja muistamista edistää se, että niitä käsitellään pitkin vuotta. Asiantuntijoiden osaamistarpeet voivat poiketa muun henkilökunnan tarpeista. Suosittelemme osallistumaan Digiturva-viikkoon 25.–29.10.2021 (linkki), hyödyntämään Digiturvallinen elämä -verkkokoulutuksia tai -mobiilipeliä (linkki) sekä seuraamaan Digi- ja väestötietoviraston tuottamia verkkotilaisuuksia (linkki tapahtumakalenteriin).

II. Harjoitustoiminnan kehittäminen. Mikäli organisaatio ei ole osallistunut yhteenkään TAISTO-harjoitukseen, se voi osallistua siihen joko marraskuussa 2021 varsinaisena harjoituspäivänä tai suorittaa digitalisoidun TAISTOmaatti-harjoituksen. Organisaation johdolla on kriittinen rooli erilaisten kriittisten häiriötilanteiden, hyökkäysten ja loukkausten hallinnan johtamisessa, ja siksi johdon ja asiantuntijoiden tulisi harjoitella yhdessä.

III. Prosessit kuntoon. Tärkeimpien prosessien kuvaaminen, jalkauttaminen ja harjoittelu sekä harjoittelun perusteella tapahtuva prosessien kehittäminen kaikilla digitaalisen turvallisuuden osa-alueilla.

IV. Säännöllinen digitaalisen turvallisuuden tilanneraportointi organisaation johdolle sovitusti, kuitenkin vähintään vuosittain käyttäen tarkoitukseen sopivia mittareita. Osana mittaristoa ja vertailupohjaa voidaan hyödyntää esimerkiksi tämän kyselyn tuloksia. Tarkastelussa tulee huomioida myös organisaation taloudelliset resurssit, käytettävissä oleva henkilöstö sekä osaaminen.

V. Digitaalisen toimintaympäristön riskienhallinnan kokonaisvaltainen kehittäminen ja ulottaminen erilaisiin toimijoihin. Riskien arviointia toteutetaan järjestelmällisesti kaikissa keskeisissä muutoksissa, häiriöissä ja poikkeamissa – niin sisäisissä kuin ulkoisissa. Vähintäänkin tulee arvioida, onko laajempi analyysi tarpeen. Vain kerran vuodessa tehtävästä riskien arvioinnista on syytä päästä useammin toteutettavaan muutosarviointiin ja uusien riskien tunnistamiseen. Prosessiin voidaan yhdistää seurantatoimet ja jäännösriskien tarkastelu. Tiheämpi toistuvuus tukee osaamisen kehittymistä, pitää kuormituksen pienempänä sekä tukee johtamista paremmalla tilannetietoisuudella. Muutosten ja riskitasojen seurannan raportointia ja mittarointia voi kehittää osana johtamisen kehittämiskohdetta 4.

VI. Harjoitustoiminnan kehittäminen ja ylläpito. Vastaajista 24 % ei harjoittele säännöllisesti, eikä 14 % päivitä harjoitusten perusteella olemassa olevia suunnitelmiaan. Koska erilaisten häiriöiden, hyökkäysten ja loukkausten määrä tulee tulevaisuudessa kasvamaan ja vaikutus laajentumaan, harjoittelemalla varautuminen on entistäkin tärkeämpää.

VII. Etäkäyttöön liittyvien riskien arviointi sekä kattava VPN-yhteyksien ja monivaiheisen tunnistautumisen käyttöönotto.

VIII. Toimiva varmuuskopiointi, jonka merkitys on kasvanut sitä mukaa kun lunnashaittaohjelmahyökkäykset ovat yleistyneet. Organisaation tulisi varmistaa säännöllisesti tehtävällä palautusharjoituksella kriittisten palveluiden ja niissä olevien tietojen saatavuus ja eheys – unohtamatta ulkoistettuja palveluja.

IX. Kattavat lokitiedot ja niiden käytettävyys. Lokitietojen tärkeys on noussut useasta eri syystä; niiden avulla voidaan tunnistaa ja ennakoida organisaatioon kohdistuvia hyökkäyksiä, selvittää toteutuneita hyökkäyksiä ja varmistaa tietojen asianmukainen käyttö eri tietojärjestelmissä.

X. Haavoittuvuuksien hallinnan ja auditointitoiminnan kehittäminen. Vuosien 2020–2021 aikana yhä useampi tietomurto ja henkilötietojen tietoturvaloukkaus on syntynyt ICT-palveluista löytyneen ohjelmistollisen haavoittuvuuden takia. Tietoverkkorikolliset ja kybervakoilijat käyttävät entistä aggressiivisemmin ja nopeammin hyödykseen haavoittuvuuksia, etenkin ns. nollapäivähaavoittuvuuksia. Tietojärjestelmissä piilevien haavoittuvuuksien tunnistaminen edellyttää sekä haavoittuvuuksien hallinnan kehittämistä että säännöllisesti suoritettavia tietoturva-auditointeja tai -tarkastuksia kriittisimmissä järjestelmissä.

XI. Tietosuojan vaikutustenarviointi. Kysymykseen kielteisesti vastanneiden (17 %) tulisi varmistaa, että kokonaisuus saadaan osaksi organisaation toimintaa.

XII. JUDO-hankkeen arkkitehtuurityön hyödyntäminen. Digi- ja väestötietovirasto kehittää digitaalisen turvallisuuden kokonaisuutta JUDO-hankkeen projekteissa, joissa tehdään myös tietoturva-arkkitehtuuriin liittyvää kehittämistä. Suosittelemme tutustumaan JUDO-hankkeeseen osoitteessa: https://www.dvv.fi/judo.

XIII. Digitaalisen turvallisuuden kehittäminen yhteistyössä palvelutuottajien kanssa. Organisaation tulisi kehittää digiturvallisuuden eri osa-alueita yhteistyössä palvelutuottajiensa kanssa joko aloittamalla palvelutoimittajatapaamiset tai lisäämällä digiturvallisuusteemat nykyisten tapaamisten agendalle.

XIV. Uhkatilanteen seuranta ja siihen liittyvien riskien hallinta. Organisaatioiden toimintaympäristö on kaikilta osin muuttumassa nopeammin kuin koskaan aikaisemmin, ja lisäksi vauhti tuntuu kiihtyvän jatkuvasti. Tämä tarjoaa uudenlaisia teknologisia mahdollisuuksia kehittää organisaation toimintaa, mutta myös organisaatioon kohdistuvat uhat ovat merkittävässä muutoksessa. Jotta organisaatio voi hyödyntää mahdollisuuksia, tunnistaa uhat ja hallita niihin liittyvät riskit, sen tulee kyetä seuraamaan ja arvioimaan toimintaympäristönsä muutoksien vaikutuksia säännöllisesti. Tämän kyvykkyyden kehitystä voidaan työstää kokonaisuutena, jossa linkittyvät eri osa-alueista sekä kyberturvallisuus, että johtamisen tarpeet, kuin myös riskienhallinnan seurantatarpeet.

XV. Salassa pidettävien ja henkilötietojen suojaaminen. Jokainen tilanne, jossa organisaation salassa pidettäviä tai henkilötietoja käsitellään ohjeiden vastaisesti, voi aiheuttaa merkittävää haittaa tai vahinkoa. Tämä on selkeä kehittämiskohde, joka tulee ottaa huomioon niin henkilöstön osaamisen kehittämiseen liittyvissä ohjeistuksissa ja koulutuksissa kuin tietojärjestelmien suunnittelussa.

XVI. Palveluiden vikasietoisuuden parantaminen. Eriasteiset tekniset häiriöt ovat keskeinen organisaation, sen asiakkaiden ja sidosryhmien toimintaa haittaava ongelma. Mitä enemmän toimintaa digitalisoidaan ja uutta teknologiaa otetaan käyttöön, sitä paremmin on huolehdittava palveluiden saatavuudesta ja varmistettava niiden vikasietoisuuden toteutuminen palveluiden kriittisyydelle annettujen vaatimusten mukaisesti. Tähän liittyy oleellisesti myös toimiva riskienhallinta ja ajan tasalla olevat jatkuvuus- ja valmiussuunnitelmat.

XVII. Päätelaitteiden suojaaminen. Vastaajista 33 % prosenttia ilmoittaa, että organisaation hallinnassa oleva päätelaite on varastettu. Tämä on valitettavan korkea lukema. Henkilöstölle tuleekin korostaa turvallista päätelaitteiden kuljettamista ja säilyttämistä osana digiturvallisuuden osaamisen kehittämistä. Vastaavasti joka kerta kun päätelaite varastetaan, laitteen tietojen tulisi olla salakirjoitettuja. Näin laitteessa olevien salassa pidettävien tietojen tai henkilötietojen luottamuksellisuus eivät vaarannu. Etenkin mobiililaitteiden järjestelmänhallintatuotteilla voidaan yrittää paikallistaa ja tuhota tietoja sekä muilla keinoilla vaikuttaa siihen, että tietoja ei voida väärinkäyttää (mm. ilmoitukset teleoperaattorille).

Ohjeistuksen kehittäminen. Vaikka vain 37 % organisaatioista raportoi, että niiden nimissä on lähetetty erilaisia huijausviestejä, tulisi jokaisella organisaatiolla olla selkeä ohjeistus ja prosessi tällaisissa tilanteissa toimimiseen ja niistä viestimiseen.