



DIGI- JA
VÄESTÖTIETO-
VIRASTO

Kuntien digitaalisen turvallisuuden selvitys

Digi- ja väestötietovirasto

25.3.2021



25.3.2021

Sisällysluettelo

1	Yleistä.....	2
1.1	Yhteenvedo	2
1.2	Raportin painopiste	2
1.3	Muut selvitykset	3
2	Kuvaus kuntien digitaalisen turvallisuuden nykytilasta	4
2.1	Edelläkävijät	4
2.1.1	Edelläkävijöiden onnistumisia digitaalisessa turvallisuudessa.....	4
2.1.2	Merkittävimmät kehittämiskohteet.....	5
2.2	Kaikki vastaukset	6
2.2.1	Merkittävimmät onnistumiset.....	6
2.2.2	Merkittävimmät kehittämiskohteet.....	9
2.3	Trendit ja nostot	10
3	Kuvaus kuntien digitaalisen turvallisuuden tavoitetilasta	12
3.1	Edelläkävijät	12
3.2	Kaikki vastaukset	15
3.3	Trendit ja nostot	17
	Liitteet.....	19



25.3.2021

1 Yleistä

1.1 Yhteenveto

Digi- ja väestötietovirastossa on käynnissä JUDO-hanke, joka perustuu Julkisen hallinnon digitaalisen turvallisuuden kehittämisohjelmaan sekä Valtioneuvoston periaatepäätökseen digitaalisesta turvallisuudesta ja sen toimeenpanosuunnitelmaan 2020-2023. Hanke sisältää useampia digitaalisen turvallisuuden kehittämisprojekteja.

Tämä raportti kokoaa yhteen keskeisiä havaintoja syksyllä 2020 kunnille tehdystä digitaalisen turvallisuuden kyselystä. Selvityksen tavoitteena oli hahmottaa kuntien digitaalisen turvallisuuden nykytilaa ja siihen liittyviä palvelutarpeita.

Selvityksen perusteella tehtiin seuraavat johtopäätökset:

- Kunnat tarvitsevat verkostoja ja tukea tarpeidensa tunnistamiseen. Verkostoissa on hyödyllistä jakaa hyviä käytäntöjä. Koska kunnat ovat erilaisia, tarvitaan yhteistyötä eri teemoilla. Yhteistyön keskeisenä tavoitteena tulisi olla ymmärryksen ja osaamisen parantaminen.
- Kunnille tuotettava tuki ja palvelut tulee olla selkeällä tavalla nähtävissä ja tavoitettavissa. Palvelua hankkiessaan kunnan tulee pystyä arvioimaan palvelun hyötyjä omiin tarpeisiinsa nähden.
- Palveluita tulee kehittää tiiviissä yhteistyössä palveluntuottajien kanssa, jolloin osapuolille syntyy yhteisymmärrystä kuntien tarpeista. Kunnilla on erilaisia syitä käyttää ostopalveluita. Resurssien vähyyden vuoksi on tärkeää keksiä innovatiivisia keinoja ratkaista digitaalisen turvallisuuden haasteita. Kehittämisen tulee tapahtua yksityisen ja julkisen sektorin yhteistyönä.
- Tekeminen tulee suunnata strategisesti merkittäviin kohteisiin ja kehittämisen taustalla tulee olla riittävä kokonaiskuva kuntien tilanteesta, joka tulee huomioida laajemmin julkisen hallinnon digitaalisen turvallisuuden ohjauksessa.

Selvityksen pohjalta laaditaan maaliskuun 2021 aikana digitaalisen turvallisuuden palveluiden kehittämissuunnitelma.

1.2 Raportin painopiste

Tämä raportti analysoi laajan kyselyn tuotoksia, jossa kartoitettiin kuntien digiturvallisuuden ja siihen liittyvien palveluiden nykytilaa ja tavoitetilaa. Vastaajia oli yhteensä 98. Kyselyssä selvitettiin digiturvaan liittyviä eri osa-alueita ja niiden toteutumista. Tämä raportti keskittyy kuntien nykytilan ja tarpeiden analysointiin, mutta kyselyn tuloksia käytetään myös kuntien

25.3.2021

digitaalisen turvallisuuden palveluiden kehittämiseen. Kehittämisestä laaditaan erillinen tiivis raportti kevään 2021 aikana.

Tähän raporttiin on koottu tiiviisti kyselyn tulosten kannalta kiinnostavia aiheita. Tulosten perusteella tunnistettiin edelläkävijöitä eli kuntia, joilla oli selkeitä onnistumisia yhdellä tai useammalla kyselyn osa-alueella. Onnistumisia kartoitettiin tarkemmin muutamilla teemahaastatteluilla. Tarkoituksena oli oppia parhaita käytäntöjä onnistumisien taustalla. Selvityksessä kiinnitettiin huomiota myös keskeisiin trendeihin ja ilmiöihin, jotka vaikuttavat kunnille tarjottavien palveluiden kehittämiseen.

Tässä raportissa kuvataan keskeisiä havaintoja kuntien antamista vastauksista. Selvityksen päätarkoitus oli kuntien tarpeiden tunnistaminen, mutta tulosten perusteella tunnistettiin selkeästi edelläkävijäkuntia. Tätä edelläkävijyyttä on pohdittu raportissa hieman laajemmin. Toisen mielenkiintoinen ryhmä oli "sinnikkäät" eli organisaatiot, joilla on käytössään vähän resursseja, mutta jotka silti onnistuvat selviytymään hyvin haasteista. Tätä ryhmää tullaan jatkossa tutkimaan tarkemmin.

JUDO-hanketta toteutetaan asiakaslähtöisin menetelmin, kuten palvelumuotoilun avulla. Asiakaslähtöisellä kehittämisellä varmistetaan projektin alusta asti aidot asiakasongelmat ja niiden juurisyys, jotta tulevaisuuden ratkaisut JUDO-hankkeessa kokonaisuudessaan palvelevat julkisen hallinnon digitaalisen turvallisuuden kehittämistä entistä paremmin.

1.3 Muut selvitykset

Myös muiden JUDO-hankkeen kehitysprojektien tuotoksia tullaan hyödyntämään jatkokehityksessä. Yksi näistä on projektin Julkisen hallinnon digitaalisen infrastruktuurin suojaaminen tuottama raportti, jossa esitellään julkisen hallinnon turvallisuusarkkitehtuurin kansallisen kyvykkyyden nykytila. Infrastruktuuriraporttiin tietoa on kerätty kuntakyselyn lisäksi toisella kyselyllä. Kaikkiaan vastauksia saatiin 186 organisaatiolta, jotka on jaoteltu ryhmiin kunnat, valtion virastot, sairaanhoitopiirit, yliopistot ja ammattikorkeakoulut.

Samanaikaisesti JUDO-hankkeen kanssa digitaalisen turvallisuuden kehittämistä tehdään Valtiovarainministeriön Haukka-hankkeessa. Hankkeet ovat edenneet rinnakkain ja ne täydentävät toisiaan. Molemmissa hankkeissa on tehty laajaa nykytilanteen selvitystyötä, johon ovat osallistuneet monet julkishallinnon organisaatiot asiantuntijoineen.

25.3.2021

2 Kuvaus kuntien digitaalisen turvallisuuden nykytilasta

2.1 Edelläkävijät

Edelläkävijöiksi nimettiin kunnat, joiden vastaustuloksista löytyi onnistumisia *yhellä tai useammalla osa-alueella*. Edelläkävijöillä tunnistettiin yhdistäviä tekijöitä, joita validoitiin myöhemmin syventävissä teemahaastatteluissa. Edelläkävijyyden kriteereitä ei kuvattu etukäteen, vaan ne tunnistettiin vasta kyselyn tuloksista.

Syventävissä teemahaastatteluissa edelläkävijöitä haastateltiin ensimmäisinä. Heidän kanssaan validoitiin heidän nykytilansa ja tavoitetilansa, sekä keskityttiin ymmärtämään miksi ja miten organisaatiot olivat onnistuneet tietyissä osa-alueissa. Parhaiden käytäntöjen oppiminen edelläkävijöiltä mahdollistaa niiden jalkauttamisen myös muille organisaatiolle. Seuraavaksi on kuvattu keskeisiä edelläkävijöiden onnistumisia.

2.1.1 Edelläkävijöiden onnistumisia digitaalisessa turvallisuudessa

Tässä kappaleessa on kuvattu edelläkävijöiden merkittäviä onnistumisia, joita on havaittu kyselyn ja teemahaastattelujen tuloksena.

Kaikki edelläkävijät kuvailivat itseään uudistumis- tai muutoshalukkaina, millä koettiin olevan vahva yhteys edelläkävijyyteen. Muutoshalukkuuteen sisältyi erityisesti asiakaslähtöisyys ja loppukäyttäjien tarpeiden tunnistaminen. Konkreettisina tekoina edelläkävijät kertoivat pyrkivänsä asiakaslähtöisempiin palveluihin niin omissa kehityshankkeissaan kuin palveluiden hankinnassa.

Yhdistävänä tekijä kaikilla edelläkävijöillä oli TAISTO-harjoituksiin osallistuminen (100 % osallistui harjoituksiin vuosittain). Harjoittelu ja koulutus nähtiin tärkeinä myös laajemmin, ja esimerkiksi digiturvallisuuden sisällyttäminen perehdytyksiin korostui edelläkävijöillä.

Edelläkävijöistä jokainen käytti useampaa ulkoistettua palvelua, joita toteutettiin joko kuntayhtymien ICT-toimijoiden tai kaupallisten toimijoiden toimesta. Ulkoistaminen koettiin hyödylliseksi etenkin resurssien niukkuuden vuoksi. Edelläkävijöiltä löytyi erilaisia tarpeita ja vaatimuksia palveluntuottajien valintaan. Osalle kunnista esimerkiksi alueellisuus ilmeni merkittävänä tekijänä, kun taas toisilla korostuivat palveluiden keskittäminen tai suositukset. Lähes kaikki edelläkävijät kokivat ulkoistamisen hyvänä asiana, mutta eroja oli asiakaskokemuksessa eri palveluntuottajien kanssa. Palveluntuottajien maantieteellisen sijainnin merkittävyyteen vaikutti alueellisuuden lisäksi myös palvelukieli.

25.3.2021

Kyselyssä havaittiin eroavaisuuksia ylimmän johdon tuessa ja ymmärryksessä, näin myös edelläkävijöiden keskuudessa. Joissain organisaatioissa johdon tuki on saavutettu siten, että kunnan avainhenkilöt ovat itse olleet kertomassa digiturvallisuudesta ja edistämässä aiheen kuuluvuutta ja näkyvyyttä vahvalla henkilökohtaisella panoksella. Lisäksi useiden edelläkävijäkuntien tietohallinnon edustajat olivat löytäneet muita keinoja saada digiturva ylimmän johdon näkyville, kuten esiintyminen tai ulkopuolisten puhujien hankkiminen tapahtumiin, joissa ylimmän johdon läsnäolo oli pakollista.

Erilaiset yhteistyö- sekä luottamusverkostot nousivat esiin etenkin teemahaastatteluissa. Niitä oli monenlaisia, esimerkiksi tietoturvapäällikön tai tietohallinnon edustajien henkilökohtaiset verkostot muiden organisaatioiden sekä palveluntuottajien edustajien kanssa. Lisäksi edelläkävijät hyödynsivät kuntien välistä yhteistyötä mm. hankkeiden ja projektien kautta. Joillain edelläkävijöillä alueellisuus oli yhteistyössä merkittävä tekijä, mutta toisilla merkittävämpää oli esimerkiksi yhteistyökuntien koko tai samankaltaisuus.

Myös vuoden 2020 aikana tietoturvaan ja tietosuojaan liittyvä, etenkin negatiivinen julkisuus ja media ovat nostaneet tietoturvan- ja tietosuojaan merkitystä sekä helpottaneet tietohallinnon asemaa ja kiinnostavuutta.

2.1.2 Merkittävimmät kehittämiskohteet

Teemahaastatteluissa paneuduttiin kyselyä syvällisemmin myös haasteisiin ja merkittävimpiin kehittämiskohteisiin.

Yksi merkittävä havainto oli ylimmän johdon sitoutumisen ja ymmärryksen puute tietoturvaan liittyvissä asioissa. Tämä näkyi esimerkiksi siinä, että tietohallinnon tai tietoturvan edustajat eivät kuulu johtoryhmään, ja näin ollen säännöllinen näkyvyys oikealla tasolla on rajallista. Yksi syy ja haaste tietohallinnon pääsyssä johtoryhmään oli kokemus siitä, ettei yhteistä kieltä johdon kanssa löydy. Johdolle kaivataan siis selkeämpää viestiä digitaalisesta turvallisuudesta. Viestinnän tulee sisältää tarpeeksi konkretiaa, kuten esimerkitapauksia, mikä nostaisi digiturvan asemaa. Muutamissa edelläkävijäkunnissa tietohallinnon edustusta oli saatu johtoryhmiin muutaman viimeisen vuoden aikana. He kertoivat, että johdon tietoisuus ja sitoutuminen on kasvanut huomattavasti, ja tämä on näkynyt digiturvallisuuteen liittyvissä asenteissa. Tietoisuuden ja sitoutumisen lisääntyminen on johtanut käytännössä digiturvallisuuden edistämiseen tähtäävien uusien hankkeiden käynnistämiseen sekä mahdollistanut hankkeiden menestyksekkään läpiviennin.

Toinen merkittävä kehittämiskohde liittyy resursseihin. Kaikki (100 %) edelläkävijöistä vastasivat, että heillä ei ole riittäviä resursseja ja 80 % vastasi, että heillä ei ole riittävää osaamista. Luvut ovat pysäyttäviä ja siksi teemahaastatteluissa paneuduttiin erityisesti resursseihin. Erityisesti resurssien määrään vaikutti se, että kokoaikaisesti tietoturvan parissa työskenteleviä asiantuntijoita ei ollut ollenkaan tai niitä oli vain muutamia. Tämä on johtanut tilanteeseen, jossa tietoturvaa tehdään muiden töiden ohella, jolloin myös sen jalkauttaminen,

25.3.2021

kouluttaminen ja vakinaistaminen kehitys- ja hankintaprojekteissa on epävakaata. Lisäksi monella edelläkävijäkunnalla oli merkittävä määrä eläköitymisiä. Asiantuntijoiden väheneminen on haastanut arkisten toimintojen suorittamista, sillä tilalle ei saada uusia resursseja tai rekrytointilupia. Myös ne edelläkävijäkunnat, joissa ei ollut eläköitymisiä lähiaikoina, kokivat hankaluuksia rekrytointilupien kanssa. Moni koki, että edes yksi asiantuntija lisää helpottaisi ja nostaisi digiturvallisuuden lähes tavoitetilaa. Asiantuntijalta odotettiin monialaista kokemusta; eniten esimerkiksi kuntasektorilta, tietoturva-alalta, Microsoft 365 -palveluista ja pilviympäristöstä.

Edelläkävijät olivat onnistuneet erilaisten palveluiden ulkoistamisessa. Samalla kuitenkin koettiin, että ulkoistuksissa etenkin suurten palveluntuottajien kanssa on suuri henkilöriski, kun kunnan asioita hoitava asiantuntija vaihtuu (tai vaihtuu usein), mutta tieto palveluntuottajalla ei kulje eteenpäin. Toinen palveluiden ulkoistuksiin liittyvä riski oli kunnan oman osaamisen katoaminen.

Palvelutarpeet ovat muuttuneet asiakaslähtöisemmiksi ja organisaatiot toivovat samaa myös palveluntuottajilta. Esimerkkinä nousi esiin jatkuvien palveluiden tarve kertaluontoisten palveluiden tilalle. Esimerkiksi vuosittaiset TAISTO-harjoitukset keräsivät kehuja siinä, että harjoitukset ovat parantuneet, ja samanlaista jatkumoa toivottiin mm. käynnistettyyn kuntien skannauspalveluun.

2.2 Kaikki vastaukset

Tässä osiossa analysoidaan kaikkien 98 vastaajan tuloksia. Tuloksista on nostettu esille merkittävimmät onnistumiset ja merkittävimmät kehittämiskohteet.

2.2.1 Merkittävimmät onnistumiset

Onnistumiseksi todetaan kyselyn osa-alueet, joissa enemmistö vastaajista on vastannut joko ”kyllä” tai ”jokseenkin samaa mieltä” sekä ”täysin samaa mieltä”.

74 % organisaatioista on tunnistanut oman toimintansa kannalta kriittisiä asioita. Näitä ovat mm.

- tärkeimmät tietojärjestelmät 92 %
- tärkeimmät toiminnot, palvelut ja prosessit 84 %
- tärkeimmät tietovarannot 62 %

25.3.2021

— tärkeimmät tiedot 37 %

63 % vastaajista sanoo järjestävänsä digitaalisen turvallisuuden koulutusta ja perehdytystä säännöllisesti. Haastatteluissa ilmeni erilaisia tapoja toteuttaa perehdytystä, mutta etenkin



digitaalisten kurssien ja koulutusten suorittaminen ovat vahvassa asemassa. Organisaatiot kokivat koulutukset erityisen tärkeiksi ja pitivät verkkokoulutuksia hyvinä. Eroavaisuuksia ilmeni suoritusten valvonnassa, sillä koulutusten toteutumista ei kaikkialla seurata, ja vain osalla kunnista digitaalisen turvallisuuden koulutukset ja perehdytykset ovat pakollisia.



Hieman yli puolet, 53 % vastaajista kertoi harjoittelevansa tietoturvahäiriötilanteissa toimimista vähintään kerran vuodessa. Harjoitusten merkitys heijastui myös onnistumiseen digitaalisessa turvallisuudessa, edelläkävijöistä 100 % harjoitteli vähintään kerran vuodessa. Etenkin TAISTO-harjoitukset olivat organisaatioiden mielestä hyvä tapa harjoitella.

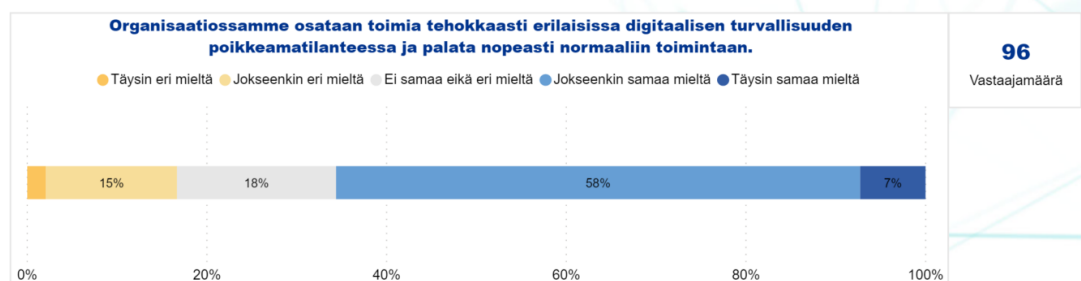
25.3.2021



Myös poikkeamatilanteiden havainnoinnissa onnistuttiin varsin hyvin; 62 % vastaajista oli jokseenkin samaa mieltä ja 5 % täysin samaa mieltä siinä, että organisaatioissa havaittiin viipymättä erilaiset tietojenkäsittelyn poikkeamat. 3 % kuitenkin vastasi olevansa täysin eri mieltä ja 22 % jokseenkin eri mieltä.



Myös reagointia koskevaan kysymykseen, eli kykyyn toimia poikkeamatilanteissa tehokkaasti ja palata nopeasti normaaliin toimintaan, 58 % vastasi olevansa jokseenkin samaa mieltä ja 7 % täysin samaa mieltä.

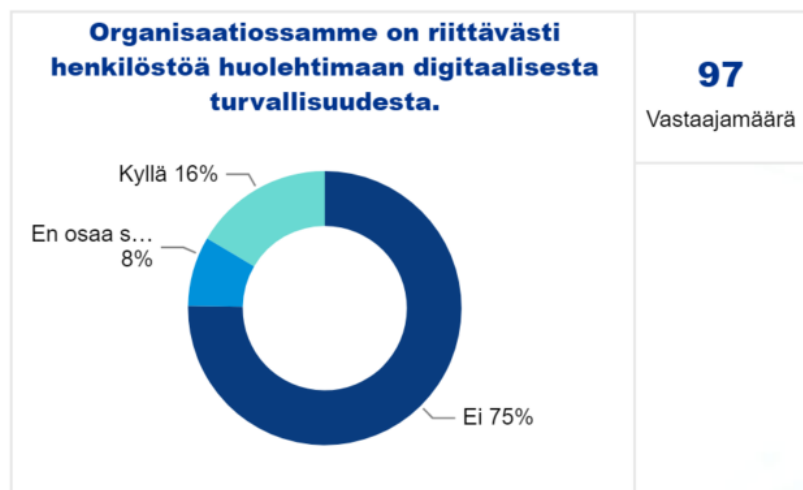


25.3.2021

2.2.2 Merkittävimmät kehittämiskohteet

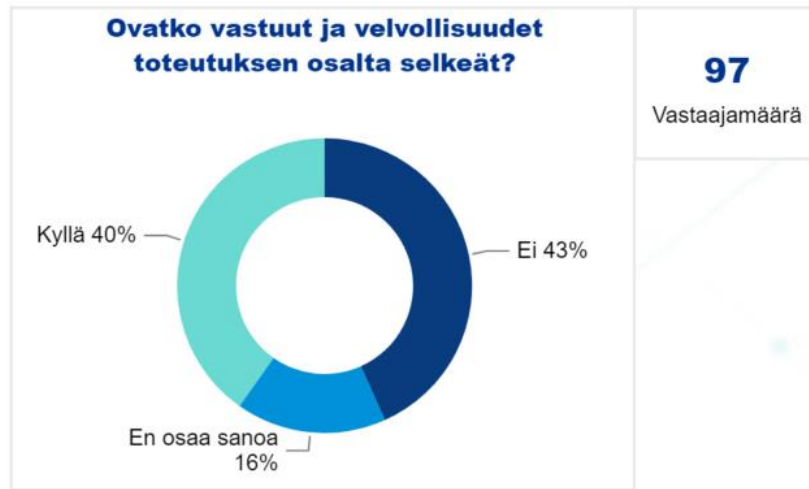
Merkittävimmiä kehittämiskohteita on nostettu osa-alueet, joissa enemmistö tai huomattava määrä vastaajista on vastannut joko "ei" tai "jokseenkin eri mieltä" sekä "täysin eri mieltä"

Kaikista vastaajista 75 % sanoi organisaatiolla olevan riittämättömät resurssit huolehtia organisaation digitaalisesta turvallisuudesta. Vain 16 % ilmoitti resurssien olevan riittävät ja 8 % ei osannut sanoa. Etenkin uusien resurssien saaminen on ollut haasteellista ja haastatte- luissa ilmeni, että vain kolmasosa esimerkiksi eläköitymisten seurauksena vapautuneista pai- koista täytetään. Yleisesti tämä nähtiin huolestuttavana asiana.

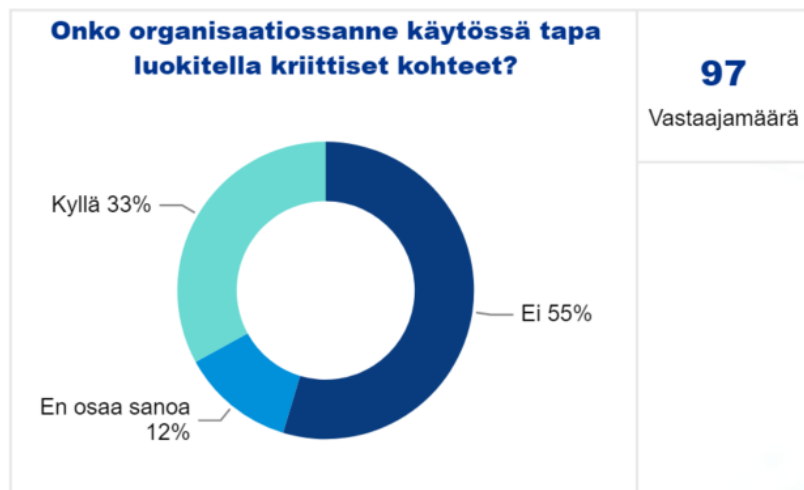


Selkeä kehittämiskohde löytyy myös vastuiden ja velvollisuuksien selkeydestä. Vastaajista 43 % koki, että vastuut ja velvollisuudet digiturvallisuuden toteutuksessa eivät ole selkeitä. 40 % koki vastuut ja velvollisuudet selkeiksi ja 16 % ei osannut sanoa, josta voidaan päätellä, etteivät vastuut ole ainakaan täysin selkeitä. Tämä johtuu osittain resurssien niukkuudesta – täysipäiväisiä digiturvallisuuden parissa työskenteleviä henkilöitä ei ole (tai ei ole riittävästi), jolloin vastuut ja velvollisuudet jäävät epäselviksi.

25.3.2021



Vaikka organisaatiot olivat hyvin tunnistaneet toiminnalle kriittisiä asioita, vain 33 % kertoi luokittelevansa kriittisiä kohteita. 55 % ei luokitellut kohteita ja 12 % ei osannut sanoa, josta voidaan päätellä, ettei luokittelu ole kovin yleinen käytäntö. Yhtenäisen luokittelukriteeristön puuttuessa voidaan olettaa, että kuntien tunnistamat kriittiset kohteet eivät kaikissa tilanteissa ole vertailukelpoisia. Kunnille tulisi tarjota soveltuva työkalu, joka mahdollistaisi yhtenäisemmän toiminnan.



2.3 Trendit ja nostot

Edelläkävijät onnistuivat eri asioissa, eri tavoin. Toisin sanoen yksi muotti ei sovi kaikille, mutta erilaisten yhdistävien tekijöiden kautta tunnistettiin kuntia, joille samankaltaiset

25.3.2021

toimintamallit sopivat. Esimerkkejä näistä ovat alueellinen sijainti; myös pienet kunnat voivat olla edelläkävijöitä hyvän verkoston tai yhteistyön avulla, vaikka resurssit olisivat vähäiset. Kaikki edelläkävijät mainitsivat kuitenkin olevansa muutoshalukkaita ja erityisesti asiakaslähettäisyys nousi esiin.

TAISTO-harjoitukset koettiin hyväksi tavaksi harjoitella ja harjoituksiin osallistumisella oli korrelaatio edelläkävijyyteen – 100 % edelläkävijöistä harjoitteli vuosittain.

Sekä kyselyn että teemahaastattelujen perusteella voitiin todeta, että useimmat kunnat painivat samojen ongelmien kanssa. Isoimmiksi kehittämiskohteiksi nousivat resurssit ja osaaminen. 100 % edelläkävijöistä vastasi, ettei heillä ole tarvittavia resursseja huolehtimaan organisaation digiturvallisuudesta. Kaikista vastaajista 89 % vastasi samoin. Resurssit oli laajempi ongelma kuin pelkkä asiantuntijoiden puute, sillä puutteita koettiin myös asiantuntijoiden osaamisessa. Etenkin kokeneita osaajia tarvitaan lisää ja 73 % vastaajista katsoi, ettei kunnalla ole riittävää osaamista.

Rekrytointi koettiin erityisen haastavaksi, etenkin kunnissa, joissa tapahtui eläköitymisiä. Uudet rekrytoinnit nähdään mahdollisuutena tuoda organisaatioon uusia ketteriä toimintatapoja, mutta kaikki haastatellut kunnat kokivat, että rekrytointilupia on vaikea saada, myös eläköityneiden tilalle.

Erilaiset yhteistyöverkostot nousivat erityisen tärkeiksi teemahaastatteluissa. Yhteistyöverkostoja on henkilökohtaisia, kunnan sisäisiä, kuntien välisiä sekä kuntien ja palveluntuottajien välisiä. Lisäksi kuntien ja viranomaisten välinen yhteistyö mainittiin haastatteluissa. Mikään yhteistyöverkoston muoto ei noussut erityisesti esiin, mutta merkittäväksi asiaksi nousi toimivien verkostojen säännöllisyys.

Merkittävä kehittämiskohde on myös kunnan ylimmän johdon ja tietohallinnon suhde. Enimmäkseen tietohallinto ei ole edustettuna kunnan johtoryhmässä, eikä digiturvallisuudella näin ollen ole säännöllistä näkyvyyttä oikealla tasolla. Haastatteluissa ilmeni, että tietohallinnon saaminen kunnan johtoryhmään voi olla jopa useamman vuoden projekti. Niissä kunnissa, joissa digiturva oli edustettuna johtoryhmissä, se koettiin merkittävänä etuna.

Teemahaastatteluissa nousi esiin myös digiturvallisuuden saama julkisuus ja mediahuomio, jotka ovat nostaneet tietoturvan asemaa ja kiinnostusta organisaatioiden johdossa. Etenkin negatiivisen julkisuuden koettiin parantavan digiturvallisuuden asemaa.

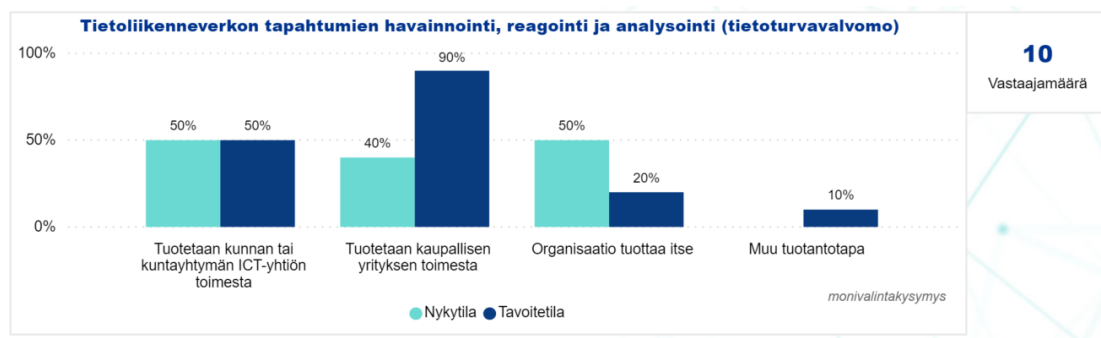
25.3.2021

3 Kuvaus kuntien digitaalisen turvallisuuden tavoitetilasta

3.1 Edelläkävijät

Edelläkävijäkunnat toimivat tavoitetilan määrittelemisessä suunnannäyttäjinä. Oletuksena on, että ne ovat ratkoneet jo useita ongelmia, joiden kanssa toiset organisaatiot vielä työskentelevät. Edelläkävijöitä haastateltiin ensimmäisenä, jotta ymmärrettäisiin syvemmin, miten ne näkevät tavoitetilan omassa organisaatiossaan ja millaista tukea ne kaipaavat sen saavuttamiseksi.

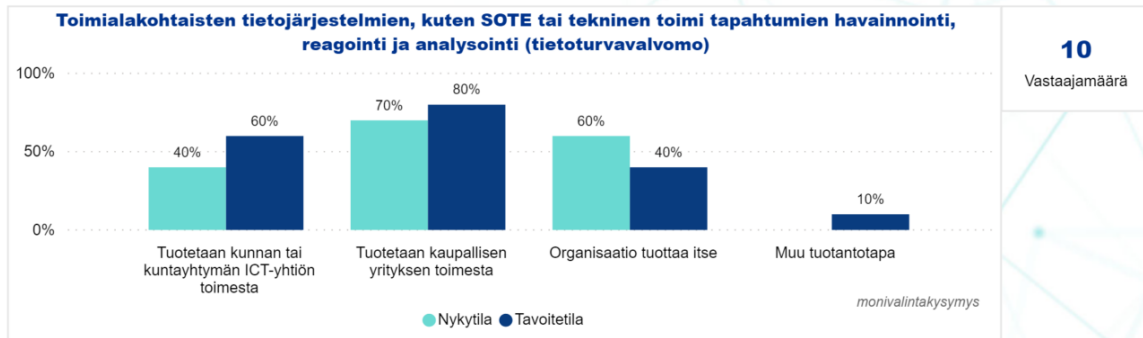
Tietoliikenneverkon tapahtumien havainnointi, reagointi ja analysointi, eli tietoturvalvomo toteutetaan nykytilassa suurelta osin yhdessä joko kuntayhtymän ICT-toimijan tai kaupallisen palvelun tuottajan kanssa. Tavoitetilassa näkyy selkeä trendi palveluiden ulkoistamiseen; 90 % edelläkävijöistä vastasi tavoitetilassa haluavansa toteuttaa tietoturvalvomon kaupallisen yrityksen toimesta. Teemahaastatteluissa organisaatiot kertoivat kuitenkin, että heillä tulee olla myös sisäistä osaamista, jotta organisaatio osaa itse toimia oikein.



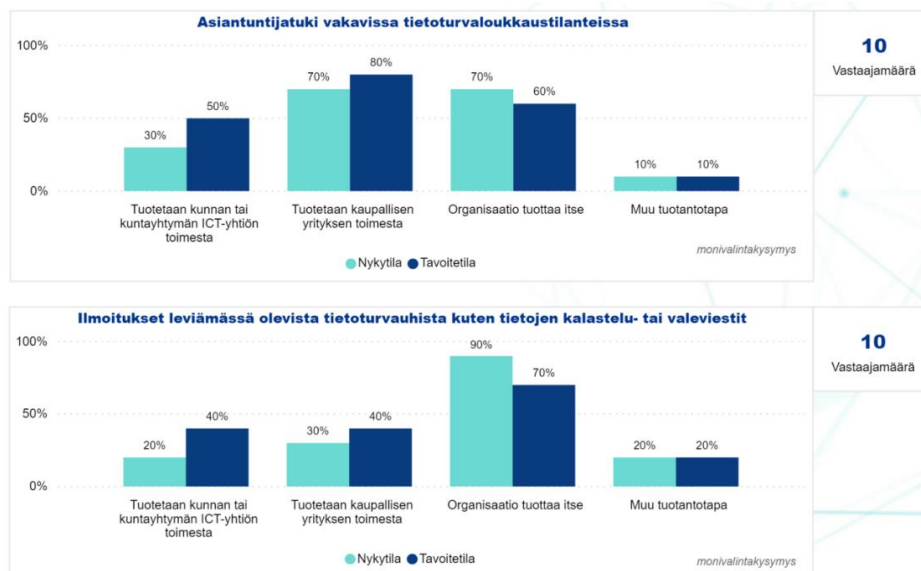
Toimialakohtaisten tietojärjestelmien tietoturvalvonta toteutetaan samankaltaisesti, nykytilassa suurelta osin yhdessä joko kuntayhtymän ICT-toimijan tai kaupallisen palvelun tuottajan kanssa. Myös tässä tavoitetilassa näkyy trendinä palveluiden ulkoistaminen, sillä 80 %

25.3.2021

edelläkävijöistä vastasi haluavansa toteuttaa toimialakohtaisen tietoturvalvomon kaupallisen yrityksen toimesta.



Vakavissa tietoturvaloukkaustilanteissa organisaatiot halusivat olla vahvasti itse mukana; 60 % vastasi haluavansa tavoitetilassa tuottaa palvelua joko yksin tai yhdessä ulkoisen palveluntuottajan kanssa. Trendi on silti jonkin verran kohti palveluiden ulkoistamista, sillä nykytilassa 70 % organisaatioista osallistuu itse asiantuntijatukeen vakavissa tietoturvaloukkaustilanteissa. Myös ilmoitukset leviämässä olevista tietoturvauhkista (kuten kalastelu- tai valeviesteistä), olivat osa-alue, jossa organisaatiot haluavat myös tavoitetilassa olla vahvasti mukana yhdessä ulkopuolisen palveluntuottajan kanssa.

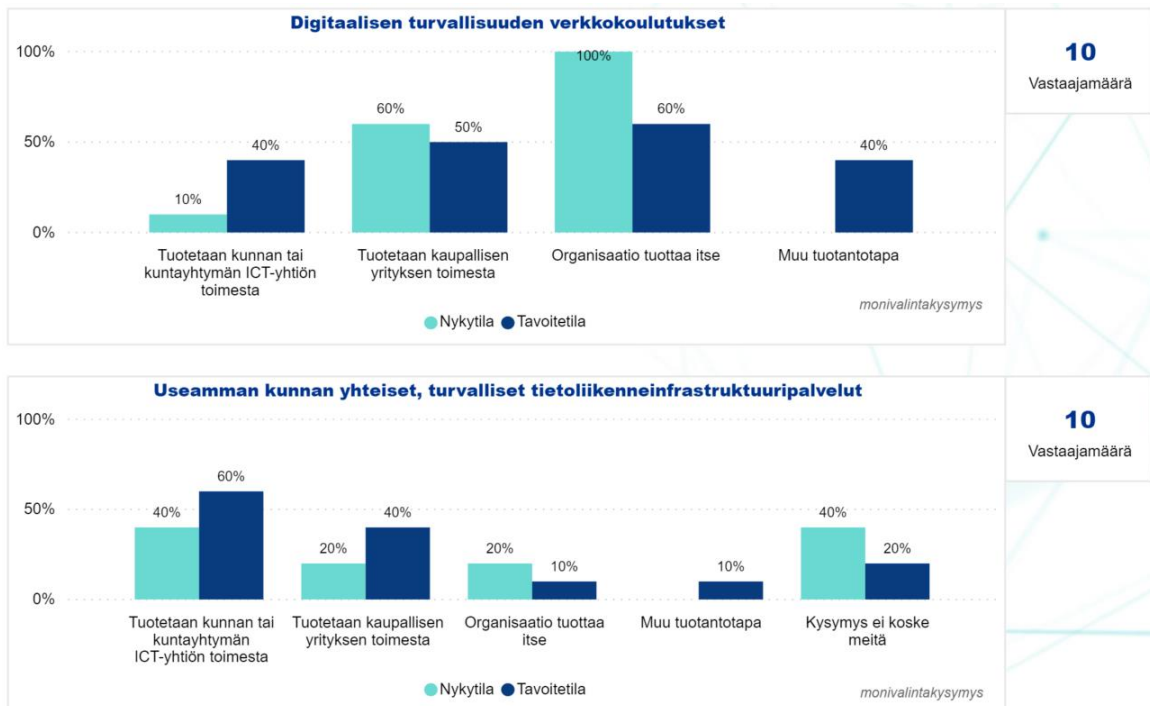


Digitaalisen turvallisuuden verkkokoulutukset erottautuvat tavoitetilassa; siinä 40 % edelläkävijöistä vastasi "Muu tuotantotapa". Tässä on huomattava ero nykytilaan, jossa 100 % edelläkävijöistä tuottaa ainakin osan digitaalisen turvallisuuden verkkokoulutuksista itse.

25.3.2021

Teemahaastatteluissa esiin nousivat TAISTO-harjoitukset. Samankaltaisia, ilmaisia verkko-koulutuksia toivottiin lisää. Syyksi toiveeseen kerrottiin harjoitusten hyvä saatavuus ja omien resurssien priorisointi muihin tehtäviin.

Useamman kunnan yhteiset, turvalliset tietoliikenneinfrastruktuuripalvelut seuraavat trendiä, jossa organisaatiot tuottavat palveluita vähemmän itse ja suosivat ulkoistamista. Edelläkävijöillä myös tietoliikenneinfrastruktuuripalveluissa kaupalliset toimijat olivat hieman kuntayhtymien ICT-toimijoita suositumpi vaihtoehto.



25.3.2021

3.2 Kaikki vastaukset

Tässä osiossa käsitellään kaikkien vastaajien tuloksia ja niistä on poimittu merkittäviä nroja, joita verrataan edelläkävijäkuntien vastauksiin.

Kaikkien vastaajien joukossa tietoliikenneverkon tapahtumien havainnointi reagoitiin ja analysoitiin, eli tietoturvalvomo, toteutetaan nykytilassa tasaisesti yhdessä joko kuntayhtymän ICT-toimijan (45 %) tai kaupallisen palveluntuottajan (44 %) kanssa. 41 % sanoi osallistuvansa tai tuottavansa palveluita myös itse. Tavoitetilassa trendi suosii palveluiden ulkoistamista, mutta ero on pieni. Tästä voidaan päätellä, että organisaatiot haluavat toteuttaa tietoturvalvomopalveluita yhdessä palveluntuottajien kanssa. Kuten edelläkävijöilläkin, myös yleisistä vastauksista voidaan päätellä, että organisaatiot haluavat ylläpitää myös sisäistä osaamista poikkeamatilanteissa toimimiseen.



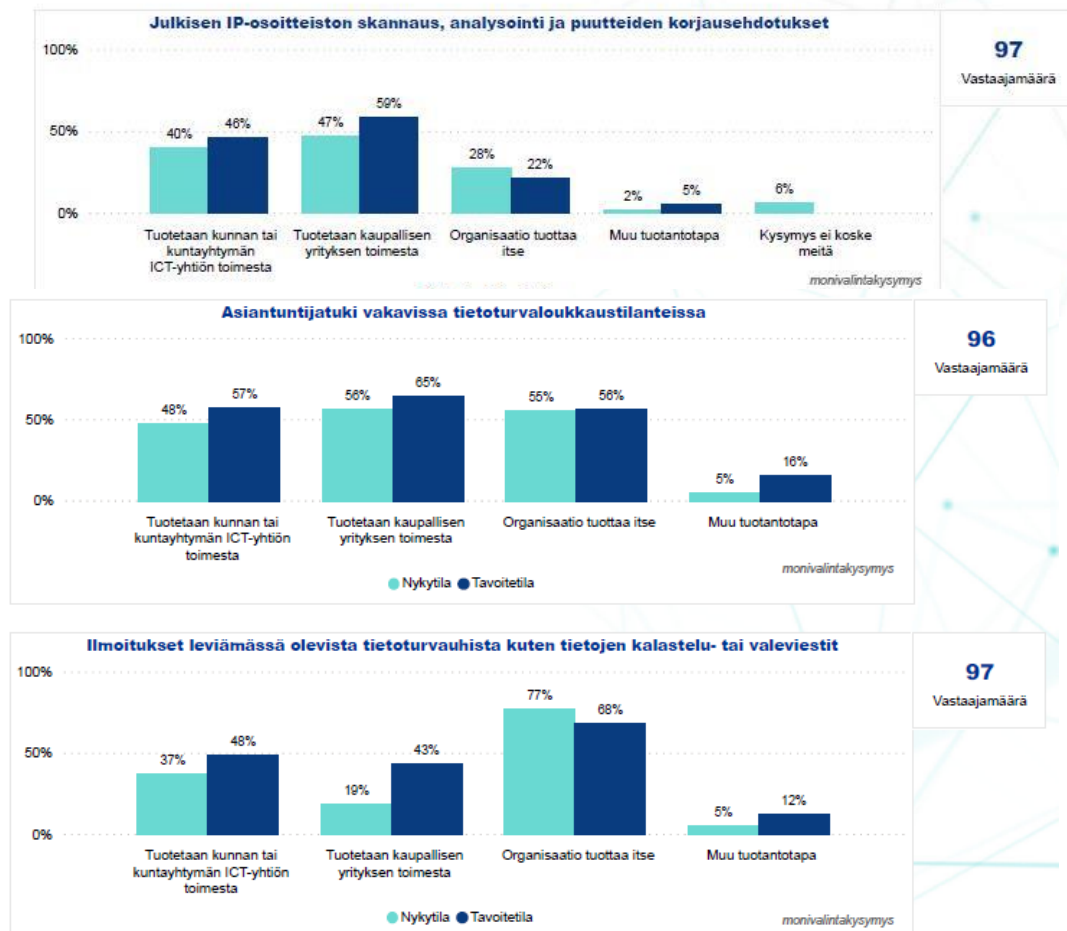
Toimialakohtaisten tietojärjestelmien tietoturvalvomo toteutetaan nykytilassa suurelta osin yhdessä joko kuntayhtymän ICT-toimijan (39 %) tai kaupallisen palvelun tuottajan kanssa (37 %). 56 % kertoi tuottavansa näitä palveluita ainakin osittain itse. Tavoitetila on mielenkiintoinen, vaikka siinäkin organisaatio tuottaa palvelua vähemmän itse. Jakauma kuntayhtymän ICT-toimijoiden (56 %) ja kaupallisten yritysten (52 %) välillä on hyvin tasainen. Mielenkiintoista on, että jakauma on hyvin tasainen, kun taas edelläkävijöistä 100 % halusi toteuttaa toimialakohtaisen tietoturvalvomon nimenomaan kaupallisen yrityksen toimesta.



25.3.2021

Syksyllä 2020 kuntien julkisia digitaalisia verkkopalveluita skannattiin DVV:n organisoimana samanaikaisesti kyselyn ja teemahaastatteluiden kanssa. Kyselyssä painottui organisaatioiden halu toteuttaa skannauspalveluita kaupallisten toimijoiden tuottamana. Etenkin tavoitetilassa toistuu trendi, jossa organisaatiot haluavat vähemmän itse toteuttaa tätä palvelua. Skannauspalvelu toimii hyvänä esimerkkinä kuntien toivomasta jatkuvasta palvelusta, jota tavoitetilassa toistetaan tasaisin väliajoin.

ICT-palveluiden järjestäminen - nykytila vs tavoitetila



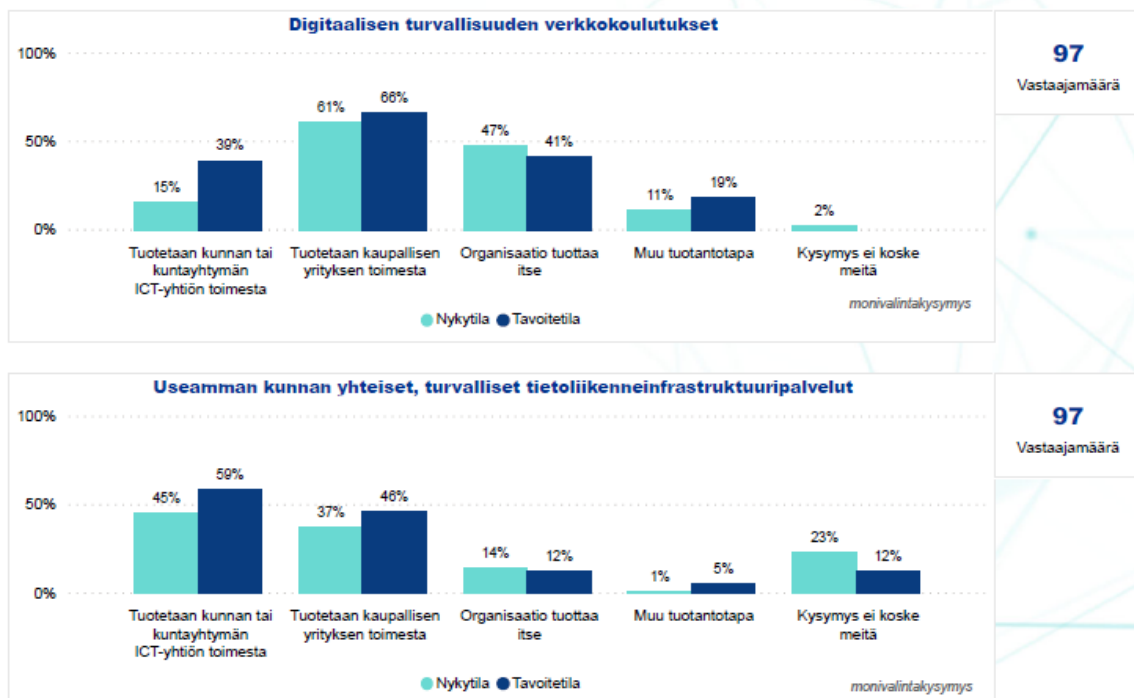
Vakavien tietoturvaloukkaustilanteiden tukitoiminnoissa organisaatiot halusivat olla vahvasti itse mukana (55 % nykytilassa). Jopa hieman enemmän, 56 %, halusi tavoitetilassa tuottaa palvelua joko yksin tai yhdessä ulkoisen palveluntuottajan kanssa. Tässä on poikkeus trendiin, jonka mukaan muutoin läpi kyselyn organisaatiot haluavat itse toteuttaa palveluita vähemmän.

Myös ilmoitukset leviämässä olevista tietoturvauhista, olivat samankaltainen poikkeus. Organisaatiot haluavat myös tavoitetilassa olla vahvasti itse mukana (68 %), joskin laskua nykytilaan (77 %) on hieman.

25.3.2021

Myös digitaalisen turvallisuuden verkkokoulutukset ovat mielenkiintoinen osa-alue. Kaikissa vastauksissa kaupalliset toimijat ovat suosituin vaihtoehto (66 %), mutta myös kuntayhtymien ICT-toimijat saivat 39 % vastauksista ja organisaation oma tuotanto 41 % vastauksista. Vain 19 % kaikista vastaajista valitsi ”Muu tuotantotapa”, kun taas edelläkävijöistä 100 % vastasi ”Muu tuotantotapa”. Tämä saattaa johtua siitä, että koska kaikki edelläkävijät osallistuivat TAISTO-harjoituksiin, he saattoivat myös jatkossa nähdä mahdollisuuden samankaltaisiin ilmaisiin verkkokoulutuksiin.

Myös useamman kunnan yhteiset, turvalliset tietoliikenneinfrastrukturipalvelut seuraavat trendiä, jossa organisaatiot tuottavat palveluita vähemmän itse ja suosivat ulkoistamista. Tässä osa-alueessa kuntayhtymien ICT-toimijat (59 %) olivat kaupallisia toimijoita (46 %) suosituimpi vaihtoehto.



3.3 Trendit ja nostot

Tavoitetilassa organisaatiot haluavat toteuttaa entistä vähemmän palveluja itse. Sen sijaan ne haluavat ulkoistaa palvelutuotantoa tai toimia yhteistyössä palveluntuottajien kanssa. Verrattuna edelläkävijöihin, jotka suosivat ulkoistuksessa hieman enemmän kaupallisia toimijoita, kaikki vastanneet organisaatiot suosivat ensisijaisesti kuntaomisteisia ICT-yhtymiä pienellä erolla. Poikkeuksina nousivat esiin ainoastaan erilaiset tukipalvelut, kuten kuntien



25.3.2021

sisäisten tietoturvaohjeiden ehkäisemisen tuki teknisellä valvonnalla. Niiden toteutuksessa kunnat haluavat olla jatkossakin vahvasti itse mukana.

Digitaalisen turvallisuuden verkkokoulutukset ja digitaalisen turvallisuuden harjoitusympäristö nousivat esiin mielenkiintoisella tavalla. Kaikki edelläkävijät osallistuivat ilmaisiin TAISTO-harjoitusten tyyppisiin verkkokoulutuksiin. Tietoturvahäiriötilanteissa toimimista vähintään kerran vuodessa harjoittelevia kuntia oli kaikista vastaajista vain 53 %, kun taas edelläkävijöissä lukema oli 100 %.

Kunnan koosta riippumatta, kaikilla organisaatioilla on nykytilassa liian vähän resursseja huolehtimaan digitaalisesta turvallisuudesta. Läpi kyselyn tämä heijastuu ulkoistamisen trendinä. Teemahaastatteluissa ilmeni kuitenkin organisaatioiden huoli siitä, että ulkoistuksien mukana sisäinen osaaminen hupenee entisestään, johon kaivataan ratkaisuja.

25.3.2021

Liitteet

Kyselytulosten tiivistelmä

Tulosten tiivistelmä

- 98+ organisaatiota
 - Erityispiirteet
- 2 toimialaa:
 - Kuntasektori
 - SOTE-kuntayhtymä/
sairaanhoitopiiri



• Edelläkävijät



• Yleiset vastaukset



• Merkittävimmät onnistumiset



• Merkittävimmät kehityskohteet



• Trendit ja nostot

Edelläkävijät

Onnistumiset



- Muutoshalukkuus
- Asiakaslähtöisyys
- Palveluiden onnistunut hankinta ja ulkoistaminen
- Digiturvallisuuden harjoittelu ja koulutus
- Yhteistyö ja luottamusverkostojen hyödyntäminen

Trendit ja nostot



- Edelläkävijät onnistuivat eri asioissa, eri tavoin
- Yksilöllä iso merkitys asioiden etenemisessä
- Säännölliset yhteistyöverkoston tapaamiset
- Digiturvallisuus julkisuudessa ja mediassa nostanut kuntien sisäisen digiturvallisuuden asemaa

Kehityskohteet



- Ylimmän johdon sitouttaminen ja ymmärryksen lisääminen digiturvaan liittyvissä asioissa
- Täysipäiväisten digiturva-asiantuntijoiden määrää kasvatettava
- Digiturvallisuuden työtehtävien vastuiden ja velvollisuuksien tunnistaminen ja organisoituminen
- Rekrytointilupien saamisen sekä rekrytoimisen hankaluus



Yleiset vastaukset



- 74 % ovat tunnistaneet oman toimintansa kannalta kriittisiä asioita
- Tahtotilana saada matalakustanteisia palveluita kunnille ja niiden asiakkaille
- 78 % organisaatioista on käytössä tietojärjestelmärekisteri tai muu tapa ylläpitää ajantasaista tietoa tietojärjestelmistä



- Valtaosa kunnista ovat halukkaita tekemään yhteistyötä samankaltaisten kuntien kanssa
- Julkishallinnon yhteisiä linjauksia ja suosituksia kaivataan
- Konkreettisia tukikeinoja kaivataan
- Palveluille kaivataan enemmän jatkuvuutta, esim skannauspalvelulle



- Resurssien vaje
- Vastuut velvollisuudet epäselkeät
- Kriittisten kohtien luokittelu heikolla tasolla
- Kunnilta puuttuu materiaaleja; suosituksia ja ohjeita, joihin kaivataan täsmäkoulutuksia
- Halu kasvattaa omien resurssien osaamista – puutteellinen aika ja varat esteenä

