DIGI- JA VÄESTÖTIETO-VIRASTO

Julkisen hallinnon digitaalisen turvallisuuden nykytilan selvitys

Raportti

25.3.2021

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

Sisällysluettelo

1 Yhteenveto

Valtiovarainministeriö ja Digi- ja väestötietovirasto vastaavat digiturvallisuuden kehittämishankkeista. Valtiovarainministeriön julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelma 2020-2023 (Haukka-hanke) toteuttaa 8.4.2020 annettua Valtioneuvoston periaatepäätöstä. Haukka-hankkeen tehtäviä Digi- ja väestötietovirastossa toteutetaan JUDO-hankkeessa. Haukka- ja JUDO-hankkeissa tehdään laajamittaisia selvitystöitä, joihin on osallistunut useita julkishallinnon ja yksityisen sektorin organisaatiota asiantuntijoineen.

Tämä raportti koskee osana toimeenpanosuunnitelmaa tehtävää digitaalisen turvallisuuden ja kriittisyyden luokitusjärjestelmien nykytilan kartoitusta sekä julkisen hallinnon turvallisuusarkkitehtuurin ja vaatimustenmukaisuuden nykytilaa. Nykytilan kartoitus toteutettiin kahdella kyselyllä, joihin osallistui kokonaisuudessaan 186 julkisorganisaatiota kattaen kunnat, valtion virastot, sairaanhoitopiirit, yliopistot ja ammattikorkeakoulut. Kyselyn analyysin tulokset on koottu tähän raporttiin. Ensimmäisen kyselyn, joka kohdistettiin kunnille ja sairaanhoitopiireille, tulokset on koottu erilliseen raporttiin, jossa käsitellään kuntien yhteisiä digitaalista turvallisuutta edistäviä palveluja ja tarpeita niille.

Tämä raportin keskeisenä havaintona tunnistettiin, että valtion virastot, sairaanhoitopiirit ja yliopistot ovat yleisesti ottaen hieman pidemmällä digitaalisen turvallisuuden toimeenpanossa kuin kunnat ja ammattikorkeakoulut, vaikkakin poikkeuksiakin löytyy. Sairaanhoitopiirien osalta digitaalisen turvallisuuden kyvykkyys johtuu paljolti sairaanhoitopiirien toiminnan luonteesta, kun taas valtion virastot ja yliopistot ovat verkostoituneet digitaalisen turvallisuuden osalta kuntia ja ammattikorkeakouluja enemmän sekä harjoittelevat digitaalisen turvallisuuden poikkeustilanteita muita enemmän.

Kyselyn analyysissa tunnistettiin vastaajajoukosta edelläkävijöitä, joilla oli selkeitä onnistumisia yhdellä tai useammalla osa-alueella. Digitaalisen turvallisuuden edelläkävijöitä yhdistivät samat ominaisuudet. Näistä ominaisuuksista keskeisimmät ovat kyky havaita ja toimia tehokkaasti digitaalisen turvallisuuden poikkeamatilanteissa, säännölliset digitaalisen turvallisuuden harjoitukset ja koulutukset, toiminnan kannalta kriittisten kohteiden luokittelu sekä digitaalisen turvallisuuden ja sen ajantasaisuuden arviointimenetelmät.

Kyselyn tulokset ovat vastaajien itsearviointia, mikä on otettava huomioon vastauksia analysoitaessa ja tulkittaessa. Tuloksissa on kunkin vastaajan osaamiseen ja kokemukseen sekä näkemyksiin perustuvaa vaihtelua. Kyselyn tuloksia onkin tarkoitus tarkentaa teemahaastatteluilla, joiden tuloksia tullaan käyttämään nyt arvioidun nykytilan lisäksi digitaalisen turvallisuuden kansallisen tavoitetilan määrittelyssä.

2 Digitaalisen turvallisuuden kansallisen kyvykkyyden nykytila

Kyselyn tavoitteena oli kartoittaa julkisen hallinnon tietoturvan kansallisen kyvykkyyden nykytilaa ensinnäkin sen selvittämiseksi, miten julkisen hallinnon organisaatiot ovat tunnistaneet ne digitaaliset palvelut, palveluprosessit, tietojärjestelmät, infrastruktuurin, tiedot ja tietovirrat, jotka ovat organisaation toiminnan kannalta kriittisiä, ja joihin saattaa liittyä erityisiä kansallisen hallinnan ja turvaamisen vaatimuksia. Toisaalta kyselyllä pyrittiin myös selvittämään, millaisia kriittisyyden luokitusjärjestelmiä

julkisella hallinnolla on käytettävissään edellä mainittujen kriittisten kohteiden tunnistamiseksi ja arvioimiseksi.

Kyselyä tullaan täydentämään kohdennetuilla teemahaastatteluilla, jotta saadaan parempi tieto siitä, miten julkinen hallinto tunnistaa sekä toimintansa että yhteiskunnan kannalta kriittisiä digitaalisia kohteita ja mikä julkisen hallinnon tietoturvan vaatimustenmukaisuuden nykytilanne on.

Tämä raportti analysoi kyselyn tuotoksia, joka lähetettiin kunnille, valtiohallinnon organisaatioille, sairaanhoitopiireille sekä yliopistoille ja ammattikorkeakouluille. Vastaajia oli yhteensä 186. Kyselyssä selvitettiin digiturvaan liittyviä keskeisiä seikkoja sekä niiden toteutumista.

Kyselytulosten perusteella tunnistettiin edelläkävijöitä eli julkisorganisaatioita, joilla oli selkeitä onnistumisia yhdellä tai useammalla osa-alueella.

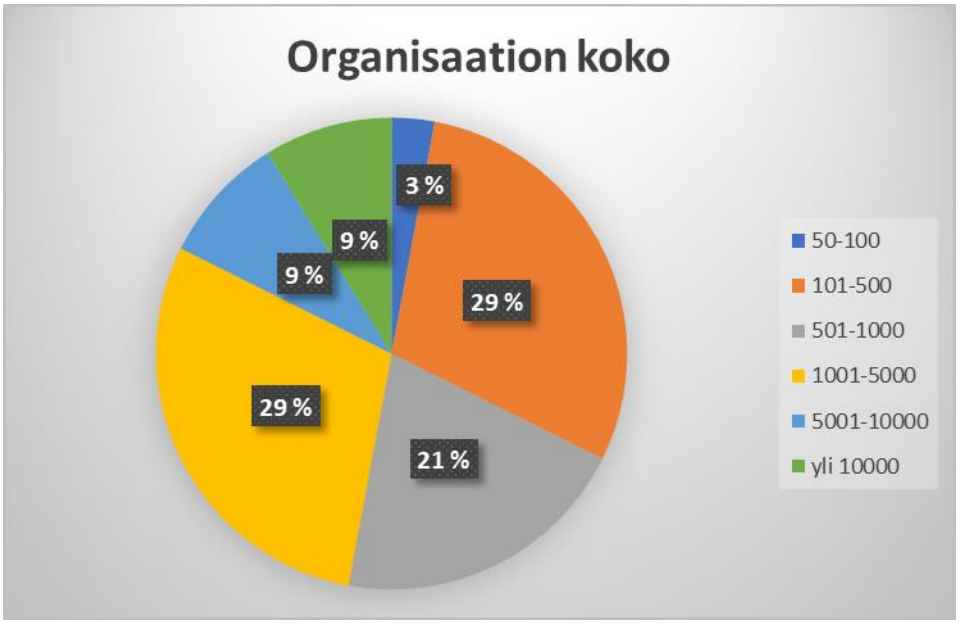
Vastaajat on jaettu organisaatiotyypin perusteella viiteen ryhmään – kuntiin, valtionhallinnon yksiköihin, sairaanhoitopiireihin, yliopistoihin ja ammattikorkeakouluihin. Sairaanhoitopiirejä, yliopistoja ja ammattikorkeakouluja tarkastellaan kutakin yhtenä ryhmänä. Kuntien ja valtionhallinnon yksiköiden vastausten analysoinnissa on otettu lisädimensiona huomioon myös organisaation henkilöstömäärä.

2.1 Digitaalisen turvallisuuden edelläkävijät

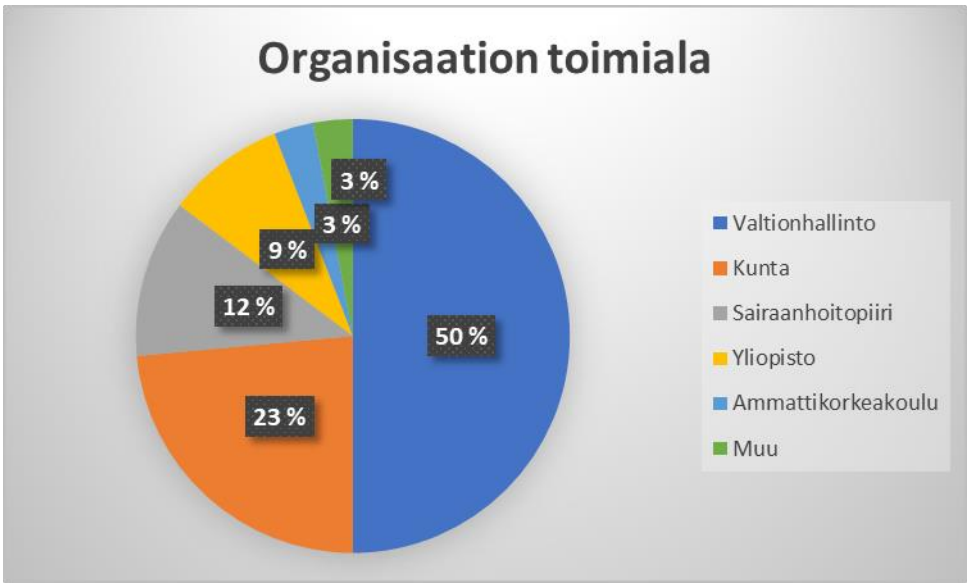
Tähän kappaleeseen on kerätty merkittävimmät menestystekijät hyvän digitaalisen turvallisuuden tason tuottamiseksi. Näiden tekijöiden perusteella kyselyaineistosta on tunnistettu digitaalisen turvallisuuden edelläkävijöitä.

Kyselyn vastauksista tunnistettiin 34 organisaatiosta koostuva ryhmä, joita voi vastausten perusteella pitää digiturvallisuuden edelläkävijöinä. Suurimman ryhmän edelläkävijöistä muodostavat keskikokoiset valtionhallinnon organisaatiot (17 kpl).

Kuvio 1. Edelläkävijöiden jakauma organisaatiokoon mukaan



Kuvio 2. Edelläkävijöiden jakauma organisaatioiden toimialan mukaan

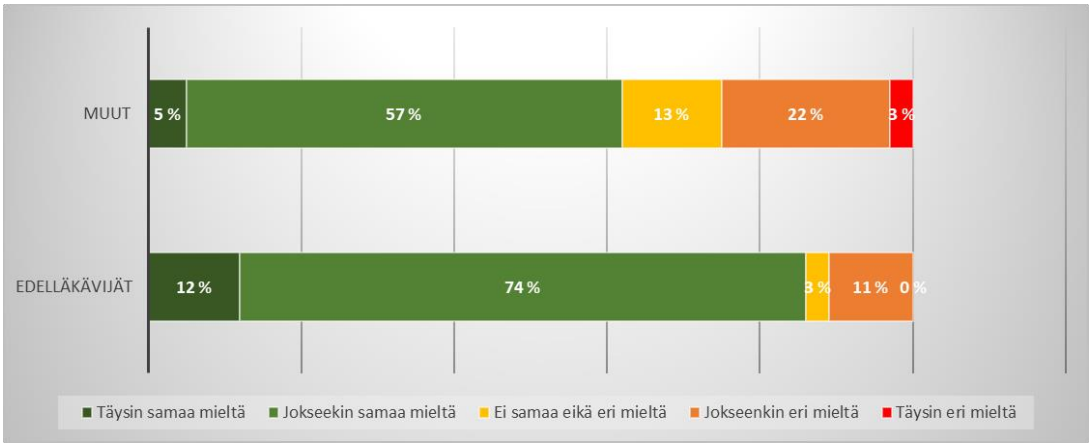


Tiivistetysti edelläkävijöiltä löytyy seuraavia ominaisuuksia:

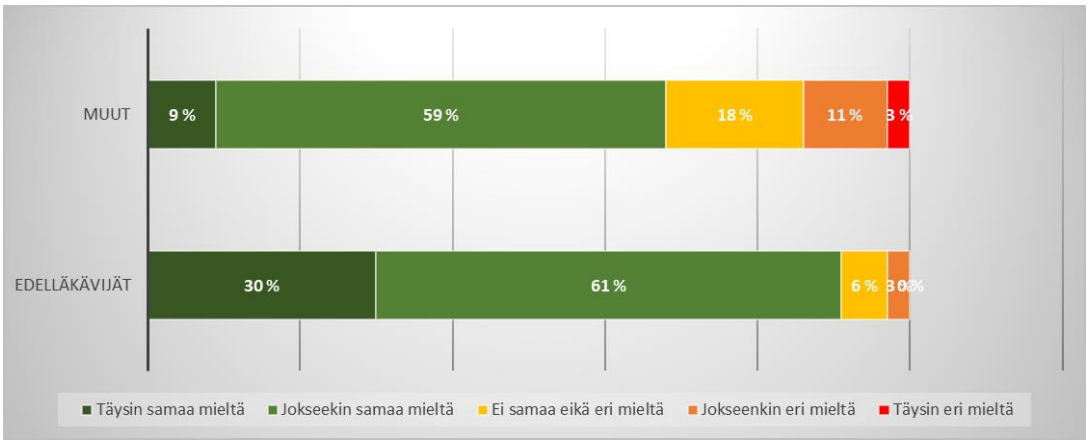
- digitaalisen turvallisuuden harjoituksia ja koulutuksia järjestetään säännöllisesti
- toiminnan kannalta kriittiset kohteet on tunnistettu ja luokiteltu
- tietoturvallisuuden ja sen ajantasaisuuden arviointiin on menetelmät

Näiden perusasioiden ollessa kunnossa, organisaatioilla on parempi luottamus siihen, että heillä on kyvykkyys havaita erilaiset tietoturvallisuuden poikkeamatilanteet (Kuvio 3, kyselyssä 86% täysin samaa mieltä tai jokseenkin samaa mieltä) ja toimia näissä poikkeamatilanteissa tehokkaasti (Kuvio 4, 91% täysin samaa mieltä tai jokseenkin samaa mieltä). Muiden vastaajien keskuudessa tulokset jäävät noin 20 prosenttiyksikköä alemmalle tasolle.

Kuvio 3. Tietojenkäsittelyn poikkeamien havainnointikyvykkyys



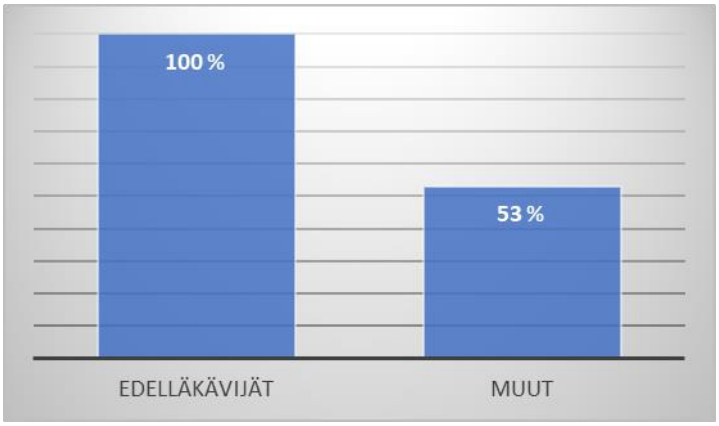
Kuvio 4. Kyvykkyys toimia tehokkaasti poikkeamatilanteissa ja palata nopeasti normaaliin toimintaan



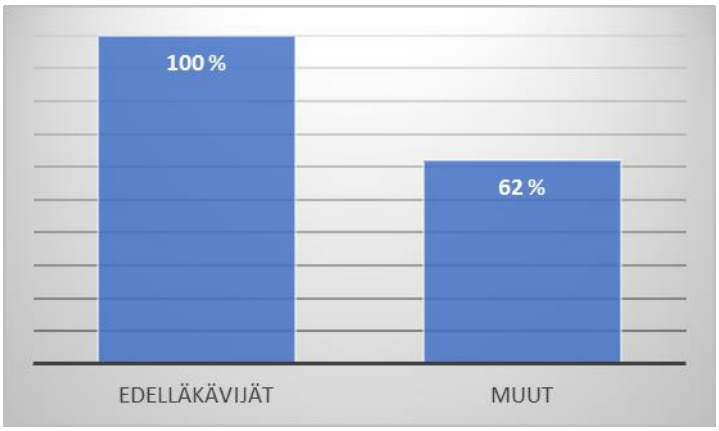
2.1.1 Harjoitukset ja koulutukset

Edelläkävijöistä kaikki (Kuvio 5) harjoittelevat toimimista tietoturvahäiriötilanteissa vähintään kerran vuodessa. Kaikki myös järjestävät digitaalisen turvallisuuden koulutusta ja perehdytystä säännöllisesti (0).

Kuvio 5. Tietoturvahäiriötilanteiden harjoittelu vähintään vuosittain

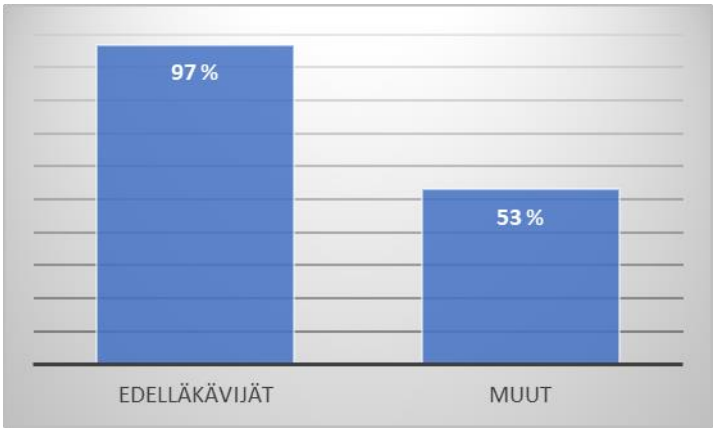


Kuvio 6. Säännöllisen digitaalisen turvallisuuden koulutus ja perehdytys



Myös lähes kaikki edelläkävijöistä (Kuvio 7, 97%) ilmoittivat osaavansa huomioida digitaalisen turvallisuuden asiat hyvin hankinnoissa.

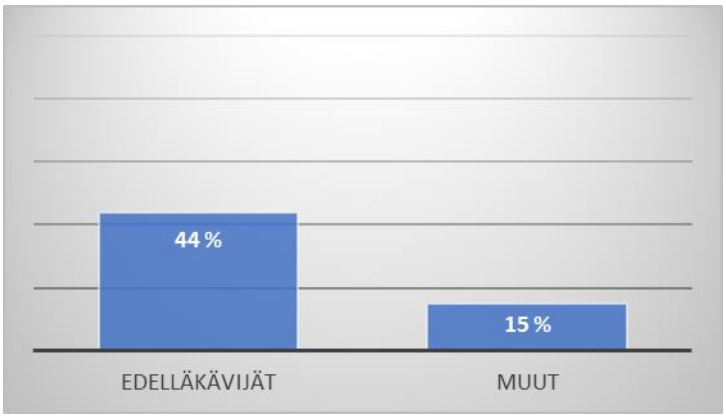
Kuvio 7. Digitaalisen turvallisuuden huomioiminen hankinnoissa



2.1.2 Henkilöstö

Edelläkävijöistä huomattavasti suurempi osa (Kuvio 8, 44 %) myös kokee, että heidän organisaatiossaan on riittävästi henkilöstöä huolehtimaan digitaalisesta turvallisuudesta. Keskiarvo muiden vastaajien joukossa oli vain 15 %.

Kuvio 8. Digitaalisen turvallisuuden henkilöstön riittävyys

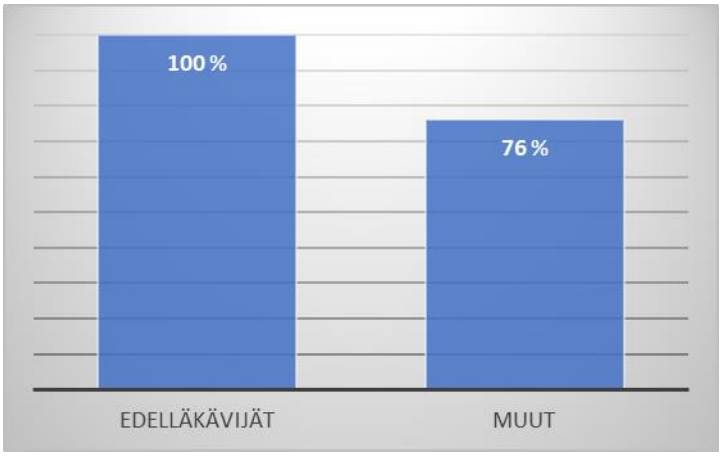


Joka tapauksessa digitaalisen turvallisuuden henkilöstön riittävyys oli kaikkien vastaajien yhteinen tunnistettu haaste, johon suositellaan kiinnitettävän huomiota joko omaa osaamista tai kumppaniverkostoa vahvistamalla.

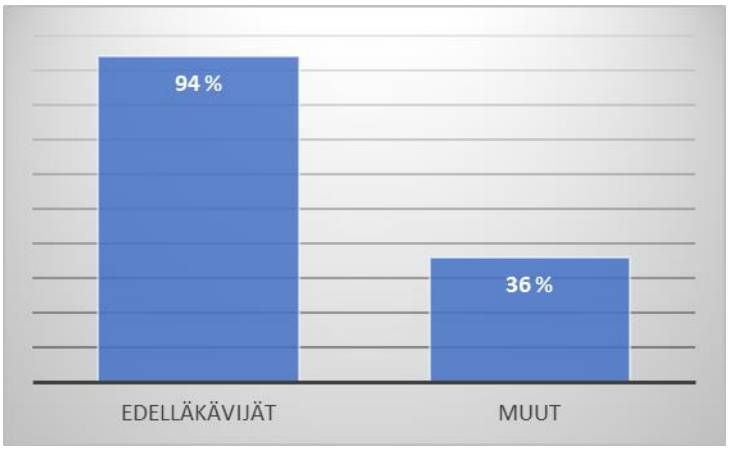
2.1.3 Kriittiset kohteet

Organisaation digiturvallisuuden kannalta kriittiset kohteet ovat edelläkävijöillä hyvin tiedossa ja luokiteltuina. Edelläkävijöistä kaikki (Kuvio 9, 100%) olivat tunnistaneet toimintansa kannalta kriittiset kohteet ja lähes kaikilla (Kuvio 10, 94%) oli myös tapa luokitella nämä kriittiset kohteet. Muiden vastaajien keskuudessa kriittisten kohteiden tunnistaminen oli hieman alemmalla tasolla (76 %). Kriittisten kohteiden luokittelumenetelmien osalta muut vastaajat olivat huomattavasti alemmalla tasolla (36 %). Tämä indikoi sitä, että organisaatiot kyllä pääsääntöisesti tunnistavat toimintansa kannalta kriittiset kohteet, mutta ne eivät tee sitä systemaattisesti tietyn menetelmän tai viitekehyksen avulla. Tämä voi johtaa siihen, ettei organisaatioilla ole kokonaiskuvaa kaikista kriittisistä kohteistaan.

Kuvio 9. Toiminnan kannalta kriittisten kohteiden tunnistaminen

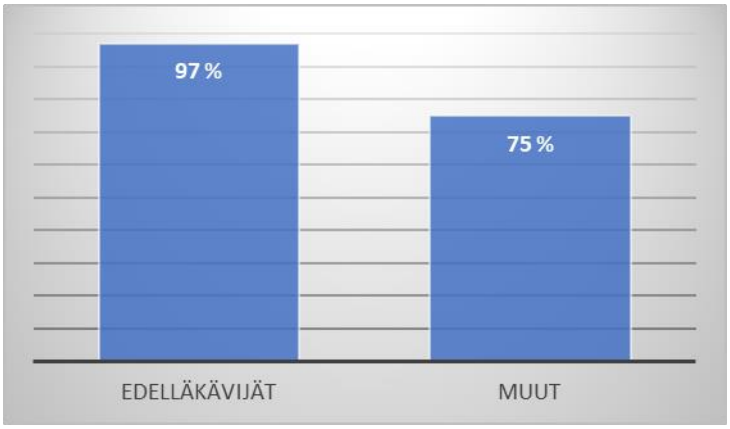


Kuvio 10. Kriittisten kohteiden luokittelumenetelmä



Lähes kaikilla edelläkävijöillä (Kuvio 11, 97%) on myös käytössään tietojärjestelmärekisteri tai muu vastaava tapa ylläpitää ajantasaista tietoa tietojärjestelmistä, kun muiden vastaajien keskuudessa tietojärjestelmä on käytössä kolmella neljästä vastaajasta. Kaikilla vastaajaryhmillä parhaiten tunnistetut kriittiset kohteet olivat tietojärjestelmät ja prosessit, tietojen ja tietovirtojen ollessa huonoiten tunnistettuja (kts. Kriittiset kohteet).

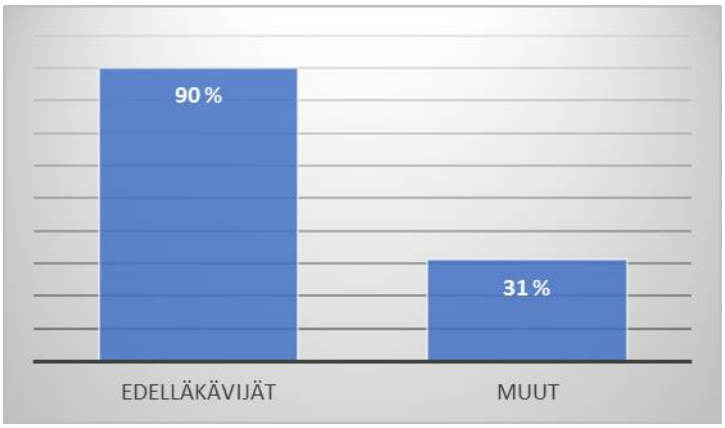
Kuvio 11. Tietojärjestelmärekisteri tai vastaava tapa ylläpitää ajantasaista tietoa tietojärjestelmistä



2.1.4 Menetelmät

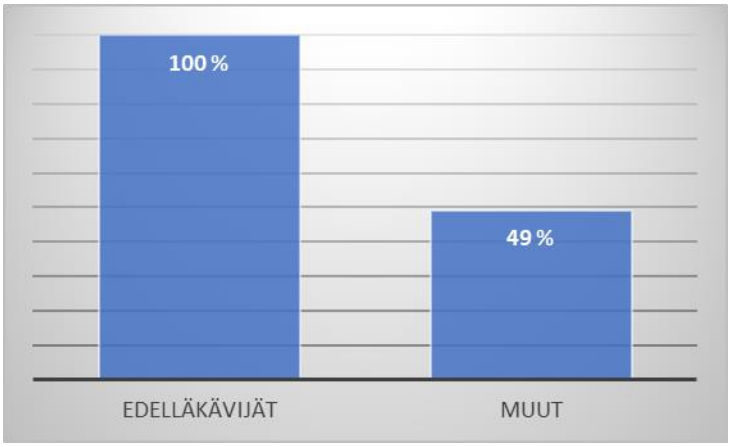
Menetelmien osalta edelläkävijät erottautuivat muista organisaatioista tietoturvallisuuden sekä sen ajantasaisuuden arvioinnissa. Likimain kaikilla (Kuvio 12, 90 %) edelläkävijöillä oli menetelmä käytössä olevien digitaalisten palvelujen ja teknologioiden tietoturvallisuuden ajantasaisuuden arvioimiseksi, tuloksen ollessa muiden vastaajien joukossa vain 31 %.

Kuvio 12. Menetelmä käytössä olevien digitaalisten palveluiden turvallisuuden arviointiin



Kaikilla (Kuvio 13) edelläkävijöillä oli myös menetelmä digitaalisten palvelujen ja teknologioiden tietoturvallisuuden arviointiin, kun keskiarvo muilla vastaajilla oli 49 %.

Kuvio 13. Hankittavien digitaalisten palveluiden ja teknologioiden tietoturvallisuuden arviointimenetelmä

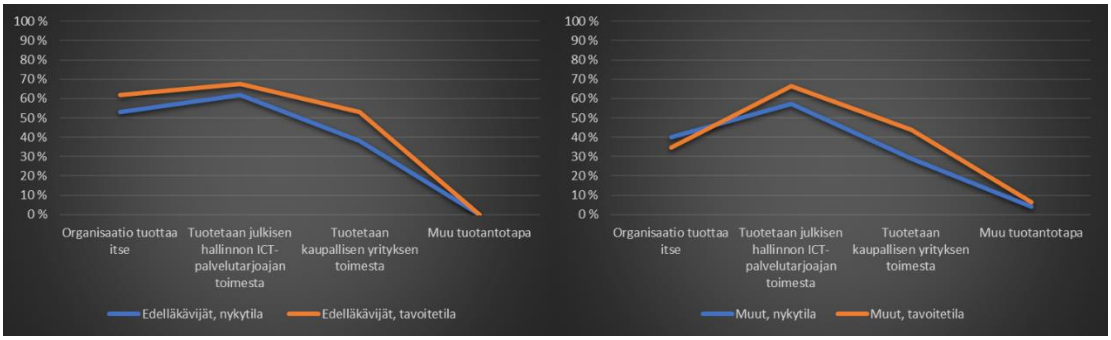


2.1.5 Palvelujen järjestäminen

ICT-palvelujen järjestämiseen liittyvissä kysymyksissä edelläkävijäorganisaatiot tuottivat johdonmukaisesti keskimääräistä enemmän palveluja itse. Ne eivät kuitenkaan luottaneet pelkästään omaan palvelutuotantoon, vaan myös kumppanit tuottavat osan palveluista. Oman osaamisen täydentäminen vahvalla kumppaniverkostolla digitaalisen turvallisuuden palvelutuotannossa näyttäisi olevan vahva trendi myös palvelutuotannon järjestämisen tavoitetilassa.

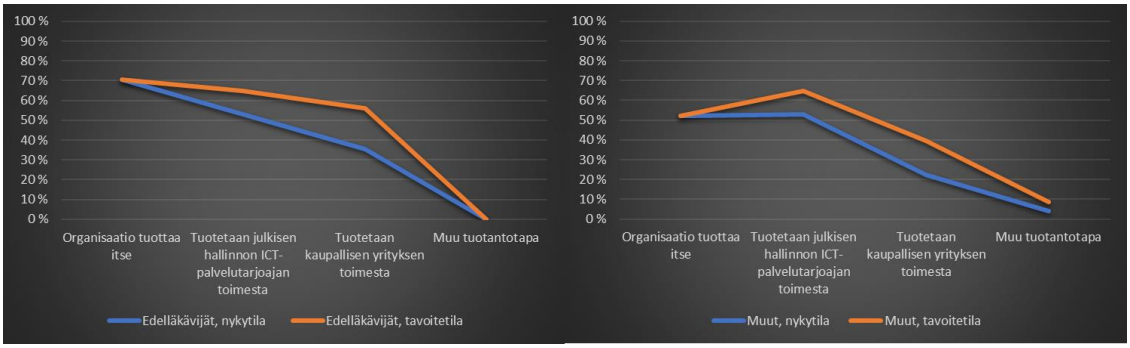
Noin puolet edelläkävijöistä tuottaa tietoliikenneverkon tapahtumien havainnointi-, reagointi- ja analysointipalvelut (tietoturvavalvomo) nykytilassa itse (Kuvio 14). Tavoitetilassa itse tuotetun palvelun suosio jopa hivenen nousee. Kuitenkin nykytilasta tavoitetilaan siirryttäessä nousee tahtotila näiden palveluiden tuottamiseen myös kaupallisen yrityksen tai julkisen hallinnon ICT-palvelutarjoajan toimesta oman palvelutuotannon lisäksi.

Kuvio 14. Tietoliikenneverkon tapahtumien havainnointi-, reagointi- ja analysointipalvelujen tuotanto nyky- ja tavoitetilassa



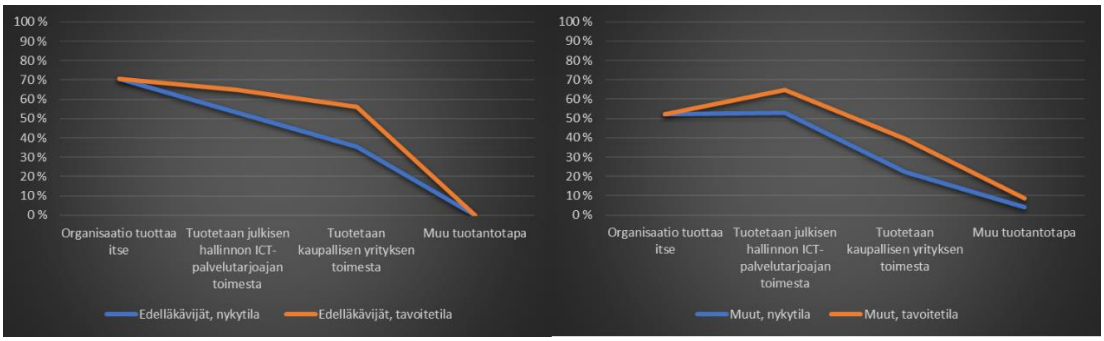
Organisaation sisäisten tietoturvauhkien havainnointi teknisellä valvonnalla itse tuotettuna ovat sekä nykytilassa että tavoitetilassa samalla tasolla. Sen sijaan palvelutuotannon laajentaminen kaupallisten yritysten tai julkisen hallinnon ICT-palvelutarjoajan palveluiden avulla nousee huomattavasti nykytilasta tavoitetilaan siirryttäessä (**Virhe. Viitteen lähdettä ei löytynyt.**).

Kuvio 15. Organisaation sisäisten tietoturvauhkien havainnointi teknisellä valvonnalla



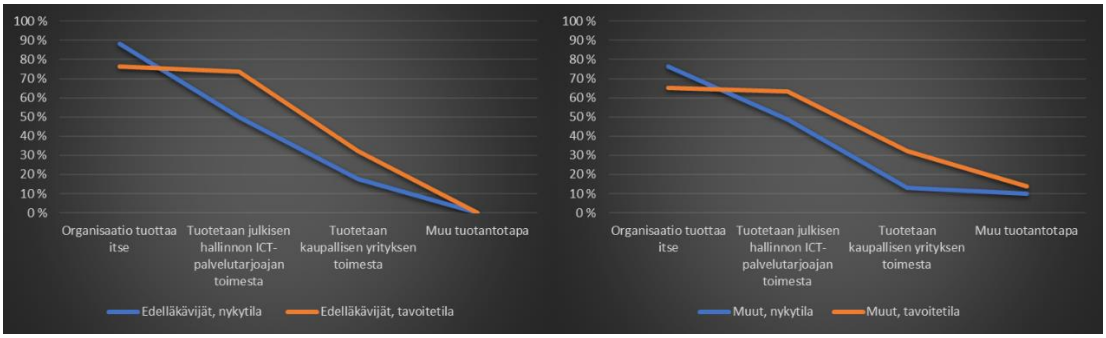
Samanlainen trendi havaitaan myös vakavien tietoturvausloukkaustilanteiden asiantuntijatukipalveluissa. Edelläkävijät tuottavat näitä palveluita voimakkaasti itse sekä nykytilassa että tavoitetilassa, mutta myös kumppaneihin (sekä kaupallisiin että julkisiin) luotetaan vahvasti tulevaisuudessa (Kuvio 16). Nykytilasta tavoitetilaan siirryttäessä lisääntyy niin Julkisen hallinnon ICT-palvelutarjoajien palveluiden kuin kaupallisten toimijoiden palveluiden käyttö.

Kuvio 16. Asiantuntijatuki vakavissa tietoturvaloukkaustilanteissa

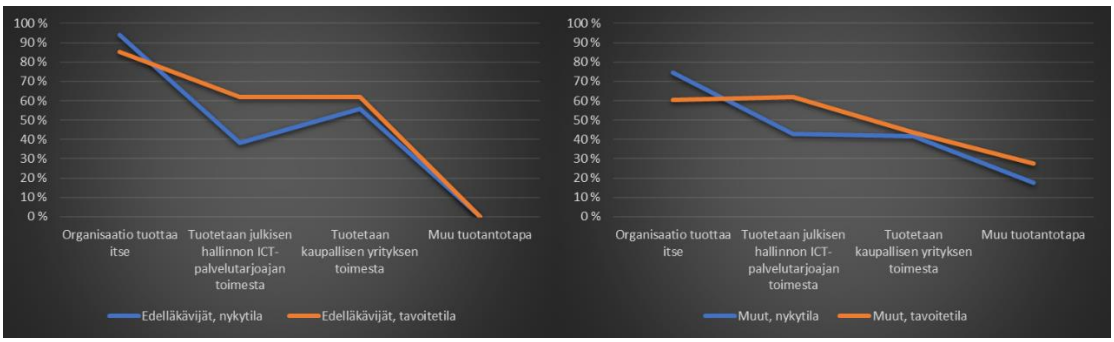


Edellä kuvattujen palveluiden lisäksi organisaatiot luottavat vahvasti omaan osaamiseensa myös leviämässä olevista tietoturvauhista ilmoitettaessa (Kuvio 17) sekä tiedonhallintalain ja digitaalisen turvallisuuden toteuttamisen asiantuntijatuessa (Kuvio 18).

Kuvio 17. Ilmoitukset leviämässä olevista tietoturvauhista



Kuvio 18. Tiedonhallintalain ja digitaalisen turvallisuuden toteuttamisen asiantuntijatuki



Itse tuotettujen palveluiden osuudet ovat edelläkävijöiden keskuudessa huomattavasti korkeammalla tasolla kuin muilla vastaajilla. Tämä ei kuitenkaan tarkoita sitä, että kaikkien pitäisi tuottaa palvelut itse. Oleellisempaa on huomioida edelläkävijöiden vastauksista ilmenevä laaja kumppaniverkosto, jonka avulla organisaatio voi itse johtaa digitaalisen turvallisuuden ICT-palvelutuotantoa ja täydentää omaa osaamistaan sopivilla joko julkisen hallinnon tai kaupallisten yritysten palveluilla.

2.2 Merkittävimmät kehityskohteet

Tähän kappaleeseen on koottu kyselyn perusteella tunnistetut merkittävimmät kehityskohteet. Tulosten perusteella tunnistettiin kehitysalueita, joiden avulla muut kuin edelläkävijät saavat parannettua digitaalisen turvallisuuden tasoaan.

Organisaatiot, joiden digitaalisessa turvallisuudessa on keskimääräistä enemmän kehitettävää, ovat kyselyn perusteella henkilöstömäärältään alle 500 hengen kuntia tai pieniä valtionhallinnon yksiköitä. Myös ammattikorkeakouluilla on digitaalisessa turvallisuudessa enemmän kehitettävää kuin yliopistoilla.

Tärkeimmät kehityskohteet ovat edellisessä kappaleessa kuvattuja osa-alueita, jotka muodostuivat menestystekijöiksi edelläkävijöiden keskuudessa. Niissä organisaatioissa, joilla oli eniten kehitettävää, digitaalisen turvallisuuden harjoituksia ja koulutuksia järjestetään epäsäännöllisesti tai ei ollenkaan. Myös kriittisten kohteiden tunnistamisessa on puutteita eikä tunnistettuja kriittisiä kohteita ole juurikaan luokiteltu. Eräs kyselyssä havaittu puute on menetelmä tietoturvallisuuden ajantasaisuuden arviointiin, niin käytössä olevissa kuin hankittavissa digitaalisissa palveluissa ja teknologioissa.

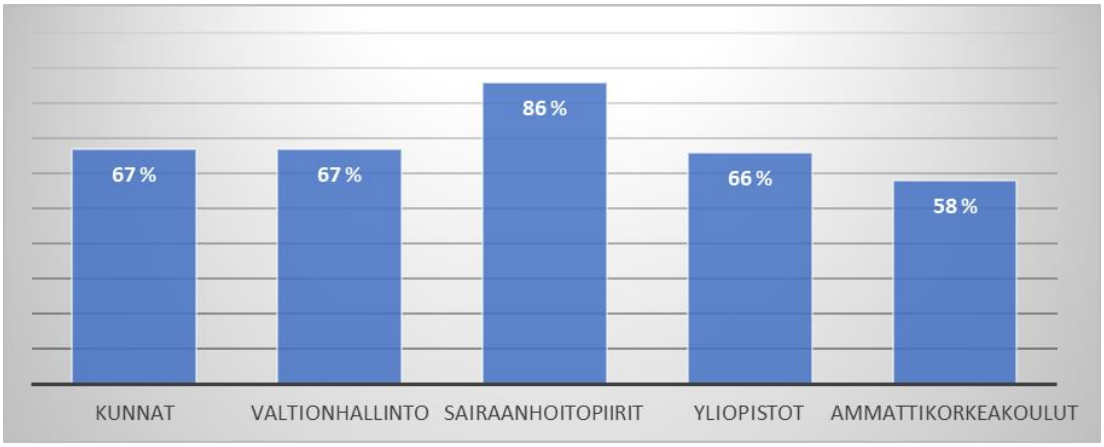
Organisaatiot, joilla on enemmän kehitettävää digitaalisessa turvallisuudessa, tuottavat itse suhteessa vähemmän ICT-palveluja kuin edelläkävijät. Tämä viittaa siihen, että ICT-palvelutuotantoa ulkoistettaessa palvelutuotannon ja digitaalisen turvallisuuden ohjaus jää puutteelliseksi, eikä organisaatiolle pääse muodostumaan realistista tilannekuvaa omasta digitaalisen turvallisuuden tasosta. Täytyy muistaa, että organisaatio on aina vastuussa omasta digitaalisesta turvallisuudesta, vaikka siihen liittyvä palvelutuotanto olisikin ulkoistettu kumppanille.

3 Digitaalisen turvallisuuden hallinta

3.1 Havainnointi- ja reagointikyky

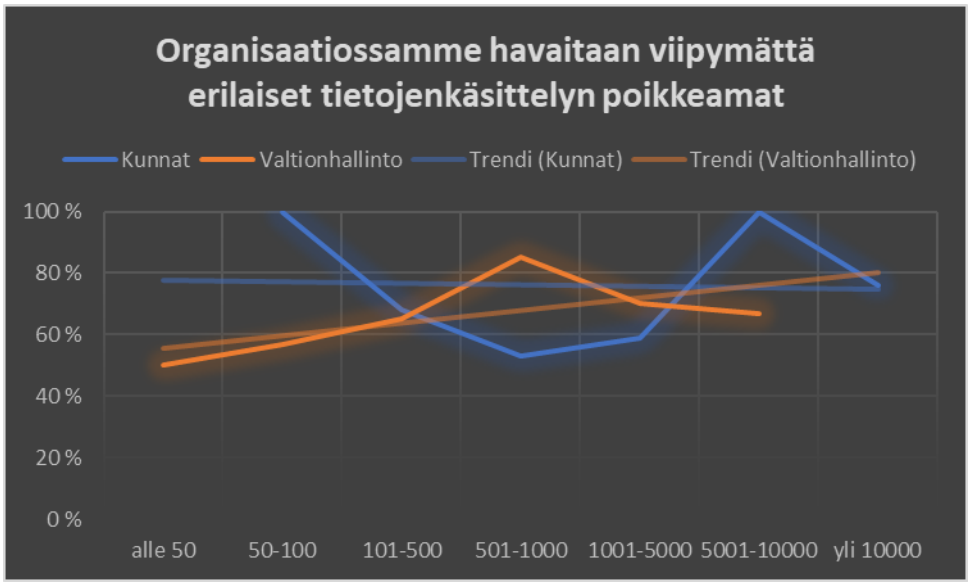
Yleisesti ottaen julkisen hallinnon organisaatioilla on korkea luottamus erilaisten tietojenkäsittelyn poikkeamien havainnointikykyyn. Julkisen hallinnon organisaatioista sairaanhoitopiirit ja SOTE-organisaatiot erottuvat edukseen.

Kuvio 19. Organisaatiossamme havaitaan viipymättä erilaiset tietojenkäsittelyn poikkeamat



Havainnointikyvyssä kunnat ja valtionhallinto näyttäisivät olevan samalla tasolla (Kuvio 19), mutta kun vastauksia tarkastellaan organisaation koon mukaan, huomataan eroja kuntien ja valtionhallinnon yksiköiden välillä (Kuvio 20). Pienet kunnat ovat havainnointikykyynsä huomattavasti luottavaisempia kuin samankokoiset valtionhallinnon yksiköt. Koon kasvaessa kuntien luottamus pienenee ja valtionhallinnon kasvaa, kunnes isojen organisaatioiden tapauksessa kuntakentän luottamus nousee taas valtionhallinnon organisaatioita suuremmaksi. Syinä tähän voivat olla pienten valtionhallinnon yksiköiden parempi tietoturvatietoisuus ja isojen organisaatioiden mahdollisuudet investoida poikkeamien havainnointikykyyn. Pienet kunnat voivat luottaa ICT-palvelukumppaneidensa havainnointikykyyn, eikä heillä välttämättä ole keinoja arvioida onko luottamukselle katetta.

Kuvio 20. Luottamus poikkeamien havainnointikykyyn (kunnat ja valtionhallinto)

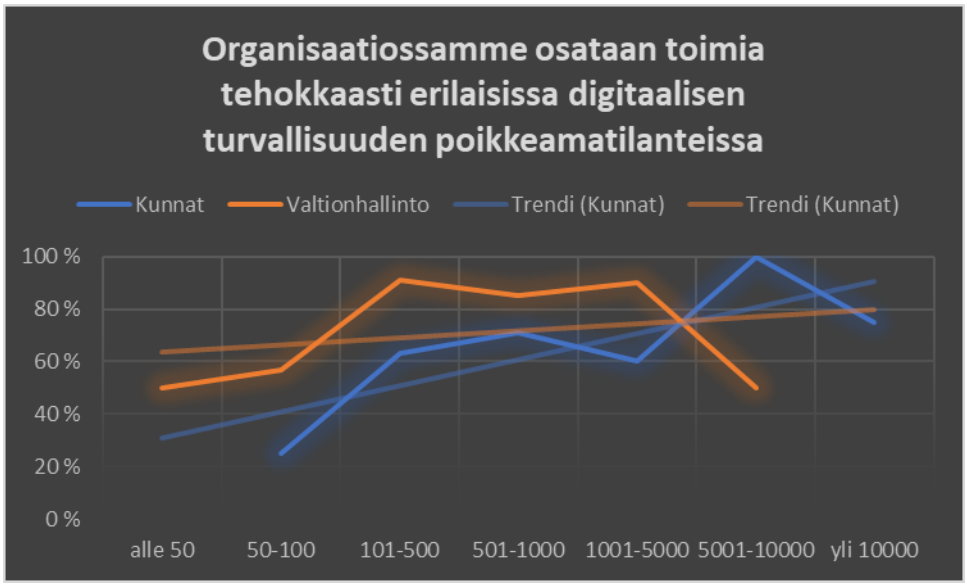


Kun tarkastellaan reagointikykyä poikkeamatilanteissa, huomataan erojen kasvavan organisaatiotyyppien välillä. Sairaanhoitopiirien ja yliopistojen reagointikyky on kaikkien vastaajien arvion mukaan kunnossa, valtionhallinto on kuntien ja ammattikorkeakoulujen reagointikykyä korkeammalla tasolla (Kuvio 21). Sairaanhoitopiirien luottamusta selittää todennäköisesti sairaanhoitopiirien toiminnan luonne sekä toiminnalle asetetut vaatimukset.

Kuvio 21. Organisaatiossamme osataan toimia tehokkaasti erilaisissa digitaalisen turvallisuuden poikkeamatilanteissa ja palata nopeasti normaaliin toimintaan

Kun tarkastellaan kuntien ja valtionhallinnon eroja, niin molemmissa ryhmissä luottamustrendi reagointikykyyn nousee organisaatiokoon kasvaessa, mutta lähtötaso on pienissä kunnissa huomattavasti vastaavan kokoisia valtionhallinnon yksiköitä alempi (Kuvio 22).

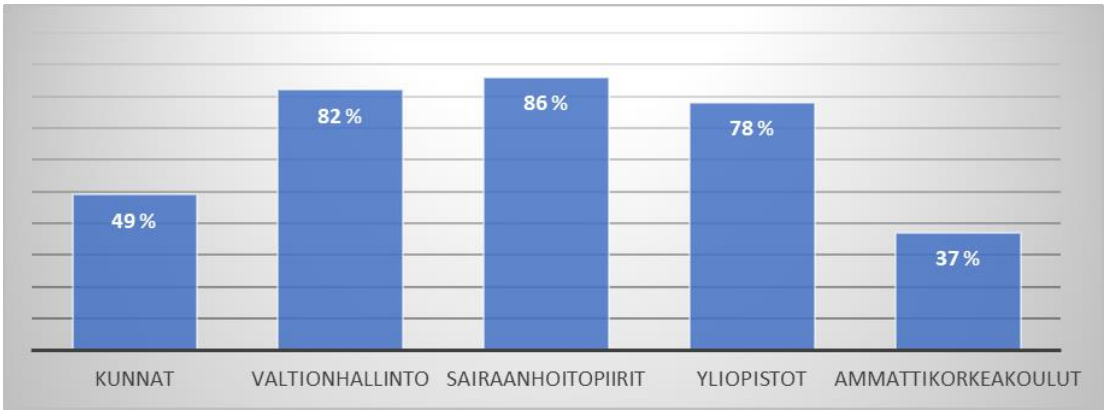
Kuvio 22. Luottamus reagointikykyyn (kunnat ja valtionhallinto)



3.2 Harjoittelu ja koulutus

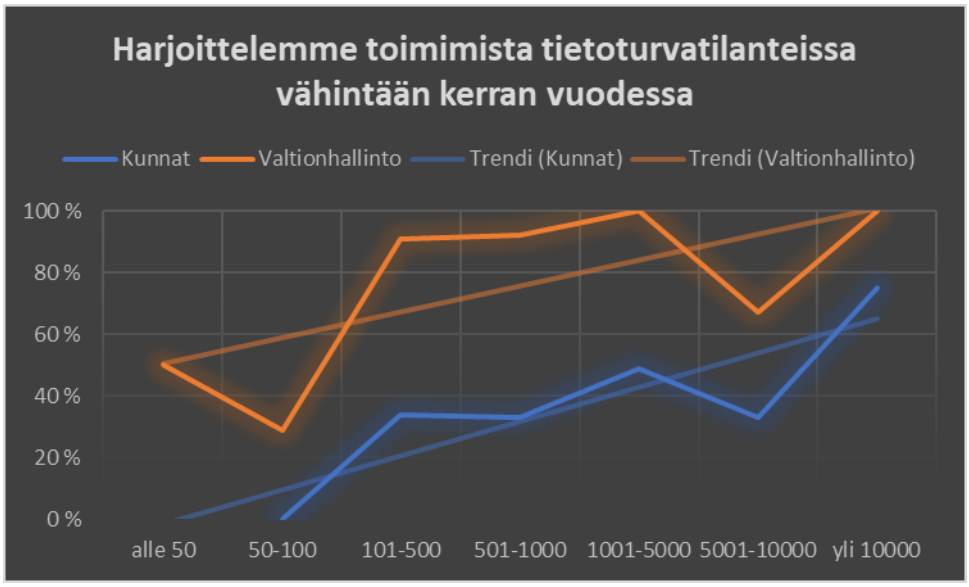
Tietoturvatilanteissa toimimista harjoitellaan valtionhallinnon yksiköissä, sairaanhoitopiireissä ja yliopistoissa selvästi enemmän kuin kunnissa ja ammattikorkeakouluissa (Kuvio 23). Ero on huomattava ja johtunee valtionhallinnon, sairaanhoitopiirien ja yliopistojen aktiivisemmasta osallistumisesta tietoturvaharjoituksiin ja tietoturvallisuuden yhteistyöverkostoihin.

Kuvio 23. Harjoittelemme toimimista tietoturvatilanteissa vähintään kerran vuodessa



Kun verrataan kuntia ja valtionhallintoa, huomataan trendi, jonka mukaan harjoittelu lisääntyy organisaatiokoon kasvaessa (Kuvio 24). Huomionarvoista on, että kuntasektorin harjoittelu pysyy organisaatiokoosta riippumatta selkeästi alemmalla tasolla kuin valtionhallinnossa. Erityisen huolestuttava tilanne on alle 100 hengen kuntaorganisaatioissa, joissa vastausten perusteella ei harjoitella ollenkaan tietoturvatilanteissa toimimista.

Kuvio 24. Tietoturvatilanteissa harjoittelu (kunnat ja valtionhallinto)

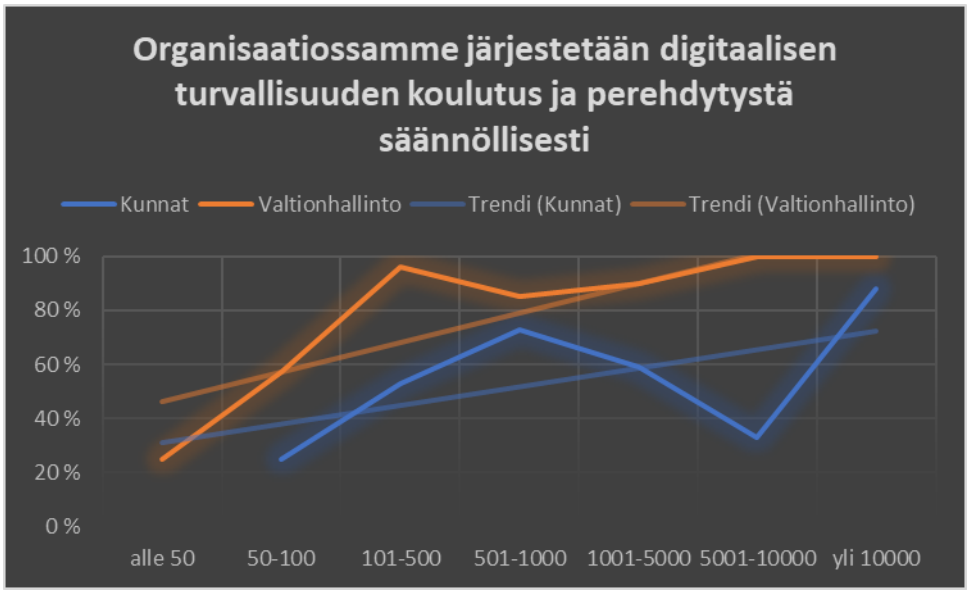


Digitaalisen turvallisuuden säännöllistä koulutusta ja perehdytystä järjestetään hyvin sairaanhoitopiireissä, yliopistoissa ja valtionhallinnon organisaatioissa (Kuvio 25). Sairaanhoitopiirien vastaajista kaikki ilmoittivat järjestävänsä säännöllistä digitaalisen turvallisuuden koulutusta, mistä muut organisaatiot voivat ottaa mallia. Kunnat ja ammattikorkeakoulut olivat tässäkin asiassa hivenen muita vastaajaryhmiä alemmalla tasolla.

Kuvio 25. Organisaatiossamme järjestetään digitaalisen turvallisuuden koulutusta ja perehdytystä säännöllisesti

Kun vertaillaan kuntia ja valtionhallintoa, huomataan sama trendi kuin havainnointikyvyssä – mitä suurempi organisaatio, sitä enemmän digitaalisen turvallisuuden koulutusta järjestetään (Kuvio 26). Oikeastaan ainoa ero käyrissä on se, että kunnat ovat kautta linjan alemmalla tasolla. Tämä on selkeä kehityskohde kunnissa, kuten myös ammattikorkeakouluissa. Vastauksista huomattiin, että ne organisaatiot, jotka harjoittelevat tietoturvahäiriöissä toimimista, järjestävät myös tietoturvakoulutusta muita organisaatioita enemmän.

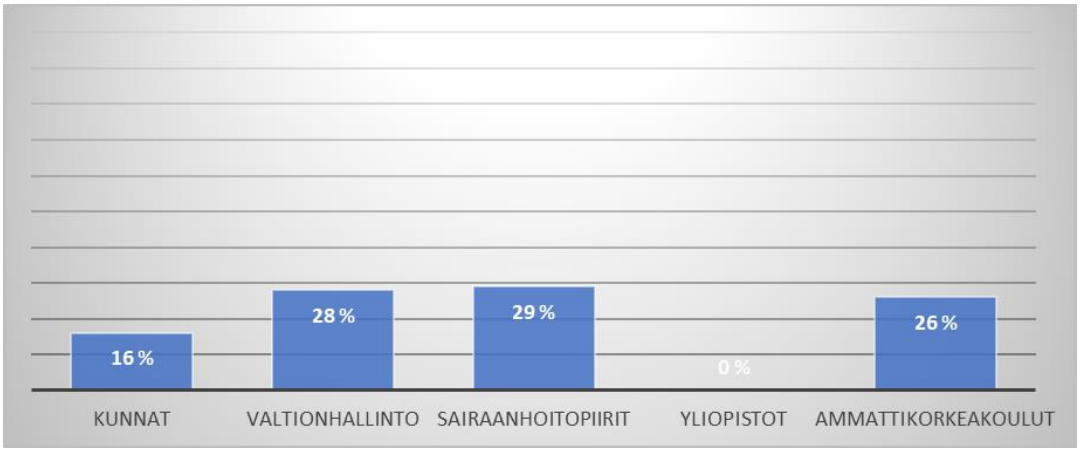
Kuvio 26. Digitaalisen turvallisuuden koulutus (kunnat ja valtionhallinto)



3.3 Digitaalisen turvallisuuden resursointi

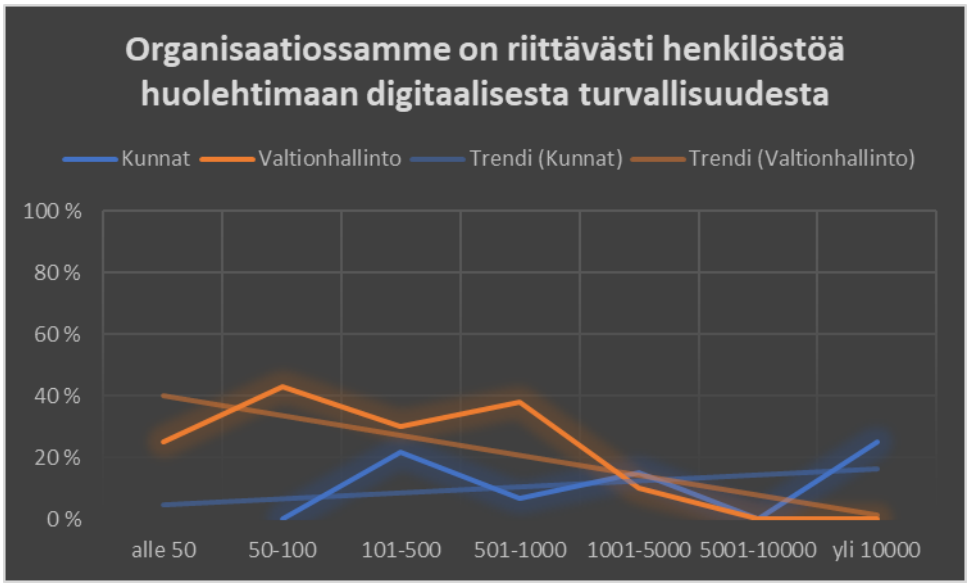
Yleisesti ottaen kaikkien vastaajien mielestä digitaalisen turvallisuuden henkilöstöä ei ole riittävästi (Kuvio 27). Kooltaan pienten organisaatioiden hivenen korkeampi kyllä-vastausten määrä voi selittyä sillä, että omien tietoturvahenkilöiden puuttuessa he luottavat isoja organisaatioita enemmän IT-palvelukumppaneihinsa, kuten kunnalliseen ICT-palvelutuotantoyritykseen tai valtionhallinnon tapauksessa esimerkiksi Valtorin palveluihin.

Kuvio 27. Organisaatiossamme on riittävästi henkilöstöä huolehtimaan digitaalisesta turvallisuudesta



Kuntia ja valtionhallintoa vertailtaessa on mielenkiintoista huomata, että organisaatiokoon kasvaessa valtiohallinnon trendi laskeva, mutta kunnilla lievästi nouseva (Kuvio 28).

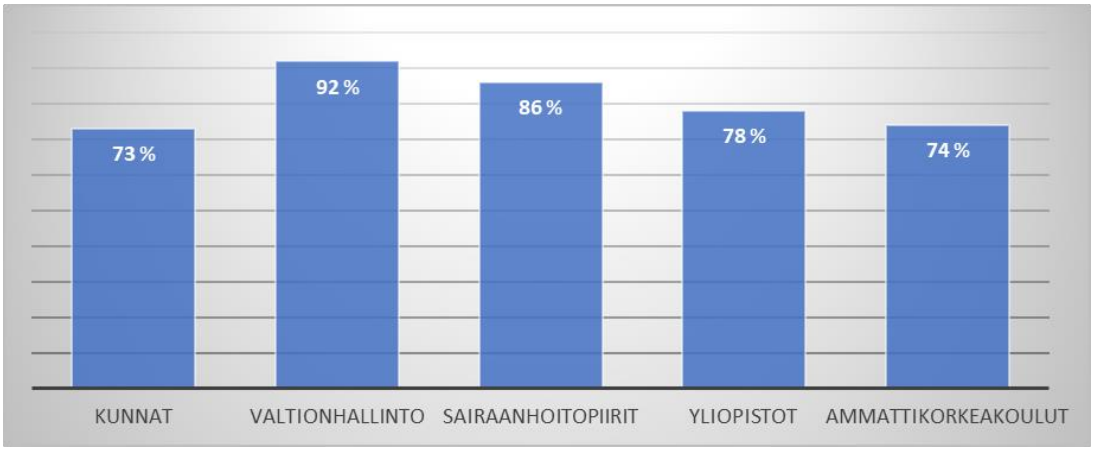
Kuvio 28. Digitaalisen turvallisuuden henkilöstö (kunnat ja valtionhallinto)



3.4 Kriittiset kohteet

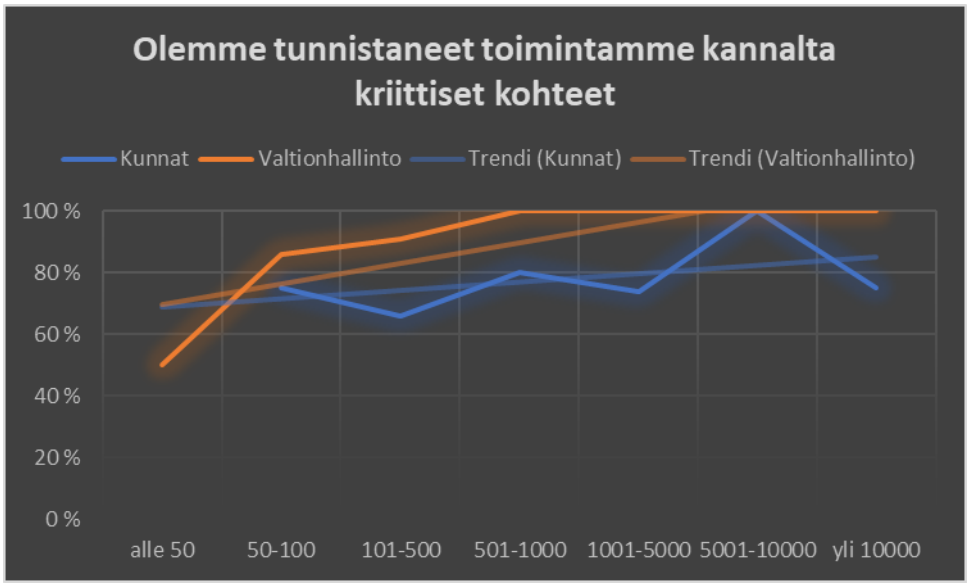
Toiminnan kannalta kriittiset kohteet on vastauksien perusteella tunnistettu hyvin (Kuvio 29). Parhaiten kriittiset kohteet, joilla tässä yhteydessä tarkoitetaan kriittisiä tietojärjestelmiä, digitaalisia palveluja ja prosesseja, tietovarantoja, tietoja ja tietovirtoja sekä infrastruktuuria, on tunnistettu valtiohallinnossa ja sairaanhoitopiireissä. Kyselyaineistosta oli havaittavissa, että ne organisaatiot, jotka olivat ylipäänsä tunnistaneet kriittiset kohteensa, luottivat muita enemmän myös havainnointi- ja reagointikykyynsä.

Kuvio 29. Olemme tunnistaneet toimintamme kannalta kriittiset kohteet



Kuntien ja valtiohallinnon vastauksissa on havaittavissa, että valtiohallinnossa yli 500 hengen organisaatiot ovat kaikki tunnistaneet kriittiset kohteensa (Kuvio 30).

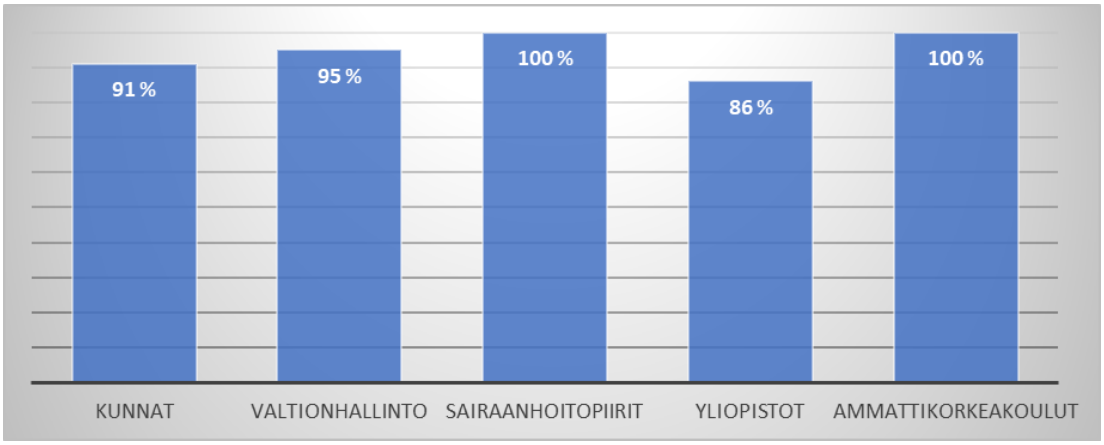
Kuvio 30. Kriittisten kohteiden tunnistus (kunnat ja valtionhallinto)



3.4.1 Kriittiset tietojärjestelmät

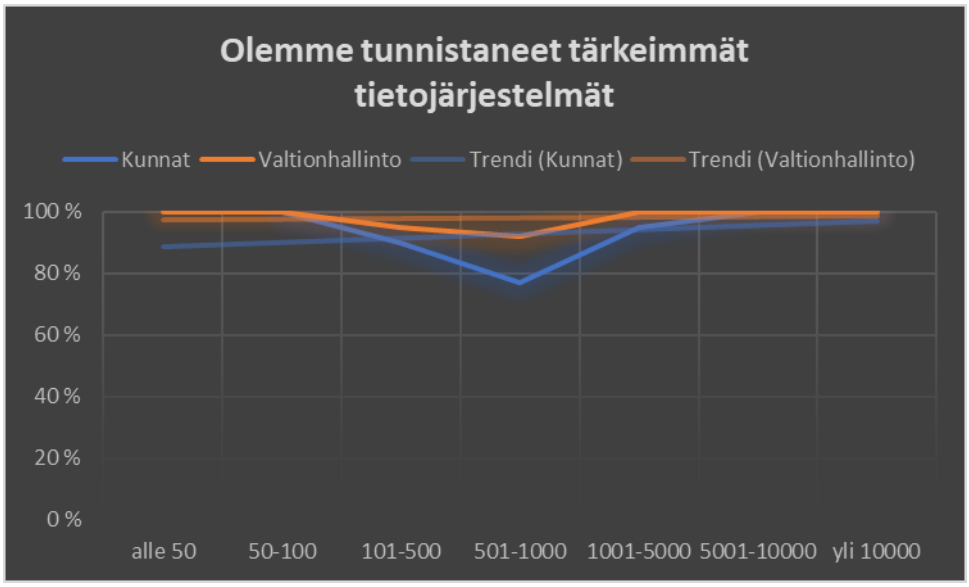
Toiminnan kannalta kriittiset tietojärjestelmät on tunnistettu lähes sataprosenttisesti niiden vastaajien keskuudessa, jotka vastasivat tunnistaneensa kriittiset kohteensa (Kuvio 31). Tämä johtunee siitä, että tietojärjestelmät ovat lähinnä käyttäjiä ja päivittäisiä käyttötapauksia. Sen vuoksi toiminnan kannalta tärkeät tietojärjestelmät on helppo tunnistaa – mikäli järjestelmä ei toimi, niin toiminta estyy. Koska oman toiminnan kannalta kriittiset tietojärjestelmät on hyvin tunnistettu, suositellaan organisaatioille pohdittavaksi myös kriittisyyttä siitä näkökulmasta, onko kriittisillä (tai muilla) tietojärjestelmillä merkitystä kansallisella tasolla.

Kuvio 31. Olemme tunnistaneet kriittiset tietojärjestelmät



Kuntien ja valtionhallinnon välillä ei oikeastaan ole muuta eroa kuin kokoluokassa 501-1000 molemmissa ryhmissä oleva notkahdus on kuntasektorilla hivenen suurempi (0).

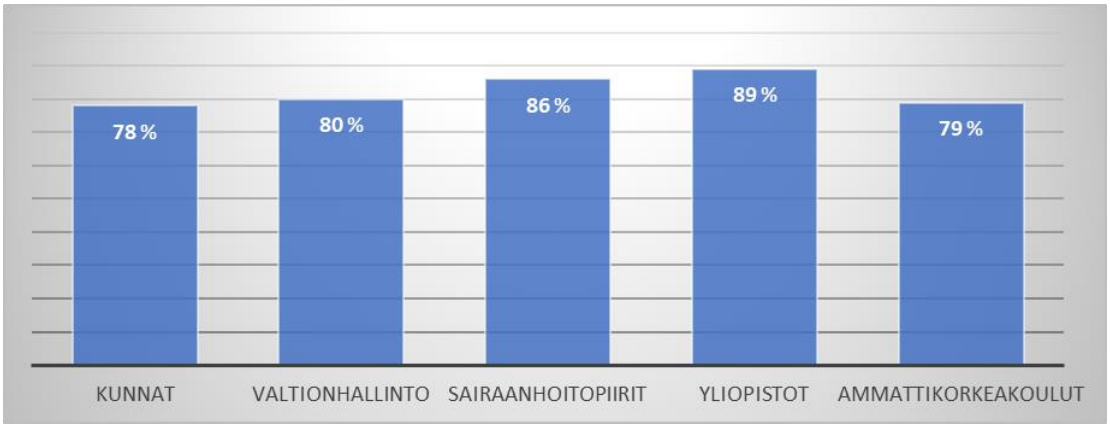
Kuvio 32. Tärkeimmät tietojärjestelmät (kunnat ja valtionhallinto)



3.4.2 Tietojärjestelmärekisteri

Koska kriittiset tietojärjestelmät on tunnistettu hyvin, ei ole yllätys, että myös suurimmalla osalla vastaajista on käytössään tietojärjestelmärekisteri tai muu tapa ylläpitää ajantasaista tietoa tietojärjestelmistä (Kuvio 33).

Kuvio 33. Organisaatiossamme on käytössä tietojärjestelmärekisteri tai muu tapa ylläpitää ajantasaista tietoa tietojärjestelmistä



Kun tarkastellaan kuntien ja valtionhallinnon välisiä eroja, niin trendi on molemmilla organisaatiokoon mukaan kasvava (Kuvio 34). Valtionhallinnossa trendikäyrä on jyrkemmin nouseva, mikä johtuu siitä, että pienimmillä valtionhallinnon yksiköillä tietojärjestelmärekisteri on harvemmin käytössä kuin suuremmilla yksiköillä. Myös pienimmillä kuntaorganisaatioilla on puutteita tietojärjestelmärekisterin käytössä.

Kuvio 34. Tietojärjestelmärekisteri (kunnat ja valtionhallinto)

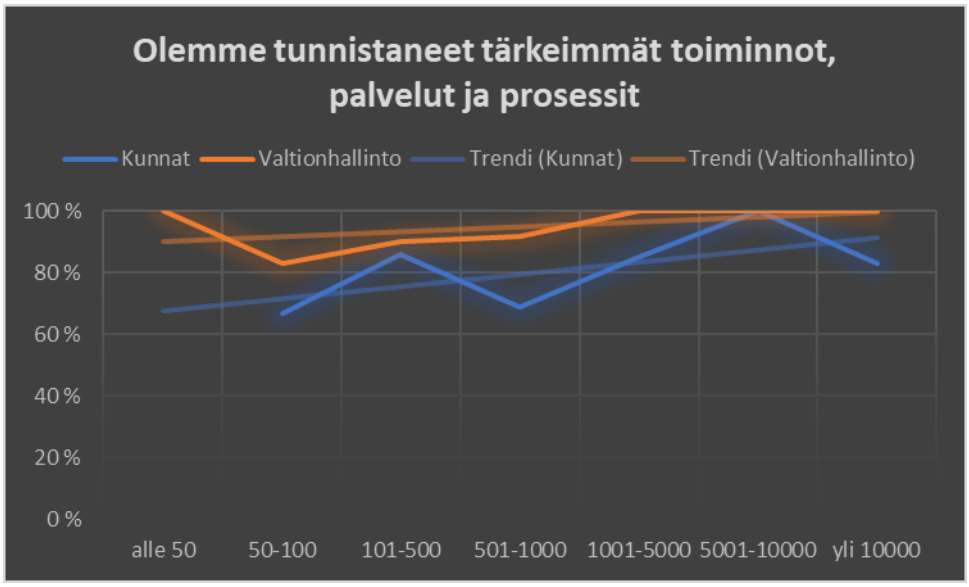
3.4.3 Kriittiset toiminnot, palvelut ja prosessit

Vastaajaorganisaatiot ovat tunnistaneet hyvin myös toimintansa kannalta kriittiset toiminnot, palvelut ja prosessit (Kuvio 35). Syy lienee sama kuin kriittisten tietojärjestelmien kohdalla, eli päivittäisen työn ja toiminnan kannalta kriittiset toiminnot, palvelut ja prosessit on suhteellisen helppo tunnistaa. Parhaiten kriittiset toiminnot, palvelut ja prosessit on tunnistettu sairaanhoitopiireissä ja valtionhallinnossa, mutta muutkaan vastaajaryhmät eivät jääneet paljoa huonommiksi.

Kuvio 35. Olemme tunnistaneet tärkeimmät toiminnot, palvelut ja prosessit

Kun vertaillaan kuntia ja valtionhallintoa, huomaamme hyvin samankaltaisen nousevan trendin (Kuvio 36). Kokonaisuudessa valtionhallinnon organisaatiot ovat aavistuksen paremmalla tasolla kuin kunnat. Valtionhallinnon organisaatioista yli 1000 hengen organisaatiot ovat kaikki tunnistaneet tärkeimmät toimintonsa, palvelunsa ja prosessinsa.

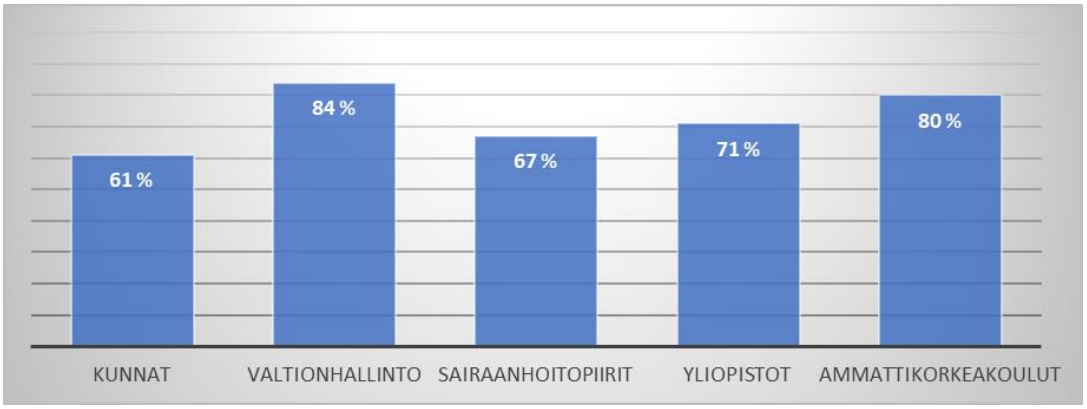
Kuvio 36. Tärkeimmät toiminnot, palvelut ja prosessit (kunnat ja valtionhallinto)



3.4.4 Kriittiset tietovarannot

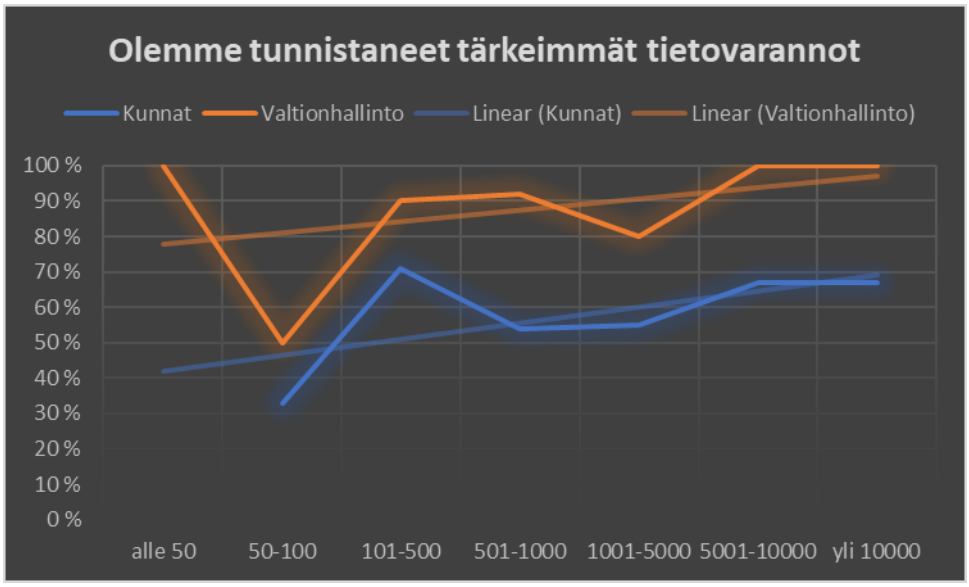
Toiminnan kannalta kriittiset tietovarannot, eli yleisimmin tietokannat, oli myös tunnistettu suhteellisen hyvällä tasolla, parhaiten valtionhallinnossa ja ammattikorkeakouluissa (Kuvio 37). Taso on kuitenkin aavistuksen alempi kuin edellisissä kohteissa. Tämä johtunee siitä, että toiminnan kannalta kriittisten tietovarantojen tunnistaminen on hivenen vaativampaa kuin tietojärjestelmien, toimintojen, palveluiden tai prosessien tunnistaminen.

Kuvio 37. Olemme tunnistaneet tärkeimmät tietovarannot



Kuntien ja valtionhallinnon välisessä vertailussa käyrät ovat jälleen hyvin samankaltaiset (Kuvio 38). Kun organisaatiokoko kasvaa, on tietovarannotkin yleisesti ottaen paremmin tunnistettu. Valtionhallinto on kuntasektoria edellä tärkeimpien tietovarantojen tunnistamisessa.

Kuvio 38. Tärkeimmät tietovarannot (kunnat ja valtionhallinto)

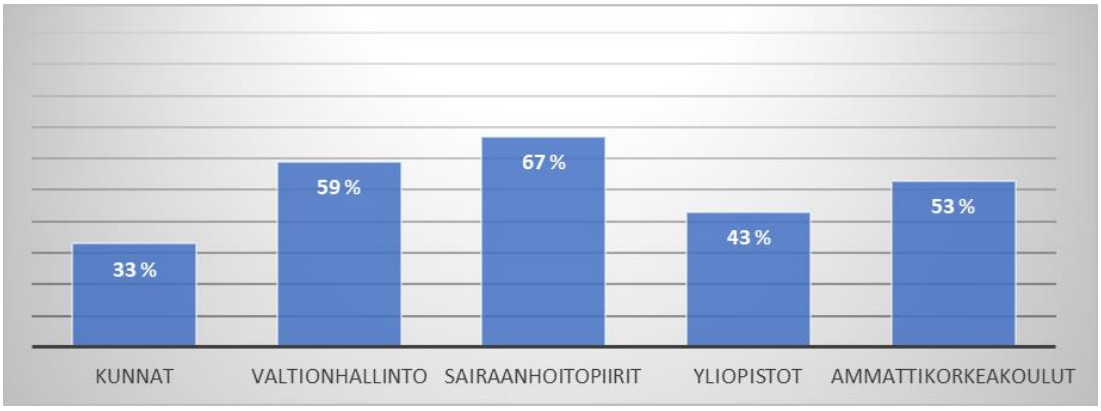


3.4.5 Kriittiset tiedot ja tietovirrat

Toiminnan kannalta kriittisten tietojen ja tietovirtojen (integraatioiden) tunnistaminen on selkeä kehityskohde kaikissa organisaatioissa (Kuvio 39). Toiminnan kannalta kriittisten tietojen tunnistaminen on sidoksissa kriittisten tietovarantojen tunnistamiseen, mutta menee askeleen syvemmälle. Tietojen tunnistamista voi lähestyä esimerkiksi kriittisten prosessien ja niissä käsiteltävien tietojen kautta.

Kriittiset tietovirrat ovat tietojen siirtoa joko organisaation sisällä esimerkiksi tietojärjestelmästä toiseen tai organisaatiosta ulospäin esimerkiksi kumppaneille. Tietovirtojen ja niissä siirrettävien tietojen tunnistaminen on tärkeää tiedonhallinnan ja henkilötietojen tapauksessa myös tietosuojan näkökulmasta.

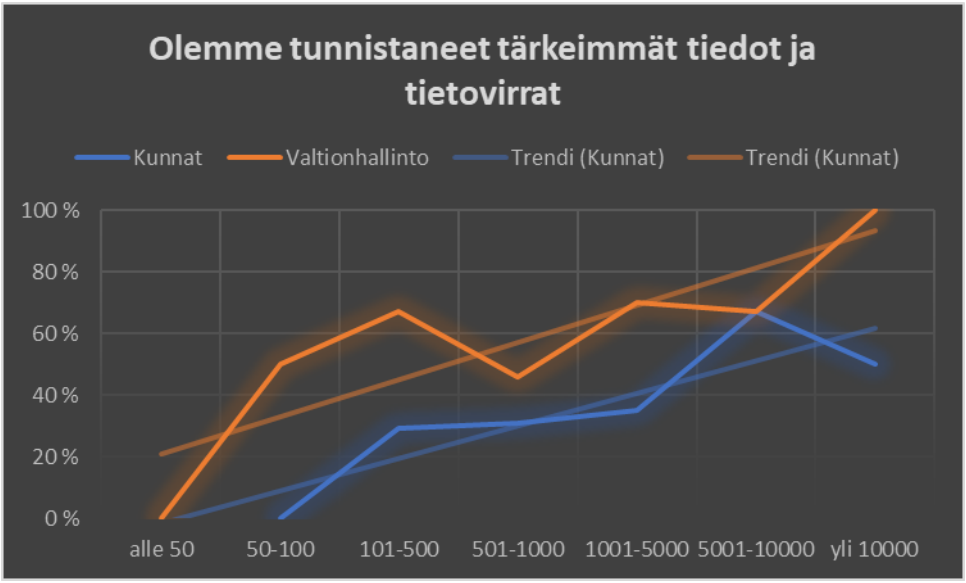
Kuvio 39. Olemme tunnistaneet tärkeimmät tiedot ja tietovirrat



Kun vertaillaan kuntia ja valtionhallintoa, havaitaan molemmissa selkeästi kasvava trendi organisaatiokoon kasvaessa (Kuvio 40). Suuret organisaatiot ovat tunnistaneet pieniä paremmin kriittiset tietonsa ja tietovirtansa. Valtionhallinto on jälleen

aavistuksen kuntasektoria edellä. Suositeltavaa on, että tietoja ja tietovirtoja lähdetään tunnistamaan kriittisten tietojärjestelmien sekä kriittisten toimintojen ja prosessien kautta, koska ne on paremmin tunnistettu.

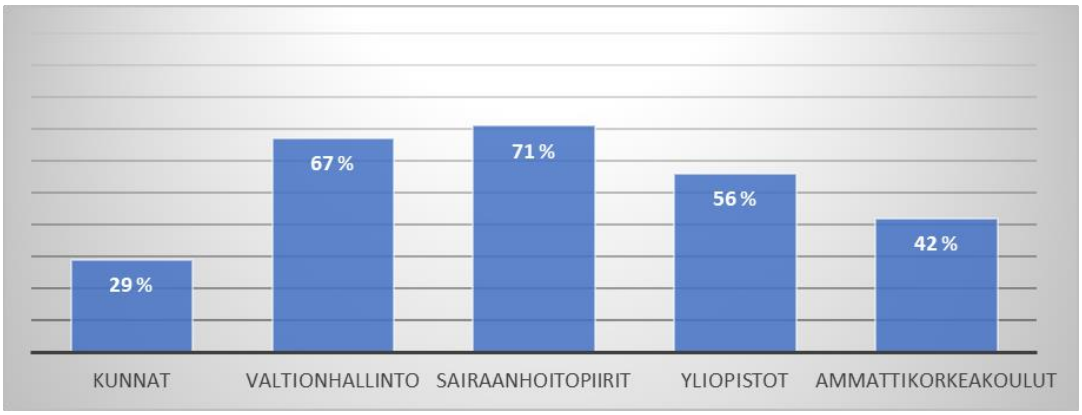
Kuvio 40. Tärkeimmät tiedot ja tietovirrat (kunnat ja valtionhallinto)



3.4.6 Kriittisten kohteiden luokittelu

Luokittelumenettely organisaatioissa, jotka olivat tunnistaneet kriittiset kohteensa, oli parhaiten käytössä sairaanhoitopiireillä ja valtionhallinnolla (Kuvio 41). Vastausten perusteella kunnissa kriittisiä kohteita kyllä tunnistetaan, mutta ne luokitellaan vapaamuotoisemmin ilman vakiintunutta menettelyä. Yliopistot ovat luokittelumenettelyn suhteen hieman ammattikorkeakouluja korkeammalla tasolla.

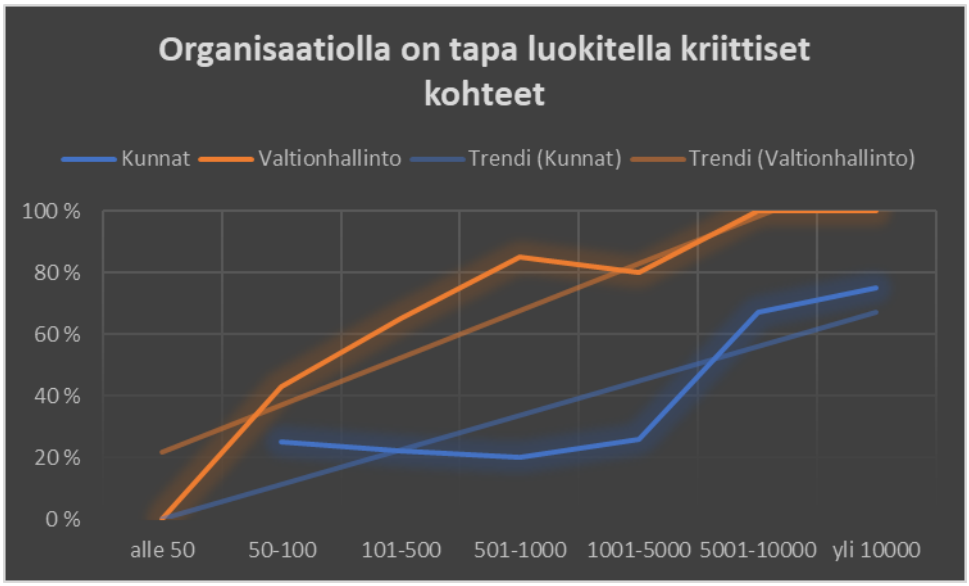
Kuvio 41. Organisaatiolla on tapa luokitella kriittiset kohteet



Kun kuntia ja valtionhallintoa tarkastellaan tarkemmin, paljastuu tuttu trendi. Mitä suurempi organisaatio, sen todennäköisemmin kriittisten kohteiden luokitteluun on

käytössä jokin menettelytapa (Kuvio 42). Valtionhallinnossa taustalla voi olla Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa, joka ohjaa valtionhallinnon organisaatioita formaaliin menettelyyn myös kriittisten kohteiden luokittelussa. Kuntasektorilla käyrä on huolestuttavan matala aina suurimpiin kuntaorganisaatioihin saakka, mikä osoittaa, ettei kuntasektorilla ole vakiintunutta kriittisyyden luokittelumenettelyä.

Kuvio 42. Kriittisten kohteiden luokittelumenettely (kunnat ja valtionhallinto)

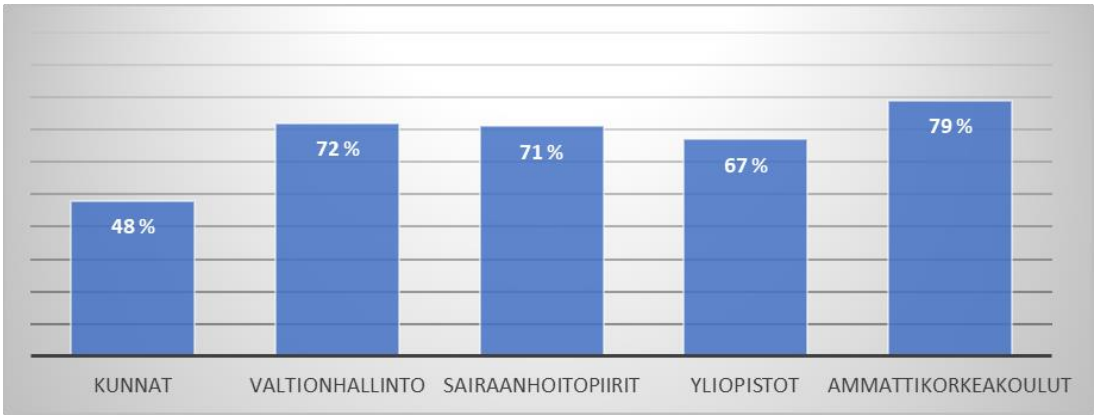


3.5 Sähköisen asioinnin palveluiden hankinta ja kehitys

3.5.1 Digitaalinen turvallisuus hankinnoissa

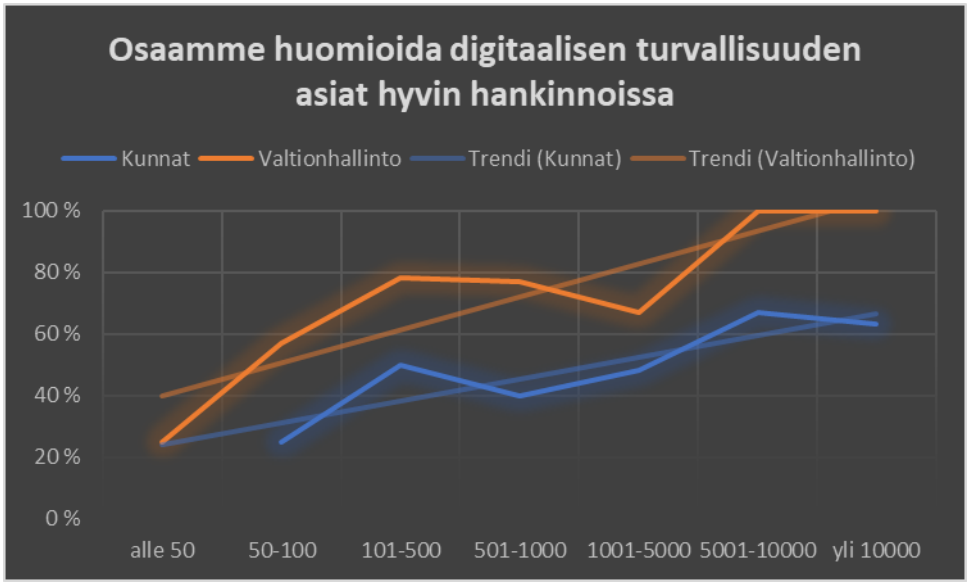
Vastausten perusteella digitaalinen turvallisuus otetaan hyvin huomioon hankinnoissa (Kuvio 43). Poikkeuksena on kuntasektori, jossa ainoastaan noin puolet vastaajista vastasi kyllä. Vastausten perusteella ammattikorkeakoulut ovat ottaneet hankinnoissa digitaalisen turvallisuuden parhaiten huomioon, joskin valtionhallinto ja sairaanhoitopiirit ovat lähes yhtä hyvällä tasolla.

Kuvio 43. Osaamme huomioida digitaalisen turvallisuuden asiat hyvin hankinnoissa



Kun tarkastelemme kuntia ja valtionhallintoa organisaatiokoon mukaan, huomaamme saman trendin kuin digitaalisen turvallisuuden koulutuksessa (0). Mitä isompi organisaatio, sitä paremmin digitaalinen turvallisuus otetaan huomioon hankinnoissa. Samaten valtionhallinnon käyrä on koko ajan ylemmällä tasolla kuin kuntakäyrä. Kehittämistä vaatii etenkin pienten kuntien ja valtionhallinnon yksiköiden kyvykkyys ottaa digitaalinen turvallisuus huomioon hankinnoissa. Koska koulutus- ja hankintatrendikäyrät ovat lähes identtiset, voidaan pohtia, antaako säännöllinen digitaalisen turvallisuuden koulutus eväitä myös parempaan digitaalisen turvallisuuden huomioimiseen hankinnoissa.

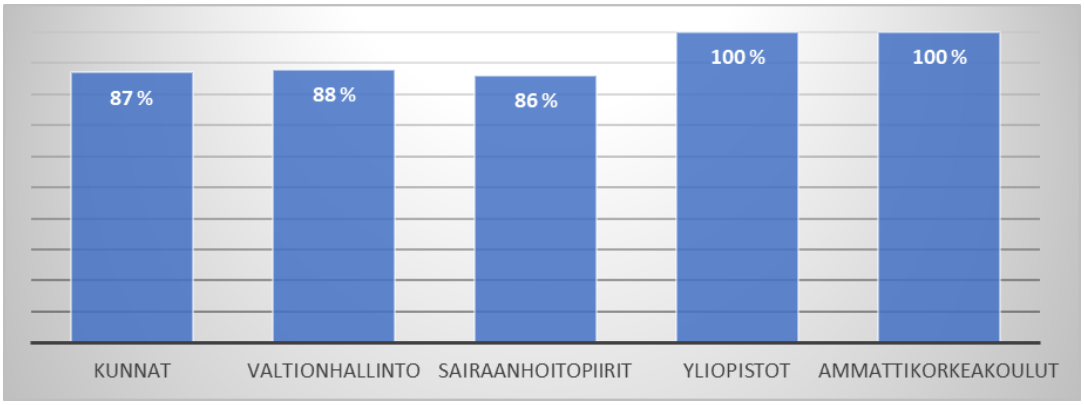
Kuvio 44. Digitaalinen turvallisuus hankinnoissa (kunnat ja valtionhallinto)



3.5.2 Tietoverkkojen turvallisuuden huomioiminen palvelukehityksessä

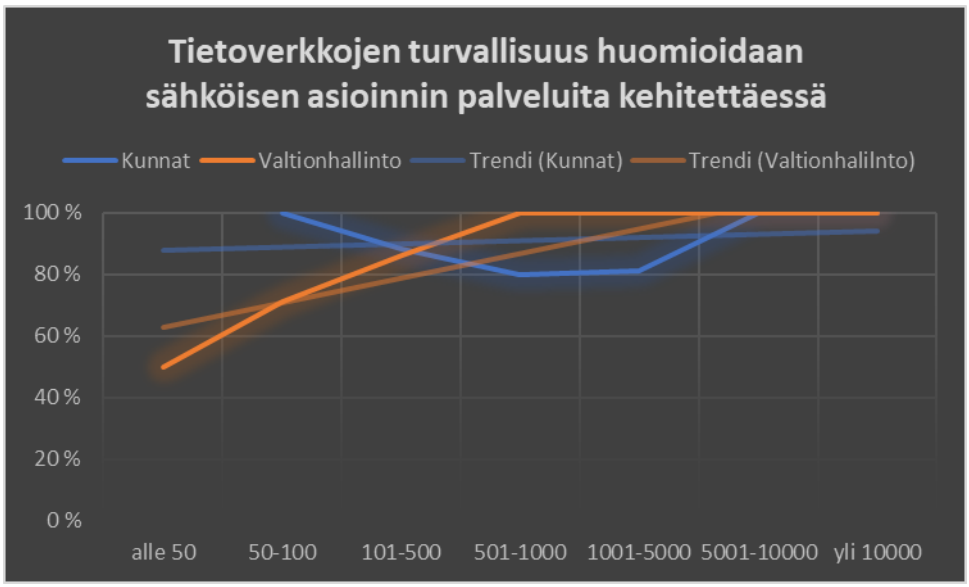
Sähköisen asioinnin palveluita kehitettäessä organisaatiot ovat vastausten perusteella hyvin huomioineet tietoverkkojen turvallisuuden (Kuvio 45). Kyllä-vastausten osuus oli kaikilla organisaatiotyypeillä yli 85 %.

Kuvio 45. Tietoverkkojen turvallisuus huomioidaan sähköisen asioinnin palveluita kehitettäessä



Kuntien ja valtionhallinnon tarkemmassa vertailussakaan ei eroja juuri tule (0). Ainoastaan pienimmät valtionhallinnon organisaatiot ovat vastausten perusteella hivenen alemmalla tasolla.

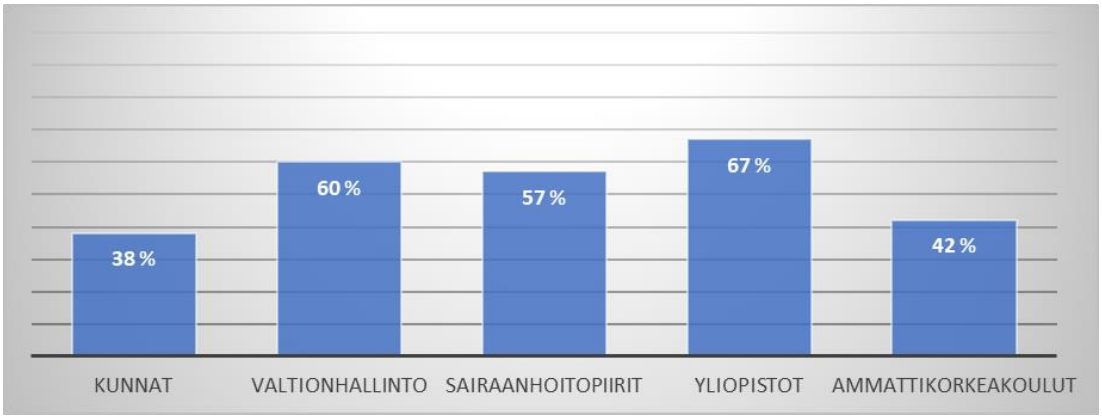
Kuvio 46. Tietoverkkojen turvallisuus sähköisen asioinnin palvelukehityksessä (kunnat ja valtionhallinto)



3.5.3 Digitaalisen turvallisuuden vastuut ja velvollisuudet

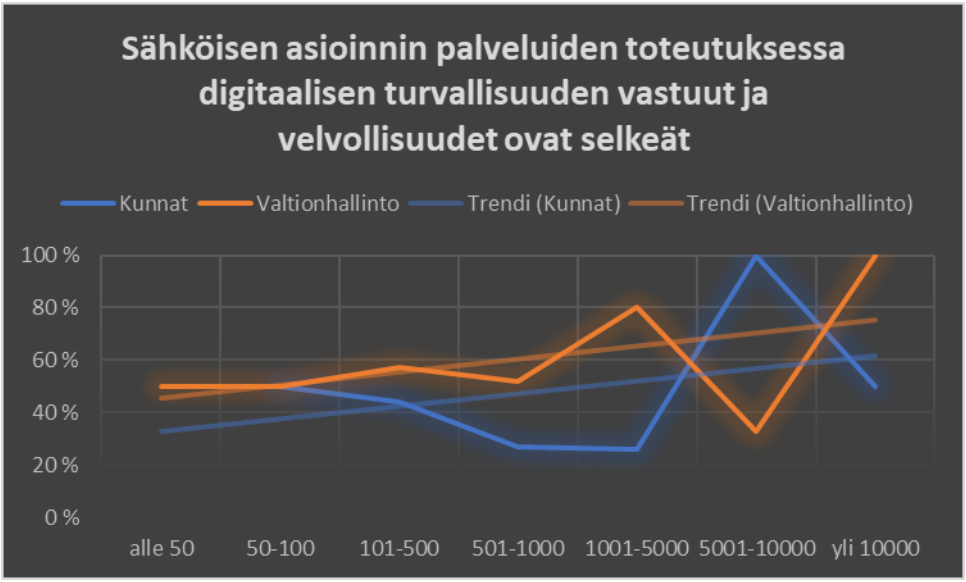
Digitaalisen turvallisuuden vastuut ja velvollisuudet eivät ole sähköisen asioinnin palveluiden toteutuksessa yhtä selkeitä kuin tietoverkkojen turvallisuuden huomioiminen (Kuvio 47). Parhaiten vastuut ja velvollisuudet ovat selvillä yliopistoilla ja valtiohallinnossa, mutta kaikilla organisaatiotyypeillä on vielä kehitettävää.

Kuvio 47. Sähköisen asioinnin palveluiden toteutuksessa digitaalisen turvallisuuden vastuut ja velvollisuudet ovat selkeät



Kun verrataan kuntakenttää ja valtiohallintoa, on trendi samankaltainen organisaatiokoon kasvaessa lievästi nouseva (0). Itse vastauksissa huomataan ongelmalliseksi kuntasektorilla kokoluokka 501-5000, jossa vain noin neljännes vastaajista sanoi vastuiden ja velvollisuuksien olevan selkeitä. Vastaava alenema on valtionhallinnossa kokoluokassa 5001-10000, jossa kolmannes vastaajista vastasi vastuiden ja velvollisuuksien olevan selkeitä.

Kuvio 48. Digitaalisen turvallisuuden vastuut ja velvollisuudet sähköisen asioinnin kehityksessä (kunnat ja valtionhallinto)



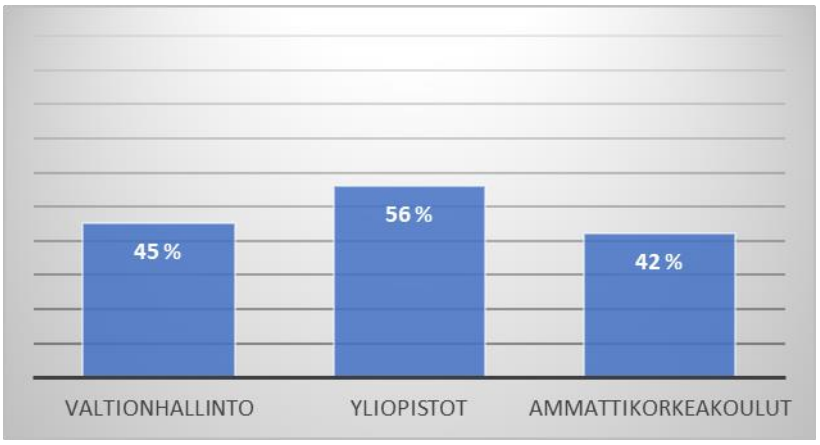
3.6 Tietoturvallisuuden arviointi

Edellisten kysymysten lisäksi valtionhallinnon yksiköiltä, yliopistoilta ja ammattikorkeakouluilta kysyttiin, miten ne arvioivat tietoturvallisuutta käytössä olevien ja hankittavien digitaalisten palveluiden osalta. Nämä kysymykset eivät sisältyneet kuntakyselyyn.

3.6.1 Käytössä olevien digitaalisten palveluiden tietoturvallisuus

Noin puolella vastaajista oli käytössä menetelmä käytössä olevien digitaalisten palveluiden ja teknologioiden tietoturvallisuuden ajantasaisuuden arvioimiseksi (Kuvio 49). Kun ajatellaan tietojärjestelmien ja digitaalisten palveluiden elinkaaren hallintaa, nousevat digitaalisen turvallisuuden arviointimenetelmät yhdeksi kehityskohteeksi, jolla organisaatioiden kyvykkyyttä voidaan parantaa.

Kuvio 49. Organisaatiossa on menetelmä käytössä olevien digitaalisten palveluiden ja teknologioiden tietoturvallisuuden ajantasaisuuden arvioimiseksi



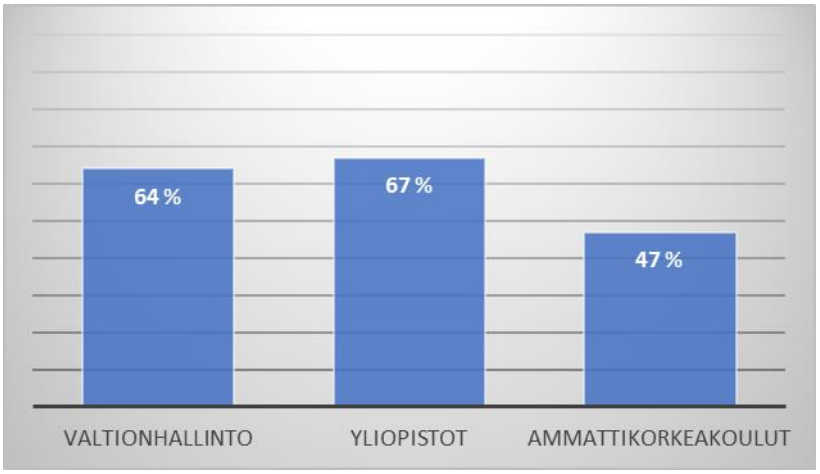
Kun tarkastellaan tarkemmin valtionhallinnon yksiköitä, huomataan arviointikyvykkyyden kasvavan voimakkaasti organisaatiokoon kasvaessa (Kuvio 50). Tämä viittaa siihen, että kehitystarve on suurin pienimmissä organisaatioissa.

Kuvio 50. Käytössä olevien digitaalisten palveluiden ja teknologioiden tietoturvallisuuden arviointikyvykkyys (valtionhallinto)

3.6.2 Hankittavien digitaalisten palveluiden tietoturvallisuuden arviointi

Hankittavien digitaalisten palvelujen ja teknologioiden tietoturvallisuuden arvioinnissa ollaan aavistuksen paremmalla tasolla, etenkin yliopistoissa ja valtionhallinnon yksiköissä (0).

Kuvio 51. Organisaatiossa on menetelmä hankittavien digitaalisten palveluiden ja teknologioiden tietoturvallisuuden arviointiin



Valtiohallinnossa trendi näyttäisi olevan samankaltainen kuin käytössä olevien palveluiden ja teknologioiden tietoturvallisuuden arvioinnissa, eli kyvykkyys kasvaa organisaatiokoon kasvaessa (Kuvio 52). Näin ollen eniten kehitettävää on pienissä, alle 100 hengen valtionhallinnon organisaatioissa.

Kuvio 52. Hankittavien digitaalisten palveluiden ja teknologioiden tietoturvallisuuden arviointikyvykkyys (valtionhallinto)

4 Tunnistetut tarpeet

Kyselyn tuloksista on havaittavissa, että julkisen hallinnon digitaalisen turvallisuuden kokonaisuutta voidaan kehittää kiinnittämällä organisaatioissa huomiota erityisesti johdonmukaiseen ja menetelmälliseen kriittisten kohteiden luokitteluun, vakiintuneiden digitaalisen turvallisuuden arviointimenetelmien käyttöön sekä henkilöstön säännölliseen koulutukseen ja poikkeamatilanteiden säännölliseen harjoitteluun.

Tässä kappaleessa on yhteenveto digitaalisen turvallisuuden tarpeisiin liittyvistä avoimista vastauksista. Tarpeet voitiin jakaa neljään kategoriaan; harjoittelu ja koulutus, resursointi, digitaalisen turvallisuuden palvelut ja muut digitaalista turvallisuutta parantavat toimenpiteet.

4.1 Harjoittelu ja koulutus

Vastauksissa toivottiin tietoturvan ja tietosuojan kehittämiseen enemmän valtakunnallista tukea ja palveluita, kuten:

- Kansallisia linjauksia ja konkreettisia ohjeita, malleja ja tarkastuslistoja tietoturvan parantamiseksi
- Julkiselle sektorille kohdistettua koulutusta tietoturvasta ja tietosuojasta
- Tietoturvaan liittyviä webinaareja ja maksuttomia tietoturvakoulutuksia
- Teknisiä suosituksia tietoverkkoihin, arkkitehtuuriin ja järjestelmiin liittyen
- Häiriötilannekoulutusta ja -apua
- Säännöllisiä kansallisia harjoituksia
- Ohjeita pilvipalveluiden käyttöönottoon
- Harjoittelua yhteistyöverkostoissa

Yleensä ottaen kaikki valtakunnallinen tuki ja toimintamallit ovat tervetulleita. Digiturvaviikkoa ja Taisto-harjoituksia pidettiin hyvinä ja niitä toivottiin lisää.

Toivottiin myös käyttäjille jatkuvaa koulutusta ja tiedotusta oman toiminnan merkityksestä. Tämä tarve on hyvä esimerkki siitä, että organisaatio on ensisijaisesti itse vastuussa tietoturvatoimenpiteiden järjestämisestä. Koulutusta on saatavilla, mutta organisaation täytyy itse sitoutua ottamaan henkilöstön jatkuva ja säännöllinen tietoturvatietoisuuden lisääminen osaksi toimintaansa.

4.2 Digitaalisen turvallisuuden resursointi

Kuten kyselystä ilmeni, kaikilla vastaajaorganisaatioilla oli niukkuutta digitaalisen turvallisuuden resursseista. Tämä heijastui myös vapaamuotoisissa vastauksissa:

- Koulutusta on helppo saada, mutta asioiden edistämiseksi tarvitaan lisää resursseja ja euroja, jotta koulutuksissa opittuja asioita voidaan jalkauttaa.
- Tietoturva ja tietosuoja vaativat uutta osaamista ja ammattitaitoa eikä niitä voida tehdä oman toimen ohella, joten tämän tulisi näkyä niin tietoturva- kuin tietosuojaresursseissa sekä näitä töitä tekevien asemassa ja palkkauksessa.
- Pienten kuntien resurssit ja osaaminen ovat riittämättömiä digitaalisen turvallisuuden ylläpitämiseen ja kehittämiseen. Tähän toivotaan kansallisia tukitoimia.
- Riittävä resursointi digitaalisen turvallisuuden varmistamiseksi. Tarve tulee korostumaan tulevaisuudessa, kun sähköisiä palveluja otetaan yhä enenevässä määrässä käyttöön.
- Henkilöstön osaamisen nosto ja johdon sitouttaminen tietoturvaan.
- Toivottiin, että julkinen sektori jakaa hyviä käytäntöjään ja osaamistaan toisilleen, koska virastokohtaiset resurssit ovat vähäiset.
- Digitaalisesta turvallisuudesta vastaavien henkilöiden määrä on organisaatiossa kovin vähäinen ja vaikuttaa, ettei samoja tyyppejä jakseta kuunnella jatkuvasti. Siksi talon ulkopuolelta tuleva vaikuttaja olisi tervetullut.
- Pienessä ICT-yksikössä ei ole erikseen tietoturvallisuuteen perehtynyttä henkilöä. Näin ollen digitaalisen turvallisuuden asioita hoidetaan muiden töiden ohella ehtimisen mukaan. Tämä ei ole ihanteellinen ratkaisu eikä edistä osaamisen kertymistä.
- Pitää olla osaaja omassakin organisaatiossa, jolla olisi hallussa kokonaisuus. Nyt kaikki toimivat omilla toimialoillaan huomiomatta kokonaisuutta, esimerkiksi tekevät hankintoja vain omalta kannalta, eikä katsota onko kokonaisuus toimiva.

4.3 Digitaalista turvallisuutta tukevat palvelut

Digitaalista turvallisuutta tukevat palvelut ovat kolmas osa-alue, jossa tarpeita tunnistettiin. Palveluihin liittyvät tarpeet vaihtelivat sparrauksesta laajoihin ja yhteisiin julkisen hallinnon teknisiin digitaalisen turvallisuuden palveluihin. Yhteisten ja

keskitettyjen palveluiden toivottiin myös olevan kustannuksiltaan mahdollisimman alhaisia. Tunnistettuja palvelutarpeita olivat:

- Yhteinen keskitetty julkisen hallinnon tietoturvavalvomo
- Ratkaisujen, kuten Havaro, mahdollisimman sujuva ja kustannustehokas käyttöönotto ja hyödyntäminen organisaatioissa
- Tietoturvaheikkouksien kartoituspalvelu
- Keskitetty tietoturvatapahtumien seurantajärjestelmä
- Kaikki keskitetysti hallinnolle tuotettavat palvelut tulisi arvioida tai auditoida, jotta niiden käyttöön velvoitetuilla organisaatioilla olisi palveluiden tilasta selkeä käsitys.
- Sparrausapua ongelma- ja muissa tilanteissa.
- Kunnat tarvitsevat keskitetyn organisaation, joka auttaa teknisesti ja operatiivisesti IT-osastoja ja tietohallintoja.
- Analyysi ja tilannekuva kuntien tietoturvan tasosta, jotta oikeita kansallisia palveluita ja toimenpiteitä voidaan kohdistaa kuntaan.
- Kyberturvallisuuskeskuksen tuotokset, esimerkiksi sosiaali- ja terveydenhuollon hankintojen tietoturva- ja tietosuojavaatimukset, jotka ovat riittävän konkreettisia käytäntöön vietäviä asioita, joilla pystytään parantamaan tietoturvan tasoa.
- Pienet virastot joutuvat luottamaan vahvasti Valtorin tarjoamiin palveluihin, joten toivotaan Valtorilta selkeästi tietylle tietoturvan tasolle auditoituja ratkaisuja sekä ratkaisuvaihtoehtoja erilaisiin salaustarpeisiin. Lisäksi Valtorilta toivotaan kehitystä teknisen valvonnan perusteella havaittujen tietoturvatapausten raportointiin asiakkaan suuntaan.
- Valtioneuvoston tietoturvayksikön asiantuntemus ja ohjaus koetaan tarpeelliseksi, koska omaa osaamista ei koeta riittäväksi. Lisäksi Digi- ja viestintäviraston digiturvapalvelut, oppimateriaalit ja Vahti-työ on koettu erittäin hyödyllisiksi.
- Keskitetty SIEM-ratkaisu tai joku muu organisaation kannalta kustannustehokas ratkaisu, haavoittuvuuksien skannauspalvelu, IDS-palvelu tai muuta kustannustehokas tapa valvoa verkkoliikennettä.
- Yhteiskäyttöisiä teknisen monitoroinnin ja testauksen ympäristöjä voisi kehittää.
- Korotetun tason ympäristöt pitäisi tarjota viranomaisten toimesta.

4.4 Digitaalisen turvallisuutta parantavat muut toimenpiteet

Edellä mainittujen osa-alueiden lisäksi vastauksissa tunnistettiin myös muita digitaalista turvallisuutta parantavia toimenpiteitä, kuten:

- Riskianalyysin käyttöönotto.

- Pilvipalveluiden arviointia on yksinkertaistettava.
- Valtorin vahvempi rooli teknisessä tietoturvallisuudessa.
- Digiturvaverkoston toiminnan kehittäminen ja syvemmän yhteistyön lisääminen keskeisten toimijoiden kesken, VIRT liian yleinen.
- Kansallisen tason yhteistyön, uhkatilanteiden viestinnän ja tiedonvaihtoverkostojen kehittäminen.
- Yhteisiä menettelytapoja julkiselle hallinnolle.
- Asennemuutosta kaivataan.
- Kaksivaiheisen tunnistautumisen käytön lisääminen.
- Mobiililaitteiden hallinnan lisääminen.
- Prosessin ja palveluiden omistajuus ja niihin liittyvä tietoturvavastuut pitää olla selkeästi tiedossa koko organisaation tasolla.
- Tehokkaampi tilannetiedon jakaminen julkisten organisaatioiden kesken.
- Sote-sektorin digitaalista turvallisuutta koskeva lainsäädäntö ja auditointivaatimukset tulisi uudistaa ja palvelutuottajille tulisi asettaa selkeät vaatimukset siitä, mitä digitaalisen turvallisuuden vaatimuksia heidän tulee täyttää voidakseen tuottaa palveluita sote-toimijoille.
- Eri toimijoiden vastuiden ja velvollisuuksien selkeyttäminen.
- Kansallisen turvaluokitellun tiedon käsittelylle tulisi olla yhtenevät vaatimukset EU-turvaluokitellun tiedon käsittelyn kanssa siten, että käytetyiltä palveluilta edellytettäisiin viranomaishyväksyntää.