Kuinka johto varmistaa organisaation toiminnan jatkuvuuden ja luottamuksen säilymisen 2020-luvulla?

Kyselyn yhteenveto

11.5.2020 Kimmo Rousku – pääsihteeri (VAHTI)

DIGI- JA VÄESTÖTIETO-VIRASTO

Raportin taustoja

- Raportin laatimisen taustalla on kesäkuun 2019 VAHTI-joryn työseminaari, jossa huoleksi nousivat uudet digitaaliseen toimintaan liittyvät uhkat – Lahden kaupunkiin kohdistettu kyberhyökkäys oli juuri tullut julkisuuteen.
- Keskustelun perusteella päätettiin tehdä raportti, jonka valmistelu käynnistyi elokuussa 2019. Raportin tuottamiseen pyydettiin oheisia kuvassa näkyviä organisaatioita.
- Raportti ja siihen liittyvä kysely toimitettiin julkisen hallinnon organisaatioiden johtoryhmien käsiteltäväksi marraskuun alkupuolella.

Raportin sisällysluettelo

Vastaajat

Saimme raporttiin liittyvään kyselyyn yhteensä 100 vastausta, jotka jakaantuivat eri toimialoille seuraavasti:

Valtionhallinto	51
Kunnat ja kuntayhtymät	41
Sairaanhoitopiirit	4
Yliopistot	4
Yhteensä	100 organisaatiota

Kyselyn tulokset – kysymys 2

2. Onko organisaationne tutustunut kesällä 2019 julkiseen hallintoon kohdistuneisiin onnistuneisiin kyberhyökkäyksiin ja arvioinut omaa kyvykkyyttään selviytyä vastaavanlaisista hyökkäyksistä?

Kyllä | Ei

Kysymys 2	Kaikki N=100	Valtion-hallinto N=51	Kunnat N=41	Sairaan-hoitopiirit N=4	Yliopistot N=4
Painotettu KA	1,23	0,94	1,41	2,00	2,00
Kyllä	74 %	65 %	80 %	100 %	100 %
Ei	26 %	35 %	20 %	0 %	0 %

Kaikki sairaanhoitopiirien (N=4) ja yliopistojen (4) vastaajat ovat tehneet arvioinnin (100 %), kunnista (41) valtaosa (80 %), mutta valtionhallinnossa (51) kyvykkyyttä on arvioitu selvästi muita vähemmän (65 %).

Kyselyn tulokset – kysymys 3

3. Onko organisaationne tunnistanut ja priorisoinut sen toiminnalle kriittiset tietojärjestelmät ja niihin liittyvät riippuvuudet muista osapuolista?

Kysymys 3	Kaikki N=100	Valtion-hallinto N=51	Kunnat N=41	Sairaan-hoitopiirit N=4	Yliopistot N=4
	1,32	1,49	1,05	1,50	1,50
Kyllä	45 %	53 %	34 %	50 %	50 %
Osittain	48 %	45 %	51 %	50 %	50 %
Ei	7 %	2 %	15 %	0 %	0 %

- Puolet sairaanhoitopiireistä ja yliopistoista on tehnyt arvioinnin, valtionhallinnossa reilut puolet (53 %), mutta kunnissa vain noin kolmasosa (34 %).
- Erityisesti kunnissa muita suurempi osa on jättänyt kokonaan tunnistamatta ja priorisoimatta (15 %). Uskoisimme, että nyt KVP on tehostanut myös tätä työtä?

Kyselyn tulokset – kysymys 4

4. Onko organisaationne johto harjoitellut vuosina 2018-2019 reagoimista laajavaikutteiseen, organisaatioon kohdistuvaan kyberhyökkäykseen sekä siitä selviämisen johtamista ja hallintaa?

Kysymys 4	Kaikki N=100	Valtion-hallinto N=51	Kunnat N=41	Sairaan-hoitopiirit N=4	Yliopistot N=4
	1,17	1,12	1,20	0,50	2,00
Kyllä	72 %	71 %	73 %	50 %	100 %
Ei	28 %	29 %	27 %	50 %	0 %

- Kaikki yliopistot ovat harjoitelleet (100 %), kunnissa (73 %) ja valtionhallinnossa (71 %) on harjoiteltu kohtuullisesti, mutta sairaanhoitopiireistä vain puolet (50%) on harjoitellut.
- Yleisimmät harjoitukset ovat olleet TAISTO18- ja TAISTO19.
- Nyt käynnissä oleva koronaviruspandemia on globaali toiminnan jatkuvuuteen liittyvä tosielämän tilanne, jonka kaikki opit pitää pystyä tehokkaasti hyödyntämään.

Kyselyn tulokset – kysymys 5

5. Onko organisaatiolla käynnissä digi- tai kyberturvallisuuden kehittämisohjelmaa?

Kysymys 5	Kaikki N=100	Valtion-hallinto N=51	Kunnat N=41	Sairaan-hoitopiirit N=4	Yliopistot N=4
	0,42	0,37	0,20	2,00	1,25
Kyllä	36 %	39 %	22 %	100 %	75 %
Mahdollisesti tai 6 kk sisällä	16 %	10 %	27 %	0 %	0 %
Ei ole	48 %	51 %	51 %	0 %	25 %

- Kaikilla sairaanhoitopiireillä (100 %) on kehittämisohjelma, myös valtaosalla yliopistoista (75 %).
- Valtionhallinnossa 39 % on kehittämisohjelma, ja yli puolella sitä ei ole (51 %).
- Kunnilla ohjelma on 22%, 27% on mahdollisesti käynnistämässä, yli puolella (51 %) sitä ei ole.
- Kokonaisuutena vajaalla puolella ei ole kehittämisohjelmaa, mikä on selkeä kehittämistavoite.

Kyselyn tulokset – kysymys 6

6. Millaisena itse arvioitte oman organisaationne digi- ja kyberturvallisuuden tason?

Kysymys 6	Kaikki N=100	Valtion-hallinto N=51	Kunnat N=41	Sairaan-hoitopiirit N=4	Yliopistot N=4
	1,29	1,39	1,12	1,25	1,50
Erittän hyvä	0 %	0 %	0 %	0 %	0 %
Hyvä	56 %	55 %	56 %	75 %	50 %
Tyydyttävä	40 %	43 %	37 %	25 %	50 %
Huono	2 %	2 %	2 %	0 %	0 %
Erittäin huono	2 %	0 %	5 %	0 %	0 %

- Yksikään vastaaja ei ilmoittanut olevansa erittäin hyvällä tasolla, hyvällä tasolla on jokaiselta toimialalta vähintään 50 %.
- Kaksi kuntaa ilmoitti olevansa erittäin huonolla tasolla. Yhteensä 4 % vastaajista ilmoitti olevansa huonolla (2 %) tai erittäin huonolla tasolla (2 %).
- Kehittämiskohde; kaikki pitäisi saada vähintään tyydyttävälle tasolle.

Keskiarvot tästä osuudesta

Keskiarvot	Kaikki N=100	Valtion-hallinto N=51	Kunnat N=41	Sairaan-hoitopiirit N=4	Yliopistot N=4
Arviointi kyberhyökkäyksiin	1,23	0,94	1,41	2,00	2,00
Tunnistus ja priorisointi	1,32	1,49	1,05	1,50	1,50
Johdon harjoittelu	1,17	1,12	1,20	0,50	2,00
Kehittämisohjelma	0,42	0,37	0,20	2,00	1,25
Digi- ja kyberturvan taso	1,29	1,39	1,12	1,25	1,50
Kaikkien keskiarvo	1,08	1,06	0,99	1,45	1,65

- Kokonaisuudessaan erot valtionhallinnon ja kuntien välillä ovat pienet. Sekä sairaanhoitopiirien että yliopistojen keskiarvoja voidaan pitää vähintään hyvinä, toisaalta vastaajien suhteellinen osuus (4 + 4) on pieni.

Riskienhallinta

- Riskienhallintaosiossa oli tarkoitus arvioida muutamia keskeisiä organisaation toimintaan liittyviä uhkia ja tunnistettuja riskejä.
- Vastauksissa organisaatioiden välillä näkyy merkittäviä eroja riippuen siitä, miten tietohallinto on toteutettu sekä miten paljon palveluita on ulkoistettu.

- Arvioinnissa käytettiin seuraavaa asteikkoa:

4 Riski on tunnistettu ja hyvin halinnassa
3 Riski on tunnistettu, siihen liittyy kuitenkin selkeitä jäännösriskejä, jotka ovat pääosin hallinnassa
2 Riski on tunnistettu, mutta emme ole kuitenkaan saaneet siihen vielä riittäviä hallintakeinoja
1 Riski on tunnistettu ja se vaarantaa tällä hetkellä merkittävästi organisaatiomme toimintaa / strategisten tavoitteiden saavuttamista
0 Emme ole tunnistaneet tätä riskiä

Yhteenveto

	Kaikki N=100	Valtion-hallinto N=51	Kunnat N=41	Sairaan-hoitopiirit N=4	Yliopistot N=4
a) organisaation omat turvallisuuden ylläpitoon ja kehittämiseen liittyvät henkilöresurssit	2,14	2,00	1,83	2,25	2,50
b) organisaation taloudellinen tilanne koskien digi- ja kyberturvallisuuden ylläpitoa ja kehittämistä	2,11	2,16	2,29	2,00	2,00
c) organisaation omien digi- ja kyberturvallisuuden asiantuntijoiden ja esimiesten osaaminen	2,06	2,14	1,85	1,50	2,75
d) oman henkilöstön ajantasainen osaaminen nopeasti kehittyvässä digitaalisessa toimintaympäristössä	1,96	1,84	1,24	2,25	2,50
e) organisaation itse tuottamien kriittisten palveluiden turvallisuuden toteuttaminen	2,59	2,41	2,20	2,75	3,00
f) kriittisten ulkoistettujen palveluiden käyttämiseen liittyvät haasteet (esimerkiksi sopimukset, raportointi)	2,22	1,92	2,22	2,25	2,50
g) organisaation toimintaan liittyvien kriittisten toimittajien ja alihankintaketjujen hallinta	2,04	2,14	1,76	1,75	2,50
h) tietoverkkorikollisten aiheuttaman uhkan kasvu koskien eri tavalla toteutettuja kyberhyökkäyksiä	2,23	2,45	1,73	2,75	2,00
i) olemme tunnistaneet olevamme sellainen kohde, jota vastaan todennäköisesti toteutetaan kohdistettuja hyökkäyksiä	2,77	2,02	2,32	3,50	3,25
Keskiarvo	2,24	2,12	1,94	2,33	2,56

- Yhdeksästä kohteesta suurimmat riskit arvioidaan liittyvän **oman henkilöstön osaamiseen** (indeksin arvo 1,96),**kriittisten toimittajien ja alihankintakertjujen hallintaan** (2,04) sekä **asiantuntijoiden ja esimiesten osaamiseen** (2,06).
- Parhaiten on tunnistettu **onko organisaatio kohdistettujen hyökkäysten kohde** (2,77). **Itse tuotettujen palveluiden turvallisuuden toteuttaminen** (2,59) koettiin seuraavaksi pienimmäksi hallituksi riskiksi.
- Parhaiten riskien tunnistaminen ja hallinta toteutuvat yliopistoissa (2,56), seuraavina sairaanhoitopiirit (2,33), valtionhallinto (2,12) ja kunnat (1,94).

a) organisaation omat turvallisuuden ylläpitoon ja kehittämiseen liittyvät henkilöresurssit

	Kaikki N=100	Valtion-hallinto N=51	Kunnat N=41	Sairaan-hoitopiirit N=4	Yliopistot N=4
a) organisaation omat turvallisuuden ylläpitoon ja kehittämiseen liittyvät henkilöresurssit	2,14	2,00	1,83	2,25	2,50
4) Riski on tunnistettu ja hyvin hallittu	2,2 %	3,9 %	4,9 %	0,0 %	0,0 %
3) Riski on tunnistettu, siihen liittyy kuitenkin selkeitä jäännösriskejä, jotka ovat pääosin hallinnassa	54,5 %	49,0 %	43,9 %	50,0 %	75,0 %
2) Riski on tunnistettu, mutta emme ole saaneet luotua siihen vielä riittäviä hallintakeinoja	39,4 %	41,2 %	41,5 %	50,0 %	25,0 %
1) Riski on tunnistettu ja se vaarantaa tällä hetkellä merkittävästi organisaatiomme toimintaa / strategisten tarvoitteiden saavuttamista	3,4 %	3,9 %	9,8 %	0,0 %	0,0 %
0) Emme ole tunnistaneet tätä riskiä	0,5 %	2,0 %	0,0 %	0,0 %	0,0 %

- Parhaiten tämä riski on tunnistettu yliopistoissa (75 %), muilla toimialoilla erot ovat pienet, mutta suurimpina henkilöresurssiriskejä pidetään kunnissa (9,8 %) ja valtionhallinnossa (3,9 %), joissa riski vaarantaa merkittävästi organisaation toimintaa.

b) organisaation taloudellinen tilanne koskien digi- ja kyberturvallisuuden ylläpitoa ja kehittämistä

	Kaikki N=100	Valtion-hallinto N=51	Kunnat N=41	Sairaan-hoitopiirit N=4	Yliopistot N=4
b) organisaation taloudellinen tilanne koskien digi- ja kyberturvallisuuden ylläpitoa ja kehittämistä	2,11	2,16	2,29	2,00	2,00
4) Riski on tunnistettu ja hyvin hallittu	2,2 %	19,6 %	12,2 %	50,0 %	0,0 %
3) Riski on tunnistettu, siihen liittyy kuitenkin selkeitä jäännösriskejä, jotka ovat pääosin hallinnassa	54,5 %	35,3 %	53,7 %	50,0 %	50,0 %
2) Riski on tunnistettu, mutta emme ole saaneet luotua siihen vielä riittäviä hallintakeinoja	39,4 %	33,3 %	26,8 %	0,0 %	50,0 %
1) Riski on tunnistettu ja se vaarantaa tällä hetkellä merkittävästi organisaatiomme toimintaa / strategisten tarvoitteiden saavuttamista	3,4 %	9,8 %	7,3 %	0,0 %	0,0 %
0) Emme ole tunnistaneet tätä riskiä	0,5 %	2,0 %	0,0 %	0,0 %	0,0 %

- Parhaiten riski on hallittu kunnissa, jossa riski on hyvin tai pääosin hallinnassa 65,9 %. Valtionhallinnossa tämä luku on 54,9 %, yliopistoissa ja sairaanhoitopiireissä 50 %.
- Toisaalta valtionhallinnossa 9,8 % ja kunnissa 7,3 % vastaajista kokee riskin vaarantavan toimintaa.

c) organisaation omien digi- ja kyberturvallisuuden asiantuntijoiden ja esimiesten osaaminen

	Kaikki N=100	Valtion-hallinto N=51	Kunnat N=41	Sairaan-hoitopiirit N=4	Yliopistot N=4
c) organisaation omien digi- ja kyberturvallisuuden asiantuntijoiden ja esimiesten osaaminen	2,06	2,14	1,85	1,50	2,75
4) Riski on tunnistettu ja hyvin hallittu	8,9 %	5,9 %	4,9 %	0,0 %	25,0 %
3) Riski on tunnistettu, siihen liittyy kuitenkin selkeitä jäännösriskejä, jotka ovat pääosin hallinnassa	42,0 %	49,0 %	43,9 %	25,0 %	50,0 %
2) Riski on tunnistettu, mutta emme ole saaneet luotua siihen vielä riittäviä hallintakeinoja	46,2 %	43,1 %	41,5 %	75,0 %	25,0 %
1) Riski on tunnistettu ja se vaarantaa tällä hetkellä merkittävästi organisaatiomme toimintaa / strategisten tarvoitteiden saavuttamista	0,6 %	0,0 %	2,4 %	0,0 %	0,0 %
0) Emme ole tunnistaneet tätä riskiä	2,3 %	2,0 %	7,3 %	0,0 %	0,0 %

- Parhaiten tämä riski on hallinnassa yliopistoissa (75 %), sen jälkeen valtionhallinnossa (54,9 %), kunnissa (48,8 %) ja sairaanhoitopiireissä (25 %).
- Yhdessä kunnassa riski uhkaa toimintaa tai strategisia tavoitteita.

d) oman henkilöstön ajantasainen osaaminen nopeasti kehittyvässä digitaalisessa toimintaympäristössä

	Kaikki N=100	Valtion-hallinto N=51	Kunnat N=41	Sairaan-hoitopiirit N=4	Yliopistot N=4
d) oman henkilöstön ajantasainen osaaminen nopeasti kehittyvässä digitaalisessa toimintaympäristössä	1,96	1,84	1,24	2,25	2,50
4) Riski on tunnistettu ja hyvin hallittu	1,0 %	3,9 %	0,0 %	0,0 %	0,0 %
3) Riski on tunnistettu, siihen liittyy kuitenkin selkeitä jäännösriskejä, jotka ovat pääosin hallinnassa	46,5 %	39,2 %	22,0 %	50,0 %	75,0 %
2) Riski on tunnistettu, mutta emme ole saaneet luotua siihen vielä riittäviä hallintakeinoja	49,1 %	52,9 %	68,3 %	50,0 %	25,0 %
1) Riski on tunnistettu ja se vaarantaa tällä hetkellä merkittävästi organisaatiomme toimintaa / strategisten tarvoitteiden saavuttamista	2,9 %	2,0 %	9,8 %	0,0 %	0,0 %
0) Emme ole tunnistaneet tätä riskiä	0,5 %	2,0 %	0,0 %	0,0 %	0,0 %

- Oman henkilöstön osaaminen koetaan keskeiseksi riskiksi, parhaana tilannetta pidettiin yliopistoissa.
- Erityisen huolestuttava tilanne on kunnissa, joissa 9,8 % vastajista kokee sen vaarantavan toimintaa.

e) organisaation itse tuottamien kriittisten palveluiden turvallisuuden toteuttaminen

	Kaikki N=100	Valtion-hallinto N=51	Kunnat N=41	Sairaan-hoitopiirit N=4	Yliopistot N=4
e) organisaation itse tuottamien kriittisten palveluiden turvallisuuden toteuttaminen	2,59	2,41	2,20	2,75	3,00
4) Riski on tunnistettu ja hyvin hallittu	7,3 %	19,6 %	9,8 %	0,0 %	0,0 %
3) Riski on tunnistettu, siihen liittyy kuitenkin selkeitä jäännösriskejä, jotka ovat pääosin hallinnassa	69,4 %	49,0 %	53,7 %	75,0 %	100,0 %
2) Riski on tunnistettu, mutta emme ole saaneet luotua siihen vielä riittäviä hallintakeinoja	16,8 %	17,6 %	24,4 %	25,0 %	0,0 %
1) Riski on tunnistettu ja se vaarantaa tällä hetkellä merkittävästi organisaatiomme toimintaa / strategisten tarvoitteiden saavuttamista	1,7 %	2,0 %	4,9 %	0,0 %	0,0 %
0) Emme ole tunnistaneet tätä riskiä	4,8 %	11,8 %	7,3 %	0,0 %	0,0 %

- Tämä on kaikista riskeistä hallinnassa toiseksi parhaiten, yliopistojen osalta se on parhaiten eli hyvin tai pääosin hallinnassa (100 %), sairaanhoitopiireillä luku on 75 %, valtionhallinnossa 68,4 % ja kunnissa 63,5 %.
- Muutamassa kuntien ja valtionhallinnon organisaatiossa tämä koetaan kriittisenä riskinä - toisaalta etenkin valtionhallinnossa ja kunnissa osa vastaajista ei tunnista riskiä, koska ilmeisesti palvelut on ulkoistettu.

f) kriittisten ulkoistettujen palveluiden käyttämiseen liittyvät haasteet (esimerkiksi sopimukset, raportointi)

	Kaikki N=100	Valtion-hallinto N=51	Kunnat N=41	Sairaan-hoitopiirit N=4	Yliopistot N=4
f) kriittisten ulkoistettujen palveluiden käyttämiseen liittyvät haasteet (esimerkiksi sopimukset, raportointi)	2,22	1,92	2,22	2,25	2,50
4) Riski on tunnistettu ja hyvin hallittu	4,4 %	7,8 %	9,8 %	0,0 %	0,0 %
3) Riski on tunnistettu, siihen liittyy kuitenkin selkeitä jäännösriskejä, jotka ovat pääosin hallinnassa	54,5 %	39,2 %	53,7 %	50,0 %	75,0 %
2) Riski on tunnistettu, mutta emme ole saaneet luotua siihen vielä riittäviä hallintakeinoja	37,8 %	47,1 %	29,3 %	50,0 %	25,0 %
1) Riski on tunnistettu ja se vaarantaa tällä hetkellä merkittävästi organisaatiomme toimintaa / strategisten tarvoitteiden saavuttamista	2,8 %	3,9 %	7,3 %	0,0 %	0,0 %
0) Emme ole tunnistaneet tätä riskiä	0,5 %	2,0 %	0,0 %	0,0 %	0,0 %

- Ulkoistamiseen liittyvät haasteet näkyvät etenkin valtionhallinnon vastauksissa. Tosin 7,8 % kokee riskien olevan hyvin hallinnassa, mutta lähes puolet (47,1 %) kokee tarvitsevansa lisää hallintakeinoja ja muutama vastaaja (3,9 %) kokee riskin vaarantavan toimintaa merkittävästi.
- Yliopistoissa (75 %), kunnissa (63,5 %) ja sairaanhoitopiireissä (50 %) tilanne koetaan parempana eli riskit ovat hyvin tai pääosin hallinnassa.

g) organisaation toimintaan liittyvien kriittisten toimittajien ja alihankintaketjujen hallinta

	Kaikki N=100	Valtion-hallinto N=51	Kunnat N=41	Sairaan-hoitopiirit N=4	Yliopistot N=4
g) organisaation toimintaan liittyvien kriittisten toimittajien ja alihankintaketjujen hallinta	2,04	2,14	1,76	1,75	2,50
4) Riski on tunnistettu ja hyvin hallittu	3,8 %	7,8 %	7,3 %	0,0 %	0,0 %
3) Riski on tunnistettu, siihen liittyy kuitenkin selkeitä jäännösriskejä, jotka ovat pääosin hallinnassa	47,6 %	49,0 %	41,5 %	25,0 %	75,0 %
2) Riski on tunnistettu, mutta emme ole saaneet luotua siihen vielä riittäviä hallintakeinoja	43,3 %	39,2 %	34,1 %	75,0 %	25,0 %
1) Riski on tunnistettu ja se vaarantaa tällä hetkellä merkittävästi organisaatiomme toimintaa / strategisten tarvoitteiden saavuttamista	4,0 %	3,9 %	12,2 %	0,0 %	0,0 %
0) Emme ole tunnistaneet tätä riskiä	1,2 %	0,0 %	4,9 %	0,0 %	0,0 %

- Toimittajien ja alihankintaketjujen hallinta koettiin toiseksi haasteellisempana riskinä.
- Hyvin tai pääosin hallinnassa tilanne on yliopistoissa 75 %, valtionhallinnossa 56,8 %, kunnissa 48,8 % ja sairaanhoitopiireissä 25 %, eli selvästi vähiten.
- Erityisesti kunnissa (12,8 %), mutta myös osin valtionhallinnossa (3,9 %) riskiä pidetään merkittävänä.

h) tietoverkkorikollisten aiheuttaman uhkan kasvu koskien eri tavalla toteutettuja kyberhyökkäyksiä

	Kaikki N=100	Valtion-hallinto N=51	Kunnat N=41	Sairaan-hoitopiirit N=4	Yliopistot N=4
h) tietoverkkorikollisten aiheuttaman uhkan kasvu koskien eri tavalla toteutettuja kyberhyökkäyksiä	2,23	2,45	1,73	2,75	2,00
4) Riski on tunnistettu ja hyvin hallittu	9,9 %	9,8 %	4,9 %	25,0 %	0,0 %
3) Riski on tunnistettu, siihen liittyy kuitenkin selkeitä jäännösriskejä, jotka ovat pääosin hallinnassa	50,6 %	60,8 %	41,5 %	50,0 %	50,0 %
2) Riski on tunnistettu, mutta emme ole saaneet luotua siihen vielä riittäviä hallintakeinoja	35,5 %	25,5 %	41,5 %	25,0 %	50,0 %
1) Riski on tunnistettu ja se vaarantaa tällä hetkellä merkittävästi organisaatiomme toimintaa / strategisten tarvoitteiden saavuttamista	3,5 %	2,0 %	12,2 %	0,0 %	0,0 %
0) Emme ole tunnistaneet tätä riskiä	0,5 %	2,0 %	0,0 %	0,0 %	0,0 %

- Tietoverkkorikollisten tuoma uhka on 60,5 % hallinnassa kaikilla toimialoilla, parhaiten sairaanhoitopiireissä (75 %), sen jälkeen valtionhallinnossa 70,8 %, yliopistoissa 50 % ja kunnissa, jotka ovat selvästi muissa jäljessä eli 46,4 %.
- Erityisesti kunnissa asia on tunnistettu kriittisenä riskinä (12,2 %), myös valtionhallinnossa muutama organisaatio (2,0 %) pitää riskiä toimintaa vaarantavana.
- Vastauksessa heijastunee vuonna 2019 kuntiin kohdistuneet onnistuneet kyberhyökkäykset.

i) olemme tunnistaneet olevamme sellainen kohde, jota vastaan todennäköisesti toteutetaan kohdistettuja hyökkäyksiä

	Kaikki N=100	Valtion-hallinto N=51	Kunnat N=41	Sairaan-hoitopiirit N=4	Yliopistot N=4
i) olemme tunnistaneet olevamme sellainen kohde, jota vastaan todennäköisesti toteutetaan kohdistettuja hyökkäyksiä	2,77	2,02	2,32	3,50	3,25
4) Riski on tunnistettu ja hyvin hallittu	27,5 %	15,7 %	19,5 %	50,0 %	25,0 %
3) Riski on tunnistettu, siihen liittyy kuitenkin selkeitä jäännösriskejä, jotka ovat pääosin hallinnassa	53,1 %	41,2 %	46,3 %	50,0 %	75,0 %
2) Riski on tunnistettu, mutta emme ole saaneet luotua siihen vielä riittäviä hallintakeinoja	10,9 %	21,6 %	22,0 %	0,0 %	0,0 %
1) Riski on tunnistettu ja se vaarantaa tällä hetkellä merkittävästi organisaatiomme toimintaa / strategisten tarvoitteiden saavuttamista	3,3 %	5,9 %	7,3 %	0,0 %	0,0 %
0) Emme ole tunnistaneet tätä riskiä	5,1 %	15,7 %	4,9 %	0,0 %	0,0 %

- Riski on tunnistettu kaikista parhaiten, erityisesti sairaanhoitopiirit (100 %) ja yliopistot (100 %) kokevat olevansa kohdistettujen hyökkäysten kohteena ja riskin olevan hyvin tai pääosin hallinnassa.
- Kunnista 65,8 % ja valtionhallinnosta 56,9 % on tunnistanut riskin ja pystyy sitä pääosin hallitsemaan. Valtionhallinnossa 15,7 % ja kunnissa 4,9 % ei tunnisteta riskiä ollenkaan.

Yhteenveto – mitä toimenpiteitä tulokset edellyttävät?

- Digi- ja väestötietovirasto arvioi, miten tulokset huomioidaan JUDO-hankkeessa ja erityisesti sen uusissa, valtiovarainministeriön asettaman digiturvalinjausten toimeenpanoa tukevan Haukka-toimeenpano-ohjelman projekteissa.
- Nämä tulokset on esitelty VAHTI-johtoryhmälle 5.3.2020 kokouksessa.
- Toimitamme jokaiselle vastanneelle organisaatiolle tämän yhteenvedon. Organisaatiot voivat verrata omia tuloksiaan näihin ottaen huomioon myös koronaviruspandemian mukanaan tuomat haasteet organisaation normaalin toiminnan toteuttamisessa.
- Käsittelemme tuloksia käynnistyvissä VAHTI-työryhmissä ja mietimme toimenpiteitä, joilla organisaatioita voidaan näiden osalta tukea.

DIGI- JA VÄESTÖTIETOVIRASTO

dvv.fi