DIGI- JA VÄESTÖTIETO-VIRASTO

Organisaation Digiturvakysely

Raportti ja keskeiset havainnot

30.5.2023

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

Digitalisaatio ja digitaalinen turvallisuus / Erja Kinnunen (DVV)

30.5.2023

Sisällysluettelo

Digitalisaatio ja digitaalinen turvallisuus / Erja Kinnunen (DVV) 30.5.2023

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), viiden VAHTI-asiantuntijaryhmän sekä valtionhallinnon tietoturvavastaavien verkoston toiminnasta. Tässä toiminnassa on mukana lähes 500 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 on koottu ja tarkasteltu hallinnollisen digitaalisen turvallisuuden tilannetietoa. Kyselyiden avulla on voitu selvittää muun muassa, miten lainsäädäntö – kuten tietoturvallisuusasetus vuonna 2010, EU:n yleinen tietosuoja-asetus vuonna 2018 sekä tiedonhallintalaki vuonna 2020 – on vaikuttanut organisaatioiden digitaalisen turvallisuuden osa-alueiden kehittymiseen. Kyselytuloksia on hyödynnetty Julkisen hallinnon digitaalisen turvallisuuden kehittämistoimenpiteiden, VAHTI-työryhmien toiminnan ja JUDO-hankkeen tehtävien suunnittelussa.

Organisaation Digiturvakysely on toteutettu saman sisältöisenä vuosina 2021–2023. Vuonna 2022 otettiin käyttöön DVV:n kehittämä verkkopalvelu, jonka avulla julkisen hallinnon organisaatioille voidaan tarjota niiden omasta digiturvatilanteesta ajantasainen tilannekuva jatkuvaan käyttöön tarkoitetulla kokonaiskuvapalvelulla sekä vertailutietoa muuhun julkiseen hallintoon.

Organisaation Digiturvakyselyn ohella DVV on toteuttanut Henkilöstön ja kansalaisten Digiturvabarometria syyskuusta 2020 alkaen. Organisaation Digiturvakyselyn avulla seurataan, miten organisaatioiden hallinnollinen digiturvallisuus kehittyy. Digiturvabarometrin avulla kartoitetaan digitaaliseen toimintaympäristöön liittyvää henkilöstön osaamista, koulutustarpeita, toteutuneita uhkia sekä luottamusta digimaailman toimijoihin ja palveluihin. Lisäksi vuonna 2021 toteutettiin ensimmäinen digiriskikysely, jota laajennettiin uusilla kysymyksillä keväällä 2023. Kysely siirrettiin verkkopalveluun vuonna 2022 ja myös se on jatkuvasti hyödynnettävissä kokonaiskuvapalvelussa. Kyselyn avulla organisaatio voi tunnistaa ja arvioida merkittäviä digitaaliseen toimintaympäristöön liittyviä uhkia ja riskejä, ja DVV pystyy sen avulla tunnistamaan, ennakoimaan ja raportoimaan julkisen hallinnon organisaatioita koskevien digiriskien kehittymistä.

Lisätietoja kyselystä antaa:

Johtava asiantuntija Erja Kinnunen, puh. 0295 53 5230, erja.kinnunen@dvv.fi

Digitalisaatio ja digitaalinen turvallisuus / Erja Kinnunen (DVV) 30.5.2023

1 Johdon tiivistelmä ja tärkeimmät kehittämistoimenpiteet

Digi- ja väestötietovirasto toteutti helmi-maaliskuussa 2023 Organisaation digiturvakyselyn, johon saatiin 194 vastausta julkisen hallinnon organisaatioilta. Saman sisältöinen kysely on tehty myös vuosina 2021 ja 2022; vastanneet organisaatiot tosin vaihtelevat vuosittain. Vuonna 2021 kyselyyn vastasi 121 ja vuonna 2022 118 organisaatiota. Vastanneiden määrää on siis saatu jonkin verran kasvatettua. Kerätyn tiedon luotettavuutta ja vertailtavuutta saadaan parannettua sitä mukaa kun uusien vastaajien määrä lisääntyy. Toivomme, että yhä useampi julkisen hallinnon organisaatio ottaisi nämä kokonaiskuvan raportointipalvelut omaan käyttöönsä ja kytkisi ne osaksi organisaation digiturvan hallintaa ja säännöllistä johdon raportointia.

Digitaalisen turvallisuuden osa-alueissa tapahtunut kehittyminen

Digiturvakysely kattaa kaikki digitaalisen turvallisuuden osa-alueet eli digiturvan johtamisen, riskienhallinnan, toiminnan jatkuvuuden ja varautumisen, tietoturvan, tietosuojan ja kyberturvallisuuden, joiden kaikkien tasapainoista kehittämistä tarvitaan digitaalisen ja fyysisen toimintaympäristön suojaamiseksi.

Tulosten perusteella voidaan todeta, että organisaatioiden hallinnollinen turvallisuus on kokonaisuudessaan pysynyt lähes samalla tasolla vuosina 2021–2023. Sen sijaan yksittäisissä osa-alueissa ja tehtävissä on tapahtunut pieniä muutoksia.

Koska digitaalisen turvallisuuden kehittämiseen on rajallinen määrä henkilöresursseja ja rahaa, organisaatiot joutuvat priorisoimaan kehittämistoimiaan. Keskimäärin resurssien määrää pidettiin liian pienenä. Reaalimaailman ilmiöt kuten koronaviruspandemia, Venäjän hyökkäyssota ja globaalin maailmantilanteen kiristyminen näkyvät kehittämistoimien priorisoinnissa. Vuonna 2022 oli nähtävissä, että organisaatiot panostivat jonkin verran enemmän riskienhallintaan ja jatkuvuuden hallintaan, kun taas vuonna 2023 parantumista on nähtävissä mm. kyberturvallisuustilanteessa. Resurssien puutteen vuoksi valitettavasti kaikkiin muihin osa-alueisiin ei aina pystytä panostamaan. Tietosuoja, jonka kehittämiseen panostettiin merkittävästi vuosina 2018–2019 EU:n yleisen tietosuoja-asetuksen soveltamisen alettua, on jonkin verran taantunut viimeisten vuosien aikana.

Alla olevassa taulukossa ovat vuosien 2021–2023 vastausten keskiarvot osa-alueittain. Mitä lähempänä arvoa 1, sitä paremmin organisaatiot ovat arvioineet suoriutuneensa kyselyssä esitetyissä väittämissä.

	2023	2022	2021
Koko kysely	**0,70**	**0,69**	**0,71**
Johtaminen	**0,65**	**0,65**	**0,65**
Riskienhallinta	**0,68**	**0,70**	**0,68**
Toiminnan jatkuvuus ja varautuminen	**0,66**	**0,67**	**0,67**
Tietoturvallisuus	**0,75**	**0,75**	**0,78**
Tietosuoja	**0,78**	**0,77**	**0,81**
Kyberturvallisuus	**0,61**	**0,59**	**0,59**

Taulukko 1. Digiturvakyselyn eri osioiden keskiarvot

Toimintaympäristön muutokset ja niiden vaikutus

Edellinen raportti Organisaation Digiturvakyselystä tuotettiin kesällä 2021. Silloin elettiin vielä korona-aikaa ja kyselyn tuloksissa oli jonkin verran nähtävissä äkillinen siirtyminen etätyöhön sekä sen aiheuttamat uudet ilmiöt.

Kyselykierros uusittiin kesällä 2022, jolloin DVV:n kokonaiskuvapalvelu otettiin käyttöön. Tuloksista ei kuitenkaan tuotettu laajaa raporttia, vaan niitä on esitelty DVV:n tilaisuuksissa. Silloin tuloksissa oli nähtävissä muuttuneen maailmantilanteen vaikutus. Venäjän hyökkäyssodan seurauksena organisaatioissa alettiin kiinnittää enemmän huomiota riskitilanteen seurantaan, riskien arviointiin ja niiden raportointiin johdolle. Lisäksi varautuminen ja harjoittelu oli lisääntynyt ja tietoturvallisuuteen budjetoitu raha lisääntynyt jonkin verran.

Vuonna 2023 Venäjän hyökkäyssota jatkuu edelleen ja Suomessakin on havaittu lisääntyneitä verkkohyökkäyksiä ja kielteistä verkkovaikuttamista. Kyselyn tuloksista on havaittavissa, että kyberturvallisuuden osa-alueella on tapahtunut pientä parantumista. Sen tulokset ovat edelleen osa-alueista heikoimmalla tasolla, mutta globaalin tilanteen kehittyminen pakottanee kiinnittämään siihen lisää huomiota myös jatkossa.

Kansainvälisesti verkkorikollisuus jatkaa kasvuaan, mutta se ei tämän kyselyn perusteella ainakaan merkittävästi näy organisaatioiden kokemien verkkohyökkäysten määrässä. Vuoden 2021 kyselyssä arviointijakso oli puolitoista vuotta, joten tulokset eivät ole täysin vertailukelpoisia.

Keskeiset kehittämiskohteet

Tämä kyselyn tulokset painottuvat julkisen hallinnon organisaatioiden hallinnollisen digiturvan kokonaiskuvaan. Hallinnollisen turvallisuuden yhteinen kehittäminen on merkittävästi helpompaa kuin teknisen tietoturvallisuuden tai jatkuvuuden hallinnan kehittäminen. Hallinnollista digitaalista turvallisuutta voidaan kehittää esimerkiksi hankkeiden, työpajojen, tukimateriaalien sekä osaamisen kehittämisen tukivälineiden avulla. Sen sijaan teknisen tietoturvallisuuden ja jatkuvuuden hallinnan parantaminen vaativat organisaatiokohtaisia keinoja, johtuen käytössä olevista teknisistä järjestelmistä ja palveluista. Tästä huolimatta olemme nostaneet esille myös sellaisia tekniseen tietoturvallisuuteen ja jatkuvuuden hallintaan liittyviä toimenpiteitä, joita suosittelemme organisaatioiden tarkastavan ja ottavan käyttöön omassa ympäristössään.

Kaikki suositellut kehittämiskohteet on lueteltu kappaleissa 2.2.1–2.2.7. Tähän osioon on nostettu erityisesti muuttuvaan geopoliittiseen uhkatilanteeseen liittyviä kehittämiskohteita, joihin jokaisen organisaation tulisi kiinnittää erityistä huomiota:

- **Kehittämiskohde 7:** Etäkäyttöön liittyvien riskien arviointi sekä kattava VPN-yhteyksien ja monivaiheisen tunnistautumisen käyttöönotto
- **Kehittämiskohde 8:** Toimiva varmuuskopiointi
- **Kehittämiskohde 9**: Kattavat lokitiedot ja niiden käytettävyys
- **Kehittämiskohde 10**: Haavoittuvuuksien hallinnan ja auditointitoiminnan kehittäminen

- **Kehittämiskohde 15:** Salassa pidettävien ja henkilötietojen suojaaminen
- **Kehittämiskohde 17**: Päätelaitteiden suojaaminen
- **Kehittämiskohde 18**: Ohjeistuksen kehittäminen (mm. huijausviesteihin)
- **Uusi kehittämiskohde 2023_2:** Tietoturvapoikkeamien havainnointi ja kirjaaminen
- **Uusi kehittämiskohde 2023_5:** Jatkuvuuden hallinnan kehittäminen ml. Harjoitustoiminnan kehittäminen (Kehittämiskohde 2)
- **Uusi kehittämiskohde 2023_7:** Varautuminen informaatiovaikuttamiseen
- **Uusi kehittämiskohde 2023_8:** Henkilötietojen tietoturvaloukkauksiin reagoiminen

2 Yhteenveto tuloksista

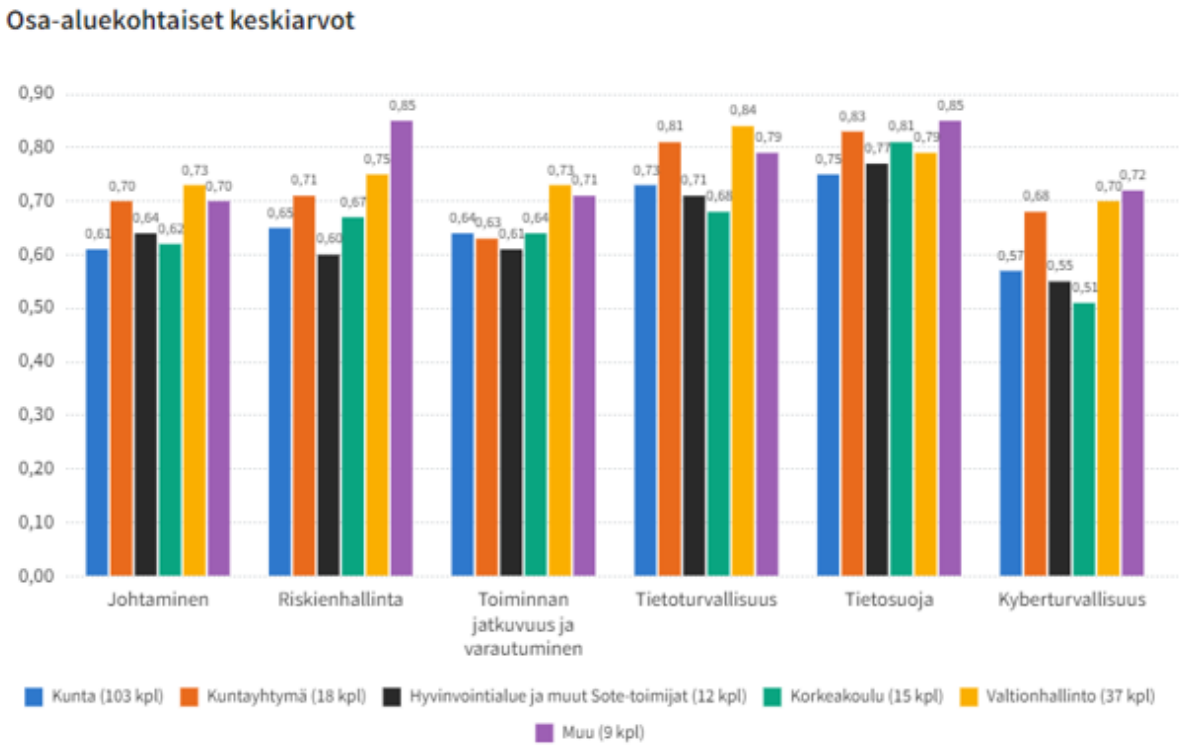
Tämä yhteenveto sisältää Digiturvan kokonaiskuvakyselyn eri osa-alueiden keskiarvotulokset, keskeiset toimiala- ja osa-aluekohtaiset havainnot sekä tulosten perusteella esille nostetut kehittämiskohteet.

Digiturvakyselyssä 2021 oli 17 taustakysymystä sekä 97 väittämää, joiden avulla kartoitettiin 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 väittämäkohtaiset keskiarvot.

2.1 Osa-alueiden keskiarvot

Kuvassa 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

Kuvion 1 tiedot on esitetty alla taulukkomuodossa (taulukko 1). Lisäksi taulukkoon on sisällytetty koko kyselyn toimialakohtaiset keskiarvot.

Taulukko 1. Digiturvakyselyn eri osioiden keskiarvot vastaajaryhmittäin

	Kaikki organisaatiot 194 kpl	**Kunta 103 kpl**	**Kuntayhtymä 18 kpl**	**Hyvinvointialue ja muut sote-toimijat 12 kpl**	**Korkeakoulu 15 kpl**	**Valtionhallinto 37 kpl**	**Muu 9 kpl**
Johtaminen	**0,65**	0,61	0,70	0,64	0,62	0,73	0,70
Riskienhallinta	**0,68**	0,65	0,71	0,60	0,67	0,75	0,85
Toiminnan jatkuvuus ja varautuminen	**0,66**	0,64	0,63	0,61	0,64	0,73	0,71
Tietoturvallisuus	**0,75**	0,73	0,81	0,71	0,68	0,84	0,79
Tietosuoja	**0,78**	0,75	0,83	0,77	0,81	0,79	0,85
Kyberturvallisuus	**0,61**	0,57	0,68	0,55	0,51	0,70	0,72
Keskiarvo	**0,70**	**0,67**	**0,73**	**0,66**	**0,66**	**0,76**	**0,77**

Korkeimmat vastauskeskiarvot saavutettiin tietosuojan (kaikkien vastausten keskiarvo 0,78) ja matalimmat kyberturvallisuuden (0,61) alueilla. Näiden ero on kuitenkin hiukan pienentynyt viime vuosina, vuonna 2021 vastaavat luvut olivat 0,81 ja 0,59. Välimaastoon asettuvat tietoturvallisuus (0,75), riskienhallinta (0,68), toiminnan jatkuvuus ja varautuminen (0,66) sekä johtaminen (0,65).

Vastaajaryhmät on muodostettu kyselyyn osallistuneiden organisaatioiden (yht. 194 organisaatiota) toimialajaottelun perusteella, ja ne ovat seuraavat:

- kunta (103 vastaajaa),
- kuntayhtymä (18 vastaajaa),
- hyvinvointialue tai muu sote-toimija (12 vastaajaa),
- korkeakoulu (15 vastaajaa),
- valtionhallinto (37 vastaajaa),
- joku muu (9 vastaajaa).

Vastanneiden määrä on kasvanut kaikissa muissa vastaajaryhmissä paitsi valtionhallinnossa, jossa se väheni jo vuonna 2022. Erityisesti kuntien ja kuntayhtymien vastausten määrä on kasvanut merkittävästi. Siitä syystä eri vuosien keskiarvoja ei voida suoraan verrata toisiinsa. Valtionhallinnon vastaajien määrää vähentää tekninen rajoite, joka toistaiseksi estää palvelun käytön Y-tunnuksettomilta organisaatioilta.

Kaikkien vastaajien osalta kyselyn keskiarvotulos on 0,70. Korkein toimialakohtainen keskiarvo on ryhmässä ”muut”, johon kuuluu mm. välillistä valtionhallintoa, kuten rahastoja, säätöitä ja laitoksia (0,77), jota seuraa valtionhallinto (0,76), kuntayhtymät (0,73), kunnat (0,67) sekä sote-toimijat ja korkeakoulut (kumpikin 0,66).

Eri vuosien vastauksia vertailtaessa on huomattava, että hyvinvointialueiden toiminta käynnistyi vasta vuoden 2023 alussa. Digiturvakyselyssä kartoitetaan organisaation toimintaprosesseja ja menettelyitä, jotka ovat aloittavissa organisaatioissa väistämättä vasta kehitysvaiheessa. Tästä syystä sote-toimijoiden tulokset ovat pudonneet huomattavasti vuodesta 2022, jolloin ne menestyivät hyvin erityisesti riskienhallinnassa ja jatkuvuuden hallinnassa.

Verrattaessa sote-toimijoiden vastauksia edellisiin vuosiin voidaan havaita, että tulokset ovat heikentyneet kaikilla osa-alueilla ja kaikkein eniten riskienhallinnassa. Erityisesti puutteita on politiikoissa, linjauksissa ja säännöllisissä prosesseissa. Myös auditointien määrä on tipahtanut ja digiturvan vastuuhenkilöiden määrä arvioidaan liian pieneksi.

Koska Digiturvakyselyn viimeinen osio ”Havainnointi” poikkeaa vastausrakenteeltaan muista, sen tuloksia ei ole mukana vertailutaulukossa. Sen sijaan vastaajaorganisaatioiden havainnoimia ja raportoimia digiturvauhkia analysoidaan erikseen kappaleessa 2.2.7.

2.2 Kysymyskohtaiset keskiarvot

Taulukoissa 2–8 eritellään Digiturvakyselyn osa-alueiden – johtaminen, riskienhallinta, jatkuvuus ja varautuminen, tietoturvallisuus, tietosuoja, kyberturvallisuus ja havainnointi – väittämäkohtaiset 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. Vertailtavuuden parantamiseksi toimialakohtaiset vastausmäärät on toistettu kunkin taulukon otsikkorivillä.

2.2.1 Johtaminen

Taulukossa 2 esitetään johtamisosion 13 väittämän vastauskeskiarvot.

Taulukko 2. Johtaminen – kysymyskohtaiset keskiarvot

Osa-alue / Väittämä	Kaikki organisaatiot 194 kpl	Kunta 103 kpl	Kuntayhtymä 18 kpl	Hyvinvointialue ja muut Sote-toimijat 12 kpl	Korkeakoulu 15 kpl	Valtionhallinto 37 kpl	Muu 9 kpl
Johtaminen	**0,65**	**0,61**	**0,70**	**0,64**	**0,62**	**0,73**	**0,70**
1. Organisaation tehtävät ja vastuut on tunnistettu ja kuvattu selkeästi.	**0,77**	**0,74**	**0,78**	**0,83**	**0,83**	**0,81**	**0,83**
2. Organisaatio on kartoittanut sen digitaalista turvallisuutta ohjaavan lainsäädännön ja tunnistanut siitä aiheutuvat velvoitteet.	**0,74**	**0,68**	**0,81**	**0,79**	**0,77**	**0,86**	**0,72**
3. Organisaatio on kartoittanut keskeiset sidos- ja asiakasryhmät sekä niiltä tulevat digiturvavaatimukset.	**0,66**	**0,59**	**0,74**	**0,75**	**0,67**	**0,73**	**0,83**
4. Organisaatiossa on riittävästi osaavaa henkilöstöä digiturvallisuuden eri osa-alueilla.	**0,45**	**0,45**	**0,64**	**0,25**	**0,33**	**0,47**	**0,50**
5. Organisaatiolla on riittävä budjetti digiturvallisuuden ylläpitoon sekä kehittämiseen.	**0,57**	**0,53**	**0,86**	**0,46**	**0,57**	**0,61**	**0,56**
6. Organisaation johto on sitoutunut digitaalisen turvallisuuden kehittämiseen.	**0,79**	**0,77**	**0,75**	**0,83**	**0,73**	**0,86**	**0,78**
7. Organisaation digitaalisen turvallisuuden osa-alueita kehitetään järjestelmällisesti hyödyntäen yhtä tai useampaa selkeää prosessia tai hallintamallia.	**0,53**	**0,49**	**0,56**	**0,46**	**0,50**	**0,64**	**0,56**
8. Henkilöstölle on olemassa riittävä ohjeistus digitaalisesta turvallisuudesta.	**0,71**	**0,72**	**0,75**	**0,63**	**0,60**	**0,74**	**0,78**
9. Henkilöstölle annetaan säännöllisesti koulutusta digitaalisesta turvallisuudesta.	**0,63**	**0,59**	**0,67**	**0,58**	**0,47**	**0,82**	**0,67**
10. Organisaatiolla on olemassa prosessi väärinkäytöksiin reagoimiseksi.	**0,77**	**0,72**	**0,81**	**0,92**	**0,83**	**0,82**	**0,83**
11. Digitaaliseen turvallisuuteen liittyvät mittarit on määritelty.	**0,33**	**0,31**	**0,28**	**0,29**	**0,33**	**0,39**	**0,50**
12. Digitaalisen turvallisuuden tilaa seurataan jatkuvasti.	**0,76**	**0,71**	**0,83**	**0,79**	**0,77**	**0,84**	**0,78**
13. Digitaalisen turvallisuuden kokonaistilanteesta raportoidaan säännöllisesti organisaation johdolle.	**0,66**	**0,57**	**0,58**	**0,75**	**0,63**	**0,85**	**0,83**

Paras kysymyskohtainen keskiarvo (0,79) oli väittämässä 6, joka koski johdon sitoutumista, ja seuraavaksi parhaat tehtävien ja vastuiden tunnistamista sekä väärinkäytöksiin reagoimista koskevissa väittämissä (0,77). Heikointa suoriutuminen on digitaalisen turvallisuuden mittaristoa koskevassa väittämässä (0,33). Lisäksi väittämät ”Organisaatiolla on riittävä budjetti digiturvallisuuden ylläpitoon ja kehittämiseen” ja ”Organisaatiossa on riittävästi osaavaa henkilöstä kehittämässä digiturvallisuuden eri osa-alueita” osoittavat, että resurssien kanssa tuskaillaan hyvin monissa organisaatiossa.

Yksi keino kehittää organisaation digiturvaan liittyvä mittaristoa on ottaa kokonaiskuvapalvelu ja siellä olevat kyselyt osaksi organisaation digiturvan mittaamista ja raportointia.

Osa-alueen kokonaiskeskiarvo (0,65) on digiturvallisuuden viidestä osa-alueesta toiseksi matalin, ja erot toimialojen kesken ovat varsin pienet; korkein keskiarvo on valtionhallinnossa (0,73) ja alin kunnilla (0,61). Valtionhallinnossa taso on hiukan noussut ja sote-toimijoilla laskenut.

Kehitys vuoteen 2021 verrattuna

Vuoden 2021 kyselyyn verrattuna kokonaiskeskiarvo on pysynyt samana, mutta yksittäisten väittämien tuloksissa on pientä vaihtelua. Väittämien keskinäinen järjestys on pysynyt kutakuinkin samana. Digiturvallisuuden tilanteen seuranta on hiukan parantunut, kenties kyberhyökkäysten määrästä ja maailmantilanteen muutoksista johtuen.

Eri toimialojen keskiarvoissa on tapahtunut pieniä muutoksia; valtionhallinnossa taso on hiukan noussut ja sote-toimijoilla laskenut. Sote-toimijoilla digiturvan johtaminen ei organisaatiomuutosten vuoksi voikaan olla vielä kovin hyvällä tasolla. Siksi onkin mielenkiintoista seurata tilanteen kehittymistä tulevina vuosina.

Johtamisen kehittämiskohteet

Kehittämiskohde 1

Henkilöstön osaamisen ja koulutustarpeiden edelleen kehittäminen. 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.–29.9.2023, hyödyntämään Digiturvallinen elämä -materiaaleja (linkki) sekä seuraamaan Digi- ja väestötietoviraston tuottamia verkkotilaisuuksia (linkki). Kuukausittaisen 15 minuutin Digiturvavartin avulla organisaation henkilöstö saa säännöllistä digiturvakoulutusta läpi vuoden. Jo tämän koulutuksen avulla organisaatioiden digiturvakoulutuksen määrää saisi nostettua seuraavalle tasolle.

Kehittämiskohde 2

Harjoitustoiminnan kehittäminen. Organisaation johdolla on kriittinen rooli erilaisten kriittisten häiriötilanteiden, hyökkäysten ja loukkausten hallinnan johtamisessa, ja siksi johdon ja asiantuntijoiden tulisi harjoitella yhdessä. Mikäli organisaatio ei ole aiemmin toteuttanut digitaalisen turvallisuuden harjoituksia, se voi osallistua siihen joko marraskuussa 2023 tai suorittaa digitalisoidun TAISTOmaatti-harjoituksen.
https://dvv.fi/taisto
TAISTOmaatti - digitaalinen harjoitus organisaation toiminnan ja jatkuvuuden mahdollistamiseksi - eOppiva

Kehittämiskohde 3

Prosessit kuntoon. Digitaaliseen turvallisuuteen liittyvät tärkeimmät prosessit tulee kuvata ja jalkauttaa, jotta niistä saadaan luontainen osa organisaation toimintaa. Prosessien toimivuutta tulee seurata ja kehittää niitä edelleen systemaattisesti. Digiturvallisuuden hallintamallien kehittämiseen löytyy materiaalia DVV:n Digiturvan tietoiskut -sivustolta

Uusi kehittämiskohde 2023_1

Digiturvan vastuuhenkilöiden nimeäminen. Jokaisen julkishallinnon organisaation tulisi nimetä henkilöt, joiden tehtäviin digitaalisen turvallisuuden osa-alueiden kehittäminen kuuluu.

Tietosuojavastaava on julkisessa hallinnossa pakollinen, mutta myös muille osa-alueille pitäisi nimetä vastuuhenkilöt.

Uusi kehittämiskohde 2023_2
Tietoturvapoikkeamien havainnointi ja kirjaaminen. Jokaisessa organisaatiossa tapahtuu poikkeamia, jotka voivat eskaloituessaan merkittävästi haitata organisaation varsinaista toimintaa. Siksi kaikkien organisaatioiden tulisi luoda menettely, jonka avulla henkilökunta voi helposti ilmoittaa havainnoistaan, ja jonka avulla poikkeamat tutkitaan sekä niiden kehittymistä ja kustannuksia seurataan.

Uusi kehittämiskohde 2023_3
Väärinkäytöksiin varautuminen. Jokaisen organisaation tulisi tiedostaa sisäisten ja ulkoisten väärinkäytösten mahdollisuus ja luoda niihin reagoimiseksi toimiva prosessi. perustana.

2.2.2 Riskienhallinta

Taulukossa 3 esitetään riskienhallinnan kahdeksan väittämän vastauskeskiarvot.

Taulukko 3. Riskienhallinta – kysymyskohtaiset keskiarvot

Osa-alue / Väittämä	Kaikki organisaatiot 194 kpl	Kunta 103 kpl	Kuntayhtymä 18 kpl	Hyvinvointialue ja muut Sote-toimijat 12 kpl	Korkeakoulu 15 kpl	Valtionhallinto 37 kpl	Muu 9 kpl
Riskienhallinta	**0,68**	**0,65**	**0,71**	**0,60**	**0,67**	**0,75**	**0,85**
14. Organisaatiolla on johdon hyväksymät, toimintaan sovitetut riskienhallinnan linjaukset, vastuut ja prosessi.	**0,73**	**0,68**	**0,72**	**0,58**	**0,80**	**0,85**	**1,00**
15. Organisaatio tekee digiturvallisuuteen liittyvää säännöllistä riskienarviointia, jossa huomioidaan uudet ilmiöt, toimintaympäristön muutokset ja oman toiminnan vaikutukset sidosryhmien ja asiakkaiden tilanteeseen.	**0,56**	**0,50**	**0,61**	**0,50**	**0,60**	**0,66**	**0,78**
16. Organisaatiossa viestitään digiturvallisuuden riskitilanteesta ja uusista riskeistä koko organisaation laajuisesti.	**0,75**	**0,76**	**0,83**	**0,71**	**0,53**	**0,77**	**0,89**
17. Organisaatiossa raportoidaan riskitilanteesta johdolle säännöllisesti.	**0,72**	**0,65**	**0,64**	**0,67**	**0,80**	**0,88**	**0,94**
18. Kriittisistä, organisaation toimintaa uhkaavista riskeistä raportoidaan johdolle välittömästi.	**0,86**	**0,83**	**1,00**	**0,88**	**0,73**	**0,91**	**0,89**
19. Organisaatio seuraa riskien ja niiden hallintatoimenpiteiden tilannetta säännöllisesti.	**0,62**	**0,61**	**0,64**	**0,50**	**0,60**	**0,68**	**0,78**
20. Organisaatiossa arvioidaan jäännösriskejä riskienhallintatoimenpiteiden toteuttamisen jälkeen ja jäännösriskit käsitellään asianmukaisella tasolla.	**0,49**	**0,50**	**0,47**	**0,42**	**0,53**	**0,46**	**0,56**
21. Organisaatiossa kehitetään riskienhallintaprosessia saatujen riskienhallinnan tavoitteiden tai saatujen kokemusten perusteella.	**0,72**	**0,68**	**0,72**	**0,58**	**0,77**	**0,78**	**0,94**

Korkein kysymyskohtainen keskiarvo saavutettiin väittämässä, joka koski kriittisten riskien raportoimista johdolle välittömästi (0,86). Heikoimmaksi tulos jää jäännösriskien arvioinnissa ja käsittelyssä (0,49) sekä säännöllisessä digiturvallisuuteen liittyvässä riskienarvioinnissa, jossa huomioidaan uudet ilmiöt, toimintaympäristön muutokset ja oman toiminnan vaikutukset sidosryhmien ja asiakkaiden tilanteeseen (0,56).

Osa-alueen keskiarvo on 0,68. Toimialakohtaisesti erot ovat tässä osa-alueessa suurimmat; korkein keskiarvo on ryhmässä Muut (0,85) ja matalin sote-toimijoilla (0,60).

Kehitys vuoteen 2021 verrattuna

Osa-alueen keskiarvo on täsmälleen sama kuin kaksi vuotta aiemmin. Väittämien keskinäisessä järjestyksessä ei ole muutoksia, mutta riskienhallinnan säännöllisyydessä ja johdolle raportoinnissa on tapahtunut pientä parannusta. Lisäksi aiemman kyselyn yksittäisten väittämien vastaajaryhmäkohtaiset heikot arvot ovat poistuneet.

Vastaajaryhmistä suurin muutos on sote-toimijoilla, joiden tulos on pudonnut merkittävästi (0,73 → 0,6) ja tämä onkin niille tärkeä kehittämiskohde.

Riskienhallinnan kehittämiskohteet

Kehittämiskohde 5
Digitaalisen toimintaympäristön riskienhallinnan kokonaisvaltainen kehittäminen. Riskien arviointia tulee toteuttaa järjestelmällisesti kaikissa keskeisissä muutoksissa, häiriöissä ja poikkeamissa – niin sisäisissä kuin ulkoisissa. Organisaatiolla tulee olla kuvattuna riskienhallinnan toteuttamista ohjaavat linjaukset, joissa kuvataan siihen liittyvät menettelytavat ja vastuut. Vain kerran vuodessa tehtävästä toiminnasta on syytä päästä useammin toteutettavaan muutosarviointiin ja uusien riskien tunnistamiseen. Toistuvuuteen tulee yhdistää seurantatoimet ja jäännösriskien tarkastelu. Muutosten ja riskitasojen seurannan raportointia johdolle pitää kehittää.

2.2.3 Toiminnan jatkuvuus ja varautuminen

Toiminnan jatkuvuus ja varautuminen -osion 16 väittämän vastauskeskiarvot ovat taulukossa 4.

Taulukko 4. Toiminnan jatkuvuus ja varautuminen – kysymyskohtaiset keskiarvot

Osa-alue / Väittämä	Kaikki organisaatiot 194 kpl	Kunta 103 kpl	Kuntayhtymä 18 kpl	Hyvinvointialue ja muut Sote-toimijat 12 kpl	Korkeakoulu 15 kpl	Valtionhallinto 37 kpl	Muu 9 kpl
Toiminnan jatkuvuus ja varautuminen	**0,66**	**0,64**	**0,63**	**0,61**	**0,64**	**0,73**	**0,71**
22. Organisaation tehtävät ja vastuut ovat selkeät myös poikkeustilanteissa ja poikkeusoloissa.	**0,80**	**0,82**	**0,74**	**0,75**	**0,80**	**0,77**	**0,83**
23. Organisaatiolla on prosessi ja valmiudet nopeaan ja tehokkaaseen digiturvallisuuden häiriöiden, uhkien ja poikkeamien käsittelyyn.	**0,73**	**0,71**	**0,78**	**0,67**	**0,73**	**0,77**	**0,83**
24. Organisaatio on kuvannut jatkuvuuden hallinnan periaatteet, tavoitteet, organisoinnin ja vastuut.	**0,61**	**0,55**	**0,56**	**0,58**	**0,67**	**0,73**	**0,72**
25. Organisaatio on tunnistanut ja dokumentoinut suojattavat kohteet.	**0,66**	**0,67**	**0,72**	**0,54**	**0,60**	**0,66**	**0,67**
26. Organisaation on tunnistanut sen toiminnan kannalta kriittiset toiminnot, palvelut, tiedot, tietovarannot ja tietojärjestelmät.	**0,76**	**0,74**	**0,82**	**0,63**	**0,70**	**0,85**	**0,67**
27. Organisaatio on määritellyt kuinka pitkiä toimintakatkoksia kriittiset toiminnot sietävät organisaation toiminnan häiriintymättä.	**0,56**	**0,53**	**0,74**	**0,46**	**0,47**	**0,65**	**0,50**
28. Toiminnan jatkuvuuden edellyttämät palvelutasovaatimukset ovat osa hankintavaatimuksia ja sopimuksia.	**0,62**	**0,58**	**0,60**	**0,67**	**0,53**	**0,69**	**0,83**

29. Jatkuvuuteen liittyviä riskejä ja riskitilanteen muutosta arvioidaan säännöllisesti.	0,45	0,42	0,44	0,46	0,27	0,54	0,72
30. Organisaatiolle ja sen kriittisille toiminnoille/palveluille on laadittu jatkuvuussuunnitelmat, jotka perustuvat tunnistettuihin riskeihin.	0,53	0,51	0,38	0,58	0,47	0,66	0,56
31. Kriittisille tietojärjestelmille on laadittu toipumissuunnitelmat.	0,58	0,53	0,62	0,67	0,50	0,68	0,67
32. Organisaatiolla on häiriö- ja kriisitilanteiden viestintäsuunnitelma.	0,84	0,86	0,58	0,71	0,90	0,91	0,83
33. Suunnitelmien sisältö on koulutettu häiriötilanteiden hallintaan osallistuville henkilöille.	0,57	0,57	0,50	0,50	0,63	0,61	0,56
34. Organisaatiossa on luotu yhteydet ja verkostot tarvittavien sidosryhmien väliseen viestintään poikkeamatilanteissa.	0,67	0,67	0,63	0,63	0,57	0,74	0,72
35. Organisaatiolla on olemassa menettely sen toimintaa kohdistuvien häiriöiden, hyökkäysten ja loukkausten ilmoittamiseksi keskeisille viranomaisille.	0,92	0,92	0,86	0,96	0,87	0,96	0,94
36. Organisaatio harjoittelee säännöllisesti sen toimintaan kohdistuvien häiriöiden, poikkeamien ja hyökkäysten havainnointia, reagointia ja johtamista.	0,65	0,60	0,53	0,58	0,83	0,81	0,61
37. Jatkuvuus-, toipumis- ja viestintäsuunnitelmia päivitetään harjoitusten tai toteutuneiden häiriötilanteiden perusteella	0,61	0,60	0,56	0,42	0,67	0,70	0,61

Osion kaikkien vastausten keskiarvo on 0,66. Korkein kysymyskohtainen keskiarvo (0,92) oli väittämässä ”Organisaatiolla on olemassa menettely sen toimintaan kohdistuvien häiriöiden, hyökkäysten ja loukkausten ilmoittamiseksi keskeisille viranomaisille”. Heikoimmat keskiarvot koskivat riskienhallinnan huomioimista jatkuvuussuunnittelussa. Siihen liittyvät väittämät ”Jatkuvuuteen liittyviä riskejä ja riskitilanteen muutosta arvioidaan säännöllisesti” (0,45) ja ”Organisaatiolle ja sen kriittisille toiminnoille/palveluille on laadittu jatkuvuussuunnitelmat, jotka perustuvat tunnistettuihin riskeihin” (0,53).

Toimialoista korkeimpaan keskiarvoon yltää valtionhallinto (0,73) ja matalin keskiarvo on sote-toimijoilla (0,61).

Kehitys vuoteen 2021 verrattuna

Osa-alueen keskiarvo on hiukan tipahtanut kahden vuoden takaisesta, jolloin se oli 0,68. Valtionhallinnossa on tapahtunut selvää parannusta (0,68 → 0,73), mutta kaikilla muilla toimialoilla keskiarvot ovat laskeneet. Kaikkein suurin pudotus on tapahtunut sote-toimijoilla, mutta se on ymmärrettävää hyvinvointialueilla, joiden toiminta käynnistyi vuoden 2023 alussa eivätkä kaikki toimintamallit ole vielä voineet vakiintua. Kokonaiskuvapalvelu ja tämä raportti tarjoavat jatkossa hyvän työkalun tilanteen kehittymisen seuraamiseen.

Väittämien keskinäisessä järjestyksessä ei ole juuri muutoksia. Useimmissa väittämissä keskiarvot ovat hiukan laskeneet, mutta harjoittelua ja viranomaisilmoituksia koskevat keskiarvot ovat nousseet: harjoittelun 0,59 → 0,65 ja viranomaisilmoitusten 0,88 → 0,92. Taisto-harjoitusten vaikutus todennäköisesti näkyy näissä kohdissa. Taistossa viranomaisilmoitusten laatiminen on olennainen tehtävä ja harjoitus on helppo tapa aloittaa kyberharjoittelu, jos organisaatio ei ole aiemmin harjoitellut.

Toiminnan jatkuvuuden ja varautumisen kehittämiskohteet

Uusi kehittämiskohde 2023_5
Jatkuvuuden hallinnan kehittäminen. Jokaisen organisaation tulisi varautua toimintaa merkittävästi haittaaviin häiriöihin. Organisaatiolla tulisi olla kuvattuna jatkuvuuden hallintaa ohjaavat linjaukset, joissa kuvataan mm. häiriötilanteiden johtaminen, vastuut ja viestintä. Kriittiset toiminnot ja palvelut tulee tunnistaa ja laatia jatkuvuussuunnitelmat ainakin niille. Olennainen osa jatkuvuuden hallintaa on häiriötilanteiden harjoittelu ja suunnitelmien päivittäminen niistä saatujen oppien perusteella.

2.2.4 Tietoturvallisuus

Taulukossa 5 esitetään Tietoturvallisuus-osion 16 väittämän vastauskeskiarvot.

Taulukko 5. Tietoturvallisuus – kysymyskohtaiset keskiarvot

Osa-alue / Väittämä	Kaikki organisaatiot 194 kpl	Kunta 103 kpl	Kuntayhtymä 18 kpl	Hyvinvointialue ja muut Sote-toimijat 12 kpl	Korkeakoulu 15 kpl	Valtionhallinto 37 kpl	Muu 9 kpl
Tietoturvallisuus	**0,75**	**0,73**	**0,81**	**0,71**	**0,68**	**0,84**	**0,79**
38. Organisaatiolla on johdon hyväksymä tietoturvapolitiikka tai vastaava tietoturvallisuuden toteuttamista ohjaava asiakirja.	**0,89**	**0,90**	**0,72**	**0,79**	**0,83**	**0,95**	**1,00**
39. Organisaatiolla on olemassa henkilöiden taustatarkistuksiin liittyvä menettely, joka kattaa oman ja palvelutoimittajien henkilöstön.	**0,48**	**0,35**	**0,32**	**0,75**	**0,19**	**0,93**	**0,31**
40. Organisaatiolla on olemassa käyttövaltuuspolitiikka ja prosessi käyttövaltuuksien hallintaan.	**0,71**	**0,69**	**0,75**	**0,63**	**0,80**	**0,73**	**0,78**
41. Käyttövaltuuksien ajantasaisuus varmistetaan säännöllisesti.	**0,63**	**0,64**	**0,81**	**0,42**	**0,50**	**0,62**	**0,67**
42. Organisaatio on määrittänyt fyysisesti suojatut turvallisuusalueet asiakirjojen käsittelyn ja tietojärjestelmien suojaamiseksi.	**0,65**	**0,58**	**0,76**	**0,67**	**0,65**	**0,80**	**0,61**
43. Organisaation tietojärjestelmät ja laitteet ovat kattavasti järjestelmänhallinnan piirissä.	**0,88**	**0,87**	**0,94**	**0,75**	**0,83**	**0,92**	**0,89**
44. Organisaatiolla on käytössä monivaiheinen tunnistus etäkäytössä.	**0,80**	**0,73**	**0,83**	**0,92**	**0,70**	**0,97**	**0,78**
45. Toimitilojen ulkopuolella työskenneltäessä yhteydet organisaation ICT-palveluihin sallitaan vain VPN-yhteydellä.	**0,86**	**0,89**	**0,85**	**0,88**	**0,75**	**0,84**	**0,78**
46. Organisaatiolla on olemassa tarvittavat tekniset ratkaisut ja menettelyt haittaohjelmien tunnistamiseen ja estämiseen.	**0,96**	**0,94**	**1,00**	**0,96**	**0,97**	**0,97**	**0,94**
47. Organisaation tiedoista ja järjestelmistä otetaan säännöllisesti varmuuskopiot.	**0,92**	**0,92**	**0,94**	**0,83**	**0,90**	**0,95**	**0,89**
48. Varmuuskopioiden palautusta testataan säännöllisesti	**0,56**	**0,57**	**0,83**	**0,33**	**0,40**	**0,51**	**0,61**
49. Tietojärjestelmien käytöstä ja tietojen luovutuksista kerätään riittävät lokitiedot.	**0,69**	**0,67**	**0,75**	**0,71**	**0,60**	**0,70**	**0,83**
50. Käytössä olevien tietojärjestelmien teknisiin haavoittuvuuksiin liittyviä tiedotteita seurataan ja niihin reagoidaan.	**0,91**	**0,90**	**0,94**	**0,88**	**0,90**	**0,96**	**0,94**
51. Tietoturvallisuuteen ja tietojärjestelmiin liittyviä auditointeja tehdään säännöllisesti.	**0,49**	**0,40**	**0,61**	**0,29**	**0,33**	**0,77**	**0,72**
52. Tietoturva- ja tietosuojavaatimukset ovat osa hankintavaatimuksia ja sopimuksia.	**0,80**	**0,74**	**0,81**	**0,92**	**0,77**	**0,92**	**0,89**
53. Tietoturva- ja tietosuojavaatimukset otetaan huomioon myös järjestelmien ja palveluiden kehittämisessä sekä ylläpidossa.	**0,81**	**0,79**	**0,97**	**0,67**	**0,67**	**0,85**	**0,94**

Kyselyn osa-alueista tietoturvallisuus yltää kokonaiskeskiarvollaan (0,75) toiseksi korkeimmalle sijalle tietosuojan jälkeen. Hyvää tulosta selittää se, että kaikista digiturvallisuuden osa-alueista tietoturvallisuutta on kehitetty pisimpään ja sitä koskeva lainsäädäntö (tiedonhallintalaki) on koskenut koko julkista hallintoa vuoden 2020 alusta lähtien.

Kysymyksistä paras kokonaiskeskiarvo koskee haittaohjelmien torjuntaa (0,96). Vaatimattomimmat tulokset ovat kohdissa ”Tietoturvallisuuteen ja tietojärjestelmiin liittyviä auditointeja tehdään säännöllisesti” (0,49) ja ”Organisaatiolla on olemassa henkilöiden taustatarkistuksiin liittyvä menettely, joka kattaa oman ja palvelutoimittajien henkilöstön” (0,48).

Toimialoista korkein keskiarvo on valtionhallinnolla (0,84) ja alin korkeakouluilla (0,68). Toimialojen väliset keskiarvoerot ovat siten kohtaisen suuria.

Kehitys vuoteen 2021 verrattuna

Osa-alueen keskiarvo on hiukan tipahtanut kahden vuoden takaisesta, jolloin se oli 0,78. Valtionhallinnossa ja kuntayhtymissä on tapahtunut pientä parannusta, muilla toimialoilla keskiarvot ovat laskeneet.

Selvimmät väittämäkohtaiset parannukset ovat tapahtuneet etäkäytön turvallisuudessa: monivaiheinen tunnistaminen (0,74 → 0,80) ja VPN-yhteydet (0,83 → 0,86). Lisäksi pienempää parannusta on tapahtunut haavoittuvuustiedotteiden seurannassa ja reagoinnissa sekä varmistusten testaamisessa. Tämä kaikki lienee seurausta verkkohyökkäysten lisääntymisestä.

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. Ulkoistettujen palvelujen osalta tulee varmistaa, että palvelun tarjoajan prosessit ovat toimivat ja riittävät tiedon turvaamiseksi myös poikkeavissa tilanteissa.

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. Lokitietojen riittävyys ja käyttökelpoisuus pitää varmistaa myös ulkoistetuissa palveluissa.

Kehittämiskohde 10
Haavoittuvuuksien hallinnan ja auditointitoiminnan kehittäminen. 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.

2.2.5 Tietosuoja

Taulukossa 6 esitetään tietosuojaosion 15 väittämän vastauskeskiarvot.

Taulukko 6. Tietosuoja – kysymyskohtaiset keskiarvot

Osa-alue / Väittämä	Kaikki organisaatiot 194 kpl	Kunta 103 kpl	Kuntayhtymä 18 kpl	Hyvinvointialue ja muut Sote-toimijat 12 kpl	Korkeakoulu 15 kpl	Valtionhallinto 37 kpl	Muu 9 kpl
Tietosuoja	**0,78**	**0,75**	**0,83**	**0,77**	**0,81**	**0,79**	**0,85**
54. Organisaatiolla on tiedossa, millaisia henkilötietoja se käsittelee (TsA 4 art. 1 kohta)	**0,94**	**0,94**	**0,97**	**0,83**	**0,87**	**1,00**	**0,94**
55. Henkilötietojen käsittelyn oikeusperusteet on tunnistettu (TsA 6, 9 ja 10 art. TsL 6 ja 29 §, TtsL 2, 3, 5 ja 6 luku)	**0,93**	**0,93**	**0,97**	**0,92**	**0,93**	**0,89**	**1,00**
56. Organisaatio on tunnistanut, milloin se toimii rekisterinpitäjänä ja milloin se toimii käsittelijänä (TsA 4 art. 7-8 kohta)	**0,90**	**0,88**	**0,94**	**0,88**	**0,93**	**0,88**	**1,00**
57. Sopimukset henkilötietojen käsittelystä on tehty ja sopimusten hallinta on kunnossa (TsA 28 art)	**0,74**	**0,71**	**0,75**	**0,75**	**0,77**	**0,76**	**0,94**
58. Yhteisrekisterinpitäjyystilanteet tunnistetaan ja yhteisrekisterinpitäjyyttä koskevista vastuista on sovittu? (TsA 26 art., huom. myös EDPB:n ohje)	**0,69**	**0,62**	**0,79**	**0,63**	**0,83**	**0,75**	**0,81**
59. Henkilötietojen käsittelyyn liittyvät oman organisaation sisäiset roolit ja vastuut on tunnistettu ja vahvistettu (TihL 4.2. §, TsA 37 art.)	**0,85**	**0,84**	**0,86**	**0,83**	**0,90**	**0,82**	**0,89**
60. Tietosuojavastaavan asema ja rooli on määritelty (TsA 37 – 39 art.)	**0,93**	**0,92**	**0,92**	**0,88**	**0,97**	**0,96**	**1,00**
61. Seloste käsittelytoimista on laadittu (TsA 30 art.)	**0,80**	**0,77**	**0,89**	**0,71**	**0,83**	**0,82**	**0,83**
62. Organisaatiolla on tiedossa missä tietojärjestelmissä henkilötietoja käsitellään	**0,87**	**0,87**	**0,97**	**0,75**	**0,83**	**0,86**	**0,89**
63. Rakenteeton tieto on tunnistettu ja sen hallinta on kuvattu	**0,47**	**0,46**	**0,56**	**0,38**	**0,43**	**0,47**	**0,50**
64. Informointikäytännöt on määritelty ja niitä noudatetaan (TsA 12-14 art. Laki digitaalisten palveluiden tarjoamisesta (306/2019)	**0,72**	**0,68**	**0,86**	**0,71**	**0,87**	**0,71**	**0,75**
65. Organisaatiolla on olemassa prosessi vaikutustenarvioinnin tarpeen tunnistamiseksi (TsA 35 (1) art.)	**0,62**	**0,55**	**0,59**	**0,88**	**0,70**	**0,68**	**0,81**
66. Organisaatiolla on olemassa henkilötietojen tietoturvaloukkausten hallintaprosessi (TsA 33-34 art.)	**0,87**	**0,85**	**0,83**	**0,92**	**0,87**	**0,91**	**0,94**
67. Jos henkilötietoja siirretään kolmansiin maihin, organisaatio on selvittänyt siirron edellytykset? (TsA 5 luku)	**0,69**	**0,62**	**0,78**	**0,80**	**0,79**	**0,69**	**0,83**
68. Organisaatiossa tietosuojasta huolehtiminen on muuttunut toiminnaksi, kulttuuriksi ja asenteeksi (TSA 5 art.)	**0,61**	**0,58**	**0,64**	**0,58**	**0,57**	**0,70**	**0,61**

Lähes jokainen organisaatio tuntee käsittelemänsä henkilötietotyypit ja on tunnistanut niiden käsittelyn oikeusperusteet. Näiden väittämäkohtaiset keskiarvot ovat 0,94 ja 0,93. Suurin haaste on rakenteettoman tiedon tunnistamisessa ja hallinnassa (0,47).

Tietosuoja-osion kokonaiskeskiarvo (0,78) on koko kyselyn korkein ja toimialojen väliset erot ovat varsin pienet. Korkein keskiarvo on ryhmässä Muut (0,85) ja pienin kunnissa (0,75).

Kehitys vuoteen 2021 verrattuna

Myös tämän osa-alueen keskiarvo on hiukan tipahtanut kahden vuoden takaisesta, jolloin se oli 0,81. Pientä pudotusta on tapahtunut kaikilla toimialoilla.

Ainoa väittämä, jonka keskiarvossa on tapahtunut pientä parannusta, on ”Organisaatiolla on olemassa prosessi vaikutustenarvioinnin tarpeen tunnistamiseksi” (0,61 → 0,62). Erityisesti sote-toimijoilla ja valtionhallinnossa keskiarvo on parantunut. Olisiko niin, että tapahtuneet organisaatiomuutokset ovat pakottaneet arvioimaan henkilötietojen käsittelyä ja sen asianmukaisuutta?

Tietosuojan kehittämiskohteet

Kehittämiskohde 11
Tietosuojan vaikutustenarviointi. Kysymykseen kielteisesti vastanneiden tulisi varmistaa, että kokonaisuus saadaan osaksi organisaation toimintaa.

Uusi kehittämiskohde 2023_6
Tietosuojan kokonaisvaltainen tarkastelu. Organisaatioiden tulee tunnistaa käsittelemänsä henkilötiedot sekä niiden käsittelyperusteet. On tärkeää laatia linjaukset siitä, missä järjestelmissä tai palveluissa (esim. pilvipalvelut) henkilötietoja käsitellään. Jos käsittelyssä havaitaan puutteita, organisaatioiden tulee kartoittaa kehittämistarpeet ja laatia kehittämissuunnitelma.

2.2.6 Kyberturvallisuus

Kyberturvallisuus-osion yhdeksän väittämän vastauskeskiarvot ovat taulukossa 7.

Taulukko 7. Kyberturvallisuus – kysymyskohtaiset keskiarvot

Osa-alue / Väittämä	Kaikki organisaatiot 194 kpl	Kunta 103 kpl	Kuntayhtymä 18 kpl	Hyvinvointialue ja muut Sote-toimijat 12 kpl	Korkeakoulu 15 kpl	Valtionhallinto 37 kpl	Muu 9 kpl
Kyberturvallisuus	**0,61**	**0,57**	**0,68**	**0,55**	**0,51**	**0,70**	**0,72**
69. Organisaatio on huomioinut digitaalisen turvallisuuden osana kokonaisarkkitehtuuria.	**0,71**	**0,72**	**0,69**	**0,63**	**0,60**	**0,74**	**0,83**
70. Organisaatiolla on riittävät resurssit ja osaaminen digitaalisen turvallisuuden kehittämiseen osana kokonaisarkkitehtuuria.	**0,50**	**0,46**	**0,66**	**0,42**	**0,53**	**0,51**	**0,72**
71. Organisaatio on tunnistanut oman roolinsa YTS:n mukaisissa tehtävissä sekä globaalissa näkökulmassa	**0,68**	**0,62**	**0,79**	**0,75**	**0,57**	**0,83**	**0,72**
72. Organisaatiossa on tunnistettu ne kriittiset palvelut, joilla on merkittävä vaikutus toisten organisaatioiden tai yhteiskunnan toimintaan.	**0,81**	**0,82**	**0,81**	**0,75**	**0,69**	**0,86**	**0,83**
73. Organisaatiossa on kattavasti tunnistettu kriittisten palveluiden riippuvuudet ulkoisista palvelutoimittajista.	**0,76**	**0,74**	**0,88**	**0,71**	**0,70**	**0,80**	**0,83**
74. Organisaation kriittisiin palveluihin liittyviä riskejä arvioidaan ja hallitaan säännöllisesti ja kattavasti yhteistyössä palvelutoimittajien kanssa.	**0,51**	**0,50**	**0,56**	**0,42**	**0,33**	**0,60**	**0,72**

75. Kriittisten toimittajien ja alihankkijoiden kanssa käsitellään digiturvallisuutta säännöllisesti toimittaja/palvelunhallintakokouksissa.	0,55	0,51	0,67	0,54	0,27	0,69	0,78
76. Organisaatio on varautunut ja laatinut suunnitelman siihen kohdistuvan mustamaalaus- tai vaikuttamiskampanjan varalta.	0,40	0,34	0,42	0,29	0,50	0,57	0,33
77. Organisaatiolla on menettely, jolla se seuraa toimintaympäristössä tapahtuvia ilmiöitä ja arvioi niiden vaikutusta organisaation toimintaan.	0,52	0,45	0,64	0,42	0,47	0,70	0,67

Korkein kysymyskohtainen keskiarvo koskee organisaatioiden valmiuksia tunnistaa sellaiset kriittiset palvelut, jotka vaikuttavat myös muiden tahojen toimintaan (0,81). Heikoin tulos on puolestaan organisaatioihin kohdistuviin mustamaalauskampanjoihin varautumisessa (0,40).

Osion kokonaiskeskiarvo (0,61) on koko kyselyn alhaisin. Toimialoista korkein keskiarvo on ryhmässä Muut (0,72) ja heikoin korkeakouluissa (0,51).

Kehitys vuoteen 2021 verrattuna

Tällä osa-alueella keskiarvo on hiukan noussut kahden vuoden takaisesta, jolloin se oli 0,59. Toimialoista parannusta on tapahtunut kunnissa (0,52 → 0,57), kuntayhtymissä (0,57 → 0,68) ja valtionhallinnossa (0,65 → 0,70). Eniten heikennystä on tapahtunut sote-toimijoissa (0,69 → 0,55).

Väittämä, jonka keskiarvossa on tapahtunut eniten parannusta, on ”Organisaatiolla on riittävät resurssit ja osaaminen digitaalisen turvallisuuden kehittämiseen osana kokonaisarkkitehtuuria” (0,41 → 0,50). Muissa väittämissä ei ole tapahtunut suuria muutoksia.

Kyberturvallisuuden kehittämiskohteet

Kehittämiskohde 12
JUDO-hankkeen arkkitehtuurityön hyödyntäminen. Digi- ja väestötietovirasto on kehittänyt digitaalisen turvallisuuden arkkitehtuuria JUDO-hankkeessa. Suosittelemme tutustumaan ja hyödyntämään arkkitehtuuria https://wiki.dvv.fi/display/DTA/Digitaalisen+turvallisuuden+arkkitehtuuri

Kehittämiskohde 12
JUDO-hankkeen arkkitehtuurityön hyödyntäminen. Digi- ja väestötietovirasto on kehittänyt digitaalisen turvallisuuden arkkitehtuuria JUDO-hankkeessa. Suosittelemme tutustumaan ja hyödyntämään arkkitehtuuria https://wiki.dvv.fi/display/DTA/Digitaalisen+turvallisuuden+arkkitehtuuri

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 niin johtamisen tarpeet, kyberturvallisuus, kuin myös riskienhallinnan seurantatarpeet.

Uusi kehittämiskohde 2023_7
Varautuminen informaatiovaikuttamiseen. Vaikuttamisyritykset organisaation julkikuvaan ja maineeseen ovat lisääntyneet erityisesti poliittisen tilanteen muutoksen ja sosiaalisen median kanavien lisääntyessä. Jokaisen organisaation tulisi varautua kielteiseen informaatiovaikuttamiseen ja laatia toimintasuunnitelmat niiden varalle.

2.2.7 Havainnointi

Osiossa organisaatiot raportoivat, kuinka eri uhat ovat toteutuneet niiden toiminnassa edellisenä kalenterivuonna (2022). Vastaukset on ryhmitelty seuraaviin luokkiin: 0, 1–5, 6–10, 11–30 ja yli 30 kertaa. Vaihtoehdot on pisteytetty keskiarvotilastoa varten seuraavasti:

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

Taulukossa 8 esitetään osion vastauskeskiarvot.

Taulukko 8. Havainnointi – kysymyskohtaiset keskiarvot

	Kaikki organisaatiot 194 kpl	Kunta 103 kpl	Kuntayhtymä 18 kpl	Hyvinvointialue ja muut Sote-toimijat 12 kpl	Korkeakoulu 15 kpl	Valtionhallinto 37 kpl	Muu 9 kpl
Havainnointi	**0,10**	**0,08**	**0,06**	**0,17**	**0,13**	**0,12**	**0,12**
Organisaation käyttämissä kriittisissä palveluissa on ollut tekninen häiriö, joka on jonkin verran haitannut organisaation toimintaa.	0,32	0,27	0,22	0,48	0,32	0,43	0,42
Organisaation käytössä olevaan palveluun on kohdistunut henkilötietojen tietoturvaloukkaus, joka on edellyttänyt ilmoitusta valvontaviranomaiselle.	0,18	0,15	0,03	0,54	0,22	0,16	0,22
Organisaation nimissä on lähetetty huijausviestejä, jossa yritetään urkkia asiakkaiden tai muiden henkilöiden tietoja.	0,17	0,13	0,15	0,15	0,30	0,16	0,22
Organisaation käytössä olevaan palveluun on kohdistunut henkilötietojen tietoturvaloukkaus, joka on edellyttänyt ilmoitusta rekisteröidyille.	0,16	0,14	0,03	0,48	0,20	0,11	0,19
Organisaation käyttämissä kriittisissä palveluissa on ollut tekninen häiriö, joka on merkittävästi haitannut organisaation toimintaa.	0,16	0,15	0,08	0,23	0,12	0,19	0,17
Organisaation henkilöstöön tai organisaation toimintaan on yritetty vaikuttaa kielteisillä keinoilla.	0,13	0,10	0,08	0,08	0,07	0,29	0,11
Organisaation julkiseen verkkoon näkyvässä tietojärjestelmässä tai verkossa on ollut kriittinen ja hyödynnettävissä ollut tietoturvahaavoittuvuus.	0,12	0,09	0,07	0,15	0,22	0,17	0,11
Organisaation salassa pidettäviä tietoja tai henkilötietoja on käsitelty ohjeiden vastaisesti luvattomilla laitteilla tai luvattomissa palveluissa.	0,11	0,07	0,04	0,25	0,25	0,13	0,28

Organisaation omistama päätelaite on varastettu	0,10	0,09	0,06	0,19	0,20	0,08	0,06
Organisaatio on vastaanottanut ICT-palvelutoimittajilta ilmoituksen hyökkäyksestä, joka on aiheuttanut tietomurron, tietovuodon tai henkilötietojen tietoturvaloukkauksen.	0,08	0,08	0,10	0,08	0,08	0,07	0,03
Organisaation käytössä olleeseen palveluun on kohdistunut palvelunestohyökkäys, joka on jonkin verran haitannut organisaation toimintaa.	0,08	0,06	0,08	0,08	0,10	0,09	0,08
Organisaation web- tai sosiaalisen median kanaviin on ulkopuolisten tahojen toimesta yritetty vaikuttaa bottien, trollitilien tai vastaavien avulla tai muilla keinoilla.	0,08	0,04	0,11	0,06	0,03	0,17	0,17
Organisaation palveluita tuottava toimittaja, alihankkija tai kumppani on toiminut vastoin sovittuja tietoturva- tai tietosuojakäytäntöjä.	0,07	0,04	0,00	0,19	0,07	0,09	0,14
Organisaation itse tuottamiin palveluihin on kohdistunut onnistunut hyökkäys, joka on aiheuttanut tietomurron, tietovuodon tai henkilötietojen tietoturvaloukkauksen	0,05	0,06	0,03	0,02	0,13	0,03	0,00
Organisaation työntekijä on tietoisesti luvattomasti käsitellyt salassa pidettäviä tietoja tai henkilötietoja.	0,05	0,04	0,03	0,27	0,02	0,06	0,06
Organisaatio on ollut räätälöidyn, kohdistetun tietoturva- tai kyberhyökkäyksen kohteena.	0,03	0,01	0,01	0,04	0,10	0,06	0,03
Organisaation käytössä olevaan päätelaitteeseen on päässyt haittaohjelma, joka on esim. lukinnut päätelaitteen salaamalla tai aiheuttanut tietovuodon.	0,02	0,02	0,01	0,02	0,03	0,01	0,00
Organisaation käytössä olleeseen palveluun on kohdistunut palvelunestohyökkäys, joka on merkittävästi haitannut organisaation toimintaa.	0,02	0,02	0,01	0,02	0,05	0,01	0,06
Organisaation käytössä olevaan palveluun on päässyt haittaohjelma, joka on esim. estänyt palvelun käytön tai aiheuttanut tietovuodon.	0,00	0,00	0,00	0,00	0,00	0,01	0,00
Organisaation kriittisiä tai lakisääteisesti säilytettäviä tietoja on korruptoitunut tai tuhoutunut lopullisesti.	0,00	0,00	0,00	0,04	0,00	0,00	0,00

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 (0,32). Vähiten mainintoja saivat puolestaan kohdat, jotka koskivat organisaatioiden kriittisten tietojen pysyvää tuhoutumista sekä haittaohjelmien aiheuttamia tietovuotoja.

Osion kokonaiskeskiarvo on 0,10, ja eniten uhkia ovat tunnistaneet sote-toimijat (0,17). Heillä korostuvat erityisesti tietosuojaan liittyvät poikkeamat, koska henkilötietoja käsitellään laajasti. Tapauksista ainakin osan on aiheuttanut henkilökunta, joka on käsitellyt tietoja luvattomasti, ja ne ovat vaatineet ilmoituksia rekisteröidyille ja tietosuojavaltuutetulle.

Kehitys vuoteen 2021 verrattuna

Havaittujen ja toteutuneiden uhkien kärkisijat ovat pysyneet pitkälti samankaltaisina. Tälläkin kertaa ensimmäisenä ovat organisaation toimintaa haitanneet tekniset häiriöt. Väittämien esiintymismäärät tai keskinäinen järjestys eivät ole juurikaan muuttuneet kahdessa vuodessa. Ainoastaan vaikuttamisyritykset web- tai some-kanavien kautta ovat hienoisesti lisääntyneet (0,06 → 0,08).

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 kehittämiskohde tulee ottaa huomioon niin henkilöstön osaamisen kehittämiseen liittyvissä ohjeistuksissa ja koulutuksissa kuin tietojärjestelmien suunnittelussa.

Kehittämiskohde 17
Päätelaitteiden suojaaminen. Henkilöstölle digiturvallisuuden osaamisen kehittämisessä tulee korostaa myös fyysisten laitteiden turvallista kuljettamista ja säilyttämistä. Laitteiden tietojen tulisi myös olla suojattuja esimerkiksi salakirjoituksella. Näin laitteessa olevien salassa pidettävien tietojen tai henkilötietojen luottamuksellisuus ei vaarannu. Lisäksi mobiililaitteiden järjestelmänhallintatuotteilla voidaan yrittää paikallistaa ja tuhota tietoja tai muilla keinoilla vaikuttaa siihen, että tietoja ei voida väärinkäyttää (mm. ilmoitukset teleoperaattorille).

Kehittämiskohde 18
Ohjeistuksen kehittäminen huijausviesteihin. 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. Varautuminen on erityisen tärkeää niille organisaatioille, joiden suoria asiakkaita ovat kansalaiset.

Uusi kehittämiskohde 2023_8
Henkilötietojen tietoturvaloukkauksiin reagoiminen. Jokaisessa organisaatiossa tulisi olla menettely tietoturvaloukkausepäilyjen ilmoittamiseen. Lisäksi tulee olla toimivat menettelyt poikkeamien käsittelyyn ja niistä ilmoittamiseen lainsäädännön asettamissa määräajoissa.

Liite 1 – Tulosten perusteella valitut kehittämiskohteet

Vuoden 2021 digiturvakyselyssä kehittämiskohteiksi nostettiin 19 toimenpidettä. Alla olevassa taulukossa on kuvattu kehittämiskohteiden tilanne, kehittyminen ja jatkosuositus sekä listattu kuhunkin kehittämiskohteeseen tarjolla olevia työvälineitä ja apukeinoja.

Numero	Toimenpide	Tilanne	Jatkosuositus	Linkit apuvälineisiin
Yleinen	Koko organisaation läpäisevä riskienhallintaprosessi	Tilanteessa ei ole tapahtunut merkittävää muutosta.	Kehittämiskohde vaatii edelleen huomiota	VAHTI-riskienhallintaohje Riskinäkemyskysely
1.	Henkilöstön osaamisen ja koulutustarpeiden kartoittaminen	Tilanteessa ei ole tapahtunut merkittävää muutosta.	Kehittämiskohde vaatii edelleen huomiota	Digiturvaviikko Digiturvatilaisuudet Digiturvallinen elämä
2.	Harjoitustoiminnan kehittäminen	Harjoitusten määrässä ja prosesseissa on tapahtunut pientä parannusta	Kehittämiskohteen merkitys tulee edelleen huomioida	Taisto-harjoitus
3.	Prosessit kuntoon (digitaaliseen turvallisuuteen liittyvät)	Joillakin toimialoilla on tapahtunut pientä parannusta	Kehittämiskohteen tärkeyttä tulee edelleen korostaa	DVV digiturvan tietoiskut
4.	Säännöllinen digitaalisen turvallisuuden tilanneraportointi organisaation johdolle	Joillakin toimialoilla on tapahtunut pientä parannusta	Sanoitettu uudelleen Uusi kehittämiskohde 2023_4	Raportoinnissa voidaan hyödyntää DVV:n kokonaiskuvapalvelua
5.	Digitaalisen toimintaympäristön riskienhallinnan kokonaisvaltainen kehittäminen	Tilanteessa ei ole tapahtunut merkittävää muutosta	Kehittämiskohteen tärkeyttä tulee edelleen korostaa	Riskinäkemyskysely
6.	Harjoitustoiminnan kehittäminen ja ylläpito (vrt. KK 2)	Harjoitusten määrässä ja prosesseissa on tapahtunut pientä parannusta	Laajennettu kehittämiskohdetta Uusi kehittämiskohde 2023_5 Erityisesti harjoittelemaan pitää saada niitä organisaatioita, jotka eivät ole aiemmin harjoitelleet	Taisto-harjoitus

7.	Etäkäyttöön liittyvien riskien arviointi sekä kattava VPN-yhteyksien ja monivaiheisen tunnistautumisen käyttöönotto	MFA- ja VPN-ratkaisujen käyttö on lisääntynyt	Ratkaisut pitää saada käyttöön mahdollisimman kattavasti	Kyberturvallisuuskeskus: Etätyön tietoturva -ohjeita organisaatioille
8.	Toimiva varmuuskopiointi	Testaaminen on hiukan lisääntynyt, mutta ei ole riittävää	Erityisesti pitää korostaa varmuuskopioiden testaamisen tärkeyttä uhkatilanteen muuttuessa	
9	Kattavat lokitiedot ja niiden käytettävyys	Lokitietojen kerääminen on hiukan lisääntynyt, mutta vaatii edelleen huomiota	Lokitietojen kerääminen tulee aina suunnitella ja toteuttaa niiden käyttötarkoituksen mukaan	Kyberturvallisuuskeskus: Näin keräät ja käytät lokitietoja
10.	Haavoittuvuuksien hallinnan ja auditointitoiminnan kehittäminen	Tilanteessa ei ole tapahtunut merkittävää muutosta	Uhkatilanteen muutos vaatii lisäpanostusta näiden kehittämiseen	
11.	Tietosuojan vaikutustenarviointi	Tilanteessa ei ole tapahtunut merkittävää muutosta	Lakisääteinen velvoite, joka vaatii edelleen huomiota	https://tietosuoja.fi/vaikutustenarviointi VAHTI hyvät käytännöt: Tietosuojan vaikutusten alkukartoitus Tietosuojan vaikutustenarviointi
12.	JUDO-hankkeen arkkitehtuurityön hyödyntäminen	Pientä parannusta tapahtunut useilla toimialoilla	DVV arkkitehtuurimallia täytyy edelleen markkinoida julkiseen hallintoon	Digitaalisen turvallisuuden arkkitehtuuri https://wiki.dvv.fi/display/DTARK/
13.	Digitaalisen turvallisuuden kehittäminen yhteistyössä palvelutuottajien kanssa	Pientä parannusta tapahtunut	Vaatii edelleen huomiota, koska useimmat organisaatiot ovat riippuvaisia ulkoisista palvelutoimittajista	
14.	Uhkatilanteen seuranta ja siihen liittyvien riskien hallinta	Pientä parannusta tapahtunut	Vaatii lisää huomiota, koska uhkatilanne muuttuu jatkuvasti	
15.	Salassa pidettävien ja henkilötietojen suojaaminen.	Tilanteessa ei ole tapahtunut merkittävää muutosta	Jokaisella organisaatiolla tulisi olla riittävä ohjeistus ja valvonta	Tiedonhallintalautakunta: Suositus salassa

				pidettävien asiakirjojen käsittelystä
16.	Palveluiden vikasietoisuuden parantaminen	Tilanteessa on tapahtunut pientä parannusta	Tärkeää toimintojen jatkuvuuden näkökulmasta, mutta ei ensisijainen digiturvan kehittämiskohde	
17.	Päätelaitteiden suojaaminen	Tilanteessa ei ole tapahtunut merkittävää muutosta	Päätelaitteet pitää suojata erityisesti varkauksien aiheuttamia tietovuotoja vastaan	
18.	Ohjeistuksen kehittäminen (mm. huijausviesteihin)	Tilanteessa ei ole tapahtunut merkittävää muutosta	Huijausviestit lisääntyvät, joten ohjeistusta tarvitaan kaikissa organisaatioissa	

Uudet kehittämiskohteet 2023

Numero	Toimenpide	Tarkenne	Linkit apuvälineisiin
1	Digiturvan vastuuhenkilöiden nimeäminen	Jokaisen julkishallinnon organisaation tulisi nimetä henkilöt, joiden tehtäviin digitaalisen turvallisuuden osa-alueiden kehittäminen kuuluu. Tietosuojavastaava on julkisessa hallinnossa pakollinen, mutta myös muille osa-alueille pitäisi nimetä vastuuhenkilöt.	
2.	Tietoturvapoikkeamien havainnointi ja kirjaaminen	Jokaisessa organisaatiossa tapahtuu poikkeamia, jotka voivat eskaloituessaan merkittävästi haitata organisaation varsinaista toimintaa. Siksi kaikkien organisaatioiden tulisi luoda menettely, jonka avulla henkilökunta voi helposti ilmoittaa havainnoistaan ja jonka avulla poikkeamat tutkitaan sekä niiden kehittymistä ja kustannuksia seurataan.	Kyberturvallisuuskeskus: Toimi näin tietoturvapoikkeamatilanteissa
3	Väärinkäytöksiin varautuminen	Jokaisen organisaation tulisi tiedostaa sisäisten ja ulkoisten väärinkäytösten mahdollisuus ja luoda niihin reagoimiseksi toimiva prosessi.	Laki Euroopan unionin ja kansallisen oikeuden rikkomisesta ilmoittavien henkilöiden suojelusta
4	Digitaalisen turvallisuuden säännöllinen mittaaminen, seuranta ja raportointi	Johdon on tärkeää ymmärtää digitaalisen turvallisuuden tilannetta ja sen merkitystä organisaation varsinaiselle toiminnalle. Jokaisen organisaation tulisikin sopia ja kuvata menettelyt, jotka mahdollistavat säännöllisen raportoinnin organisaation johdolle. Ne toimivat myöskin digitaalisen turvallisuuden	Kokonaiskuvapalvelu

		systemaattisen kehittämisen ja resursoinnin perustana.	
5	Jatkuvuuden hallinnan kehittäminen	Jokaisen organisaation tulisi varautua toimintaa merkittävästi haittaaviin häiriöihin. Organisaatiolla tulisi olla kuvattuna jatkuvuuden hallintaa ohjaavat linjaukset, joissa kuvataan mm. häiriötilanteiden johtaminen, vastuut ja viestintä. Kriittiset toiminnot ja palvelut tulee tunnistaa ja laatia jatkuvuussuunnitelmat ainakin niille. Olennainen osa jatkuvuuden hallintaa on häiriötilanteiden harjoittelu ja suunnitelmien päivittäminen niistä saatujen oppien perusteella.	VAHTI jatkuvuuden hallinnan ohje
6	Tietosuojan kokonaisvaltainen tarkastelu	Organisaatioiden tulee tunnistaa käsittelemänsä henkilötiedot sekä niiden käsittelyperusteet. On tärkeää laatia linjaukset siitä, missä järjestelmissä tai palveluissa (esim. pilvipalvelut) henkilötietoja käsitellään. Jos käsittelyssä havaitaan puutteita, organisaatioiden tulee kartoittaa kehittämistarpeet ja laatia kehittämissuunnitelma.	Tietosuojavaltuutetun ohjeet organisaatioille
7	Varautuminen informaatiovaikuttamiseen	Vaikuttamisyritykset organisaation julkikuvaan ja maineeseen ovat lisääntyneet erityisesti poliittisen tilanteen muutoksen ja sosiaalisen median kanavien lisääntymisen myötä. Jokaisen organisaation tulisi varautua kielteiseen informaatiovaikuttamiseen ja laatia toimintasuunnitelmat sen varalle.	Kyberturvallisuuskeskuksen vinkkejä informaatiovaikuttamisen tunnistamiseksi
8	Henkilötietojen tietoturvaloukkauksiin reagoiminen	Jokaisessa organisaatiossa tulisi olla menettely tietoturvaloukkausepäilyjen ilmoittamiseen. Lisäksi tulee olla toimivat menettelyt poikkeamien käsittelyyn ja niistä ilmoittamiseen lainsäädännön asettamissa määräajoissa.	Tietosuojavaltuutetun ohjeet tietoturvaloukkauksiin

DIGI- JA VÄESTÖTIETO-VIRASTO