



Rousku Kimmo (DVV)

Raportti - versio 1.10.

Koronaviruspandemian vaikutukset digitaaliseen turvallisuuteen



VAHTI / Rousku Kimmo (DVV)

Dokumentinhallinta

Omistaja	VAHTI-johtoryhmä
Laatinut	Kimmo Rousku
Tarkastanut	Erja Kinnunen
Hyväksynyt	VAHTI-johtoryhmä

Version hallinta

versionro	mitä tehty	pvm/henkilö
0.90	Luonnosversio	KR 9.6.2020
0.95	Päivitetty luonnosversio	EK 10.6.2020
0.99	VAHTI-joryn esittelyversio	KR 10.6.2020
1.00	VAHTI-joryn hyväksymä versio	11.6.2020 KR
1.10	Päivitetty versio – liite 1.	KR 29.11.2020 KR



VAHTI / Rousku Kimmo (DVV)

Sisällysluettelo

1	Raportin vastaajat ja toimialat	10
2	Kyselyn toteutustapa ja tulokset	10
2.1.1	Kysymys 1 - Miten arvoisitte organisaationne lakisääteisten tehtävien toiminnan sujuneen keskimäärin maaliskuun 2020 alun jälkeen?	10
2.1.2	Kysymys 2 - Kuinka hyvin siirtyminen etätöihin on onnistunut organisaatiossanne?	12
2.1.3	Kysymys 3 - Miten hyvin tietojärjestelmät ja sähköiset palvelut ovat tukeneet valmiuslain mukaista toimintaa?	13
2.1.4	Kysymys 4 - Miten hyvin olette pystyneet huolehtimaan digiturvallisuuden ERI osaluista maaliskuun 2020 alun jälkeen?	14
2.1.5	Kysymysten 1-4 keskiarvot	16
2.2	Organisaatioiden kokemat uhkat	17
2.2.1	Eri uhkien toteutuminen	17
2.2.2	Uhkiiin liittyvän riskienhallinnan toteutuminen	20
2.2.3	Toteutuneiden uhkien laajuus / uhka	22
2.2.4	Uhkien saaminen riskienhallinnan piiriin	23
2.3	Toiminnan kehittäminen muuttuneessa toimintaympäristössä	24
2.3.1	Prosessien ja turvallisuuteen liittyvien toimintamallien muuttaminen	24
2.3.2	Muutosten laajuus	26
2.4	Avoimet kysymykset	27
2.4.1	VAHTI-toiminnalta toivottu apu	27
2.5	Kommentteja, ideoita ja palautetta	29
3	Liite 1.	30
3.1	Yhteenveto	30
3.2	Uhkien toteutuminen toimialakohtaisesti	30
3.2.1	Etätyöyhteyksiin liittyvät häiriöt 81%	30
3.2.2	Tietoliikennekapasiteettiin liittyviä häiriöitä 62%	31
3.2.3	Uudenlaisia sähköpostin avulla toteutettuja huijaus- tai hyökkäysviestejä 59%	31
3.2.4	Salassa pidettävän tiedon vuotamista 8 %	31
3.2.5	Datan ja ohjelmistojen menetyksiä 1 %	32
3.3	Toiminnan kehittäminen ja sen mahdollistaminen muuttuneessa toimintaympäristössä ..	32
3.3.1	Prosessien tai palvelujen käyttöönotto	32
3.3.2	Työkalujen tai prosessien turvallisuustestaus	33
3.3.3	Turvallisuuteen liittyvät prosessit	34
3.3.4	Materiaalien käyttö etätöissä	34



VAHTI / Rousku Kimmo (DVV)

3.3.5	Henkilöstön ohjeistaminen ja kouluttaminen	35
3.3.6	Henkilötietojen käsittelyyn liittyvät prosessit.....	36



VAHTI / Rousku Kimmo (DVV)

Raportti - versio 1.10.

Yleistä

Tämän raportin on tuottanut Digi- ja väestötietovirastossa (DVV) toimiva Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä (VAHTI). Raportin sisällön tuottamiseksi VAHTI-sihteeristö järjesti koronaviruspandemiaa koskevan kyselyn, johon saatiin 136 vastausta. Tulokset on jaoteltu neljään kategoriaan vastaajien toimialan mukaan.

Tämä on raportin päivitetty versio 1.1, johon olemme täydentäneet lisätietoa toimialakohtaisista tiedoista. Kaikki uudet tiedot löytyvät uudesta liitteestä 1.

Raportin tarkoitus on muun muassa

- selvittää, miten julkisen hallinnon organisaatiot ovat onnistuneet kevään 2020 koronaviruspandemian aikana digitaalisessa toimintamuutoksessa esimerkiksi etätöiden järjestämisessä ja digitaalisten palveluiden tuottamisessa
- kuvata, millaisia toimintaan ja palveluihin kohdistuvia uhkia organisaatiot ovat tunnistaneet sekä kuinka uhkia ja niistä syntyneitä riskejä on hallittu
- tunnistaa, millaista apua ja tukea julkisen hallinnon organisaatiot toivovat VAHTI:lta

Raportti toimitetaan tiedoksi julkisen hallinnon organisaatioille sekä kaikille VAHTI-johtoryhmän ja VAHTI-asiantuntijaryhmän jäsenille. Esittelemme raporttia keskeisille sidosryhmille sekä kerromme tuloksista ja tarvittavista digiturvan kehittämistoimenpiteistä syksyn 2020 tilaisuuksissa.

Raportin kohderyhmiä ovat organisaation johto sekä digitaalisen turvallisuuden (riskienhallinta, toiminnan jatkuvuus ja varautuminen, tietoturva, kyberturvallisuus sekä tietosuojat) vastuuhenkilöt ja asiantuntijat.

DVV:n vastuulla on julkisen hallinnon digitaalisen turvallisuuden eri osa-alueiden kokonaiskuvan kerääminen. Käynnissä olevassa julkisen hallinnon digitaalisen turvallisuuden kehittämishankkeessa (JUDO) toteutetaan digitaalinen palvelu, jonka avulla voimme seuraavina vuosina toteuttaa vastaavanlaisia kyselyitä. Palvelun tarkoituksena on kerätä enemmän ajantasaista tietoa sekä tuottaa julkisen hallinnon organisaatioille raportteja omasta digiturvallisuuden tilasta ja vertailutietoa muista vastaavista organisaatioista.



VAHTI / Rousku Kimmo (DVV)

Johdon tiivistelmä

Nopeutettu digiloikka

Maaliskuussa 2020 koronaviruksen aiheuttama globaali pandemia ja siitä johtunut siirtyminen poikkeusololainsäädännön alaisuuteen Suomessa aiheutti julkisen hallinnon organisaatioille aivan uudenlaisen tilanteen. Valtaosa henkilöstöstä ohjattiin etätöihin työskentelemään pääosin kotoa käsin, mutta samanaikaisesti tuli kyetä varmistamaan viranomaisten lakisääteisten tai muuten kriittisten tehtävien ja palveluiden tuottaminen nopeasti muuttuneessa tilanteessa. Organisaatioiden tuli tuottaa kansalaisille tarkoitetut asiointipalvelut sekä fyysisessä että digitaalisessa ympäristössä ja varmistaa tarvittava palveluiden suorituskyvyn skaalautuminen.

Etukäteen arvioituna tällaisen muutoksen onnistumista pidettäisiin hyvin haasteellisenä. Kuitenkin jälkikäteen tämän ja muiden kyselyiden perusteella muutoksen voidaan arvioida toteutuneen hyvin, osin jopa erittäin hyvin. Myös muissa valtioissa on toteutettu vastaavanlainen ”digiloikka”, mutta esimerkiksi Eurofoundin¹ tutkimuksen mukaan Suomessa lähes 60 % henkilöstöstä siirtyi etätöihin, joka on enemmän kuin missään muussa vertailussa olleessa 26 valtiossa. Yksi vastaajista totesi, että heidän henkilöstöstään 92 % siirtyi etätöihin erittäin nopeasti ja onnistuneesti.

Pitkäjänteisestä digitalisoinnista hyviä tuloksia

Tämä onnistuminen ei ole pelkkää sattumaa tai hyvää onnea, vaan pitkäaikaisen, järjestelmällisen digitaalisen yhteiskunnan kehittämisen tulos. Suomessa on panostettu merkittävästi kymmeniä vuosia toiminnan digitalisointiin, sähköisiin asiointipalveluihin sekä henkilöstölle ja kansalaisille suunnattuihin palveluihin. Suomi on ollut pitkään maailman eniten mobiilidatayhteyksiä käyttävä kansakunta² ja etätöiden edellyttämät prosessit ja tarvittavat tekniset laitteet ovat olleet hyvin saatavilla. Eräs kyselystä nousut havainto oli, että joillain alueilla on ollut tilapäisiä hankaluuksia tiettyjen ICT-laitteiden saatavuuden kanssa (esimerkiksi kannettavat tietokoneet, näytöt sekä videoneuvottelupalveluissa tarvittavat kuulokemikrofonit), mutta toimivien logistiikkaketjujen takia nämä eivät ole muodostaneet suurempaa ongelmaa.

Digitaalisesta turvallisuudesta uusia skaalautuvia toimintamalleja

Koronaviruspandemia on edellyttänyt digitaalisen turvallisuuden kaikkien viiden osa-alueen (riskienhallinta, toiminnan jatkuvuus ja varautuminen, tietoturvallisuus, kyberturvallisuus ja tietosuojat) ylläpitoa ja kehittämistä. Kyselyssä oli esitetty 12 uhkaa. Vaikka niistä jokainen oli toteutunut vähintään yhdessä vastaajaorganisaatiossa, nämä uhkat ja näistä syntyneet riskit oli pystytty hallitsemaan hyvin.

Vastauksissa nousi kolme uhkaa, joita oli esiintynyt vähintään puolella vastaajista:

¹ https://www.eurofound.europa.eu/sites/default/files/ef_publication/field_ef_document/ef20058en.pdf

² <https://www.traficom.fi/sites/default/files/media/file/Telecommunications-Markets-in-the-Nordic-and-Baltic-Countries-2018.pdf>



VAHTI / Rousku Kimmo (DVV)

<i>Etätyöyhteyksiin liittyviä häiriöitä</i>	81 %
<i>Tietoliikennekapasiteettiin liittyviä häiriöitä</i>	62 %
<i>Uudenlaisia sähköpostin avulla toteutettuja huijaus- tai hyökkäysviestejä</i>	59 %

Vaikka tietoliikenteen määrä kansallisesti ja kansainvälisesti on kasvanut merkittävästi, operaattorit ovat voineet taata tarvittavan suorituskyvyn ja siirtokapasiteetin Suomessa. Osassa palveluita on esiintynyt hidastumista ja toiminnallisia katkoksia merkittävästi kasvaneiden käyttäjämäärien vuoksi, ja tämä näkyy häiriöinä etätyöyhteyksissä (81 %) ja tietoliikennekapasiteetissa (62 %). Sama ilmiö on havaittu osin käytettäessä Suomen ulkopuolella sijaitsevia palveluita. Useimmat meistä ovat huomanneet, että tietoverkkorikolliset ovat ketterästi muuttaneet huijausmenetelmiään sopimaan Covid-19- ja muihin koronaviruspandemia-aiheisiin, mikä näkyy osalla vastaajista uudenlaisina huijaus- tai hyökkäysviesteinä (59 %).

Toiminnallinen muutos on edellyttänyt lukuisia muutoksia niin ICT-palveluiden tuottamisessa kuin henkilöstön työskentelytavoissa. Koska muutokset tehtiin hyvin lyhyessä ajassa, esimerkiksi perusteelliset muutoksiin liittyvät vaikutus-, uhka- ja riskiarvioinnit eivät olleet mahdollisia. Monissa organisaatioissa osa henkilöstöstä on saattanut joutua etätöihin ensimmäistä kertaa, jolloin olemassa olevien ohjeiden ja prosessien soveltaminen ja kehittäminen sekä henkilöstön pikaohjeistus ja koulutus ovat olleet tärkeässä roolissa.

Toistaiseksi Suomessa ei ole tapahtunut laajavaikutteisia tai muuten merkittäviä tietoturmoja, tietovuotoja tai kyberhyökkäyksiä, jotka voitaisiin yhdistää tähän pandemia-aikaan. Tämä ei tarkoita sitä, etteikö organisaatioiden tule jatkaa digitaalisen turvallisuuden kehittämistä. Kahdestatoista digitaalisen turvallisuuden uhkasta kolme vähiten toteutunutta osoittavat, että palveluiden saatavuuden ja eheyden, tietojen luottamuksellisuuden ja tietosuojan osalta pitää jatkaa aktiivista kehittämistä:

Palvelunestohyökkäyksiä	10 %
Salassa pidettävän tiedon vuotamista	8 %
Datan ja ohjelmistojen menetyksiä	1 %

Mitä apua vastaajat toivovat saavansa?

Kyselyssä pyysimme vastaajia esittämään toiveita siitä, millaista apua he haluaisivat jatkossa tai miten muuten kevään 2020 poikkeuksellinen tilanne tulisi huomioida toiminnan kehittämisessä. Eniten toivottiin yhteisesti käytettävien viestintäpalveluiden turvallisuuden varmistamiseen sekä etätöyöhön liittyvää yhtenäistä ohjeistusta. Toisena asiana esille nostettiin tarve yhteensovittaa ja yhdenmukaistaa viranomaisten suorittamia kyselyitä niin sisällön kuin käytettävien palveluiden osalta. Kolmantena toiveena pyydettiin tukea siihen, miten voisimme yhdessä kehittää näitä asioita hyödyntäen eri tahoilla kerättyjä parhaita kokemuksia ja oppia myös virheistä.



VAHTI / Rousku Kimmo (DVV)

Viisi keskeistä havaintoa

Alla on viisi keskeistä havaintoa, jotka ilmenivät tuloksista. Kaksi positiivista havaintoa liittyy toimintamuutoksen onnistumiseen ja kolme digitaalisen turvallisuuden kehittämiseen. Kussakin kohdassa on lisäksi poimintoja saadusta avoimesta palautteesta.

1. Siirtyminen etätöihin ja siihen liittyvät tekniset ratkaisut on saatu toimintaan vähintään hyvin, osin jopa erittäin hyvin, ja merkittäviä poikkeamia ei ole toistaiseksi havaittu.

Digiturvallisuuden vastuuhenkilöt ja asiantuntijat näkevät kevään aikana tapahtuneen toiminnan muutoksen positiivisena, hyvin onnistuneena kokonaisuutena.

”Toiminta- ja palvelukyky on ollut lähes normaali maaliskuun alun jälkeisen ajan.”

”Etätö on ollut useassa toiminnossa jo aiemmin käytössä, vaikkakaan ei koronatilanteen mukaisessa laajuudessa. Kriittisimmät toiminnot on kuitenkin toteutettu edelleen toimipistesidonnaisesti.”

”Suurimmat haasteet tulevat siitä, että käyttöön on otettu uusia palveluita ja prosesseja ilman, että niiden turvallisuudesta on voitu varmistua samalla tavalla kuin normaalioloissa.”

”Osalla siirtyminen haasteellisempaa, johtuen työtehtävien luonteesta sekä etäyhteyksissä ilmenevistä häiriöistä.”

Digi- ja väestötietovirasto toteutti huhti-toukokuussa 2020 viisi eri digitaalisen turvallisuuden asiantuntijoille suunnattua verkkolähetystä, joissa asiantuntijoilta kysyttiin, ”Miten työskentely poikkeusoloissa on sujunut?”. 462 vastaajan näkemys tukee tämän kyselyn tulosta:

<i>Huonosti</i>	0 %
<i>Tyydyttävästi</i>	5 %
<i>Hyvin</i>	62 %
<i>Erinomaisesti</i>	33 %

2. Organisaatioiden käyttämien tai tuottamien lakisäätelien palveluiden saatavuus ja turvallisuus on pysynyt korkealla tasolla.

Vaikka useasta vastauksesta käy ilmi, että sähköisen asioinnin määrä on kasvanut jopa merkittävästi, suurempia ongelmia ei ole havaittu kansalaisille tai asiakkaille suunnatuissa palveluissa. Mahdolliset ongelmat koskevat enemmän organisaation sisäisiä, esimerkiksi etätyöskentelyyn liittyvien teknisiä ratkaisuja.

”Pandemiolla ei ole ollut vaikutusta käytettyjen tietojärjestelmien toimivuuteen. Tartuntamäärät Suomessa ovat niin pieniä, ettei tietojärjestelmien ylläpito ole häiriintynyt.”



VAHTI / Rousku Kimmo (DVV)

”Tietojärjestelmät ja muu tekninen ympäristö on ollut vakaa läpi poikkeustilan ja säilyttänyt suorituskykynsä.”

”Näiden osalta poikkeusoloihin ja etätöihin siirtyminen edellytti muutamien viikkojen ajan merkittävää lisätyötä, mutta sen ansiosta järjestelmät on saatu tukemaan toimintaa hyvin.”

3. Käyttöön otettujen uusien viestintäjärjestelmien sekä mahdollisten pilvipalveluiden turvallisuuden tarkastamisesta ja turvallisesta käytöstä puuttuvat yhtenäiset ohjeet ja linjaukset.

Vastauksista käy hyvin ilmi, että osa organisaatioista on joutunut ottamaan käyttöön uusia palveluita hyvin nopealla aikataululla. Voidaan havaita, että palveluiden käytöstä on hyvin vaihtelevia tulkintoja julkisen hallinnon eri organisaatioilla. Osa organisaatioista on saattanut kokonaan kieltää jonkun palvelun käyttämisen, jotkut mahdollistavat käytön jonkin lisäkontrollin avulla ja loput organisaatiot sallivat palvelun käyttämisen sellaisenaan.

”Riskiskenaarioiden analysointi, varautumisen kehittäminen ja ohjeistukset esim. etätyössä koordinoitusti (tietoturva, tietosuoja näkökulmat). Erilaisien viestintä- ja etäkokousvälineiden (Meet, Skype, Teams, Zoom) puolueeton tietoturva-auditointi tms. arviointi valtakunnallisesti.”

”Tarvitaan yhtenäisiä ja selkeitä toimintaohjeita esim. etätyön toteuttamiseen laajasti kunnan toiminnoissa sekä lain edellyttämien sähköisten toimintojen (esim. sähköinen allekirjoitus) toteuttamiseen etäyhteyksin. Sähköisen asiakaspalvelun luottamuksellisuuden ohjeistus (mm. opetustoimi, varhaiskasvatus), sähköisen asiakaspalvelun toteuttaminen käytännössä.”

Digi- ja väestötietovirasto toteutti huhti-toukokuussa 2020 viisi eri digitaalisen turvallisuuden asiantuntijoille suunnattua verkkolähetystä, joissa asiantuntijoilta kysyttiin, ”Mihin suuntaan digitaalinen turvallisuus on heidän mielestään kehittynyt viimeisten kuukausien aikana?”. 454 vastausta jakautuivat seuraavasti:

<i>Parantunut jonkin verran</i>	10%
<i>Pysynyt samana</i>	47%
<i>Huolestuttavaan</i>	42%
<i>Erittäin huolestuttavaan</i>	2 %

44% tähän kyselyyn osallistuneista totesi, että turvallisuus on kehittymässä huolestuttavaan suuntaan. Vastaavasti 10% vastaajista on kokenut digitaalisen turvallisuuden parantuneen, joka todennäköisesti johtuu siitä, että kyseiset organisaatiot ovat joutuneet ottamaan huomioon ja kenties parantamaan esimerkiksi tietoturvaa tai varautumista häiriötilanteisiin. Vaikka asiantuntijat ovat tunteneet huolta, kyselymme osoittaa, että toistaiseksi nämä huolet eivät ole laajamittaisesti konkretisoituneet.



4. Etätöön yhdenmukainen ohjeistaminen puuttuu

Yksi selkeä kehittämiskohde liittyy henkilöstön etätöskentelyyn ja erityisesti käsiteltävien salassa pidettävien tai henkilötietojen luottamuksellisuuden varmistamiseen. Osaa asiantuntijoista huolestuttaa, miten salassa pidettäviä tai henkilötietoja käsitellään turvallisesti etätöissä. Lisäksi huolena on se, että kun valtaosa työskentelystä tapahtuu etänä, turvallisuuden takaaminen ja valvominen on merkittävästi hankalampaa kuin toimitiloissa.

”Kansallinen ohjaus mm. etätövälineiden valinnassa. Riskien hallinnan prosessit - yhteisten toimintatapojen valinta-apua.”

”Etätöissä tietosuojariski kasvaa. Ohjeistusten noudattamisen valvominen jopa mahdotonta. Osalle esimiehistä etätöön valvominen vierasta.”

”Mielestäni tietoturvaa ja tietosuoja on heikentänyt yksikön verran se, että enempi on jäänyt työntekijän vastuulle kotioloissa asioista huolehtiminen.”

5. Yhtenäisen tilannekuvan ja sen tietojen keräämiseen liittyvien prosessien kehittäminen

Turvallisuuteen liittyväksi kehityskohteeksi nousi myös ”tilannekuvan” kerääminen sekä organisaation sisällä että viranomaisten kesken. Vastaajat ovat saaneet eri viranomaisilta lukuisia, osin päällekkäisiä kyselyitä. Toteutettujen kyselyiden ja käytettävien raportointipalveluiden tietoturvallisuuden taso tuntuu vaihtelevan. Tämän raportin mahdollistanut kysely toteutettiin Excel-tiedostona, jonka kyselyyn vastanneet luokittelivat oman ohjeistuksensa mukaisesti ja toimittivat vastauksensa pääasiassa turvapostilla.

”Tilannekuvan muodostamiseksi tarvittavia tietoja ei ollut, järjestelmiä on kehitetty nopealla aikataululla”

”Sähköinen analyysi- ja tilannekuvajärjestelmä puuttuu. Liian Word, Powerpoint, sähköposti painotteista.”

”Emme aina tiedä, millaista tietoa meille lähetettyyn kyselyyn uskaltaa vastata, koska käytetty työkalu ei kerro sen turvallisuudesta”

VAHTI-johtoryhmä on käsitellyt tätä raporttia kokouksessaan 11.6.2020, jossa tarkasteltiin keskeisiä havaintoja ja ehdotettiin niiden perusteella toteutettavaksi toimenpiteitä. Osa toimenpiteistä ohjataan kesällä 2020 perustettaville viidelle VAHTI-työryhmälle. Ryhmät raportoivat toiminnastaan johtoryhmälle säännöllisesti sekä esittelevät toimintansa tuloksia VAHTI-tilaisuuksissa. Päivitämme näitä havaintoja ja kehittämistoimenpiteitä tämän raportin versioon 2.0.



VAHTI / Rousku Kimmo (DVV)

1 Raportin vastaajat ja toimialat

Koronaviruspandemiaa koskeva kysely toimitettiin 11.5. noin 490 julkisen hallinnon organisaation kirjaamoihin, vastausaika siihen päättyi 29.5. Tiedämme, että organisaatioilta on kevään aikana pyydetty lukuisia muita raportteja ja osallistumaan lukuisiin muihin kyselyihin. Saatua 136 vastausta ja vastausprosenttia 26% voidaan pitää hyvinä käytettävissä olevaan vastausaikaan ja ajankohtaan nähden. Kokemuksemme mukaan tällainen vastausmäärä ja -prosentti antavat riittävän luotettavan pohjan kokonaiskuvan muodostamiseksi.

Vastaukset jakaantuivat toimialoittain seuraavasti:

1. Kunnat ja kuntayhtymät	60 kpl	44%
2. Sairaanhoidopiiri tai muu sote-toimija	12 kpl	9%
3. Valtionhallinto ja välillinen valtionhallinto	55 kpl	40%
4. Yliopisto tai muu oppilaitos	9 kpl	7%

2 Kyselyn toteutustapa ja tulokset

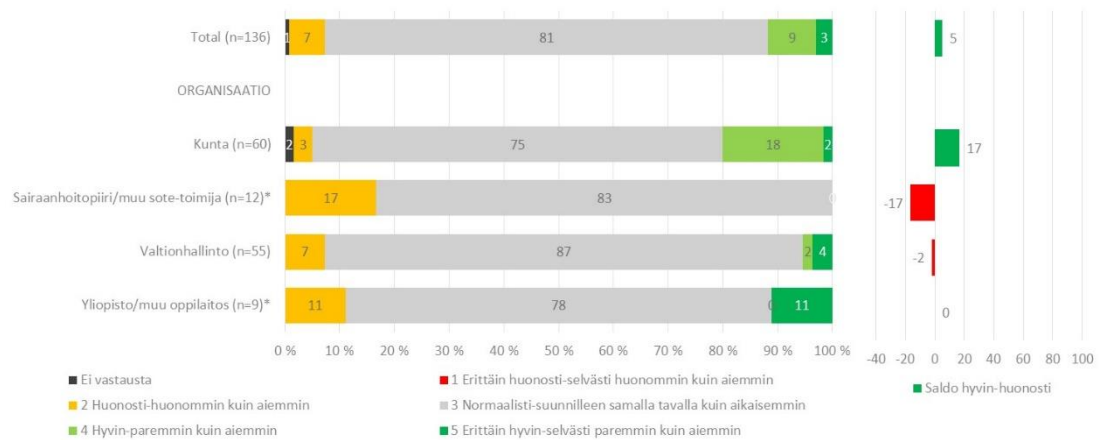
Kysely koostui viidestä monivalintakysymyksestä ja kahdesta avokysymyksestä. Niissä kysyttiin, millaista apua organisaatiot toivoisivat sekä palautetta kyselystä. Kysely haluttiin pitää tiiviinä ja nopeasti vastattavana, koska organisaatiot ovat samanaikaisesti joutuneet vastaamaan lukuisiin muihin kyselyihin. Myös kyselyyn vastanneiden henkilöiden työtilanne on kiireinen vallitsevan tilanteen takia.

2.1.1 Kysymys 1 - Miten arvioisitte organisaationne lakisääteisten tehtävien toiminnan sujuneen keskimäärin maaliskuun 2020 alun jälkeen?

Kysymyksen tarkoituksena oli selvittää, miten organisaatioiden lakisääteisten tehtävien hoitaminen on sujunut maaliskuun 2020 jälkeen. Kysymyksessä haluttiin keskittyä organisaation toiminnan kannalta kriittiseen toimintaan, koska on selvää, että osassa organisaatioista on jouduttu priorisoimaan muuta toimintaa, prosesseja ja palveluita.



VAHTI / Rousku Kimmo (DVV)



Kuva 1. Kaavio. Lakisääteisten tehtävien hoitaminen keväällä 2020.

Kokonaisuutena organisaatioiden toiminta on toteutunut pääasiassa normaalisti, suunnilleen samalla tavalla kuin aiemmin. Suurimmat erot näkyvät kahden toimialan välillä; kunnissa ja kuntayhtymissä on pystytty toimimaan merkittävästi paremmin kuin aiemmin ja vastaavasti sairaanhoitopiireissä ja muissa sote-toimijoissa hieman aiempaa huonommin. Keskiarvoisesti ollaan hieman aiempaa tasoa paremmassa tilanteessa, mutta ero ei ole merkittävä. Sairaanhoitopiirien ja sote-toimijoiden tilanteeseen vaikuttaa todennäköisesti Koronaviruspandemian aiheuttama työkuormitus sekä organisaatioiden toimintaan kohdistuvat hallinnolliset ja tekniset muutokset ja muut uhat.

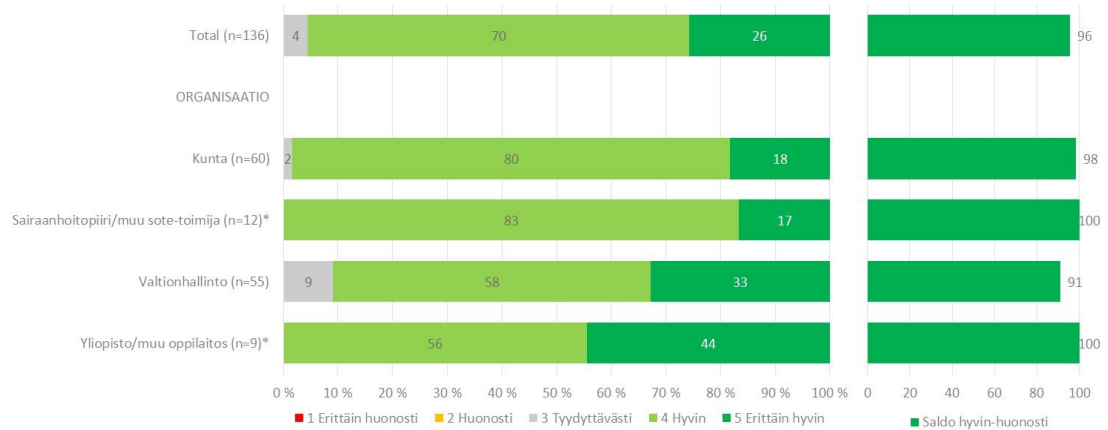
	Kaikki yhteensä	Kunta/kuntayhtymä	Sairaanhoitopiiri / muu sote-toimija	Valtionhallinto	Yliopisto/muu oppilaitos
Ei vastausta	1 %	2 %	0 %	0 %	0 %
1 Erittäin huonosti - selvästi huonommin kuin aiemmin	0 %	0 %	0 %	0 %	0 %
2 Huonosti - huonommin kuin aiemmin	7 %	3 %	17 %	7 %	11 %
3 Normaalisti - suunnilleen samalla tavalla kuin aikaisemmin	81 %	75 %	83 %	87 %	78 %
4 Hyvin - paremmiin kuin aiemmin	9 %	18 %	0 %	2 %	0 %
5 Erittäin hyvin - selvästi paremmiin kuin aiemmin	3 %	2 %	0 %	4 %	11 %
Yhteensä	100 %	100 %	100 %	100 %	100 %

Kuva 1. Tekstitalukko. Lakisääteisten tehtävien hoitaminen keväällä 2020.



2.1.2 Kysymys 2 - Kuinka hyvin siirtyminen etätöihin on onnistunut organisaatiossanne?

Kenties Koronaviruspandemian keskeisin muutos oli tarve siirtyä nopeasti ja merkittävässä määrin etätöihin. Kysymyksellä haluttiin selvittää, pitääkö yleinen positiivinen mielikuva asioiden toimivuudesta etätyöskentelyssä paikkansa.



Kuva 2. Kaavio. Etätöihin siirtyminen keväällä 2020.

Vastaukset osoittavat, että etätyöt ovat sujuneet hyvin ja osalla vastaajista erittäin hyvin. Yksikään vastaaja ei ilmoittanut, että etätöiden osalta toiminta olisi mennyt huonompaan suuntaan. Jokainen toimiala on merkittävässä määrin tyytyväinen etätöihin liittyvään toimintamuutokseen, ainoastaan valtionhallinnossa 9% vastaajista on todennut siirtymisen tapahtuneen tyydyttävästi.

	Kaikki yhteensä	Kunta/kuntayhtymä	Sairaanhoidopiiri / muu sote-toimija	Valtionhallinto	Yliopisto/muu oppilaitos
1 Erittäin huonosti	0 %	0 %	0 %	0 %	0 %
2 Huonosti	0 %	0 %	0 %	0 %	0 %
3 Tyydyttävästi	4 %	2 %	0 %	9 %	0 %
4 Hyvin	70 %	80 %	83 %	58 %	56 %
5 Erittäin hyvin	26 %	18 %	17 %	33 %	44 %
Yhteensä	100 %	100 %	100 %	100 %	100 %

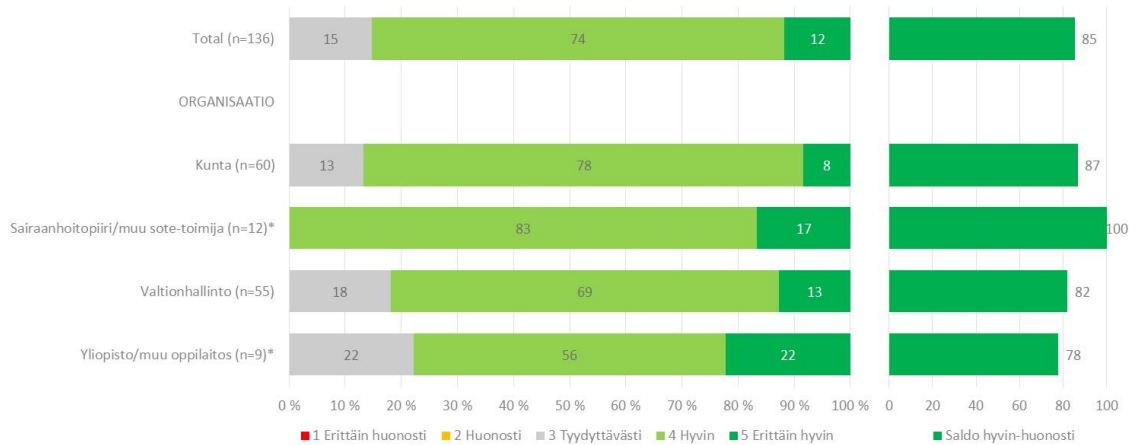
Kuva 2. Tekstitalukko. Etätöihin siirtyminen keväällä 2020.



VAHTI / Rousku Kimmo (DVV)

2.1.3 Kysymys 3 - Miten hyvin tietojärjestelmät ja sähköiset palvelut ovat tukeneet valmiuslain mukaista toimintaa?

Kolmannessa kysymyksessä haluttiin selvittää, miten ensimmäistä kertaa Suomen historiassa tapahtunut siirtyminen valmiuslain mukaiseen toimintaan on tapahtunut tietojärjestelmien ja sähköisten palveluiden osalta.



Kuva 3. Kaavio. Tietojärjestelmien ja palveluiden tuki valmiuslain mukaiselle toiminnalle.

Eräs kyselyn yllättävämpiä positiivisia yllätyksiä oli se, että vastausten perusteella Suomessa aiemmin vain erilaisissa harjoituksissa vastaan tullut valmiuslain käyttöön-otto ja sen alaisuudessa toimiminen ovat sujuneet keskimäärin hyvin, osalla jopa erittäin hyvin.

Erityisesti sairaanhoitopiirien ja muiden sote-toimijoiden tilanne on jonkin verran parempi kuin muilla toimialoilla, joiden välillä on havaittavissa vain pieniä eroja.

	Kaikki yhteensä	Kunta/kunta-yhtymä	Sairaanhoitopiiri / muu sote-toimija	Valtionhallinto	Yliopisto/muu oppilaitos
1 Erittäin huonosti	0 %	0 %	0 %	0 %	0 %
2 Huonosti	0 %	0 %	0 %	0 %	0 %
3 Tyydyttävästi	15 %	13 %	0 %	18 %	22 %
4 Hyvin	74 %	78 %	83 %	69 %	56 %
5 Erittäin hyvin	12 %	8 %	17 %	13 %	22 %
Yhteensä	100 %	100 %	100 %	100 %	100 %

Kuva 3. Tekstitalukko. Tietojärjestelmien ja palveluiden tuki valmiuslain mukaiselle toiminnalle.

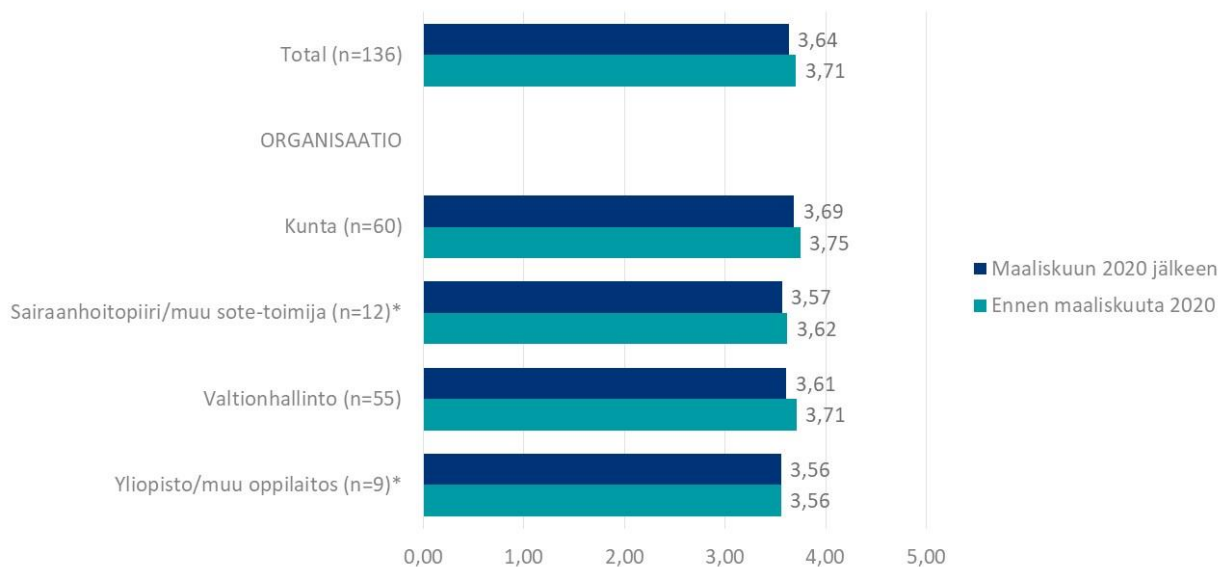


VAHTI / Rousku Kimmo (DVV)

2.1.4 Kysymys 4 - Miten hyvin olette pystyneet huolehtimaan digiturvallisuuden ERI osaluista maaliskuun 2020 alun jälkeen?

Kysymyksellä haluttiin selvittää, miten organisaatiot arvioivat digitaalisen turvallisuuden viitekehysten mukaisten viiden eri osa-alueen toiminnan kehittymistä Koronaviruspandemian aikana. Digitaalisen turvallisuuden viitekehys koostuu seuraavista osaluista:

- Riskienhallinta
- Toiminnan jatkuvuus ja varautuminen
- Tietoturvallisuus
- Kyberturvallisuus
- Tietosuoja



Kuva 4. Kaavio. Digitaalisen turvallisuuden kehittyminen kevään 2020 aikana.

Kysymykseen liitetty ennako-odotus oli, että organisaatiot kertoisivat yksittäisten digiturvan osa-alueiden, kuten tietoturvallisuuden tai tietosuojan, heikentyneen selkeästi kevään toimintamuutoksen seurauksena. Vastausten perusteella voidaan todeta, että organisaatiot arvioivat kyenneensä huolehtimaan digiturvalisuudesta lähes yhtä hyvin kuin ennen korona-aikakautta.

Ennen maaliskuuta saavutettu keskiarvo on 3,71 (kyselyn asteikolla hyvä-). Koronaviruspandemian aiheuttamaa 0,07 yksikön heikennystä voidaan pitää pienenä. Prosentuaalisesti 37% vastaajista kokee, että heidän digiturvallisuutensa on heikentynyt,



VAHTI / Rousku Kimmo (DVV)

mutta vastaavasti 16% vastaajista kokee, että tilanne on parantunut. Kokonaisuutena arviota ja olemassa olevan tason säilymistä voidaan pitää erittäin hyvänä tuloksena.

	Kaikki yhteensä	Kunta/kuntayhtymä	Sairaanhoidopiiri / muu sote-toimija	Valtionhallinto	Yliopisto/ muu oppilaitos	Keskiarvo
Miten hyvin olette pystyneet huolehtimaan digiturvallisuuden ERI osaluista maaliskuun 2020 alun jälkeen?	3,64	3,69	3,57	3,61	3,56	3,61
Ennen maaliskuuta 2020	3,71	3,75	3,62	3,71	3,56	3,67
Erotus	-0,07	-0,06	-0,05	-0,10	0,00	-0,06

Miten hyvin olette pystyneet huolehtimaan digiturvallisuuden ERI osaluista maaliskuun

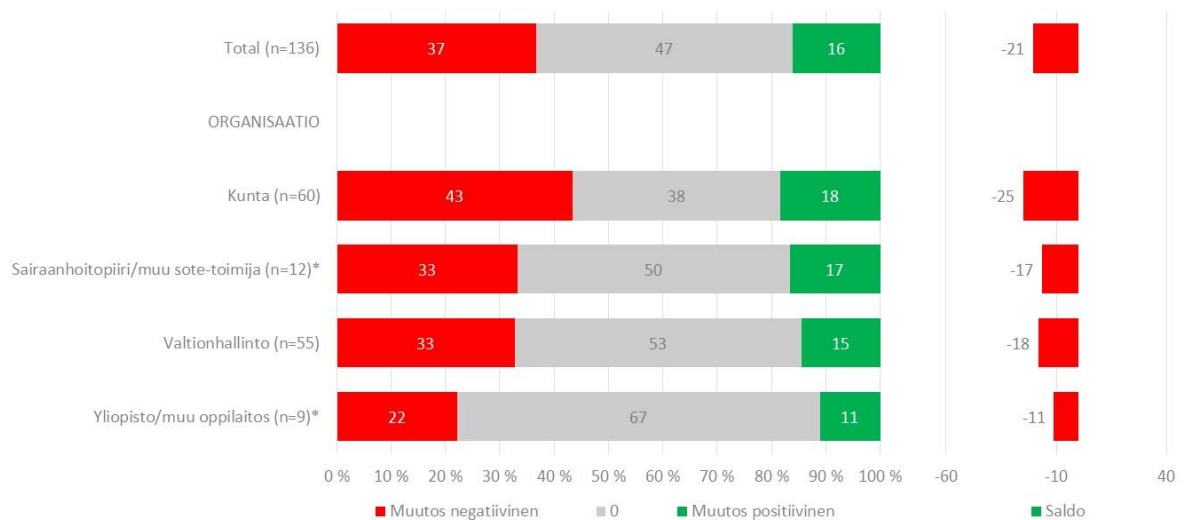
2020 alun jälkeen?

Ennen maaliskuuta 2020

Erotus

Kuva 4. Tekstitalukko. Digitaalisen turvallisuuden kehittyminen kevään 2020 aikana.

Edellisestä kaaviosta on mahdollista tuottaa toisenlainen näkymä, joka kuvaa paremmin digiturvallisuuden kehittymistä toimialoittain. Eniten tilanne on prosentuaalisesti heikentynyt, mutta toisaalta parantunut, kunnissa ja kuntayhtymissä. Tässä ryhmässä 43% vastaajista arvioi, että digiturvallisuus on heikentynyt ja 18% vastaajista se on parantunut.



Kuva 5. Kaavio. Digitaalisen turvallisuuden kehittyminen toimialoittain kevään 2020 aikana.



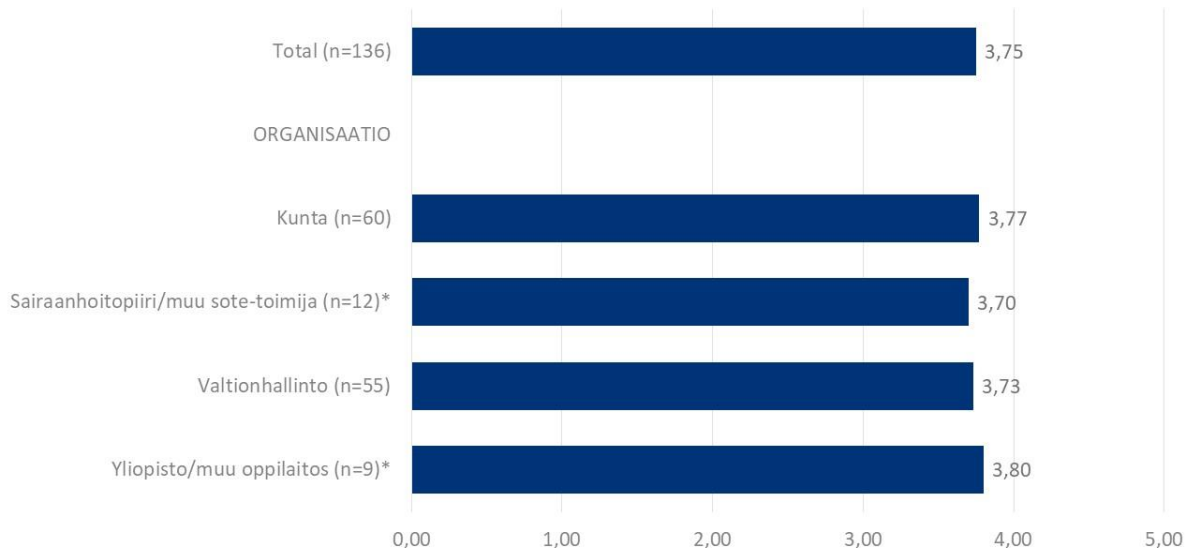
VAHTI / Rousku Kimmo (DVV)

	Kaikki yhteensä	Kunta/kuntayhtymä	Sairaanhoidopiiri / muu sote-toimija	Valtionhallinto	Yliopisto/ muu oppilaitos
Heikentynyt	37 %	43 %	33 %	33 %	22 %
Pysynyt samalla tasolla	47 %	38 %	50 %	53 %	67 %
Parantunut	16 %	18 %	17 %	15 %	11 %
Yhteensä	100 %	100 %	100 %	100 %	100 %

Kuva 5. Tekstitalukko. Digitaalisen turvallisuuden kehittyminen toimialoittain kevään 2020 aikana.

2.1.5 Kysymysten 1-4 keskiarvot

Tähän kappaleeseen olemme laskeneet neljän edellisen kysymyksen keskiarvon, jonka avulla on mahdollista arvioida toimialojen välisiä eroja – tai ennemminkin niiden puuttumista.



Kuva 5. Kaavio. Kysymysten 1-4 keskiarvo.

Kaikkien vastausten keskiarvo on 3,75 eli hieman alle hyvän. Toimialojen väliset erot ovat tässä erittäin pieniä, vain 0,05 keskiarvon molemmin puolin. Tämä osoittaa sen, että Koronaviruspandemia on näkynyt kyselyyn osallistuneille toimialoille hyvin samankaltaisena. Joissakin kysymyksissä erot ovat hiukan suurempia, kokonaisuutena ne ovat kuitenkin varsin pieniä.



VAHTI / Rousku Kimmo (DVV)

	Kaikki yhteensä	Kunta/kuntayhtymä	Sairaanhoidopiiri / muu sote-toimija	Valtionhallinto	Yliopisto/ muu oppilaitos
Edellisten kohtien 1-4 keskiarvo	3,75	3,77	3,70	3,73	3,80

Kuva 5. Tekstitalukko. Kysymysten 1-4 keskiarvo.

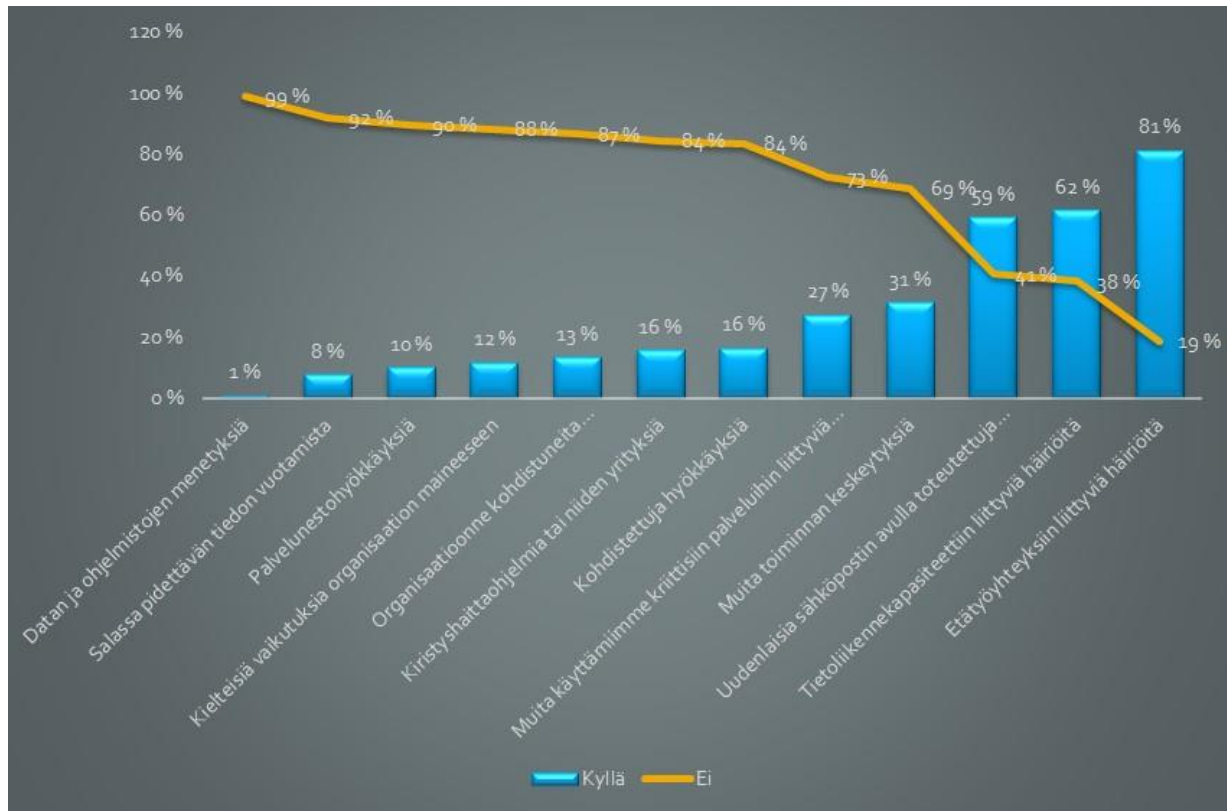
2.2 Organisaatioiden kokemat uhkat

Kyselyn toinen osio koostui uhkien tunnistamiseen ja toiminnan kehittämiseen liittyvistä kysymyksistä. Niiden tarkoituksena oli selvittää, millaisia toimintaan liittyviä uhkia kevään aikana on toteutunut ja kuinka hyvin niitä on saatu hallintaan. Samalla haluttiin selvittää, miten organisaatiot ovat kehittäneet toimintaansa ja kuinka digiturvallisuus on voitu siinä huomioida.

2.2.1 Eri uhkien toteutuminen

Organisaatioilta kysyttiin, kuinka 12 ennalta valittua uhkaa on toteutunut heidän toiminnassaan. Vastausvaihtoehtoina kullekin uhalle oli joko kyllä tai ei. Lisäksi tuli arvioida, kuinka paljon uhkia on toteutunut ja kuinka ne on saatu huomioitua riskienhallinnassa.

VAHTI / Rousku Kimmo (DVV)



Kuva 6. Kaavio. Vastajaorganisaatioiden tunnistamat uhat, sininen palkki kuvaa prosenttimäärää, kuina monella vastajaorganisaatiolla uhka on toteutunut - oranssi viiva kuvaa niiden organisaatioiden määrää, jolla uhka ei ole toteutunut.

Ylivoimaisesti eniten ongelmia ovat aiheuttaneet etäyhteyksiin liittyvät häiriöt (81 %), joista tosin voidaan todeta, että alkuvaiheen jälkeen niihin liittyvät ongelmat on saatu paremmin hallintaan.

Toiseksi eniten ongelmia ovat aiheuttaneet tietoliikennekapasiteettiin liittyvät häiriöt (62%). Tämän seurauksena on näkynyt tarve rajoittaa tai ohjeistaa henkilöstön toimintaa, esimerkiksi VPN-palvelun käytössä. Osalla vastaajista tämä uhka on toteutunut kansainvälisten pilvipalveluiden hidasteluna ja ylikuormituksena. Suomessa tietoliikenneyhteyksiä tarjoavat operaattorit ovat sen sijaan pystyneet menestyksekkäästi tarjoamaan tietoliikennekapasiteettia huomattavasta kuormituksen kasvusta huolimatta.

Kolmanneksi yleisin uhka on ollut "Uudenlaisia sähköpostin avulla toteutettuja huijaus- tai hyökkäysviestejä" (59%). Käytännössä useat rikollisjärjestöt ja verkkorikolliset vaihtoivat olemassa olevat huijausmenetelmänsä nopeasti Covid-19 tai koronaviruspandemia -aiheisiksi. Organisaatioiden käyttämät haittaohjelmaratkaisut saavat nämä yleensä suodatettua, käytännössä ne ovat suurempi ongelma vapaa-ajalla sähköpostia käyttäville henkilöille.



VAHTI / Rousku Kimmo (DVV)

Loput yhdeksän uhkaa jäivät toteumissa alle 50%. Niistä kannattaa huomata kohtalaisen korkea määrä kohdassa Kiristyshaittaohjelmia tai niiden yrityksiä (16%). Tätä lukua voi osin selittää se, että monille henkilöille tulee yksittäisiä huijauskiristyssähköpostiviestejä. Niissä usein uhkaillaan henkilöön liittyvän törkyvideon julkaisulla, mikäli henkilö ei maksa kiristäjälle. Luonnollisesti organisaatioiden tulee varoittaa ja ohjeistaa henkilöstöä toimimaan oikein näissä tilanteissa.

Positiivista oli havaita, että vähiten toteutuneita uhkia olivat palvelunestohyökkäykset (10%), salassa pidettävien tietojen vuotaminen (8%) sekä erityisesti datan ja ohjelmistojen menetykset (1%).

Uhka	Kyllä	Ei
Etätyöyhteyksiin liittyviä häiriöitä	81 %	19 %
Tietoliikennekapasiteettiin liittyviä häiriöitä	62 %	38 %
Uudenlaisia sähköpostin avulla toteutettuja huijaus- tai hyökkäysviestejä	59 %	41 %
Muita toiminnan keskeytyksiä	31 %	69 %
Muita käyttämiimme kriittisiin palveluihin liittyviä häiriöitä	27 %	73 %
Kohdistettuja hyökkäyksiä	16 %	84 %
Kiristyshaittaohjelmia tai niiden yrityksiä	16 %	84 %
Organisaatioonne kohdistuneita informaatiovaikutus- tai muita kampanjoita	13 %	87 %
Kielteisiä vaikutuksia organisaation maineeseen	12 %	88 %
Palvelunestohyökkäyksiä	10 %	90 %
Salassa pidettävän tiedon vuotamista	8 %	92 %
Datan ja ohjelmistojen menetyksiä	1 %	99 %

Kuva 6. Tekstitalukko. Vastaaajaorganisaatioiden tunnistamat uhat, eniten uhkia toteutuneet kohdat ylimpänä ja vähiten toteutuneet alimpana.



VAHTI / Rousku Kimmo (DVV)

2.2.2 Uhkiin liittyvän riskienhallinnan toteutuminen

Organisaatioilta kysyttiin, kuinka he hyvin ovat tunnistaneet ja hallinneet edellä mainittuja riskejä. Seuraavasta taulukosta näkyy, että pääosin riskienhallinta vastaa toteutuneiden riskien tunnistamista; mitä enemmän uhka on haitannut organisaation toimintaa, sitä enemmän kyseisen riskin hallintaan on kiinnitetty huomiota.

Riskien hallintaa arvioitiin seuraavalla asteikolla:

4 Uhka on tunnistettu ja siitä syntyvä riski on hallittu hyvin

3 Uhka on tunnistettu ja siihen liittyvät jäännösriskit ovat pääosin hallinnassa

2 Uhka on tunnistettu, mutta siihen liittyy selkeitä, osin tuntemattomia ja hallitsemattomia riskejä

1 Uhka on tunnistettu ja siihen liittyy merkittäviä toimintaamme uhkaavia hallitsemattomia riskejä

0 Emme ole tunnistaneet ja käsitellee tätä uhkaa lainkaan

Uhka	Riskinhallinta
Etätyöyhteysliittymiä häiriöitä	2,88
Uudenlaisia sähköpostin avulla toteutettuja huijaus- tai hyökkäysviestejä	2,59
Tietoliikennekapasiteettiin liittyviä häiriöitä	2,45
Muita toiminnan keskeytyksiä	1,87
Muita käyttämiimme kriittisiin palveluihin liittyviä häiriöitä	1,95
Kohdistettuja hyökkäyksiä	1,70
Kirstyshaaittaohjelmia tai niiden yrityksiä	1,84
Organisaatioonne kohdistuneita informaatiovaikutus- tai muita kielteisiä kampanjoita	1,76
Kielteisiä vaikutuksia organisaation maineeseen	1,73
Palvelunestohyökkäyksiä	1,78
Salassa pidettävän tiedon vuotamista	1,76
Datan ja ohjelmistojen menetyksiä	1,76

Kuva 7. Tekstitalukko. Vastajat ovat tunnistaneet ja saaneet hallintaan eri uhkia

Taulukosta näkyy, että esimerkiksi kohdat "Muita toiminnan keskeytyksiä", "Kohdistettuja hyökkäyksiä", "Kielteisiä vaikutuksia organisaation maineeseen" ja "Palvelunestohyökkäyksiä" eivät ole ihan samassa järjestyksessä, kuin niitä on organisaatioihin kohdistunut, mutta erot eivät ole merkittäviä. Tärkeintä on, että kolme ylivoimaisesti eniten toimintaa haitannutta riskiä on tunnistettu ja niiden hallintaan on kiinnitetty huomiota.



VAHTI / Rousku Kimmo (DVV)

Huomaa!

*Osalla organisaatioista on vastattu yksittäisiin uhkiin valitsemalla vaihtoehto **1 Uhka on tunnistettu ja siihen liittyy merkittäviä toimintaamme uhkaavia hallitsemattomia riskejä.***

Jokaisen vastanneen organisaation tulisi läpikäydä vastauksensa ja uudelleenarvioida, millaisia hallintatoimenpiteitä tällaiselle riskille tulisi tehdä. Tässä tulee käyttää apuna edellä olevaa taulukkoa, mitä enemmän tällainen uhka on esiintynyt muilla organisaatioilla, sitä tärkeämpää on saada tällainen toimintaa uhkaava hallitsematon riski hallintaan.

Julkaisemme elokuussa 2020 tästä raportista päivitetyn version, jossa käsittelemme eri osa-alueita yksityiskohtaisemmin. Edellä olevaa taulukkoa voidaan tulkita myös siten, että vaikka organisaatio ei ole nyt tunnistanut listalla oleviin uhkiin liittyviä riskejä, heidän tulisi ehkä jatkossa ottaa ne paremmin hallintaan.

Kaikkien tunnistettujen eli vastattujen riskien osalta riskien hallintaa koskeva keskiarvo on 3,23, jota voidaan pitää yllättävän korkeana. Tulee kuitenkin huomata, että osa vastaajista oli tunnistanut vain yhden tai kaksi heihin kohdistunutta uhkaa. Jos ne olivat hyvin hallinnassa, niin vastaus oli 4 eli uhka ja siitä syntyvä riski olivat hyvin hallinnassa.

Vastanneet organisaatiot voivat tarkistaa omista vastaustaulukoistaan Yhteenveto-vastauksista -välilehdeltä kohdan ”Kuinka paljon olette eri uhkia kokeneet - minimi on 0 ja maksimi on 12 (mitä suurempi, sitä huolestuttavampi tilanteenne on)”. Alla olevasta taulukosta näkyy kuinka monta uhkaa eri organisaatiot ovat keskimäärin tunnistaneet heihin kohdistuneen.

	Kaikki	Kunta/kuntayhtymät	Sairaanhoidopiiri/ muu sote-toimija	Valtionhallinto	Yliopisto/ muu oppilaitos
Toteutuneiden uhkien määrä: Kuinka paljon olette eri uhkia kokeneet - minimi on 0 ja maksimi on 12	3,39	3,13	3,00	3,67	3,89

Kuva 8. Tekstitalukko. Kuinka paljon eri uhkia organisaatiot ovat kappalemääräisesti toimialoitain keskimäärin tunnistaneet.

Eniten toteutuneita uhkia ovat tunnistaneet yliopistot ja muut oppilaitokset (3,89 kpl / organisaatio) ja vastaavasti vähiten sairaanhoidopiirit ja muut sote-toimijat (3 kpl / organisaatio) keskiarvon ollessa 3,39.



VAHTI / Rousku Kimmo (DVV)

2.2.3 Toteutuneiden uhkien laajuus / uhka

Vastanneet organisaatiot voivat tarkistaa omista vastaustaulukoistaan Yhteenvetovastauksista -välilehdeltä kohdan ”Toteutuneiden uhkien laajuus: Kuinka paljon eri uhkia on määrällisesti teihin kohdistunut”. Alla olevasta taulukosta näkyy, kuinka paljon eri uhkia on toteutunut eri toimialoilla.

Organisaatiot valitsivat kunkin toteutuneen uhan osalta niiden määrän, josta he saivat pisteitä seuraavasti:

Ei lainkaan	0 pistettä
Yksittäisiä / vähän	1 piste
Jonkin verran	2 pistettä
Merkittävässä määrin	3 pistettä
Paljon	4 pistettä

Näistä on laskettu vertailuluku, joka on sitä suurempi mitä enemmän organisaatiossa on uhkia toteutunut.

	Kaikki	Kunta/kuntayhtymät	Sairaanhoidopiiri/ muu sote-toimija	Valtionhallinto	Yliopisto/ muu oppilaitos
Toteutuneiden uhkien laajuus: Kuinka paljon eri uhkia on määrällisesti teihin kohdistunut - minimi on 0 ja maksimi on 48	5,02	4,40	4,50	5,78	5,22

Kuva 9. Tekstitalukko. Kuinka paljon eri uhkia organisaatioissa on määrällisesti toteutunut.

Vertailuluvun keskiarvo on 5,02. Määrällisesti eniten tunnistettuja uhkia on toteutunut valtionhallinnossa, vastaavasti vähiten kunnissa ja kuntayhtymissä.

Tässä yhteydessä kannattaa erikseen mainita, että valtaosa toteutuneiden uhkien määrään liittyvistä vastauksista oli joko yksittäisiä/vähän tai jonkin verran. Ainoastaan muutama organisaatio oli yksittäisen uhan kohdalla havainnut niitä merkittävässä määrin ja vaihtoehto paljon oli valittu vain yhdessä vastauksessa.

Tätä havainnollistaa myös se, että kun kohdan keskiarvo 5,02 jaetaan toteutuneiden uhkien keskimäärällä 3,39, saadaan arvoksi 1,48 – tämä arvo sijoittuu välille yksittäisiä/vähän ja jonkin verran.

Määrällisesti eniten ongelmia oli myös eniten toteutuneissa uhkissa eli:

- Etätyöyhteyksiin liittyviä häiriöitä
- Uudenlaisia sähköpostin avulla toteutettuja huijaus- tai hyökkäysviestejä



VAHTI / Rousku Kimmo (DVV)

- Tietoliikennekapasiteettiin liittyviä häiriöitä

2.2.4 Uhkien saaminen riskienhallinnan piiriin

Vastanneet organisaatiot voivat tarkistaa omista vastaustaulukoistaan Yhteenveto-vastauksista -välilehdeltä kohdan ”Miten riskienhallintanne on saanut nämä uhat hallintaa?”. Tässä kappaleessa on kuvattu, miten hyvin organisaatiot ovat keskimäärin saaneet uhat hallintaan.

Organisaatioiden arviot kunkin 12 uhkan riskienhallinnan tasosta on pisteytetty seuraavasti:

4 Uhka on tunnistettu ja siitä syntyvä riski on hallittu hyvin	0 pistettä
3 Uhka on tunnistettu ja siihen liittyvät jäännösriskit ovat pääosin hallinnassa	1 piste
2 Uhka on tunnistettu, mutta siihen liittyy selkeitä, osin tuntemattomia ja hallitsemattomia riskejä	2 pistettä
1 Uhka on tunnistettu ja siihen liittyy merkittäviä toimintaamme uhkaavia hallitsemattomia riskejä	3 pistettä
0 Emme ole tunnistaneeet ja käsitelleet tätä uhkaa lainkaan	

Vertailuluvun minimi on 0 pistettä ja maksimi 36 pistettä, mitä pienempi pistemäärä on, sitä paremmin uhat on saatu hallintaan.



VAHTI / Rousku Kimmo (DVV)

	Kaikki	Kunta/kuntayhtymät	Sairaanhoidopiiri/ muu sote-toimija	Valtionhallinto	Yliopisto/ muu oppilaitos
Uhkien tunnistaminen ja hallinta: Miten riskienhallintanne on saanut nämä uhat hallintaan?	6,67	6,50	7,17	5,80	12,44

Kuva 10. Tekstitalukko. Miten riskienhallinnassa on saanut uhat hallintaan?

Vastauksen keskiarvo on 6,67. Pienimmän pistemäärän saa valtionhallinto (5,80), ainoastaan yliopistot ja muut oppilaitokset poikkeavat merkittävästi keskiarvosta. Vastauksia arvioitaessa tulee huomata, että arvoon vaikuttaa myös se, kaikki vastaajat eivät ole tunnistaneet ja käsitelleet kaikkia uhkia ja tässä on merkittäviä eroja eri vastaajien kesken.

2.3 Toiminnan kehittäminen muuttuneessa toimintaympäristössä

Kyselyn viimeiset kaksi kysymystä koskivat sitä, miten organisaatio on mahdollisesti muuttanut digitaalisen turvallisuuden toimintaperiaatteitaan muuttuneessa toimintaympäristössä.

2.3.1 Prosessien ja turvallisuuteen liittyvien toimintamallien muuttaminen

Vastanneet organisaatiot voivat tarkistaa omista vastaustaulukoistaan Yhteenvetovastauksista -välilehdeltä kohdan ” Kuinka paljon olette joutuneet muuttamaan olemassa olevia prosessejanne ja turvallisuuteen liittyviä toimintamalleja?”.

Tässä kohdassa kysyttiin seuraavia kysymyksiä:

Toiminnan kehittäminen ja sen mahdollistaminen muuttuneessa toimintaympäristössä

- a) Olemme ottaneet käyttöön uusia prosesseja tai palveluita ilman riittävää riskienhallintaa VAI
- b) Riskienhallinnasta ei ole tingitty, vaikka olemme ottaneet käyttöön uusia prosesseja tai palveluita VAI
- c) sekä että

- a) Olemme ottaneet käyttöön uusia työkaluja tai palveluita ilman riittävää turvallisuustestausta VAI
- b) Olemme ottaneet käyttöön uusia työkaluja tai palveluita riittävän turvallisuustestauksen jälkeen VAI
- c) sekä että

- a) Olemme heikentäneet turvallisuuteen liittyviä prosesseja palveluiden saatavuuden mahdollistamiseksi VAI



VAHTI / Rousku Kimmo (DVV)

- b) Emme ole heikentäneet turvallisuuteen liittyviä prosesseja palveluiden saatavuuden mahdollistamiseksi VAI
c) sekä että
- a) Henkilöstö on voinut käsitellä etätyössä sellaisia materiaaleja, joita ei aiemmin ole sallittu käsitellä VAI
b) Henkilöstö ei ole voinut käsitellä etätyössä sellaisia materiaaleja, joita ei ole aiemminkaan sallittu käsitellä VAI
c) sekä että
- a) Henkilöstön ohjeistaminen ja kouluttaminen muuttuneeseen tilanteeseen on ollut puutteellista VAI
b) Henkilöstön ohjeistaminen ja kouluttaminen muuttuneeseen tilanteeseen on ollut riittävää VAI
c) sekä että
- a) Olemme joutuneet heikentämään henkilötietojen käsittelyyn liittyviä prosesseja VAI
b) Emme ole joutuneet heikentämään henkilötietojen käsittelyyn liittyviä prosesseja VAI
c) sekä että

Ensimmäisestä vastausvaihtoehdosta on annettu 4 pistettä, toisesta vaihtoehdosta 0 pistettä ja kolmannelta 2 pistettä. Kokonaispistemäärän minimi on 0 (turvallisuudesta ei ole tingitty lainkaan) ja maksimi on 24 (prosesseja on jouduttu muuttamaan merkittävässä määrin).

Vastauksissa korkein yksittäisen organisaation pistemäärä oli 16 pistettä, mutta 10 tai enemmän pisteitä sai noin 20 vastaajaa. Pienin pistemäärä oli 2, jonka sai kaksi vastaajaa.

	Kaikki	Kunta/kuntayhtymät	Sairaanhoitopiiri/ muu sote-toimija	Valtionhallinto	Yliopisto/ muu oppilaitos
--	--------	--------------------	-------------------------------------	-----------------	---------------------------

Kuinka paljon olette joutuneet muuttamaan olemassa olevia prosessejanne ja turvallisuuteen liittyviä toimintamalleja?

5,07 4,88 4,33 5,33 5,78

Kuva 11. Tekstitalukko. Kuinka paljon olette joutuneet muuttamaan olemassa olevia prosessejanne ja turvallisuuteen liittyviä toimintamalleja.

Kaikkien vastaajien keskiarvo on 5,07. Pienin keskiarvo on sairaanhoitopiireillä ja muilla sote-toimijoilla (4,33), ja vastaavasti korkein yliopistoilla ja muilla oppilaitoksilla (5,78). Mitä enemmän organisaatio on joutunut tekemään kompromisseja tai heikennyksiä olemassa oleviin digiturvallisuuden toimintamalleihin tai prosesseihin, sitä



VAHTI / Rousku Kimmo (DVV)

huolellisemmin sen tulee varmistaa toimintansa ja tietojensa turvallisuus sekä tietosuojan toteutuminen palattaessa takaisin normaalitilanteeseen.

2.3.2 Muutosten laajuus

Vastanneet organisaatiot voivat tarkistaa omista vastaustaulukoistaan Yhteenvetovastauksista -välilehdeltä kohdan ”Kuinka paljon olette joutuneet muuttamaan olemassa olevia prosessejanne ja turvallisuuteen liittyviä toimintamalleja?”. Tässä kappaleessa on vertailtu, miten laajasti organisaatio on näitä muutoksia joutunut toiminnassaan suorittamaan.

Vastaukset on annettu seuraavalla asteikolla:

- Ei lainkaan
- Yksittäisiä / vähän
- Jonkin verran
- Merkittävässä määrin
- Paljon

Taulukossa on laskettu vertailuluku, joka perustuu edellisessä kohdassa valittuun vaihtoehtoon sekä muutoksen laajuuteen. Esimerkiksi jos organisaatio on ottanut käyttöön ”Käyttöön uusia prosesseja tai palveluita ilman riittävää riskienhallintaa” ja näitä on tapahtunut ”Paljon”, siitä saa 16 pistettä. Vastaavasti jos organisaatio on valinnut ”Emme ole heikentäneet turvallisuuteen liittyviä prosesseja palveluiden saatavuuden mahdollistamiseksi”, siitä saa 0 pistettä.

Tämän vertailuluvun minimi on 0 (turvallisuutta ei ole lainkaan tai äärimmäisen vähän jouduttu heikentämään) ja maksimi on 96 (turvallisuuden heikennyksiä on jouduttu toteuttamaan myös määrällisesti paljon).

	Kaikki	Kunta/kuntayhtymät	Sairaanhoidopiiri/ muu sote-toimija	Valtionhallinto	Yliopisto/ muu oppilaitos
--	--------	--------------------	-------------------------------------	-----------------	---------------------------

Missä laajuudessa olette näitä muutoksia joutuneet toteuttamaan?

4,44

3,93

4,50

4,75

5,89

Kuva 12. Tekstitalukko. Missä laajuudessa organisaatio on näitä muutoksia joutunut toteuttamaan.

Vaikka asteikko on tässä kysymyksessä muita laajempi, keskiarvo pysyy maltillisella tasolla (4,44). Tässä kohdassa kunnat ja kuntayhtymät saavat pienimmän vertailuluvun ja yliopistot ja muut oppilaitokset vastaavasti suurimman (5,89). Toimialojen välistä eroja voidaan pitää pieninä.



VAHTI / Rousku Kimmo (DVV)

Kaikkiaan noin 15 organisaatiota saa tässä korkeamman arvon kuin 10 ja kaksi organisaatiota yli 30.

Myös tämän kysymyksen avulla organisaatioita on herätelty arvioimaan sitä, millaisia digiturvallisuuteen liittyviä muutoksia ne ovat tehneet ja millaisia vaikutuksia sillä voi olla organisaation turvallisuuteen. Muutokset tulisi olla kirjattuna ylös ja niihin liittyvät riskit arvioituna, jotta normaalioloihin palattaessa voidaan varmistua toiminnan turvallisuuden ja luotettavuuden palauttamisesta vähintään koronaviruspandemiaa edeltävälle tasolle.

2.4 Avoimet kysymykset

2.4.1 VAHTI-toiminnalta toivottu apu

Kyselyn lopussa oli kaksi avokysymystä, joista ensimmäinen oli kysymys ”Millaista apua toivoisitte VAHTI-toiminnalta tai muilta viranomaisilta tässä tilanteessa tai palautumisen mahdollistamiseksi sekä turvallisuuden ja luottamuksen varmistamiseksi?”

Tähän saatiin 49 vastausta, joiden muutamaiset keskeiset toiveet nousevat tiivistetysti esille alla olevasta sanapilvestä.

Varsinaista apua organisaatiot eivät Koronaviruspandemian hoitamiseen juurikaan odota, koska tilanne koetaan olevan hallinnassa, mutta tiivistyksenä esille nousevat seuraavat ehdotukset:

- etätöön työkalujen ja mobiiliratkaisuiden, pilven tietoturvallisuuden arviointia (yleensä käytettävien palveluiden puolueetonta turvallisuuden arviointia)
- edelleen lisää ohjeistusta ja koulutusta digiturvan eri osa-alueisiin
- tilannekuvanraportointia
- tietoliikennekapasiteetin riittävyyden varmistaminen
- verkostomaista työskentelyä yhteistyön ja parhaiden kokemusten jakamiseksi
- harjoittelua ja harjoituksia vastaavia tilanteita varten
- pilvipalveluiden käytön ohjeistaminen ja linjaaminen
- yhteinen riskiraportointi ja skenaariot
- kriisiytön aikana rauhoitustila päälle – kaiken turhan karsiminen
- organisaation johdon osaamisen ja tietoisuuden kehittämistä
- tukea kriittisten palveluiden ja prosessien tunnistamiseen
- VAHTI voisi kerätä kaikki koronaviruksen opit yhteen

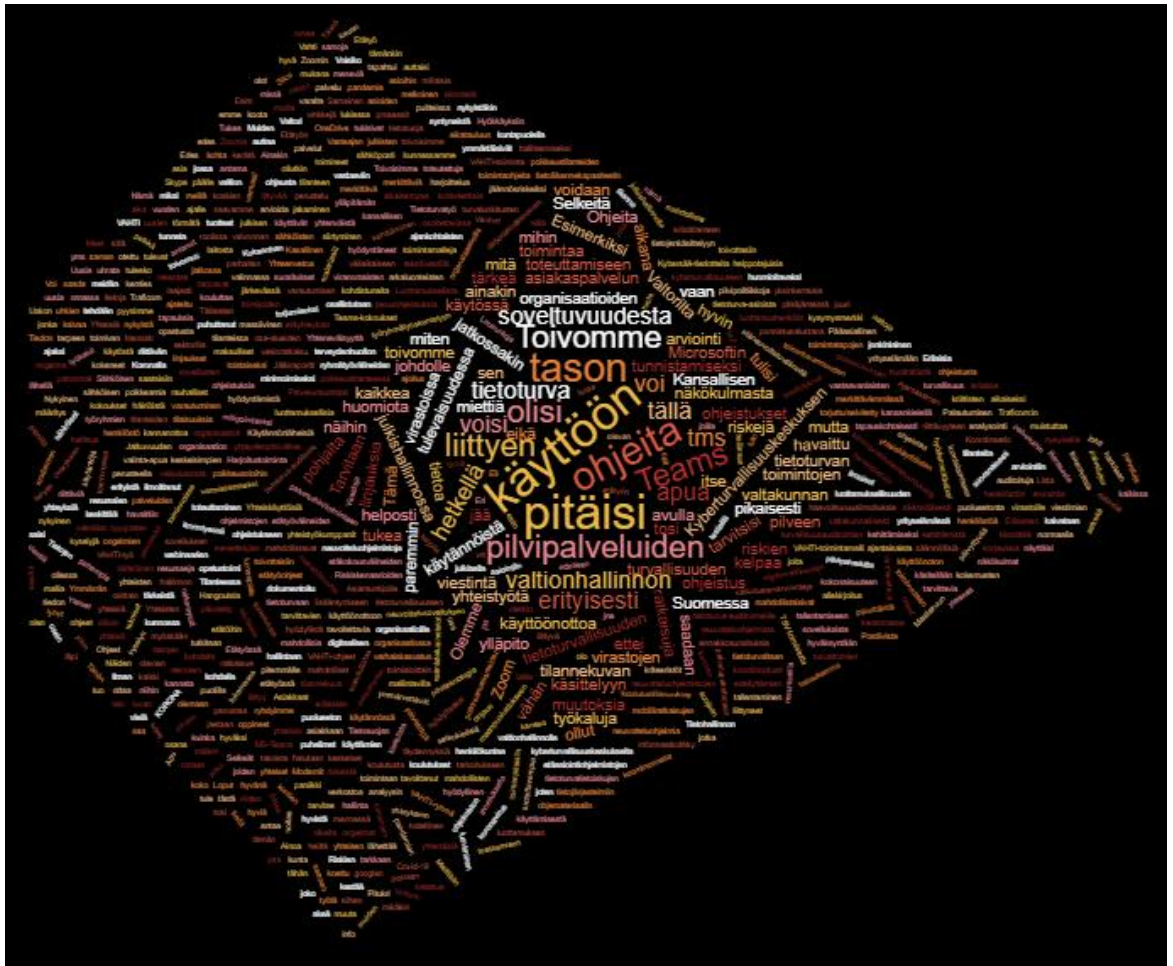


VAHTI / Rousku Kimmo (DVV)

Ohessa kolme vastauksista poimittua toivetta:

- ”VAHTI-työ pitäisi keskittää siihen, että organisaation 20 %:n resursseilla saadaan katettua ja hallittua 80 % riskeistä. Loput jää jäännöriskeiksi ja niihin ei kannata resursseja uhrata.”
- ”Yhteenvedoa siitä, että millaisia kyberturvallisuuden kohdistuneita tapauksia pandemian aikana Suomessa on havaittu ja miten niitä on torjuttu/selvitetty.”
- ”Yleiset ja helposti ymmärrettävät etättyöohjeet (henkilöstö + luottamushenkilöt).”

Sekä tässä vastauksessa että osassa aikaisempia kysymyksiä nousi esille Liikenne- ja viestintävirastossa sijaitsevan Kyberturvallisuuskeskuksen antama tuki ja tuottamat materiaalit sekä muu viestintä ei pelkästään nyt Koronaviruspandemian hallitsemisessa vaan yleisemmin tieto- ja kyberturvallisuuden kehittämisessä.



Kuva 12. Kuva. Sanapilvi kehittämisideoista.



VAHTI / Rousku Kimmo (DVV)

2.5 Kommentteja, ideoita ja palautetta

Lopuksi saimme 36 muuta kommenttia. Palautteissa kiiteltiin ja pidettiin kyselyä tarpeellisena. Eniten kehitysehdotuksia saivat viimeiset kysymykset, koska niissä ei ollut kaikkia vastaajaorganisaation toivomia vastausvaihtoehtoja. Samoin palautetta tuli siitä, että kaikissa kysymyksissä käytettävät asteikot tulisi olla yhtenäisiä. Lisäksi toivottiin, että kyselyyn vastaaminen onnistuisi sähköisen palvelun kautta.

Nämä palautteet otetaan huomioon, kun Digi- ja väestötietoviraston JUDO-hankkeessa kehitetään digitaalisen turvallisuuden kokonaiskuvapalvelua, jonka avulla tällaiset kyselyt voidaan jatkossa toteuttaa.

Ohessa kolme vastauksista poimittua palautetta:

”Kiitos kyselystä, hyvä että näitä asioita kootaan yhteen. Täyttö asiantuntijaryhmässä oli antoisaa.”

”Kuntatoimijana hankala täyttää tätä taulukkoa, koska toiminta on niin laaja-alaista.”

”Vastaamisesta sinänsä on hyöty organisaatiolle ja käytämme tätä lomaketta omaan seurantaan. Vastausten kokoaminen ja sisäinen käsittely auttoi tiedottamaan ylimmälle johdolle digiturvallisuuteen liittyvistä asioista sopivan tiiviissä muodossa, vaikkakin kevään kaikki muut kiireet ja huolet ovat kuormittaneet johtoa ja digiturva itsessään ei ole ollut ylimmän johdon huolina korona-tilanteessa.”



VAHTI / Rousku Kimmo (DVV)

3 Liite 1.

Tähän liitteeseen on koottu keskeiset toimialakohtaiset havainnot kesällä 2020 suoritettujen tietojen tarkemman analysoinnin perusteella.

3.1 Yhteenveto

Tarkempien tietojen perusteella voidaan todeta, että vähiten turvallisuuden toteuttamiseen liittyvää toimintaa ovat muuttaneet sairaanhoitopiirit ja vastaavasti eniten toimintaa ovat joutuneet muuttamaan yliopistot. Valtionhallinnon ja kuntien osalta löytyy jonkin verran kysymyskohtaisia eroja.

Erityisesti valtionhallinnossa kärsittiin alkuvaiheessa uhkien toteutumisesta; sekä etätyöyhteyksiin että tietoliikennekapasiteettiin liittyvistä ongelmista, mutta uhkat saatiin varsin nopeasti hallintaan. Kulunut kesä ja lomien jälkeinen aika ovat osoittaneet, että nämä riskit näyttävät olevan hyvin hallinnassa. Sen sijaan kolmas uhka, joka koskee sähköpostin avulla toteutettuja huijaus- tai hyökkäysviestejä, tuntuu pysyvän edelleen korkeana. Sekä Kyberturvallisuuskeskus että Keskusrikospoliisin Kyberkeskus ovat nostaneet sähköpostin ja puhelinsoittojen avulla toteutettuja hyökkäyksiä katsauksiinsa.

3.2 Uhkien toteutuminen toimialakohtaisesti

Tuloksista nousi esille erityisesti kolme keskeistä useimmilla toimialoilla toteutunutta uhkaa sekä kaksi uhkaa, jotka ovat toteutuneet harvemmillä organisaatioilla, mutta herättivät jonkin verran huolta:

<i>Etätyöyhteyksiin liittyviä häiriöitä</i>	81 %
<i>Tietoliikennekapasiteettiin liittyviä häiriöitä</i>	62 %
<i>Uudenlaisia sähköpostin avulla toteutettuja huijaus- tai hyökkäysviestejä</i>	59 %

ja

<i>Salassa pidettävän tiedon vuotamista</i>	8 %
<i>Datan ja ohjelmistojen menetyksiä</i>	1 %

Kun näitä viittä eri kohtaa arvioitiin tarkemmin, niin niissä havaittiin jonkin verran toimialakohtaisia eroja.

3.2.1 Etätyöyhteyksiin liittyvät häiriöt

81%

Kyselyssä selväksi ykköseksi nousi etätyöyhteyksiin liittyvät häiriöt. Tämä on aiheuttanut vähiten häiriöitä sairaanhoitopiireille ja selvästi eniten valtionhallinnon organisaatioille.

- sairaanhoitopiirit 62%
- yliopistot 73%
- kunnat 78%



VAHTI / Rousku Kimmo (DVV)

- valtionhallinto 90%

Kuten riskienhallintaa koskevassa osuudessa on todettu, tämä yleisin uhka on pääosin pystytty saamaan varsin hyvin hallintaan, ja kesälomien jälkeen tilanne on pysynyt vähintään hyvänä, ellei jopa erinomaisena. Sama koskee seuraavaa uhkaa eli tietoliikennepalveluita tarjoavien operaattoreiden kansallisen tason tilannetta.

3.2.2 Tietoliikennekapasiteettiin liittyviä häiriöitä 62%

Tietoliikennekapasiteetteihin liittyvät ongelmat voivat olla osasyitä ja osin seuraus edelliseen etätyöyhteyksissä koettuihin ongelmiin, koska myös tässä järjestys on sama. Ongelmasta ovat kärsineet vähiten sairaanhoitopiirit (31%) ja eniten valtionhallinnon organisaatiot (75%).

- sairaanhoitopiirit 31%
- yliopistot 46%
- kunnat 46%
- valtionhallinto 75%

3.2.3 Uudenlaisia sähköpostin avulla toteutettuja huijaus- tai hyökkäysviestejä 59%

Toimialakohtaisissa tuloksissa kenties yllättävin havainto koskee huijaus- tai hyökkäysviestien määrää. Yliopistot ovat kärsineet niistä merkittävästi muita vähemmän, kuntien ja valtionhallinnon ollessa hyvin lähellä keskiarvoa. Merkittävästi eniten niitä ovat kokeneet sairaanhoitopiirit. Osin tätä selittänee se, että monet tietoverkkorikolliset ovat muuttaneet aikaisemmat hyökkäysmenetelmiensä teemat koskemaan koronaviruksen ympärillä olevia aiheita. Tällöin myös hyökkäyksiä on merkittävästi kohdistettu sote-puolen toimijoihin.

- yliopistot 46%
- kunnat 58%
- valtionhallinto 59%
- sairaanhoitopiirit 85%

3.2.4 Salassa pidettävän tiedon vuotamista 8 %

Kaksi kyselyn huolestuttavinta havaintoa olivat salassa pidettävän tietojen vuotaminen sekä datan ja ohjelmistojen menetykset. Kyselyssä ei pyydetty tarkemmin arvioimaan, millaisesta tiedosta tai menetyksistä oli kysymys. Valtionhallinnossa salassa pidettävän tiedon vuotamista oli jonkin verran muita vähemmän ja vastaavasti sairaanhoitopiireissä selvästi muita enemmän.

- valtionhallinto 6%
- yliopistot 9%



VAHTI / Rousku Kimmo (DVV)

- kunnat 9%
- sairaanhoitopiirit 15%

Vastaajilta kysyttiin myös, miten organisaation riskienhallinta on tunnistettujen uhkien osalta toteutunut. Tässä kohdassa kaikki vastaajat olivat tunnistaneet uhkan ja hallinneet siihen liittyvät jäännösriskit pääosin tai hyvin. Käytännössä kyse on ollut yksittäisistä tapauksista, joten koronaviruspandemialla ei ole ollut välttämättä vaikutusta asiaan.

3.2.5 Datan ja ohjelmistojen menetyksiä

1 %

Ainoastaan sairaanhoitopiireistä saatiin kaksi vastausta, joissa ilmoitettiin datan ja ohjelmistojen menetyksistä.

Riskienhallinnan osalta tässä asiassa toisella vastaajalla on ollut osin tuntemattomia ja hallitsemattomia riskejä, ja toisella uhka on tunnistettu ja siitä syntyvä riski on hallittu hyvin.

3.3 Toiminnan kehittäminen ja sen mahdollistaminen muuttuneessa toimintaympäristössä

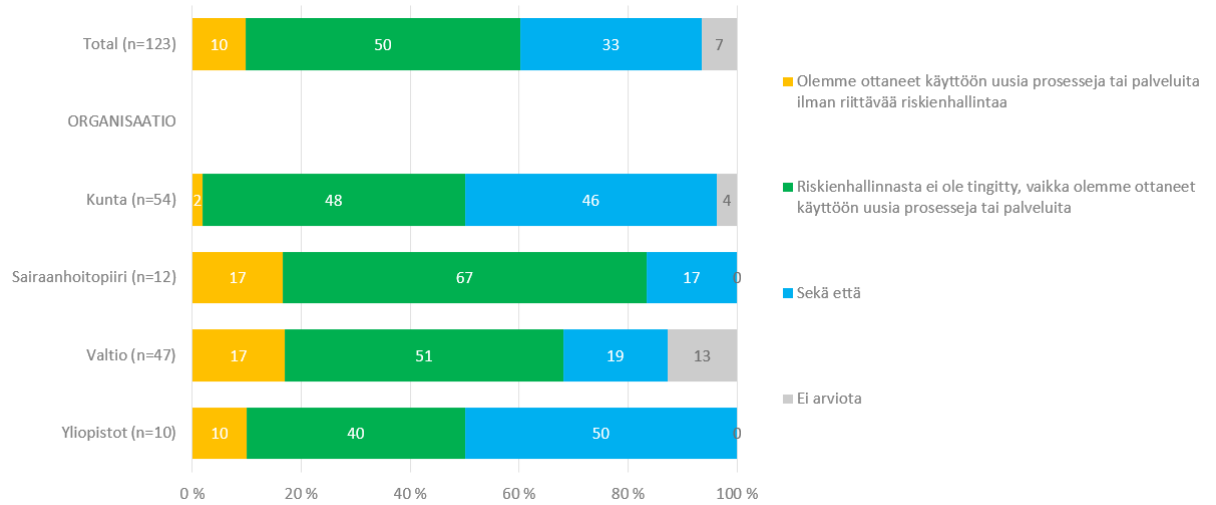
Kysymyksillä haluttiin selvittää, kuinka paljon organisaatiot ovat koronaviruspandemian takia muuttaneet keskeisiä turvallisuuteen liittyviä prosessejaan. Yhteenvetona voidaan todeta, että muutoksia on jouduttu tekemään, mutta useimmissa tapauksissa on pystytty huolehtimaan tarvittavasta riskienhallinnasta. Erityisesti niiden, jotka ovat joutuneet tinkimään riskienhallinnasta, tulisi tarkistaa tilanne nyt loppuvuoden 2020 aikana ja arvioida uudelleen mahdollisesti tarvittavia lisätoimenpiteitä jäännösriskien hallitsemiseksi.

3.3.1 Prosessien tai palvelujen käyttöönotto

Vastaajista 10% totesi, että he ovat ottaneet käyttöön uusia prosesseja tai palveluita ilman riittävää riskienhallintaa. Vastaavasti 50% vastaajista ei ole tinkinyt riskienhallinnasta, 33% on tehnyt osin kompromisseja ja 7% ei ole tätä kohtaa arvioinut. Vähiten riskienhallinnasta ovat tinkineet sairaanhoitopiirit (67% ei ole tinkinyt lainkaan), seuraavina valtio (51%), kunnat (48%) ja yliopistot (40%). Edellistä tulosta sairaanhoitopiirien osalta heikentää se, että sekä sairaanhoitopiirit ja valtionhallinto ovat ottaneet eniten käyttöön uusia prosesseja ja palveluita ilman riittävää riskienhallintaa (17%). Kompromisseja ovat tehneet eniten yliopistot (50%) ja kunnat (46%).



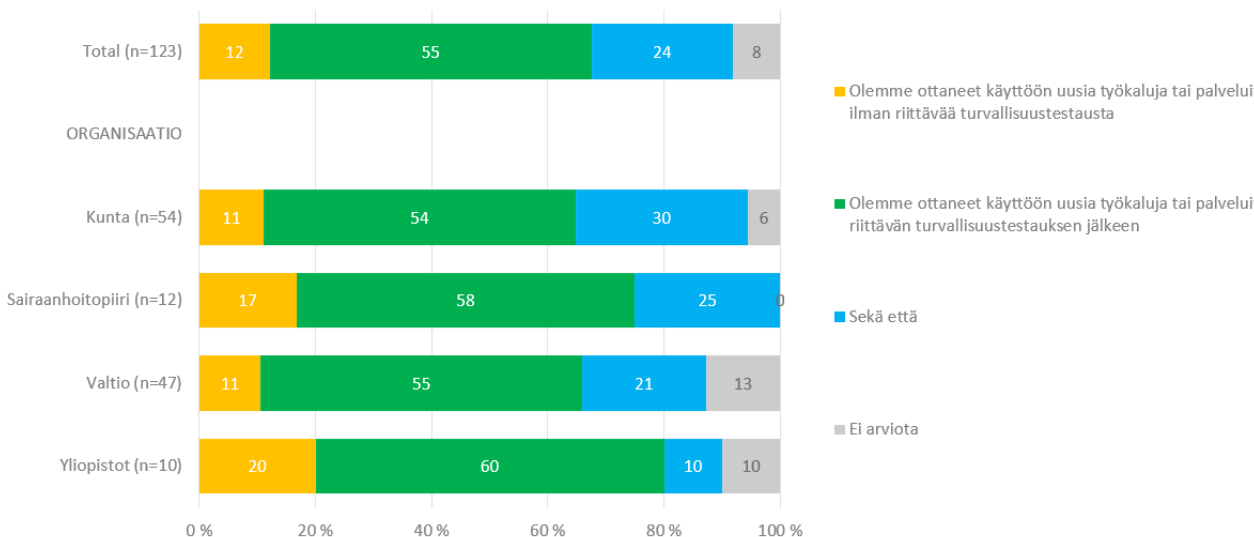
VAHTI / Rousku Kimmo (DVV)



Kuva 13. Kaavio. Prosessien tai palvelujen käyttöönotto ja niissä suoritettu riskienhallinta.

3.3.2 Työkalujen tai prosessien turvallisuustestaus

Koronaviruspandemia on vaikuttanut myös käyttöön otettavien työkalujen ja prosessien turvallisuustestaukseen. Koska näitä kysymyksiä ei ole aikaisemmin esitetty, vertailua koronaviruspandemiaa edeltäneeseen aikakauteen on hankala tehdä. Käytännössä jokaisella toimialalla vähintään puolet työkaluista tai prosesseista otetaan käyttöön vasta riittävän turvallisuustestauksen jälkeen. Mikäli tämä kohdistuu organisaation toiminnalle kriittisiin osa-alueisiin, tulosta voidaan pitää vähintään tyydyttävänä, koska lisäksi 24% vastaajista tekee tätä osittain.



Kaaviossa 13 on kuvattu prosessien tai palvelujen käyttöönotossa suoritettu riskienhallinta. Tulokset on avattu tekstiosuudessa. Eniten työkaluja tai prosesseja ovat ottaneet käyttöön ilman riittävää turvallisuustestausta yliopistot (20%),



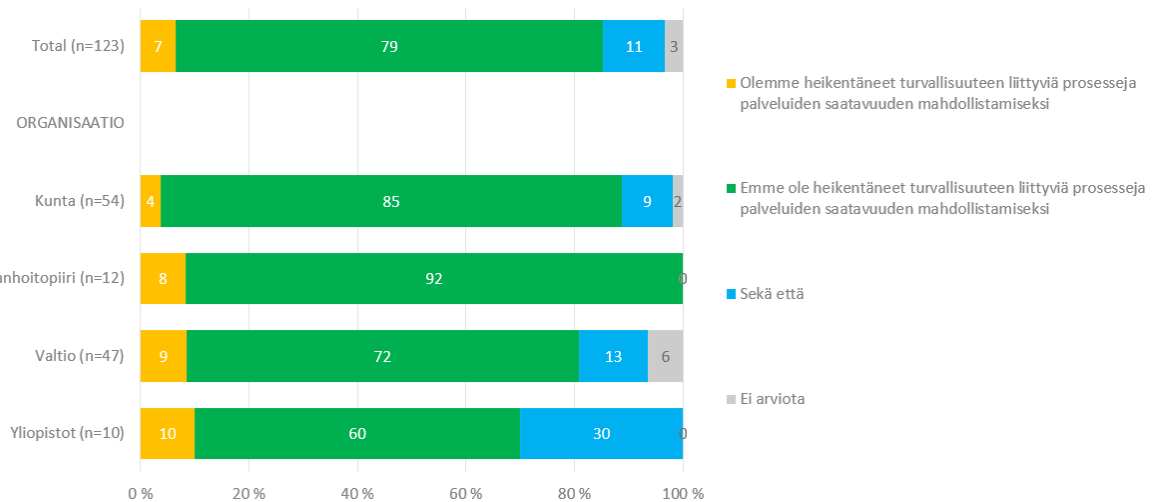
VAHTI / Rousku Kimmo (DVV)

tämän jälkeen sairaanhoitopiirit (17%), valtionhallinto (11%) ja kunnat (11%). Erot erityisesti tässä kysymyksessä eri toimialojen välillä ovat muita kysymyksiä pienemmät.

Kuva 14. Kaavio. Työkalujen tai prosessien turvallisuustestaus.

3.3.3 Turvallisuuteen liittyvät prosessit

Eräs kyselyn positiivisimmista havainnoista koski turvallisuuteen liittyvien prosessien toteutumista. Vain 7% vastaajista totesi, että he ovat ottaneet käyttöön uusia prosesseja tai palveluita ilman riittävää riskienhallintaa. 79% vastaajista ei ole tinkinyt riskienhallinnasta, 11% on tehnyt osin kompromisseja ja 3% ei ole tätä kohtaa arvioinut.



Kuva 15. Kaavio. Turvallisuuteen liittyvät prosessit.

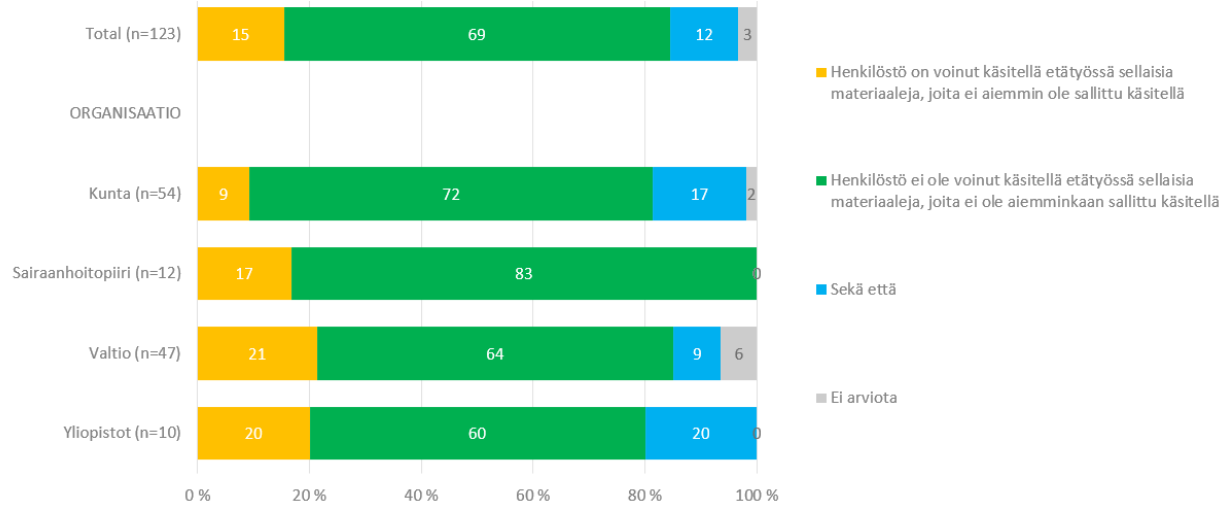
Kuten edellisessä kohdassa, vähiten prosesseja ovat heikentäneet sairaanhoitopiirit (92% ei ole heikentänyt), seuraavina kunnat (85%), valtionhallinto (72%) ja yliopistot (60%). Samalla tulee kuitenkin huomata, että kunnat ovat heikentäneet vain 4% palveluiden saatavuuteen liittyviä prosesseja, mutta 9% sekä-että. Vastaavasti sairaanhoitopiireissä 8% on heikentänyt turvallisuusprosesseja, mutta sekä-että vastauksia ei ole lainkaan.

3.3.4 Materiaalien käyttö etätöissä

Koronaviruspandemia aiheutti etätöiden tekemiseen merkittävän muutoksen. Eräs keskeinen huoli liittyy siihen, miten etätöissä on pystytty huolehtimaan turvallisesta tietoaineistojen käsittelystä. Vastausten perusteella 15% organisaatioista ja niissä työskentelevistä henkilöstöstä on pystynyt käsittelemään etätöissä sellaisia materiaaleja, joita ei ole aiemmin sallittu. Vastaavasti 69% henkilöstöstä ei ole saanut käsitellä etätöissä sellaisia materiaaleja, joita ei ole aiemminkaan sallittu. 12% vastaajista on joutunut tekemään kompromisseja eli "Sekä että", 3% ei ole antanut tähän arviota.



VAHTI / Rousku Kimmo (DVV)



Kuva 16. Kaavio. Materiaalien käyttö etätöissä.

Materiaalien käyttöä ovat eniten avanneet valtionhallinto (21%), yliopistot (20%) ja sairaanhoitopiirit (17%), kunnissa tarve on ollut pienempi (9%).

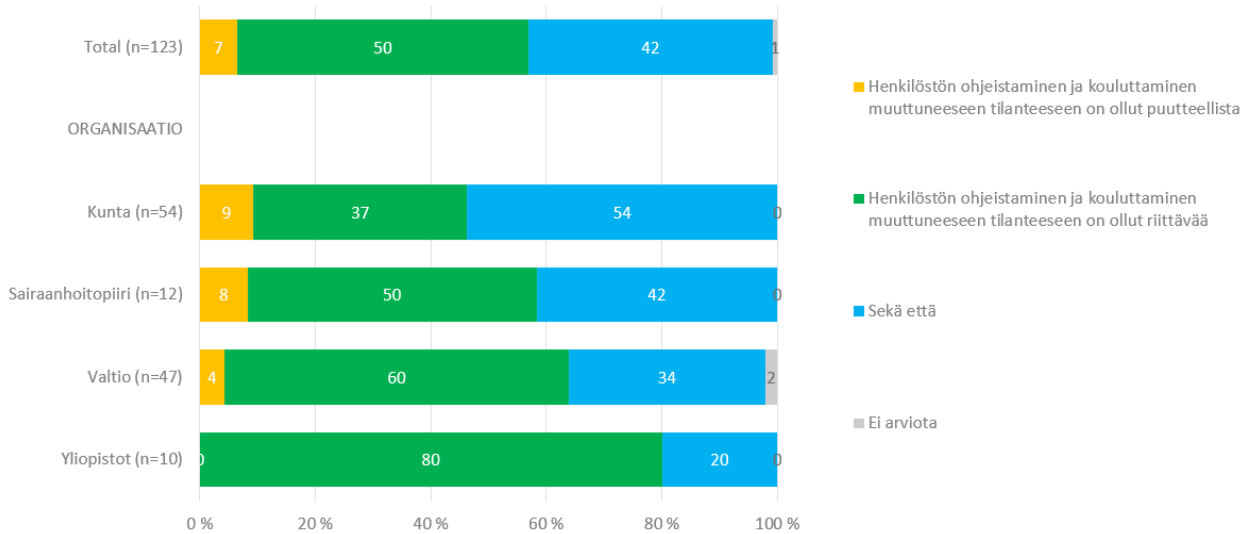
Mikäli organisaatio on sallinut etätöissä sellaisten tietoaisteiden käsittelyä, joita ei ole aikaisemmin sallittu, riskienhallinnassa erittäin keskeiseen rooliin nousee henkilöstön ohjeistaminen ja kouluttaminen. Samoin organisaatioiden tulee varmistaa, että tällaiset tiedot palautetaan työpaikalle sen jälkeen, kun niitä ei tarvita. Samoin mahdollinen tietoaisteiden hävittäminen ei saa tapahtua kotona.

3.3.5 Henkilöstön ohjeistaminen ja kouluttaminen

Etätyö sekä muut uudet toimintatavat ovat luoneet tarpeen uudelleen ohjeistamiseen. Vastaajista 7% henkilöstön ohjeistaminen ja kouluttaminen muuttuneessa tilanteessa on ollut puutteellista 50% ohjeistaminen ja kouluttaminen on ollut riittävää, 42% sekä että ja 1% ei ole arvioinut tätä. Käytännössä on todennäköistä, että osalla organisaatioista koulutus ei ole ollut riittävän kattavaa johtuen hyvin nopeasti muuttuneesta tilanteesta.



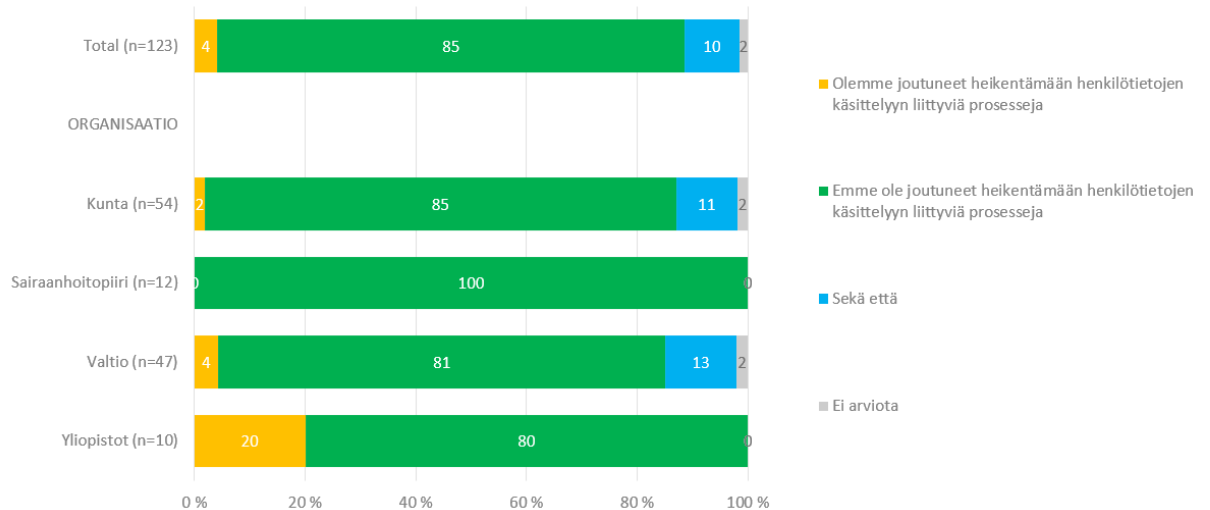
VAHTI / Rousku Kimmo (DVV)



Kuva 17. Kaavio. Henkilöstön ohjeistaminen ja kouluttaminen.

3.3.6 Henkilötietojen käsittelyyn liittyvät prosessit

Toimialakohtaisissa tuloksissa koko kyselyn positiivisin havainto koskee henkilötietojen käsittelyyn liittyviä prosesseja. Ainoastaan 4% vastaajista on todennut, että he ovat joutuneet heikentämään henkilötietojen käsittelyyn liittyviä prosesseja, 85% ei ole heikentänyt, 10% on joutunut tekemään jotain kompromisseja ja 2% ei ole tätä arvioinut.



Kuva 18. Kaavio. Henkilötietojen käsittelyyn liittyvät prosessit.

Tulosta voidaan pitää hyvänä ja se osoittaa, kuinka sitoutuneita organisaatiot ovat henkilötietojen vaatimustenmukaiseen käsittelyyn. Tuloksissa pistää silmään erityisesti sairaanhoitopiirit, joista 100% on käsitellyt tietoja samoin kuin aiemmin.



VAHTI / Rousku Kimmo (DVV)

Yliopistoissa 20% vastaajista (kaksi vastaajaa) on todennut, että ne ovat joutuneet heikentämään prosessejaan.