VALTIOVARAINMINISTERIÖ

VAHTI

Henkilöstön ja johdon tietoturvabarometri

Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä – VAHTI 3/2016

Julkisen hallinnon ICT

VAHTI 3/2016

Henkilöstön ja johdon tietoturvabarometri

Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä – VAHTI 3/2016

Valtiovarainministeriö, Julkisen hallinnon ICT, Helsinki 2016

Valtiovarainministeriö

ISBN PDF: 978-952-251-812-5

Kuvat ja taulukot: Matti Kuivalainen

Taitto: Valtioneuvoston hallintoyksikkö, Tietotuki- ja julkaisuyksikkö, Anne-Marie Paakkari

Helsinki 2016

Kuvailulehti

Julkaisija	Valtiovarainministeriö		12.12.2016
Tekijät	Matti Kuivalainen, Kimmo Rousku		
Julkaisun nimi	Henkilöstön ja johdon tietoturvabarometri		
Julkaisusarjan nimi ja numero	VAHTI 3/2016		
ISBN painettu	978-952-251-811-8	**ISSN painettu**	1455-2566
ISBN PDF	978-952-251-812-5	**ISSN PDF**	1798-0860
URN-osoite	URN:ISBN:978-952-251-812-5		
Sivumäärä	94	**Kieli**	suomi
Asiasanat	VAHTI, tietoturvallisuus, barometri		

Tiivistelmä

Valtiovarainministeriön asettama Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä (VAHTI) toteutti syksyllä 2016 julkisen hallinnon organisaatioille ja henkilöstölle suunnatun VAHTI-tietoturvabarometrin. Tähän vapaaehtoiseen kyselyyn osallistui 97 organisaatiota: 66 valtionhallinnon ministeriötä, virastoa tai laitosta, 30 kuntaa sekä yksi sairaanhoitopiiri. Mahdollisia vastaajia kyselyyn oli yli 168 000 ja vastauksia saatiin 13 915, jolloin vastausprosentiksi muodostui 8,3 %. Organisaatioiden johdolle esitettiin erikseen 15 lisäkysymystä koskien tietoturvallisuuden tärkeyttä, sen toteuttamisen vaikeutta sekä toteuttamisen onnistumista organisaatiossa. Näihin kysymyksiin saatiin 742 vastausta.

Kyselyssä tuli esiin useita myönteisiä havaintoja, mutta myös kehitettävää. Kyselyn positiivisimpia havaintoja oli se, että vastaajat pitävät tietoturvallisuutta keskeisenä työnteon mahdollistajana (93,1 %). Lisäksi lähes kaikki vastaajat (96,4 %) kokivat olonsa joko hyvin turvalliseksi tai melko turvalliseksi päätelaitteilla työskennellessään. Valtaosa vastaajista (96,2 %) piti myös tietoturvallisuuden toteuttamista organisaatioissa vähintään hyvänä. Johto näki tietoturvallisuuden hyvin tärkeäksi (3,60 asteikolla 1–4), sen toteuttamisen keskivaikeaksi (2,52) ja toteutumisen kohtalaisen hyväksi omassa organisaatiossa (2,82).

Kehittämiskohteeksi nousevat henkilöstön säännöllinen tietoturvallisuuden eri osa-alueet kattava koulutus ja tiedottaminen ajankohtaisista tietoturvallisuuden uhkakuvista. Erityisesti mobiililaitteiden käyttö, häiriötilanteessa toimiminen sekä salasanojen hallinta edellyttävät lisäkoulutusta. Vastaavasti tyytyväisimpiä koulutuksen ja ohjeistuksen määrään oltiin toimitilaturvallisuuden (44,4 %), sähköpostin käytön (43,7 %) ja henkilötietojen käsittelyn (43,5 %) suhteen. Myös teknistä tietoturvallisuutta tulee kehittää edelleen, esimerkiksi ottamalla käyttöön salasanojen hallintaohjelmia sekä tunnistamalla ja estämällä uusia huijauskeinoja.

Kustantaja	Valtiovarainministeriö
Julkaisun myynti/ jakaja	Sähköinen versio: julkaisut.valtioneuvosto.fi Julkaisumyynti: julkaisutilaukset.valtioneuvosto.fi

Presentationsblad

Utgivare	Finansministeriet		12 december 2016
Författare	Matti Kuivalainen, Kimmo Rousku		
Publikationens titel	Personalens och ledningsgruppens barometer för dataskydd		
Publikationsseriens namn och nummer	VAHTI 3/2016		
ISBN tryckt	978-952-251-811-8	**ISSN tryckt**	1455-2566
ISBN PDF	978-952-251-812-5	**ISSN PDF**	1798-0860
URN-adress	URN:ISBN:978-952-251-812-5		
Sidantal	94	**Språk**	finska
Nyckelord	VAHTI, informationssäkerhet, barometer		

Referat

Den styrgrupp för statsförvaltningens informations- och cybersäkerhet (VAHTI) som har tillsatts av finansministeriet genomförde hösten 2016 en dataskyddsbarometer riktad till organisationerna och personalen inom den offentliga förvaltningen. I den frivilliga enkäten deltog 97 organisationer: 66 ministerier, ämbetsverk eller inrättningar inom statsförvaltningen, 30 kommuner och ett sjukvårdsdistrikt. Antalet svarande uppgick till över 168 000 och antalet inkomna svar till 13 915, vilket utgör en svarsprocent på 8,3 %. Till ledningen inom organisationerna ställde man 15 separata, extra frågor om vikten av informationssäkerhet, om svårigheterna med den och om huruvida man lyckats med informationssäkerheten i organisationen. På dessa frågor fick man 742 svar.

I enkäten framfördes många positiva iakttagelser, men även sådant som kan utvecklas. En av de positivaste iakttagelserna var att de svarande anser att informationssäkerheten är en central förutsättning för att kunna sköta arbetet. Nästan alla svarande (96,4 %) upplevde dessutom säkerheten som mycket bra eller ganska bra när de arbetar med terminalutrustning. Största delen av de svarande (96,2 %) ansåg också att informationssäkerheten sköts bra inom organisationerna. Ledningen ansåg att informationssäkerheten är mycket viktig (3,60 på nivån 1–4), att det är medelsvårt att upprätthålla den (2,52) och att den upprätthålls rätt bra i den egna organisationen (2,82).

Barometern visar att det finns ett utvecklingsbehov som gäller att regelbundet ge personalen utbildning om alla olika delområden inom informationssäkerheten samt information om aktuella hotbilder i fråga om den. Särskilt för användningen av mobilutrustning, agerandet i störningssituationer och hanteringen av lösenord krävs det ytterligare utbildning. Mest nöjd med utbildnings- och anvisningsmängden var man när det gällde säkerheten i utrymmen (44,4 %), användningen av e-post (43,7 %) och hanteringen av personuppgifter (43, 5 %).

Även den tekniska informationssäkerheten borde vidareutvecklas t.ex. genom att ta i bruk program för hantering av lösenord samt identifiera och förhindra nya metoder för bedrägeri.

Förläggare	Finansministeriet
Beställningar/ distribution	Elektronisk version: julkaisut.valtioneuvosto.fi Beställningar: julkaisutilaukset.valtioneuvosto.fi

Description sheet

Published by	Ministry of Finance		12 December 2016
Authors	Matti Kuivalainen, Kimmo Rousku		
Title of publication	Information security barometer for personnel and management		
Series and publication number	VAHTI 3/2016		
ISBN (printed)	978-952-251-811-8	**ISSN (printed)**	1455-2566
ISBN PDF	978-952-251-812-5	**ISSN (PDF)**	1798-0860
Website address (URN)	URN:ISBN:978-952-251-812-5		
Pages	94	**Language**	Finnish
Keywords	VAHTI, information security, barometer		

Abstract

Appointed by the Ministry of Finance, the Government Information Security Management Board (VAHTI) completed a VAHTI information safety barometer concerning public administration organisations and personnel in the autumn of 2016. A total of 97 organisations responded to this voluntary survey: 66 central government ministries, offices or institutions, 30 municipalities and one hospital district. The number of potential respondents to the survey exceeded 168,000, 13,915 responses were received, and the response rate was 8.3 per cent. To an additional 15 questions presented separately to the management of the various organisations, 742 responses were received; these questions concerned the importance of information security and the difficulty and success of its implementation within the organisation.

The survey revealed room for improvements, as well as a number of positive findings. One of the most positive findings indicated that the respondents consider information security a key enabler of work (93.1%). In addition, almost all respondents (96.4%) felt either very safe or fairly safe when working on terminal devices. Most respondents (96.2%) also considered the implementation of information security at least good within their respective organisations. The management considered information security very important (3.60 on a scale of 1–4), difficulty in its implementation average (2.52) and realisation fairly good within their organisations (2.82).

Regular staff training in the various aspects of information security and information on current information security threats emerged as issues requiring further development. Additional training is required, particularly in the use of mobile devices, how to act during disruptions and password management. Correspondingly, the respondents were most satisfied with the amount of training and instructions with respect to the security of premises (44.4%), the use of email (43.7%) and the processing of personal data (43.5%). Technical information security is another issue requiring further development, through actions such as the introduction of password management software and the identification and blocking of new methods of online scamming.

Publisher	Ministry of Finance
Publication sales/ Distributed by	Online version: julkaisut.valtioneuvosto.fi Publication sales: julkaisutilaukset.valtioneuvosto.fi

Sisältö

Johdanto

Valtiovarainministeriö vastaa julkisen hallinnon tietoturvallisuuden yleisestä kehittämisestä ja valtionhallinnon tietoturvallisuuden ohjauksesta. Valtiovarainministeriön asettama Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä (VAHTI) toimii julkisen hallinnon tietoturvallisuuden ja tietosuojan kehittämisestä ja ohjauksesta vastaavien hallinnon organisaatioiden yhteistyö-, valmistelu- ja koordinaatioelimenä.

VAHTIn tavoitteena on tieto- ja kyberturvallisuutta kehittämällä parantaa valtionhallinnon toimintojen luotettavuutta, jatkuvuutta, laatua, riskienhallintaa ja varautumista. Tavoitteena on myös edistää tieto- ja kyberturvallisuuden sekä ICT-varautumisen saattamista kiinteäksi osaksi hallinnon toimintaa, johtamista ja tulosohjausta sekä tietojärjestelmien, tietoverkkojen ja ICT-palvelujen kehittämistä, ylläpitoa ja käyttöä. Suomen kyberturvallisuusstrategian mukaisesti VAHTI käsittelee ja yhteen sovittaa valtionhallinnon keskeiset tieto- ja kyberturvallisuuden linjaukset.

Valtiovarainministeriö on toteuttanut vuosittain valtionhallinnon tietoturvakyselyn, VAHTI-kyselyn, organisaatioiden tietoturvakyselynä jo 2000-luvun alkupuolelta lähtien. Näiden kyselyiden tuloksista on raportoitu toimintakertomuksissa. Organisaatiokyselyn mittareiden avulla on voitu seurata, miten eri kehitysohjelmat sekä vuonna 2010 asetettu tietoturvallisuusasetus ovat vaikuttaneet tieto- ja kyberturvallisuuden kehittymiseen valtionhallinnon organisaatioissa. Kunnille VAHTI toteutti vastaavanlaisen kyselyn ensimmäistä kertaa kesällä 2015.

Organisaatiokyselyistä ei käy kuitenkaan tarkalla tasolla ilmi, miten henkilöstö ja johto kokevat tietoturvallisuuden ja kuinka heidän mielestään sitä tulisi kehittää. Täydentääkseen tietoturvallisuuden ohjauksen tietopohjaa valtiovarainministeriö päätti syyskuussa 2015 järjestää vuonna 2016 ensimmäisen henkilöstön ja johdon tietoturvabarometrin. Tämä kysely on vastaajapohjaltaan aiempia kyselyitä huomattavasti laajempi: vastaaminen oli mahdollista kaikille valtionhallinnon organisaatioille, kunnille ja sairaanhoitopiireille.

VAHTI-tietoturvabarometri oli menestys

VAHTIn historian ensimmäistä tietoturvabarometria voidaan pitää erittäin onnistuneena. Kyselyyn osallistui yhteensä 97 vastaajaorganisaatiota valtionhallinnosta ja kuntasektorilta. Kokonaisvastaajamäärä oli 13 915, joista valtiolla työskenteli 6 655 ja kunnissa 7 260 henkeä. Potentiaalisia vastaajia oli yhteensä 168 195 henkeä ja vastausprosentiksi saatiin näin 8,27 %.

Kyselyssä selvitettiin laaja-alaisesti vastaajien kokemuksia ja näkemyksiä tietoturvallisuuden toteutumisesta heidän omassa organisaatiossaan. Näin saatiin valtiovarainministeriön sekä osallistujaorganisaatioiden käyttöön tietoa tietoturvallisuuden tilasta ja kehittämistarpeista. Lisäksi saatiin hyvä yleiskuva tietoturvallisuuden toteutumisesta julkishallinnossa henkilöstön ja johdon näkökulmasta.

Tietoturvabarometrin tuloksien perusteella tietoturvallisuuden edistäminen ei ole kiinni ainakaan asenteista. Suurin osa vastaajista oli sitä mieltä, että tietoturvallisuus mahdollistaa laadukkaan toiminnan ja antaa heidän organisaatioistaan luotettavan kuvan. Tätä havaintoa tukee se, että organisaation johtoryhmään kuuluvat kokivat eri tietoturvallisuuden osa-alueet pääsääntöisesti erittäin tärkeiksi.

Vastaajien turvallisuudentunne päätelaitteilla työskennellessä oli korkea ja huolestuneisuus eri uhista yleensä olematonta tai vähäistä. Turvallisuudentunne ja huolestuneisuudenpuute eivät ole kuitenkaan linjassa vastaajien saaman koulutuksen ja ohjeistuksen määrän kanssa: ainoastaan 29,7 % vastaajista koki saaneensa eri tietoturvallisuuden osa-alueisiin riittävästi koulutusta. Esimiehiä ja johtoa oli koulutettu enemmän, mutta ei kuitenkaan riittävästi, joka ilmenee esimerkiksi avovastauksissa. Tuttu väittämä ”henkilöstö on tietoturvallisuuden heikoin lenkki” voidaan kuitenkin kumota ennen kaikkea ohjeistamalla ja kouluttamalla – osaava, uhkiin reagoiva henkilöstö on merkittävä voimavara turvallisuuden toteuttamisessa.

Merkittäviä tietoturvapoikkeamia on raportoitu Suomessa viime vuosina verrattain vähän, ja tämä voi olla yksi syy hyvään turvallisuudentunteeseen. Jatkossa onkin mielenkiintoista verrata, miten tässä kyselyssä luotujen mittarien tulokset vertautuvat mahdollisiin tuleviin kyselyihin.

Tietoturvallisuudessa ja sen mahdollistamassa toiminnan digitalisaatiossa ei onnistuta ilman koulutusta ja ohjeistusta. Saadun tietoturvakoulutuksen ja -ohjeistuksen oletettua pienempi määrä onkin mielenkiintoinen, mutta myös hälyttävä ilmiö. Koulutukseen ja ohjeistukseen panostaminen sekä yleisellä että organisaatiotasolla on välttämätöntä. Havaitut puutteet ja riskit voidaan kääntää osaamiseksi ja mahdollisuuksiksi. Riittävällä kou-

lutuksella ja ohjeistuksella voidaan parantaa sekä käytännön tason toiminnan tietoturvallisuutta, että turvallisuudentunnetta entisestään.

Koulutus ja ohjeistus sekä turvallisuudentunne olivat valtionhallinnossa kuntasektoria korkeammalla tasolla. Kuntasektorin valtionhallintoa hieman vaatimattomammat tulokset voivat johtua esimerkiksi siitä, että tietoturvallisuuden kehittäminen ei ole samalla tavalla vakiintunutta ja verkostomaista kuin valtionhallinnossa, jossa VAHTI on vastannut kehittämisestä kahdenkymmenen vuoden ajan. Lisäksi valtionhallintoa koskee vuonna 2010 voimaan astunut tietoturvallisuuden kouluttamista edellyttävä tietoturvallisuusasetus. Näitä havaintoja tukee myös vuonna 2015 kunnille toteutettu valtiovarainministeriön toteuttama VAHTI-kuntien tietoturvakysely.

Raportin keskeisin havainto on, että koulutusta tulee selvästi kehittää. Valtiovarainministeriön on mahdollista toteuttaa VAHTIn ja yhdessä sidosryhmien kanssa kustannustehokkaasti kattava julkishallinnon koulutuskokonaisuus, joka käsittelee tässä raportissa tunnistettuja kehittämistä edellyttäviä osa-alueita.

VAHTI tietoturvabarometri on laajuudeltaan kansainvälisestikin arvioituna merkittävä tietoturvallisuuden tilan selvitys. Jotta tietoturvallisuuden tarjoamat mahdollisuudet saataisiin hyödynnettyä, on kyselyssä esiin tulleisiin tarpeisiin vastattava. Tietoturvallisuuteen liittyvät asenteet paranevat entisestään, kun perusasioihin, kuten koulutukseen ja ohjeistukseen, toimiviin ohjelmiin, salasanojen hallintaan sekä turvallisiin toimitiloihin, kiinnitetään huomiota.

VAHTIn tehtävänä on tukea koko julkishallintoa tietoturvallisuuden kehittämisessä. VAHTIn toimintaan eri tavoin osallistuvat tahot ovat tässä työssä korvaamaton apu. Kiitos tämän tietoturvabarometrin onnistumisesta kuuluu kaikille niille toimijoille, jotka olivat mukana valmistelemassa ja toteuttamassa kyselyä, sekä osallistuneille organisaatioille ja niiden henkilöstölle. Tietoturvallisuus tehdään yhdessä.

Keskeiset havainnot ja suositukset

Tietoturvallisuutta koskevat asenteet ja tarpeet

Tietoturvabarometrin tuloksien perusteella asennoituminen tietoturvallisuuteen on erittäin myönteistä. Peräti 60,8 % vastaajista oli sitä, mieltä että tietoturvallisuus mahdollistaa laadukkaan toiminnan ja antaa heidän organisaatioistaan luotettavan kuvan. Vastaajista 32,3 % oli sitä mieltä, että tietoturvallisuutta tarvitaan, jotta he voivat käsitellä työssään tarvitsemiaan tietoja. Lisäksi 6,7 % ymmärsi tietoturvan merkityksen, vaikka se aiheutti toisinaan ylimääräistä työtä. Ainoastaan 0,2 % piti tietoturvaa toimintaansa haittaavana tekijänä. Tietoturvallisuus on siis suuren enemmistön mielestä *laadukkaan toiminnan tarpeellinen mahdollistaja*. Tätä havaintoa tukee se, että johto koki tietoturvallisuuden eri osa-alueet pääsääntöisesti erittäin tärkeiksi.

Jotta tietoturvallisuuden tarjoamat mahdollisuudet saataisiin hyödynnettyä, on kyselyssä esiin tulleisiin tarpeisiin vastattava. Avovastauksissa korostuivat muun muassa toimitilaturvallisuuden, ajantasaisten ja päivitettyjen ohjelmien sekä selkeiden roolien ja vastuiden tarve - koulutusta ja ohjeistusta unohtamatta. Tietoturvallisuuden edistämisessä on siis kyse suurelta osin perusasioista huolehtimisesta. Salasanojen hallinnan ja sähköpostin käytön toivotaan olevan helpompaa. Salasanojen turvallisuutta voidaan parantaa kohdistetulla ohjeistuksella sekä ottamalla käyttöön kustannustehokkaita salasanojen hallintaohjelmistoja.

Avoimiin kysymyksiin saadut vastaukset keskittyivät ongelmiin, mikä saattaa vaikuttaa ristiriitaiselta suhteessa vastaajien muutoin myönteiseen asenteeseen tietoturvaa kohtaan. Avoimissa kysymyksissä selvitettiin kehittämistarpeita sekä tietoturvallisuuden ongelmakohtia, ja nämä näkökulmat korostuvat siksi vastauksissa. Sitä, mikä tietoturvallisuudessa oli jo toteutettu *hyvin*, ei kysytty, ja tämä tulee ottaa huomioon raportin tuloksia tulkittaessa.

Turvallisuudentunne suhteessa koulutukseen ja ohjeistukseen

Vastaajista lähes kaikki (96,4 %) koki olonsa joko hyvin turvalliseksi tai melko turvalliseksi päätelaitteilla työskennellessään. Heille tärkeät tietoturvallisuuden osa-alueet eivät keskimäärin joko huolestuttaneet ollenkaan (52 %) tai huolestuttivat vain vähän (37,4 %). Turvallisuudentunne oli siis korkea ja huolestuneisuus eri uhista yleensä olematonta tai vähäistä. Kuntasektorilla turvallisuudentunne oli hieman valtionhallintoa matalammalla tasolla ja huolestuneisuus suurempaa.

Turvallisuudentunne ja huolestuneisuudenpuute eivät ole kuitenkaan linjassa vastaajien saaman koulutuksen ja ohjeistuksen määrän kanssa. Ainoastaan 29,7 % vastaajista oli saanut eri tietoturvallisuuden osa-alueisiin keskimäärin riittävästi koulutusta. Jonkin verran koulutusta ja ohjeistusta oli saanut 39,8 %. Keskimäärin 22,1 % ilmoitti, ettei ollut saanut

eri osa-alueisiin ollenkaan koulutusta ja ohjeistusta. Valtionhallinnossa tilanne oli jonkin verran kuntasektoria parempi. Valtionhallinnon kuntasektoria parempi turvallisuudentunne ja vähäisempi huolestuneisuus saattaa siis olla seurausta siitä, että koulutusta ja ohjeistusta oli saatu enemmän.

Vastaajat kokivat päätelaitteilla työskentelyn varsin turvalliseksi, mutta samanaikaisesti myös tietoturvallisuuskoulutuksen ja -ohjeistuksen riittämättömäksi, mikä on sekä mielenkiintoinen että huolestuttava havainto. Tilanne oli huolestuttava esimerkiksi mobiililaitteiden käytön osalta. Huolimatta siitä, että työskentely päätelaitteilla koettiin turvalliseksi, ainoastaan 18,0 % vastaajista ilmoitti, että oli saanut riittävästi koulutusta ja ohjeistusta mobiililaitteiden käyttöön. Vastaajista 31,3 % ilmoitti, ettei tarpeesta huolimatta ollut saanut ollenkaan koulutusta ja ohjeistusta. Tietoturvaan tulisikin panostaa alusta alkaen, kuten eräs vastaaja totesi.

> ”Tietoturvallisuuteen liittyvät asiat pitäisi ohjeistaa kaikille työntekijöille heti ensimmäisenä työpäivänä ja olla osa perehdytystä.”

Riittävän koulutuksen ja ohjeistuksen puute ei siis aiheuta heikkoa turvallisuudentunnetta. Kyse voi olla esimerkiksi siitä, että saatua koulutusta ja ohjeistusta ei välttämättä tunnisteta, tai henkilö on saanut koulutusta ja osaamista vapaa-ajalla. Vastaajat eivät myöskään todennäköisesti tunnista kaikkia niitä riittämättömään koulutukseen ja ohjeistukseen liittyviä riskejä, joita he kohtaavat työssään. Saattaa olla, että vastaajien luottamus omiin taitoihinsa on korkealla, vaikka he havaitsevatkin saamansa koulutuksen ja ohjeistuksen riittämättömyyden.

Valtionhallinnon ja kuntasektorin vertailusta

Kuten aiemmasta kävi ilmi, kuntasektorilla on valtionhallintoa jonkin verran enemmän kehitettävää. Koulutus ja ohjeistus, turvallisuudentunne ja huolestuneisuus olivat valtiolla paremmalla tasolla kuin kunnissa. Kuitenkin myös valtionhallinnossa oli runsaasti kehittämistarpeita, eivätkä tulokset olleet kaikin osin odotetulla tasolla. Kuntasektorilla tietyt osa-alueet, kuten tietojen luokittelu sekä henkilötietojen käsittelyyn liittyvä ohjeistus ja koulutus, oli valtionhallintoa paremmin toteutettu.

Kuntasektorin valtionhallintoa hieman heikommat tulokset voivat johtua esimerkiksi siitä, että tietoturvallisuuden kehittäminen ei ole samalla tavalla vakiintunutta ja verkostomaista kuin valtionhallinnossa. Tähän vaikuttaa merkittävästi myös valtionhallintoa velvoittava tietoturvallisuusasetus, joka astui voimaan vuonna 2010. VAHTIn toteuttamissa organisaation tieto- ja kyberturvallisuuskyselyissä on havaittu valtionhallinnon vastaustuloksissa kokonaisuutena yli 10 % parannus, yksittäisissä osa-alueissa yli 30 % parannus asetuksen

voimaantulon jälkeen. Valtionhallinnon tietoturvallisuus on siis kehittynyt mitattavasti parempaan suuntaan vuosina 2011–2015.

Kuntien vastaajat olivat keskimäärin työskennelleet valtiolla työskenteleviä lyhyemmän aikaa, mikä voi osaltaan selittää esimerkiksi koulutuksen ja ohjeistuksen heikompaa tilaa kuntasektorilla. Kuntien vastaajista 38 % oli ollut työssään 0–5 vuotta, kun valtiolla vastaava lukema oli 33 %. Sisällyttämällä tietoturvakoulutus osaksi uusien työntekijöiden perehdytystä tuloksia voitaneen parantaa oleellisesti.

Havaintoihin perustuvat suositukset

Tietoturvallisuus on digitalisaation mahdollistaja

VAHTIn henkilöstön ja johdon tietoturvabarometrin tuloksissa korostuu se, että vastaajat suhtautuvat vakavasti ja myönteisesti tietoturvaan. Tässä raportissa havaitut kehittämistarpeet tulee ottaa huomioon koko julkishallinnossa, kun tietoturvallisuutta kehitetään edelleen. Kyselyyn osallistuneet korostivat tätä avovastauksissaan.

> ”Toivottavasti vastaukset aiheuttavat myös harkittuja ja järkeviä jatkotoimenpiteitä.”

> ”Toivoisin, että Suomessa ruvettaisiin käyttämään aikaa turvallisuuden kehittämiseen ja palauttamiseen kaikilta osa-alueilta.”

Tietoturvallisuutta pidetään jo itsessään tärkeänä. Ennen kaikkea se on kuitenkin laadukkaan toiminnan mahdollistaja. Riittävä tietoturvallisuuden taso on keskeisessä roolissa, kun toimintaa digitalisoidaan. Ilman tietoturvallisuutta ei ole toiminnan digitalisaatiota, robotisaatiota tai muita keskeisiä tulevaisuuden yhteiskunnallisia menestystekijöitä. Tietoturvallisuuden tulisi olla rakennettuna sisään kaikkeen toimintaan ”security by design” -periaatteella. Samalla tavalla tulisi toimia myös tietosuojan kanssa henkilötietoja käsittelevissä prosesseissa ja tietojärjestelmissä (”privacy by design”).

Koulutukseen ja ohjeistukseen on kiinnitettävä huomiota

Tietoturvallisuudessa ja sen mahdollistamassa toiminnan digitalisaatiossa ei onnistuta ilman koulutusta ja ohjeistusta. Saadun tietoturvakoulutuksen ja -ohjeistuksen vähäinen määrä on mielenkiintoinen, mutta myös hälyttävä ilmiö. Koulutukseen ja ohjeistukseen panostaminen sekä koko julkishallinnossa, että kunkin organisaation tasolla on välttämätöntä. Julkishallinnon työntekijöiden turvallisuudentunne on korkealla tasolla huolimatta siitä, että koulutuksen ja ohjeistuksen määrä koetaan riittämättömäksi. Lisäkoulutuksella

ja -ohjeistuksella voidaan parantaa sekä tietoturvallisuutta että turvallisuudentunnetta entisestään.

Koulutuksessa ja ohjeistuksessa on kyse suurelta osin perusasioista.. Eräs kyselyä kiitellyt vastaaja antoi konkreettisia ehdotuksia koulutuksen ja ohjeistuksen kehittämiseksi.

> ”Hyvä, että kysely järjestettiin. Verkkokoulu ja osaamistesti voisivat auttaa suuntaamaan koulutusta kehittämiskohteisiin. Lisäksi voitaisiin järjestää eri teema-alueille suuntautuvaa tietoturvakoulutusta esimerkiksi virustorjunnasta, salasanakäytännöistä, henkilötietojen käsittelystä, tietosuojasta ja mobiililaitteiden tietoturvasta.”

Koulutuksessa ja ohjeistuksessa havaitut puutteet ja riskit on pyrittävä kääntämään osaamiseksi ja mahdollisuuksiksi. Mobiililaitteiden käytön ohjeistusta tietoturvallisuus mukaan luettuna tulee lisätä, koska tulevaisuudessa niillä tehdään yhä suurempi osa töistä – joustavasti, ajasta ja paikasta riippumatta. Näiden mahdollisuuksien lisäämiseen tullaan kiinnittämään huomiota myös VAHTIn toiminnassa. On myös otettava huomioon, että pelkkä koulutus ja ohjeistus eivät riitä, vaan myös teknisen tietoturvan tulee olla kunnossa ja kehittyä uhkatilanteen kehittymisen myötä.

Uudistuva VAHTI laatii tulosten perusteella koulutuksen kehittämisohjelman

Vuonna 2017 kaksikymmentä vuotta täyttävän VAHTIn toiminta painottuu aiempaa enemmän työryhmiin. VAHTI tulee edelleen vastaamaan tietoturvallisuuden kehittämisestä valtionhallinnossa ja toimimaan entistä keskeisemmässä roolissa myös julkisessa hallinnossa.

Kyselyn tulokset vahvistivat sitä käsitystä, että jatkossakin kuntien kannattaa hyödyntää VAHTIn kehittämiä hyviä toimintamalleja. Yhteistyö Julkisen hallinnon tietohallinnon neuvottelukunnan (JUHTA) asettaman tietoturvan, tietosuojan, ja varautumisen asiantuntijaryhmän kanssa antaa entistä paremmat valmiudet koko julkisen hallinnon turvallisuuden kehittämiseen.

VAHTIn toiminnassa pyritään jatkuvasti tieto- ja kyberturvallisuuden vaikuttavuuden lisäämiseen sekä tietosuojan toteutumisen edistämiseen. Kuten VAHTIn toiminnan tuloksia yleensä, voidaan myös tämän raportin löydöksiä hyödyntää julkishallinnon lisäksi myös yhteiskunnassa ja yrityksissä. VAHTI itse tulee hyödyntämään tietoturvabarometrin tuloksia omaa toimintaansa suunnitellessaan ja toteuttaessaan.

Koulutuksen ja ohjeistuksen kehittämisen tukeminen on tietoturvabarometrin tulosten perusteella VAHTIn toiminnassa erityisen tärkeää.

Inledning

Finansministeriet ansvarar för den allmänna utvecklingen av informationssäkerheten inom den offentliga förvaltningen och styrningen av informationssäkerheten inom statsförvaltningen. Finansministeriet har tillsatt Ledningsgruppen för informations- och cybersäkerheten inom statsförvaltningen (VAHTI) som samarbets-, berednings- och samordningsorgan för organisationer som svarar för utveckling och styrning av informationssäkerheten och dataskyddet inom den offentliga förvaltningen.

VAHTI har som mål att förbättra pålitligheten, kontinuiteten, kvaliteten, riskhanteringen och beredskapen i statsförvaltningens verksamhet genom att utveckla informations- och cybersäkerheten. Dessutom vill man främja integrationen av informations- och cybersäkerheten samt ICT-beredskapen till en fast del av verksamheten, ledandet och resultatstyrningen inom förvaltningen samt främja utvecklandet, underhållet och användningen av informationssystem, datanät och ICT-tjänster. I enlighet med strategin för cybersäkerheten i Finland behandlar och samordnar VAHTI de centrala riktlinjerna för statsförvaltningens informations- och cybersäkerhet.

Sedan början av 2000-talet har Finansministeriet varje år genomfört en VAHTI-enkät om dataskyddet inom statsförvaltningen i form av en enkät om organisationernas dataskydd. Resultaten från dessa enkäter har rapporterats i verksamhetsberättelserna. Med organisationsenkätens mätare har det varit möjligt att följa upp på vilket sätt olika utvecklingsprogram och förordningen om informationssäkerhet utfärdad 2010 har påverkat utvecklingen av informations- och cybersäkerheten i organisationerna inom statsförvaltningen. VAHTI genomförde en motsvarande enkät för kommunerna första gången sommaren 2015.

Av organisationsenkäterna framgår dock inte exakt på vilket sätt personalen och ledningen har upplevt informationssäkerheten och hur informationssäkerheten enligt dem bör utvecklas. För att komplettera informationsunderlaget för styrning av informationssäkerheten beslutade Finansministeriet i september 2015 att genomföra en första informationssäkerhetsbarometer för personalen och ledningen under 2016. När det gäller antalet svarspersoner är denna enkät betydligt mer omfattande än de tidigare enkäterna: alla organisationer inom statsförvaltningen, kommunerna och sjukvårdsdistrikten har haft möjlighet att svara på enkäten.

VAHTI-informationssäkerhetsbarometern var en framgång

Den första informationssäkerhetsbarometern i VAHTIs historia kan anses vara mycket framgångsrik. I enkäten deltog sammanlagt 97 svarsorganisationer inom statsförvaltningen och den kommunala sektorn. Det totala antalet svarspersoner var 13 915, av vilka 6 655 personer arbetade inom staten och 7 260 personer inom kommunerna. Antalet potentiella svarspersoner var 168 195 och svarsprocenten var på så sätt 8,27.

I enkäten utreddes inom flera olika områden svarspersonernas erfarenheter och åsikter om hur informationssäkerheten har genomförts i deras organisationer. På så sätt erhölls information om informationssäkerhetens läge och utvecklingsbehov, som Finansministeriet och deltagarorganisationerna kan utnyttja. Dessutom erhölls en bra allmän bild av genomförandet av informationssäkerheten inom den offentliga förvaltningen ur personalens och ledningens synvinkel.

Utifrån resultaten från informationssäkerhetsbarometern är det åtminstone inte attityderna som utgör ett hinder för att främja informationssäkerheten. Största delen av svarspersonerna ansåg att informationssäkerheten möjliggör en högklassig verksamhet och ger en tillförlitlig bild av deras organisationer. Denna iakttagelse stöds av att de personer som hörde till organisationens ledningsgrupp ansåg att de olika delområdena av informationssäkerheten huvudsakligen var mycket viktiga.

Svarspersonernas säkerhetskänsla i arbetet med terminaler var hög och oron för olika hot i regel obefintlig eller liten. Säkerhetskänslan och bristen på oro ligger dock inte i linje med svarspersonernas utbildning och mängden anvisningar: endast 29,7 procent av svarspersonerna ansåg att de hade fått tillräcklig utbildning i de olika delområdena av informationssäkerheten. Cheferna och ledningen hade fått mer utbildning men inte tillräckligt, vilket framgår bland annat av öppna svar. Det kända påståendet ”personalen är den svagaste länken i informationssäkerheten” kan dock dementeras framför allt genom att ge anvisningar och utbildning – en kompetent personal som reagerar på hot är en betydande resurs vid genomförande av säkerhet.

De senaste åren har tämligen få betydande informationssäkerhetsincidenter rapporterats i Finland, vilket kan vara en orsak till en bra säkerhetskänsla. Därför är det framöver intressant att jämföra hur resultaten från de mätare som tagits fram för denna enkät kan jämföras med eventuella framtida enkäter.

Utan utbildning och anvisningar är det omöjligt att lyckas i informationssäkerheten och den digitalisering av verksamhet som informationssäkerheten möjliggör. Utbildningen i och anvisningarna om informationssäkerhet har varit mindre än väntat, vilket är en intressant men också oroväckande företeelse. Satsning på utbildning och anvisningar är nöd-

vändig på både en allmän nivå och organisationsnivå. Upptäckta brister och risker kan omvandlas till kompetens och möjligheter. Genom tillräcklig utbildning och tillräckliga anvisningar är det möjligt att ytterligare förbättra såväl informationssäkerheten i det praktiska arbetet som säkerhetskänslan.

Utbildningen och anvisningarna samt säkerhetskänslan låg på högre nivå inom statsförvaltningen än den kommunala sektorn. Resultaten var en aning sämre inom den kommunala sektorn än statsförvaltningen. Detta kan bero exempelvis på att utvecklingen av informationssäkerheten inte är på samma sätt etablerad inom den kommunala sektorn som statsförvaltningen, där VAHTI har svarat för utvecklingen under de senaste tjugo åren. Dessutom omfattas statsförvaltningen av informationssäkerhetsförordningen som trädde i kraft 2010 och som förutsätter utbildning i informationssäkerhet. Dessa iakttagelser stöds också av en enkät om informationssäkerheten i VAHTI-kommunerna, som Finansministeriet genomförde för kommunerna 2015.

Den viktigaste iakttagelsen i rapporten är att utbildningen bör utvecklas betydligt. Finansministeriet har möjlighet att i samarbete med VAHTI och intressenterna på ett kostnadseffektivt sätt genomföra en omfattande utbildningshelhet för den offentliga förvaltningen, som behandlar de delområden som behöver utvecklas och som har identifierats i denna rapport.

Till omfattningen är VAHTI-informationssäkerhetsbarometern även i internationell jämförelse en viktig utredning om informationssäkerhetens läge. För att de möjligheter som informationssäkerheten medför ska kunna utnyttjas, bör de behov som framkom i enkäten tillgodoses. Attityderna mot informationssäkerheten förbättras ytterligare när uppmärksamhet fästs vid de grundläggande frågorna, som utbildning och anvisningar, fungerande program, administration av lösenord samt säkra och trygga verksamhetslokaler.

VAHTIs uppgift är att stöda hela den offentliga förvaltningen i att utveckla informationssäkerheten. De som på olika sätt deltar i VAHTIs verksamhet är en oersättlig hjälp i detta arbete. För att denna informationssäkerhetsbarometer har lyckats får vi tacka alla de aktörer som var med och beredde och genomförde enkäten samt de deltagande organisationerna och deras personal. Vi bygger upp informationssäkerhet tillsammans.

De viktigaste iakttagelserna och rekommendationerna

Attityder och behov i fråga om informationssäkerheten

Utifrån resultaten från informationssäkerhetsbarometern är attityderna mot informationssäkerheten mycket positiva. Hela 60,8 procent av svarspersonerna ansåg att informationssäkerheten möjliggör en högklassig verksamhet och ger en tillförlitlig bild av deras organisationer. Totalt 32,3 procent av svarspersonerna ansåg att informationssäkerhet behövs för att de ska kunna behandla de uppgifter som de behöver i sitt arbete. Dessutom förstod 6,7 procent hur viktig informationssäkerheten är trots att den ibland medför extra arbete. Endast 0,2 procent ansåg att informationssäkerheten är en faktor som utgör hinder i arbetet. Enligt majoriteten är informationssäkerheten med andra ord en behövlig faktor som möjliggör en högklassig verksamhet. Denna iakttagelse stöds av att de personer som hörde till ledningen ansåg att de olika delområdena av informationssäkerheten huvudsakligen var mycket viktiga.

För att de möjligheter som informationssäkerheten medför ska kunna utnyttjas, bör de behov som framkom i enkäten tillgodoses. I de öppna svaren betonades behovet av bland annat säkerhet i verksamhetslokalerna, aktuella och uppgraderade program samt tydliga roller och ansvarsområden, utan att glömma utbildning och anvisningar. I främjandet av informationssäkerheten är det på så sätt till en stor del fråga om att sörja för de grundläggande frågorna. Administrationen av lösenord och användningen av e-posten önskas vara enklare. Lösenordens säkerhet kan förbättras genom riktade anvisningar och genom att införa kostnadseffektiva program för administration av lösenord.

Svaren på de öppna frågorna handlade främst om problem, vilket kan verka motstridigt med svarspersonernas överlag positiva attityder mot informationssäkerheten. I de öppna frågorna utreddes utvecklingsbehov och problem med informationssäkerheten, och därför betonas dessa synpunkter i svaren. Svarspersonerna tillfrågades inte vad man har gjort bra när det gäller informationssäkerheten, och detta bör beaktas när resultaten i rapporten tolkas.

Säkerhetskänsla i relation till utbildningen och anvisningarna

Nästan alla (96,4 %) av svarspersonerna ansåg att de känner sig mycket säkra eller ganska säkra när de arbetar med terminaler. De delområden av informationssäkerheten som var viktiga för svarspersonerna bekymrade i genomsnitt inte svarspersonerna alls (52 %) eller bekymrade dem endast föga (37,4 %). Säkerhetskänslan var med andra ord hög och oron för olika hot i regel obefintlig eller liten. Säkerhetskänslan var en aning lägre och oron större inom den kommunala sektorn än statsförvaltningen.

Säkerhetskänslan och bristen på oro ligger dock inte i linje med svarspersonernas utbildning och mängden anvisningar. Endast 29,7 procent av svarspersonerna hade i genomsnitt fått tillräcklig utbildning i de olika delområdena av informationssäkerheten. Sammanlagt 39,8 procent hade fått utbildning och anvisningar i liten omfattning. I genomsnitt 22,1 procent angav att de inte hade fått vare sig utbildning eller anvisningar i de olika delområdena. Läget var något bättre inom statsförvaltningen än den kommunala sektorn. Orsaken till att säkerhetskänslan var högre och oron mindre inom statsförvaltningen än den kommunala sektorn kan därför vara en följd av att svarspersonerna hade fått utbildning och anvisningar i större omfattning.

Svarspersonerna ansåg att arbetet med terminaler var synnerligen säkert, men att informationssäkerhetsutbildningen och -anvisningarna samtidigt var otillräckliga. Detta är både en intressant och en oroväckande iakttagelse. Läget var oroväckande till exempel när det gäller användningen av mobila enheter. Trots att arbetet med terminaler ansågs vara säkert, angav endast 18,0 procent att de hade fått tillräcklig utbildning och tillräckliga anvisningar om användning av mobila enheter. Totalt 31,3 procent av svarspersonerna angav att de trots behovet inte hade fått vare sig utbildning eller anvisningar. Man bör satsa på informationssäkerheten från början, som en svarsperson konstaterade.

> ”Samtliga anställda bör ges anvisningar om informationssäkerheten genast på den första arbetsdagen och informationssäkerhetsfrågorna bör vara en del av arbetsintroduktionen.”

Bristen på tillräcklig utbildning och tillräckliga anvisningar orsakar med andra ord inte en svag säkerhetskänsla. Det kan till exempel vara fråga om att den utbildning och de anvisningar som har fåtts inte nödvändigtvis identifieras eller att personen har fått utbildning och kunskaper och färdigheter på fritiden. Dessutom identifierar svarspersonerna sannolikt inte alla de risker med otillräcklig utbildning och otillräckliga anvisningar som de möter i arbetet. Det är möjligt att svarspersonernas förtroende för sina kunskaper och färdigheter är högt trots att de märker att utbildningen och anvisningarna är otillräckliga.

Jämförelse mellan statsförvaltningen och den kommunala sektorn

Som det ovan framgått, har den kommunala sektorn fler områden som bör utvecklas än statsförvaltningen. Utbildning och anvisningar, säkerhetskänsla och oro låg på en bättre nivå inom staten än kommunerna. Statsförvaltningen hade dock också gott om utvecklingsbehov och resultaten låg inte till alla delar på den väntade nivån. Vissa delområden, som klassificering av uppgifter samt anvisningar om och utbildning i behandling av personuppgifter, hade genomförts bättre inom den kommunala sektorn än statsförvaltningen.

Resultaten var en aning sämre inom den kommunala sektorn än statsförvaltningen. Detta kan bero exempelvis på att utvecklingen av informationssäkerheten inte är på samma sätt etablerad och nätverksliknande inom den kommunala sektorn som statsförvaltningen. Detta påverkas betydligt av informationssäkerhetsförordningen som förpliktar statsförvaltningen och som trädde i kraft 2010. I VAHTIs enkäter om organisationens informations- och cybersäkerhet har statens svarsresultat som en helhet förbättrats med över 10 procent och i fråga om de enskilda delområdena med över 30 procent efter att förordningen trädde i kraft. Med andra ord har informationssäkerheten inom statsförvaltningen utvecklats i en mer positiv riktning 2011–2015.

Svarspersonerna inom kommunerna hade i genomsnitt arbetat inom kommunerna under en kortare tid än svarspersonerna inom staten. Detta kan vara en orsak exempelvis till det sämre läget inom den kommunala sektorn vad gäller utbildning och anvisningar. Av svarspersonerna inom kommunerna hade 38 procent arbetat inom kommunen i 0–5 år medan motsvarande siffra inom staten var 33 procent. Resultaten kan förmodligen förbättras väsentligt om informationssäkerhetsutbildning inkluderas i arbetsintroduktionen för nya anställda.

Rekommendationer utifrån iakttagelserna

Informationssäkerheten möjliggör digitalisering

I resultaten från VAHTIs informationssäkerhetsbarometer för personal och ledning betonas att svarspersonerna förhåller sig allvarliga och positiva till informationssäkerheten. De utvecklingsbehov som har upptäckts i denna rapport bör beaktas inom hela den offentliga förvaltningen när informationssäkerheten vidareutvecklas. Deltagarna i enkäten underströk detta i sina öppna svar.

> ”Förhoppningsvis ger svaren också upphov till begrundade och kloka fortsatta åtgärder.”

> ”Jag hoppas att man i Finland börjar använda mer tid på att utveckla säkerheten och återställa den när det gäller alla delområden.”

Informationssäkerheten betraktas redan i sig som viktig. Framför allt är den dock en faktor som möjliggör en högklassig verksamhet. En tillräcklig informationssäkerhetsnivå har en viktig roll när verksamhet digitaliseras. Utan informationssäkerhet finns ingen digitalisering av verksamhet, robotisering eller andra viktiga samhälleliga framgångsfaktorer i framtiden. Informationssäkerheten bör vara inbyggd i all verksamhet enligt principen ”security

by design". På samma sätt bör man också agera med dataskyddet i processer och datasystem som behandlar personuppgifter ("privacy by design").

Uppmärksamhet bör fästas vid utbildning och anvisningar

Utan utbildning och anvisningar är det omöjligt att lyckas i informationssäkerheten och den digitalisering av verksamhet som informationssäkerheten möjliggör. Utbildningen i och anvisningarna om informationssäkerhet har varit obetydliga, vilket är en intressant men också oroväckande företeelse. Satsning på utbildning och anvisningar är nödvändig både inom hela den offentliga förvaltningen och i varje organisation. Säkerhetskänslan hos de anställda inom den offentliga förvaltningen ligger på en hög nivå trots att mängden utbildning och anvisningar anses vara otillräcklig. Både informationssäkerheten och säkerhetskänslan kan förbättras ytterligare genom tilläggsutbildning och -anvisningar.

I utbildning och anvisningar är det till en stor del fråga om grundläggande frågor. En svarsperson som berömde enkäten gav konkreta förslag för att utveckla utbildningen och anvisningarna.

> "Det är bra att enkäten genomfördes. En webbskola och ett kompetenstest kan hjälpa till att rikta utbildning till olika utvecklingsområden. Dessutom kan man ordna informationssäkerhetsutbildning med olika teman, till exempel virusbekämpning, lösenordsprinciper, behandling av personuppgifter, dataskydd och informationssäkerhet i mobila enheter.

De brister och risker som har upptäckts i utbildningen och anvisningarna bör kunna omvandlas till kompetens och möjligheter. Anvisningarna om användning av mobila enheter, inbegripet informationssäkerhet, bör utökas, eftersom en allt större del av arbetet i framtiden utförs med mobila enheter – smidigt oberoende av tid och plats. Även i VAHTIs verksamhet kommer uppmärksamhet att fästas vid att öka dessa möjligheter. Dessutom ska det beaktas att utbildning och anvisningar ensamt inte räcker till, utan att den tekniska informationssäkerheten också ska vara i ordning och förbättras om hotläget utvecklas.

VAHTI som förnyas kommer att skapa ett program för utveckling av utbildning utifrån resultaten

VAHTI, som fyller tjugo år 2017, kommer att fokusera en allt större del av sin verksamhet på arbetsgrupper. VAHTI kommer fortfarande att svara för utvecklingen av informationssäkerheten inom statsförvaltningen och ha en allt viktigare roll även inom den offentliga förvaltningen.

Resultaten från enkäten stärkte uppfattningen om att kommunerna även framöver bör utnyttja de bra verksamhetsmodeller som VAHTI har tagit fram. Samarbetet med den sakkunniggrupp för informationssäkerhet, dataskydd och beredskap som tillsatts av delegationen för informationsförvaltningen inom den offentliga förvaltningen (JUHTA) ger allt bättre färdigheter att utveckla säkerheten inom hela den offentliga förvaltningen.

VAHTIs verksamhet strävar kontinuerligt efter att öka genomslagskraften i informations- och cybersäkerheten och att främja dataskyddet. Resultaten i denna rapport kan på samma sätt som resultaten av VAHTIs verksamhet i allmänhet utnyttjas både inom den offentliga förvaltningen och i samhället och företag. VAHTI kommer självt att utnyttja resultaten från informationssäkerhetsbarometern när det planerar och genomför sin verksamhet.

Utifrån resultaten från barometern är det i VAHTIs verksamhet särskilt viktigt att man stöder utvecklingen av utbildningen och anvisningarna.

Introduction

The Ministry of Finance is responsible for the general development of the information security of public administration and the steering of the information security of the central government. The Steering Group for Information and Cybersecurity in the Central Government (VAHTI) appointed by the Ministry of Finance acts as the cooperation, preparation and coordination body of the administrative organisations responsible for the development and steering of public administration information security and data protection.

The objective of VAHTI is to improve the reliability, continuity, quality, risk management and preparedness of the central government's functions through the development of information and cybersecurity. Another objective is to promote making information and cybersecurity and ICT preparedness an integral part of the operation, management and performance management of the administration, and the development, maintenance and use of information systems, information networks and ICT services. In accordance with Finland's cybersecurity strategy, VAHTI reviews and reconciles the central government's key information and cybersecurity policies.

The Ministry of Finance has carried out an annual central government information security survey – the VAHTI survey – as an information security survey of the organisations since the early 2000s. The results of these surveys are reported in the organisation's annual reports. The metrics of the organisational survey have allowed monitoring of the impact that the different development programmes and the Information Security Decree of 2010 has had on the development of information and cybersecurity in central government organisations. VAHTI carried out a corresponding survey on the municipalities for the first time in the summer of 2015.

However, these organisational surveys do not reveal at a fine-grained level the personnel and management experience of information security and how they think it should be developed. In order to complement the knowledge base of information security steering, the Ministry of Finance decided in September 2015 to carry out the first information security barometer for its personnel and management in 2016. This survey had a significantly broader base of respondents: all central government organisations, municipalities and hospital districts could take part in the survey.

The VAHTI information security barometer was a success

The first information security barometer in the history of VAHTI can be considered to have been a roaring success. A total of 97 central government and municipal sector organisations took the survey. The total number of respondents was 13,915, of which 6,655 were government employees and 7,260 were municipal employees. There were a total of 168,195 potential respondents, resulting in a response percentage of 8.27%.

The survey involved an extensive examination of the respondents' experiences and views on the realisation of information security in their own organisations. This provided information on the state and development needs of information security for the use of the Ministry of Finance and the participating organisations. The survey also provided a good overall idea of the realisation of information security in public administration from the viewpoint of the personnel and management.

Based on the results of the information security barometer, the promotion of information security will not fail due to attitudes. A majority of the respondents were of the opinion that information security makes high-quality operations possible and gives a trustworthy image of their organisations. This observation is supported by the members of the organisation's management team and largely found the different areas of information security to be extremely important.

The feeling of security of the respondents while working on terminal devices was high, and their concern about various threats was usually non-existent or minor. However, the feeling of security and lack of concern do not go hand in hand with the amount of training and instruction the respondents have received: only 29.7% of the respondents felt like they had received a sufficient amount of training in the different areas of information security. The supervisors and management had received more training, but not enough, which is evident in the freeform answers, for example. The familiar claim "people are the weakest link in information security" can be overcome, however, by providing instructions and training, first and foremost – competent personnel who respond to threats are an important resource in the realisation of security.

During the last several years, only a relatively small number of significant information security deviations have been reported in Finland, and this could be one cause of the high feeling of security. In the future, it will be interesting to compare how the results of the metrics created in this survey compare with possible future surveys.

Information security and the digitalisation of operations it enables will not succeed without training and instructions. Indeed, the smaller-than-assumed amount of information security training and instructions received is an important yet alarming issue. Investing

in training and instructions at both the general and organisational levels is essential. The detected deficiencies and risks can be converted into know-how and opportunities. Sufficient training and instructions can be used to further improve both the information security of practical-level operations and the feeling of security.

In the central government, training and instructions and the feeling of security were at a higher level than in the municipal sector. The slightly more moderate results of the municipal sector may be caused by, for example, the fact that the development of information security is not as established and networked as in the central government, where VAHTI has been responsible for its development for twenty years. Furthermore, the Information Security Decree of 2010 requiring information security training applies to the central government. These observations are also supported by the VAHTI information security survey for municipalities carried out in 2015 by the Ministry of Finance.

The key observation of the report was that training should clearly be improved. It is possible for the Ministry of Finance to implement a comprehensive training system for public administration in cooperation with VAHTI and stakeholders, which concerns the areas requiring improvement identified in this report.

The scope of the VAHTI information security barometer is an important survey of the state of information security even when examined from an international viewpoint. In order to leverage the possibilities offered by information security, the needs that arose during the survey must be met. Attitudes related to information security will be improved further, when attention is paid to basic issues such as training and instructions, functional software, password management and secure premises.

The duty of VAHTI is to support the entire public administration in improving information security. The parties participating in VAHTI's operations in different ways are an indispensable help in this work. The thanks for the success of this information security barometer are due to all the actors involved in the preparation and implementation of the survey as well as the organisations and their personnel who took the survey. Information security is made together.

Key observations and recommendations

Attitudes and needs concerning information security

Based on the results of the information security barometer, attitudes towards information security is extremely positive. As many as 60.8% of the respondents were of the opinion that information security makes high-quality operations possible and gives a trustworthy image of their organisations. 32.3% of the respondents were of the opinion that information security is necessary for them to be able to handle the information they need in their work. Furthermore, 6.7% understood the importance of information security, although it sometimes causes extra work. Only 0.2% considered information security to be detrimental to their operations. A large majority thus thinks that information security is a necessary enabler of high-quality operations. This observation is supported by the fact that the management primarily found the different areas of information security to be extremely important.

In order to leverage the possibilities offered by information security, the needs that arose during the survey must be met. The freeform answers highlighted the need for the security of premises, up-to-date and updated software, and clear roles and responsibilities – including not forgetting training and instructions. In other words, promoting information security is, to a large extent, taking care of the basics. Respondents hoped that password management and use of e-mail was easier. Password security can be improved through targeted instructions and by adopting cost-efficient password management programmes.

The answers to the open questions concentrated on problems, which may appear to be in conflict with the otherwise positive attitude of the respondents towards information security. The purpose of the open questions was to determine the development needs and problems of information security; these viewpoints were thus emphasised in the answers. The survey did not ask what had already been implemented well in information security, and this must be taken into consideration when interpreting the results of the report.

The feeling of security relative to training and instructions

Almost all of the respondents (96.4%) felt either very secure or rather secure while working on their terminal devices. On average, the information security areas important to them caused them either no concern at all (52%) or only a little concern (37.4%). Thus, their feeling of security was high, and their concern for various threats was usually either non-existent or minor. In the municipal sector, the feeling of security was at a slightly lower level and the level of concern was higher.

However, the feeling of security and lack of concern do not go hand in hand with the training and instructions received by the respondents. Only 29.7% of the respondents had received, on the average, a sufficient amount of training in the different areas of information security. 39.8% had received some training and instructions. On average, 22.1% stated that they had not received any training and instructions in the various areas. In the central government, the situation was somewhat better than in the municipal sector. The better feeling of security and lower level of concern in the central government may therefore be a result of additional training and instructions they have received.

The respondents found working on the terminal devices to be rather secure, while they also found the information security training and instructions to be insufficient, which is both an interesting and worrisome observation. The situation was troubling with regard to the use of mobile devices, for example. Despite the respondents finding working on the terminal devices to be secure, only 18.0% of the respondents stated that they had received a sufficient amount of training and instruction in the use of mobile devices. 31.3% of the respondents stated that despite needing them, they had not received any training or instructions. Information security should be the focus from the start, as one respondent stated.

> "All employees should be instructed in information security issues immediately on the first working day as part of the orientation."

The lack of sufficient training and instructions does not therefore cause a low feeling of security. It may be a question of, for example, the persons not necessarily recognising the training and instructions they have received, or they have received training and competence during their leisure time. The respondents are also likely unable to identify all the risks related to the insufficient training and instructions they encounter during their work. It may be that the respondents' trust in their own skills is high, even if they realise the insufficiency of the training and instructions they have received.

On the comparison of the central government and the municipal sector

As became evident from the above, the municipal sector has somewhat more development to handle than the central government. Training and instructions, the feeling of security and the level of concern were all at a higher level in the central government than in the municipal sector. However, there were plenty of development needs in the central government, too, and the results were not at the expected level in all parts. In the municipal sector, certain areas such as the classification of information and the instructions and training related to the processing of personal data were implemented better than in the central government.

The slightly poorer results of the municipal sector may be caused by, for example, the fact that the development of information security is not as established and networked as in the central government. The Information Security Decree of 2010, which placed obligations on the central government, also has a significant impact on this. The organisational information and cybersecurity surveys carried out by VAHTI have identified an overall improvement of over 10% in the responses of the central government, with improvements of over 30% in individual areas, after the decree came into force. Information security in the central government has thus measurably improved during 2011–2015.

On average, the respondents in the municipal sector had worked for a shorter time than those working for the central government, which could be a contributing factor to the poorer state of training and instructions in the municipal sector. Of the respondents in the municipal sector, 38% had worked 0 to 5 years, while the corresponding number in the central government was 33%. Including information security training as part of the orientation of new employees could likely bring about a significant improvement in the results.

Recommendations based on the observations

Information security is an enabler of digitalisation

The results of the VAHTI information security barometer for personnel and management highlight the respondents having a serious and positive attitude towards information security. The development needs identified in this report must be taken into consideration in the entire public administration, when information security is further developed. The survey participants emphasised this in their freeform answers.

> ”I hope these answers also result in considerate and sensible further actions.”

> ”I hope that time would be spent in Finland in the development and restoration of security in all areas.”

Information security is considered to be important in and of itself. First and foremost, however, it is an enabler of high-quality operations. A sufficient level of information security plays a key role in the digitalisation of operations. Without information security, there is no digitalisation of operations, robotisation, or other key societal success factors of the future. Information security should be in-built in all operations under the ‘security by design’ principle. The same measures should also be taken with regard to data protection in processes and information systems handling personal data (”privacy by design”).

Attention must be paid to training and instructions

Information security and the digitalisation of operations it enables will not succeed without training and instructions. The small amount of information security training and instructions received is an important but also alarming issue. Investing in training and instructions in both the entire public administration and in each organisation is essential. The feeling of security of public administration employees is at a high level despite them finding the amount of training and instruction to be insufficient. Additional training and instructions can further improve both information security and the feeling of security.

To a large extent, the training and instructions concern the basics. One respondent who praised the survey gave concrete suggestions of how to develop training and instructions.

> "It is good that the survey was carried out. An online school and a skills test could help steer the training towards the development targets. Furthermore, information security training could be arranged, concentrating on different thematic areas, such as antivirus protection, password policies, processing of personal data, data protection and the information security of mobile devices."

An attempt must be made to convert the deficiencies found in training and instructions into know-how and opportunities. Instruction in the use of mobile devices, including information security, must be increased, because in the future, more and more work will be done on them – flexibly and regardless of the time and place. The attention that will be paid to increasing these opportunities will also be paid to VAHTI's operations. It must also be taken into consideration that training and instructions alone are not enough, but the technical information security must also be in order and develop with the development of the threat.

Based on the results, the process of reforming VAHTI will include the preparation of a training development programme

The operations of VAHTI, which will turn 20 years old in 2017, will increasingly focus on working groups. VAHTI will continue to be responsible for the development of information security in the central government and play an even more central role in public administration as well.

The results of the survey reinforced the view that the best practices developed by VAHTI will continue to be useful for the municipalities. Cooperation with the expert group handling information security, data protection and preparedness, which was established by the Advisory Committee on Information Management in Public Administration (JUHTA), will provide even better preparedness for the development of the security of the entire public administration.

VAHTI's operations constantly aim at increasing the impact of information and cybersecurity, and at promoting the realisation of data protection. As the results of VAHTI's operations in general, the findings of this report can also be utilised by society and companies in addition to public administration personnel. VAHTI itself will utilise the results of the information security barometer in the planning and implementation of its operations.

Based on the results of the information security barometer, supporting the development of training and instructions is particularly important in VAHTI's operations.

1 Yleistä tietoturvabarometriin liittyen

1.1 Raportin rakenne

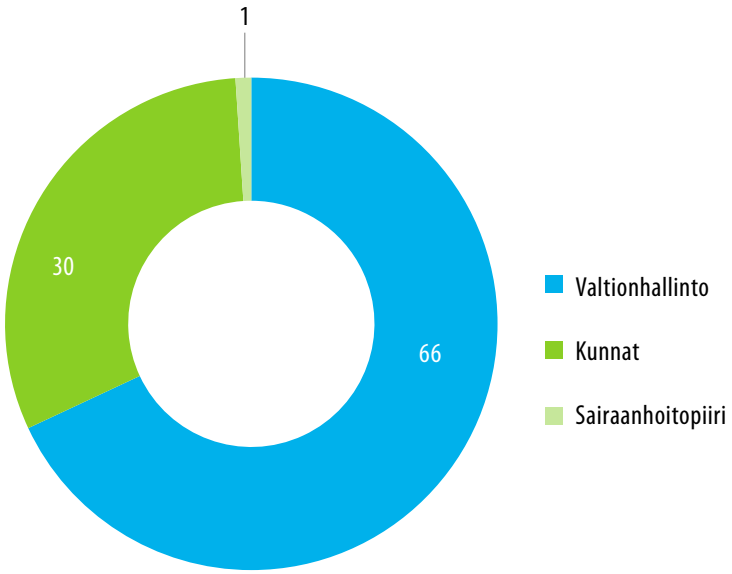
Tietoturvabarometrin tulokset esitellään kyselyn toteuttamisjärjestyksessä. Ensin esitellään vastaajien taustatiedot ja kyselyn yksityiskohtaiset tulokset. Lopuksi analysoidaan kyselystä saatua palautetta ja luodaan katsaus mahdollisiin tuleviin kyselyihin. Liitteessä esitellään tarkemmin kyselyn toteutusta.

Tässä raportissa on esitelty rinnakkain koko julkishallinnon yhteiset tulokset sekä valtionhallinnon ja kuntasektorin tulokset, joita on vertailtu keskenään. Kyselyyn osallistunut sairaanhoitopiiri on laskettu osaksi kuntasektoria näissä vertailuissa. Suurin osa tuloksista esitellään kuvailevan tilastotieteen keinoin, mutta joukossa on myös avokysymyksiin saatujen vastausten laadullista tarkastelua.

1.2 Vastaajaorganisaatiot

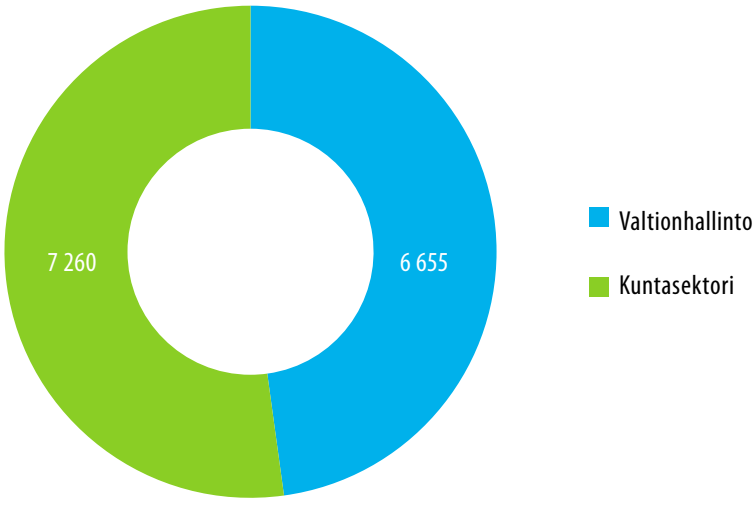
Kyselyyn osallistui yhteensä 97 organisaatiota. Valtionhallinnosta mukana oli 66 organisaatiota, joista ministeriöitä 12. Kuntia oli mukana 30 ja sairaanhoitopiirejä 1. Vastaajaorganisaatioilta kysyttiin potentiaalinen vastaajamäärä, jota verrattiin toteutuneeseen vastaajamäärän. Näin saatiin selville kyselyn kokonaisvastausprosentti ja organisaatiokohtaiset vastausprosentit.

Kuva 1. Kyselyyn osallistuneet organisaatiot luokittain (97 organisaatiota).



Potentiaalisia vastaajia oli kaiken kaikkiaan 168 195, joista valtiolla 48 069 ja kuntasektorilla 120 126[1]. Kyselyyn vastasi yhteensä 13 915 henkilöä. Vastaajista valtiolla työskenteli 6 655 henkilöä eli 47,8 % vastaajista ja kuntasektorilla 7 260 henkilöä eli 52,2 % vastaajista. Koko kyselyn vastausprosentiksi tuli 8,27 %, valtion 13,84 % ja kuntasektorin 6,04 %. Potentiaalisten vastaajien määrä oli valtionhallinnossa keskimäärin 717 per organisaatio ja kuntasektorilla 3 875. Valtionhallinnon organisaatiosta tuli keskimäärin 95 vastausta ja kuntasektorilta 234 vastausta.

Kuva 2. Kyselyyn osallistuneet vastaajat valtionhallinnossa ja kuntasektorilla (13 915 vastaajaa).



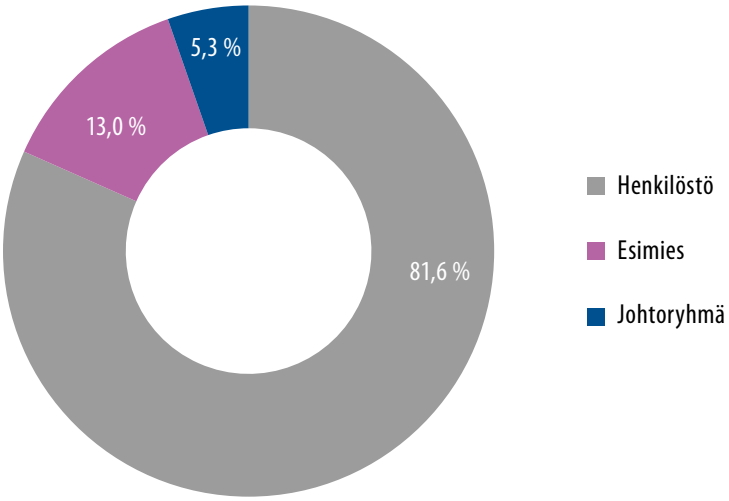
1 Kuntasektorin luvussa on mukana myös sairaanhoitopiirin vastaajat.

1.3 Vastaajien taustatiedot

1.3.1 Vastaajien asema

Vastaajilta kysyttiin taustatietona, kuuluivatko he organisaationsa johtoryhmään ja esimiehiin. Ne vastaajat, jotka eivät kuuluneet kumpaankaan ryhmään, luokiteltiin henkilöstöön. Johtoryhmäksi laskettiin kyselyssä ministeriön, viraston ja kuntien ylimmän johtoryhmän jäsenet – ei esimerkiksi jonkin kunnan tietyn viraston johtoryhmän jäseniä. Vastaajan asemaa kysyttiin, jotta saataisiin kerättyä tietoja eri ryhmien eroista ja yhtäläisyyksistä tietoturvaan liittyen. Kaikista vastaajista henkilöstöä oli 81,6 %, esimiehiä 13,0 % ja johtoryhmän jäseniä 5,3 %.[2]

Kuva 3. Vastaajien toimenkuva (kaikki vastaajat).



Valtionhallinnon ja kuntasektorin välillä oli pieniä eroja. Valtion vastaajista 81,8 % kuului henkilöstöön, kun kuntasektorilla luku oli 81,5 %. Esimiehiin kuului valtiolla 13,0 % ja organisaationsa johtoryhmään 5,2 %. Kunnissa vastaavat luvut olivat 13,0 % ja 5,5 %. Vastaajajoukon toimenkuvat olivat siis varsin samankaltaiset valtiolla ja kunnissa.

2 Eri ryhmien vertailuita ei esitellä kaikista kohdista, vaan mukaan on valittu kaikista mielenkiintoisimmat havainnot. Monet johtoryhmän jäsenet toimivat myös esimiehinä. Nämä vastaajat laskettiin tässä kuviossa pelkästään johtoryhmäläisiksi. Myöhemmissä vertailuissa esimiehiksi on laskettu kaikki esimiehet – myös johtoryhmiin kuuluvat.

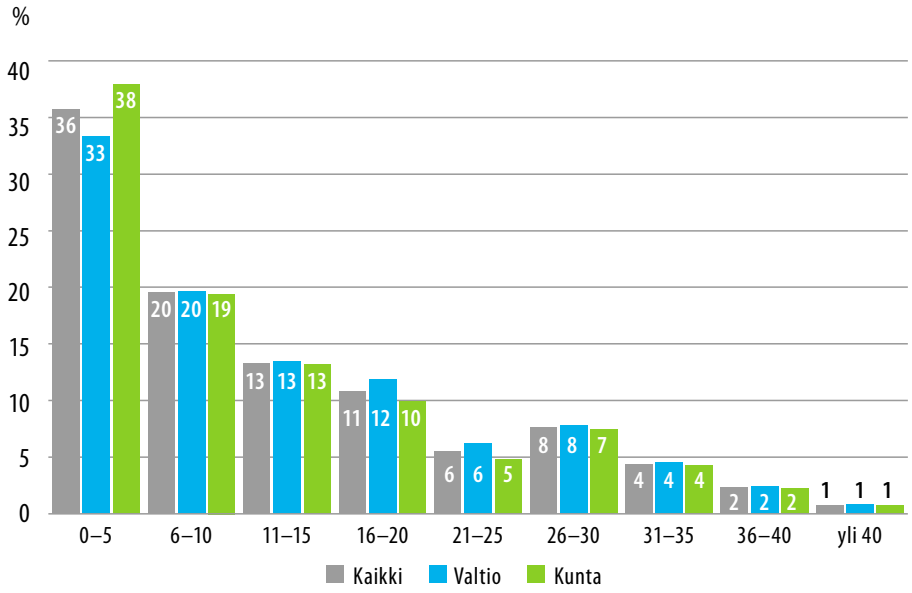
Taulukko 1. Vastaajien toimenkuva.

Toimenkuva	Kaikki	%	Valtio	%	Kunnat	%
Henkilöstö	11360	81,6 %	5443	81,8 %	5917	81,5 %
Esimies	1813	13,0 %	868	13,0 %	945	13,0 %
Johtoryhmä	742	5,3 %	344	5,2 %	398	5,5 %
Yhteensä	**13915**	**100,0 %**	**6655**	**100,0 %**	**7260**	**100,0 %**

1.3.2 Vastaajien palvelusvuodet

Lisäksi taustatiedoista selvitettiin, kuinka kauan vastaajat olivat työskennelleet nykyisessä organisaatiossaan yhden täyden työvuoden – ei kalenterivuoden – tarkkuudella. Yleisin määrä työvuosia vastaajien joukossa oli 1. Palvelusvuosia oli kertynyt vastaajille keskimäärin 12,23. Valtionhallinnon vastaajat olivat työskennelleet keskimäärin 12,64 vuotta. Kuntasektorilla palvelusvuosia oli kertynyt keskimäärin 11,85 eli joitain kuukausia valtionhallintoa vähemmän.

Kuva 4. Vastaajien palvelusvuodet nykyisessä organisaatiossa.



2 Tulokset

2.1 Käytännön arki ja tietoturva

Käytännön arkeen ja tietoturvaan liittyen vastaajilta kysyttiin kahdeksan kysymystä. Kohta olikin koko tietoturvabarometrin laajin ja kenties tärkein. Tietoturvallisuus toteutuu arjessa, sekä työssä että vapaa-ajalla. Kohdan kysymykset liittyivät päätelaitteiden käyttöön, tietoturvallisuuteen liittyen saatuun ohjeistukseen ja koulutukseen, käyttäjätunnuksiin ja salasanoihin sekä vastaajien kokemuksiin ja huoliin tietoturvallisuuteen liittyen.

2.1.1 Vastaajien työtehtävissään käyttämät päätelaitteet

Vastaajilta kysyttiin, mitä päätelaitteita he käyttivät työtehtävissään. Vastausvaihtoehtoja oli kahdeksan, joista oli mahdollista valita yhdestä kahdeksaan vaihtoehtoa. Kysymyksessä selvitettiin seuraavien päätelaitteiden käyttöä:

- Työantajan kannettava tietokone
- Työnantajan pöytätietokone
- Työnantajan tabletti
- Työnantajan älypuhelin
- Oma kannettava tietokone
- Oma pöytätietokone
- Oma tabletti
- Oma älypuhelin

Omalla päätelaitteella tarkoitettiin vastaajan henkilökohtaisen päätelaitteen ohella esimerkiksi kirjaston, puolison tai ystävän päätelaitetta.

Yleisimmin käytettiin työantajan kannettavaa tietokonetta (60,2 % kaikista vastaajista), työantajan pöytätietokonetta (57,5 %) ja työnantaja älypuhelinta (53,1 %). Muut päätelaitteet eli työantajan tabletti (9,3 %), oma älypuhelin (8,0 %), oma kannettava tietokone (6,6 %), oma pöytätietokone (4,5 %) ja oma tabletti (3,8 % vastaajista) olivat käytössä työteh-

tävissä huomattavasti harvemmin kuin kärkikolmikko. Vastaajat käyttivät työtehtävissään keskimäärin 2,03 laitetta.

Valtionhallinnon ja kuntasektorin välillä oli huomattavia eroja päätelaitteiden käytössä. Valtionhallinnossa käytettiin paljon enemmän työnantajan kannettavaa tietokonetta ja työantajan älypuhelinta kuin kunnissa. Kaikkien muiden selvitettyjen päätelaitetyyppien, erityisesti pöytätietokoneiden, käyttö oli yleisempää kunnissa. Valtionhallinnossa oli käytössä työtehtävissä keskimäärin 1,93 päätelaitetta, kun taas kunnissa niitä oli 2,12.

Kunnissa saatetaan käyttää enemmän omia päätelaitteita, koska työnantaja ei tarjoa niitä työntekijöiden käyttöön yhtä yleisesti kuin valtionhallinnossa. Tablettien käytön yleisyyttä kunnissa voivat selittää esimerkiksi opetustehtävät, joissa tablettien käyttö on yleistä.

Taulukko 2. Vastaajien (13 915) työtehtävissään käyttämät päätelaitteet.

Päätelaite	Kaikki (13915)	%	Valtio (6655)	%	Kunta (7260)	%
Työnantajan kannettava	8375	60,2 %	4674	70,2 %	3701	51,0 %
Työnantajan pöytätietokone	7998	57,5 %	3012	45,3 %	4985	68,7 %
Työnantajan tabletti	1291	9,3 %	385	5,8 %	906	12,5 %
Työnantajan älypuhelin	7383	53,1 %	3927	59,0 %	3456	47,6 %
Oma kannettava tietokone	919	6,6 %	249	3,7 %	670	9,2 %
Oma pöytätietokone	625	4,5 %	165	2,5 %	460	6,3 %
Oma tabletti	533	3,8 %	136	2,0 %	397	5,5 %
Oma älypuhelin	**1115**	**8,0 %**	**303**	**4,6 %**	**812**	**11,2 %**

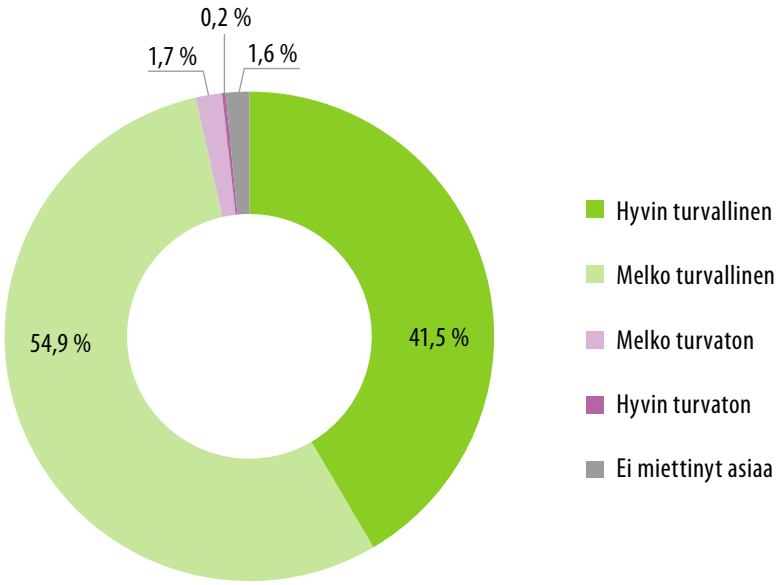
Omien päätelaitteiden käyttäminen esimerkiksi sähköpostin lukemiseen voi muodostaa tietoturvariskin, mikäli käyttöä ei ole huolella ohjeistettu. Toisaalta kaikissa työtehtävissä ei aina käsitellä sellaista tietoa, että omien päätelaitteiden käyttäminen olisi ongelmallista. Opettaja, joka soittaa omalle puhelimellaan kollegalleen virkistyspäivän ajankohdasta, tuskin aiheuttaa suurta vaaraa.

2.1.2 Päätelaitteilla työskentely ja koettu turvallisuus

Osallistujia pyydettiin vastaamaan heidän kokemukseensa perustuen, miten turvallisesksi he kokivat työskentelyn käyttämillään päätelaitteilla. Kysymyksessä ei kysytty erikseen, miten turvalliseksi työskentely koettiin työantajan laitteilla ja omilla laitteilla, vaan tietoa haettiin kaikkiin päätelaitteisiin liittyen.

Kaikista vastaajista suurin osa (96,4 %) koki olonsa joko hyvin turvalliseksi tai melko turvalliseksi päätelaitteilla työskennellessään. Melko turvattomaksi tai hyvin turvattomaksi olonsa tunsi yhteensä alle 2 %. 1,6 % ei ollut miettinyt asiaa tarkemmin.

Kuva 5. Turvallisuudentunne päätelaitteilla työskennellessä (13908 vastaajaa).



Esimiesten ja johtoryhmäläisten sekä kaikkien vastaajien turvallisuudentunne oli hyvin samankaltainen. Esimiehet (97,4 %) ja johto (97,5 %) tunsivat olonsa kaikkia vastaajia hieman useammin hyvin turvalliseksi tai melko turvalliseksi.

Kunnissa ja valtiolla vastaukset erosivat toisistaan hieman. Valtiolla oli enemmän niitä, jotka tunsivat olonsa hyvin turvalliseksi ja kunnissa niitä, jotka eivät olleet miettineet asiaa.

Taulukko 3. Turvallisuudentunne päätelaitteilla työskennellessä.

Turvallisuudentunne	Kaikki	%	Valtio	%	Kunnat	%
Hyvin turvallinen	5776	41,5 %	2865	43,1 %	2911	40,1 %
Melko turvallinen	7641	54,9 %	3586	53,9 %	4054	55,9 %
Melko turvaton	242	1,7 %	116	1,7 %	126	1,7 %
Hyvin turvaton	33	0,2 %	18	0,3 %	15	0,2 %
Ei miettinyt asiaa	216	1,6 %	66	1,0 %	150	2,1 %
Yhteensä	**13908**	**100,0 %**	**6651**	**100,0 %**	**7256**	**100,0 %**

Turvallisuutta lähestyttiin kysymyksessä *tunteena*. Muita keskeisiä turvallisuuden osa-alueita ovat todellisuus, sietokyky ja kulttuuri. Todellinen turvallisuusympäristö ja subjektiivinen turvallisuudentunne eivät välttämättä kohtaa. Olo voidaan tuntea hyvin turvalliseksi, jos ympärillä olevia uhkia ei tunnisteta. Toisaalta taas iltapäivälehtiä lukemalla saattaa tulla tunne, että joka puolella on uusia vaaroja, vaikka Suomi on muuttunut monella tapaa aiempaa turvallisemmaksi.[3] Turvallisuudentunne eli turvallisuuteen ja turvattomuuteen liitetyt mielikuvat ja ymmärrys kasvattavat jatkuvasti merkitystään todellisen turvallisuuden luojina.

2.1.3 Vastaajien saama ohjeistus ja koulutus

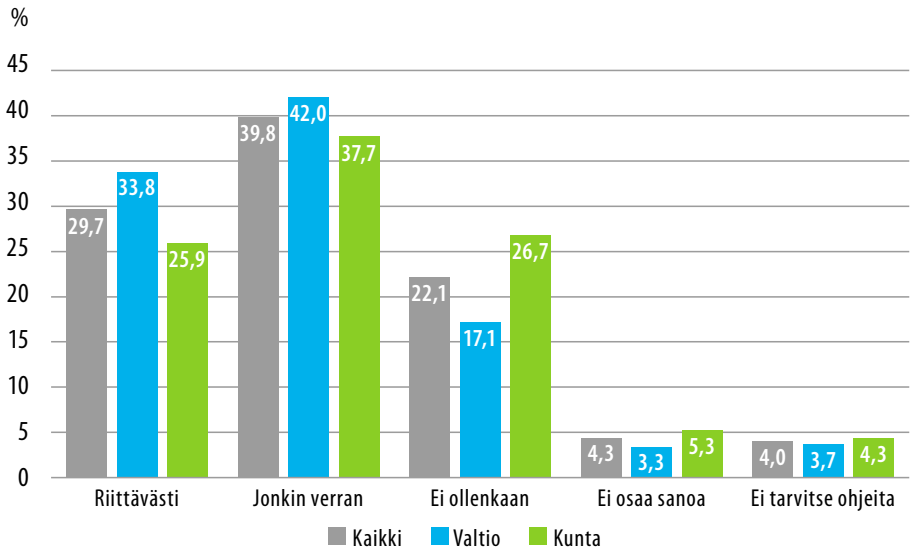
Vastaajilta kysyttiin seuraavaksi, mihin tietoturvaan liittyviin asioihin he olivat saaneet ohjeita ja koulutusta. Vastaajien tuli valita sopivin vastausvaihtoehto kustakin kohdasta, joita oli yhteensä 14. Kohdissa selvitettiin saatua koulutusta esimerkiksi toimitilaturvallisuuteen, tietojen luokitteluun ja sosiaalisen median käyttöön liittyen.

Ohjeistuksella ja koulutuksella tarkoitettiin työhön liittyen annettuja ohjeita ja työpaikan järjestämää koulutusta. Ohjeistus ja koulutus oli voitu antaa esimerkiksi suullisesti työpaikalla, sisäisessä koulutuksessa tai ulkopuolisen toimijan järjestämissä tilaisuuksissa, kuten esimerkiksi luennoilla tai seminaareissa.

Vastaajista koulutusta ja ohjeistusta riittävästi oli saanut keskimäärin 29,7 %. Valtionhallinnossa tilanne oli kuntasektoria parempi. Jonkin verran koulutusta ja ohjeistusta oli saanut keskimäärin 39,8 %, valtiolla useammin kuin kunnissa. Koulutusta ja ohjeistusta ei ollut saatu ollenkaan 22,1 % tapauksista. Kuntasektorilla tämä oli valtionhallintoa huomattavasti yleisempää. 4,3 % vastaajista ei osannut sanoa, kuinka paljon koulutusta ja ohjeistusta oli saanut ja 4,0 % ilmoitti, ettei tarvitse niitä.

3 http://www.hs.fi/kotimaa/a1474169511702

Kuva 6. Vastaajien eri tietoturvallisuuden osa-alueisiin keskimäärin saama koulutus ja ohjeistus.



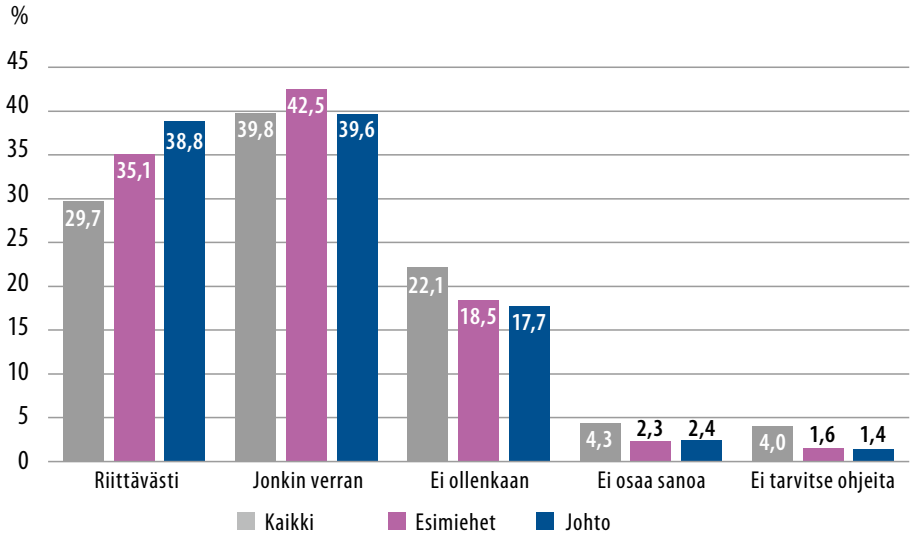
Vastaajien saaman ohjeistuksen ja koulutuksen perusteella sekä kuntasektorilla että valtionhallinnossa on edelleen kehitettävää. Se, että asiat ovat valtionhallinnossa jonkin verran kuntia paremmalla tolalla, on todennäköisesti vuonna 2010 voimaan astuneen tietoturvallisuusasetuksen (681/2010) seurausta.

Tietoturvallisuusasetus velvoitti valtionhallinnon organisaatiot järjestämään säännönmukaista tietoturvallisuuskoulutusta, jota VAHTI on yhtenä keskeisenä toimijana edistänyt. Tietoturvallisuusasetuksen seurauksena valtionhallinnossa on pitänyt toteuttaa tietoturvallisuuden perustaso, johon kuuluvat muun muassa tietoturvallisuusriskien kartoittaminen, tiettyjen vastuiden määrittely sekä tietojen saatavuuden ja käytettävyyden turvaaminen.

Kaikkien vastaajien sekä esimiesten ja johdon vastauksia vertailtaessa korostuu se, että johtoryhmiin ja esimiehiin kuuluvat vastaajat ovat saaneet huomattavasti enemmän koulutusta tietoturvallisuuden eri osa-alueisiin kuin kaikki vastaajat keskimäärin.[4]

4 Kaikissa vastaajissa ovat mukana myös esimiehiin ja organisaatioidensa johtoryhmiin kuuluneet vastaajat, sillä esimiehet ja johtoryhmä ovat myös osa henkilöstöä.

Kuva 7. Eri vastaajatyyppien tietoturvallisuuden osa-alueisiin keskimäärin saama koulutus ja ohjeistus.



Kysymyksiin annetut vastaukset vaihtelivat runsaasti kohdittain. Riittävän koulutuksen osalta heikoin tilanne oli mobiililaitteiden käytön, tietojen luokittelun sekä tiedostojen salaamisen suhteen. Näissä osa-alueissa erityisesti kuntasektorilla koulutus oli jäänyt vähäiseksi tai olemattomaksi. Kuntasektorilla oli toisaalta enemmän epävarmoja vastaajia.

Mobiililaitteiden käyttöä oli ohjeistettu enemmän valtionhallinnossa. Niiden vastaajien määrä, jotka kertoivat, etteivät tarvitse ohjeistusta ja koulutusta, oli kohdassa varsin korkea (8,0 %). Tämä voi johtua siitä, ettei mobiililaitteita käytetä tai siitä, että mobiililaitteiden käyttö on vastaajille tuttua vapaa-ajalta.

Taulukko 4. Mobiililaitteiden käyttöön saatu koulutus ja ohjeistus.

Koulutus ja ohjeistus	Kaikki	%	Valtio	%	Kunnat	%
Riittävästi	2494	18,0 %	1339	20,2 %	1155	16,0 %
Jonkin verran	5283	38,1 %	2725	41,0 %	2557	35,4 %
Ei ollenkaan	4338	31,3 %	1783	26,8 %	2555	35,4 %
Ei osaa sanoa	639	4,6 %	260	3,9 %	379	5,2 %
Ei tarvitse	1108	8,0 %	534	8,0 %	574	8,0 %
Yhteensä	**13862**	**100,0 %**	**6641**	**100,0 %**	**7220**	**100,0 %**

Esimiehet (22,4 %) ja johto (26,6 %) olivat saaneet kaikkia vastaajia useammin riittävästi koulutusta ja ohjeistusta mobiililaitteiden käyttöön. He olivat saaneet myös huomattavasti useammin jonkin verran koulutusta (esimiehet 46,2 % ja johtoryhmäläiset 43,4 %).

Tietojen luokittelun osalta korostui koulutuksen jääminen vähäiseksi sekä epävarmojen vastaajien suuri määrä (13,3 %). Tämä saattaa olla merkki siitä, ettei vastaaja tiedä, mistä tietojen luokittelussa on kyse.

Taulukko 5. Tietojen luokitteluun saatu koulutus ja ohjeistus.

Koulutus ja ohjeistus	Kaikki	%	Valtio	%	Kunnat	%
Riittävästi	2507	18,1 %	1588	23,9 %	918	12,7 %
Jonkin verran	5191	37,4 %	2969	44,7 %	2222	30,8 %
Ei ollenkaan	3775	27,2 %	1272	19,2 %	2503	34,7 %
Ei osaa sanoa	1841	13,3 %	608	9,2 %	1233	17,1 %
Ei tarvitse	548	4,0 %	204	3,1 %	344	4,8 %
Yhteensä	**13862**	**100,0 %**	**6641**	**100,0 %**	**7220**	**100,0 %**

Tiedostojen salaamiseen ei ollut saanut ollenkaan koulutusta 37,5 % vastaajista, mikä oli korkein luku täysin vailla koulutusta olleita vastaajia. 5,3 % ilmoitti, ettei tarvitse ohjeita ja koulutusta.

Taulukko 6. Tiedostojen salaamiseen saatu koulutus ja ohjeistus.

Koulutus ja ohjeistus	Kaikki	%	Valtio	%	Kunnat	%
Riittävästi	2574	18,6 %	1292	19,5 %	1282	17,8 %
Jonkin verran	4527	32,7 %	2460	37,0 %	2066	28,6 %
Ei ollenkaan	5195	37,5 %	2205	33,2 %	2990	41,4 %
Ei osaa sanoa	835	6,0 %	313	4,7 %	522	7,2 %
Ei tarvitse	731	5,3 %	371	5,6 %	360	5,0 %
Yhteensä	**13862**	**100,0 %**	**6641**	**100,0 %**	**7220**	**100,0 %**

Paras tilanne riittävän koulutuksen ja ohjeistuksen suhteen oli turvalliseen toimintaan organisaation toimitiloissa (44,4 %), sähköpostin käyttöön (43,7 %) ja henkilötietojen käsittelyyn (43,5 %) liittyen. Sitä, miksi näihin osa-alueisiin liittyen oli saatu niin paljon enemmän ohjeistusta ja koulutusta kuin edellä mainittuihin tietoturvallisuuden osa-alueisiin tulisi pohtia. Kuinka saataisiin esimerkiksi mobiililaitteiden käytön ohjeistus ja koulutus sähköpostin käyttöön saadun koulutuksen ja ohjeistuksen tasolle?

Valtion ja kuntien välillä oli jälleen suuria eroja, varsinkin tilaturvallisuuteen liittyen.

Taulukko 7. Turvalliseen toimintaan organisaation toimitiloissa saatu koulutus ja ohjeistus.

Koulutus ja ohjeistus	Kaikki	%	Valtio	%	Kunnat	%
Riittävästi	6149	44,4 %	3600	54,2 %	2548	35,3 %
Jonkin verran	5784	41,7 %	2508	37,8 %	3276	45,4 %
Ei ollenkaan	1380	10,0 %	370	5,6 %	1010	14,0 %
Ei osaa sanoa	412	3,0 %	127	1,9 %	285	3,9 %
Ei tarvitse	137	1,0 %	36	0,5 %	101	1,4 %
Yhteensä	**13862**	**100,0 %**	**6641**	**100,0 %**	**7220**	**100,0 %**

Sähköpostin käyttöä oli samoin ohjeistettu ja koulutettu hyvin. Kuntasektorilla on valtionhallintoa enemmän kehittämistarpeita.

Taulukko 8. Sähköpostin käyttöön saatu koulutus ja ohjeistus.

Koulutus ja ohjeistus	Kaikki	%	Valtio	%	Kunnat	%
Riittävästi	6060	43,7 %	3239	48,8 %	2821	39,1 %
Jonkin verran	6110	44,1 %	2796	42,1 %	3313	45,9 %
Ei ollenkaan	1395	10,1 %	491	7,4 %	904	12,5 %
Ei osaa sanoa	149	1,1 %	67	1,0 %	82	1,1 %
Ei tarvitse	148	1,1 %	48	0,7 %	100	1,4 %
Yhteensä	**13862**	**100,0 %**	**6641**	**100,0 %**	**7220**	**100,0 %**

Henkilötietojen käsittelyyn oli saatu myös runsaasti koulutusta. Kuntasektorilla riittävästi koulutusta oli saatu valtionhallintoa useammin. Valtionhallinnossa oli myös enemmän vastaajia, jotka sanoivat, etteivät tarvitse koulutusta ja ohjeita

Taulukko 9. Henkilötietojen käsittelyyn saatu koulutus ja ohjeistus.

Koulutus ja ohjeistus	Kaikki	%	Valtio	%	Kunnat	%
Riittävästi	6031	43,5 %	2765	41,6 %	3266	45,2 %
Jonkin verran	5412	39,0 %	2655	40,0 %	2756	38,2 %
Ei ollenkaan	1582	11,4 %	742	11,2 %	840	11,6 %
Ei osaa sanoa	277	2,0 %	128	1,9 %	149	2,1 %
Ei tarvitse	560	4,0 %	351	5,3 %	209	2,9 %
Yhteensä	**13862**	**100,0 %**	**6641**	**100,0 %**	**7220**	**100,0 %**

Tietoturvapoikkeamissa ja häiriötilanteissa toimimiseen liittyen koulutuksen ja ohjeistuksen tila näyttää kokonaisuudessaan varsin samankaltaiselta. Kuntasektorilla tilanne on hieman parempi häiriötilanteissa toimimiseen saatuun koulutukseen liittyen.

Poikkeama- ja häiriötilanteissa toimimista kannattaisi harjoitella. Kun joudutaan toimimaan ilman ohjeistusta, saattaa häiriö aiheuttaa suurempia ongelmia kuin sellaisessa tilanteessa, jossa koulutusta on saatu. Tietoturvapoikkeamia ja häiriötilanteita varten harjoittelu kasvattaa sietokykyä eli resilienssiä, joka on yksi turvallisuuden osa-alueista.

Taulukko 10. Tietoturvapoikkeamissa toimimiseen saatu koulutus ja ohjeistus.

Koulutus ja ohjeistus	Kaikki	%	Valtio	%	Kunnat	%
Riittävästi	3015	21,8 %	1935	29,1 %	1080	15,0 %
Jonkin verran	5534	39,9 %	3014	45,4 %	2519	34,9 %
Ei ollenkaan	4431	32,0 %	1408	21,2 %	3023	41,9 %
Ei osaa sanoa	740	5,3 %	255	3,8 %	485	6,7 %
Ei tarvitse	142	1,0 %	29	0,4 %	113	1,6 %
Yhteensä	**13862**	**100,0 %**	**6641**	**100,0 %**	**7220**	**100,0 %**

Taulukko 11. Häiriötilanteissa toimimiseen saatu koulutus ja ohjeistus.

Koulutus ja ohjeistus	Kaikki	%	Valtio	%	Kunnat	%
Riittävästi	2821	20,4 %	1620	24,4 %	1201	16,6 %
Jonkin verran	5752	41,5 %	2878	43,3 %	2873	39,8 %
Ei ollenkaan	4404	31,8 %	1789	26,9 %	2615	36,2 %
Ei osaa sanoa	766	5,5 %	316	4,8 %	450	6,2 %
Ei tarvitse	119	0,9 %	38	0,6 %	81	1,1 %
Yhteensä	**13862**	**100,0 %**	**6641**	**100,0 %**	**7220**	**100,0 %**

Salassa pidettävien tietoaineistojen käsittelyyn saatu koulutus ja ohjeistus olivat hieman heikommalla tasolla kuin henkilötietojen käsittelyn vastaavat lukemat. Valtionhallinnon ja kuntasektorin välillä ei ollut suuria eroja.

Taulukko 12. Salassa pidettävien tietoaineistojen käsittelyyn saatu koulutus ja ohjeistus.

Koulutus ja ohjeistus	Kaikki	%	Valtio	%	Kunnat	%
Riittävästi	5363	38,7 %	2660	40,1 %	2702	37,4 %
Jonkin verran	6049	43,6 %	2998	45,1 %	3051	42,3 %
Ei ollenkaan	1687	12,2 %	616	9,3 %	1071	14,8 %
Ei osaa sanoa	362	2,6 %	156	2,3 %	206	2,9 %
Ei tarvitse	401	2,9 %	211	3,2 %	190	2,6 %
Yhteensä	**13862**	**100,0 %**	**6641**	**100,0 %**	**7220**	**100,0 %**

Internetin käyttöön liittyen tilanne oli valtionhallinnossa kuntia parempi. Kunnissa 19,3 % vastaajista ei ollut saanut ohjeistusta ja koulutusta.

Taulukko 13. Internetin käyttöön saatu koulutus ja ohjeistus.

Koulutus ja ohjeistus	Kaikki	%	Valtio	%	Kunnat	%
Riittävästi	5452	39,3 %	2922	44,0 %	2530	35,0 %
Jonkin verran	5736	41,4 %	2760	41,6 %	2975	41,2 %
Ei ollenkaan	2186	15,8 %	795	12,0 %	1391	19,3 %
Ei osaa sanoa	243	1,8 %	89	1,3 %	154	2,1 %
Ei tarvitse	245	1,8 %	75	1,1 %	170	2,4 %
Yhteensä	**13862**	**100,0 %**	**6641**	**100,0 %**	**7220**	**100,0 %**

Sosiaalisen median suhteen tilanne oli internetin käyttöä heikompi. Myös niiden vastaajien osuus, jotka eivät kokeneet tarvitsevansa koulutusta ja ohjeistusta oli suhteellisen korkea (8,4 %)

Taulukko 14. Sosiaalisen median käyttö saatu koulutus ja ohjeistus.

Koulutus ja ohjeistus	Kaikki	%	Valtio	%	Kunnat	%
Riittävästi	3676	26,5 %	1870	28,2 %	1806	25,0 %
Jonkin verran	5083	36,7 %	2628	39,6 %	2454	34,0 %
Ei ollenkaan	3470	25,0 %	1403	21,1 %	2067	28,6 %
Ei osaa sanoa	466	3,4 %	189	2,8 %	277	3,8 %
Ei tarvitse	1167	8,4 %	551	8,3 %	616	8,5 %
Yhteensä	**13862**	**100,0 %**	**6641**	**100,0 %**	**7220**	**100,0 %**

Etätyöskentelyn kouluttaminen ja ohjeistaminen oli otettu huomioon valtionhallinnossa ja kunnissa vaihtelevasti. 24,8 % ilmoitti, ettei ole saanut ollenkaan koulutusta työskentelyyn toimipaikan ulkopuolella. Etätyöskentelyä käsitellään myös tämän raportin kohdassa 2.3. sivulta 54 alkaen.

Taulukko 15. Etätyöskentelyyn tai työskentelyyn toimipaikan ulkopuolella saatu koulutus ja ohjeistus.

Koulutus ja ohjeistus	Kaikki	%	Valtio	%	Kunnat	%
Riittävästi	2929	21,1 %	1896	28,5 %	1033	14,3 %
Jonkin verran	4422	31,9 %	2419	36,4 %	2002	27,7 %
Ei ollenkaan	3439	24,8 %	1106	16,7 %	2333	32,3 %
Ei osaa sanoa	754	5,4 %	267	4,0 %	487	6,7 %
Ei tarvitse	2318	16,7 %	953	14,4 %	1365	18,9 %
Yhteensä	**13862**	**100,0 %**	**6641**	**100,0 %**	**7220**	**100,0 %**

Ajankohtaista tietoturvaohjeistusta ja yleistä tietoturvakoulutusta oli saatu yleensä jonkin verran. Vain 0,6 % vastaajista ilmoitti, ettei tarvitse näitä ollenkaan.

Taulukko 16. Saatu ajankohtainen tietoturvaohjeistus ja koulutus.

Koulutus ja ohjeistus	Kaikki	%	Valtio	%	Kunnat	%
Riittävästi	3004	21,7 %	1823	27,5 %	1181	16,4 %
Jonkin verran	6802	49,1 %	3584	54,0 %	3217	44,6 %
Ei ollenkaan	3323	24,0 %	1000	15,1 %	2323	32,2 %
Ei osaa sanoa	643	4,6 %	217	3,3 %	426	5,9 %
Ei tarvitse	90	0,6 %	17	0,3 %	73	1,0 %
Yhteensä	**13862**	**100,0 %**	**6641**	**100,0 %**	**7220**	**100,0 %**

Tietoturvalliseen salasanojen hallintaan saatu ohjeistus ja koulutus oli vastausten perusteella kohtuullisen hyvällä tasolla. Riittävästi tai jonkin verran koulutusta oli saanut 80 % vastaajista. Valtionhallinnossa tilanne oli jonkin verran parempi kuin kunnissa.

Taulukko 17. Tietoturvalliseen salasanojen hallintaan saatu koulutus ja ohjeistus.

Koulutus ja ohjeistus	Kaikki	%	Valtio	%	Kunnat	%
Riittävästi	5554	40,1 %	2870	43,2 %	2684	37,2 %
Jonkin verran	5534	39,9 %	2678	40,3 %	2855	39,5 %
Ei ollenkaan	2357	17,0 %	944	14,2 %	1413	19,6 %
Ei osaa sanoa	291	2,1 %	111	1,7 %	180	2,5 %
Ei tarvitse	126	0,9 %	38	0,6 %	88	1,2 %
Yhteensä	**13862**	**100,0 %**	**6641**	**100,0 %**	**7220**	**100,0 %**

2.1.4 Käyttäjätunnukset ja salasanat

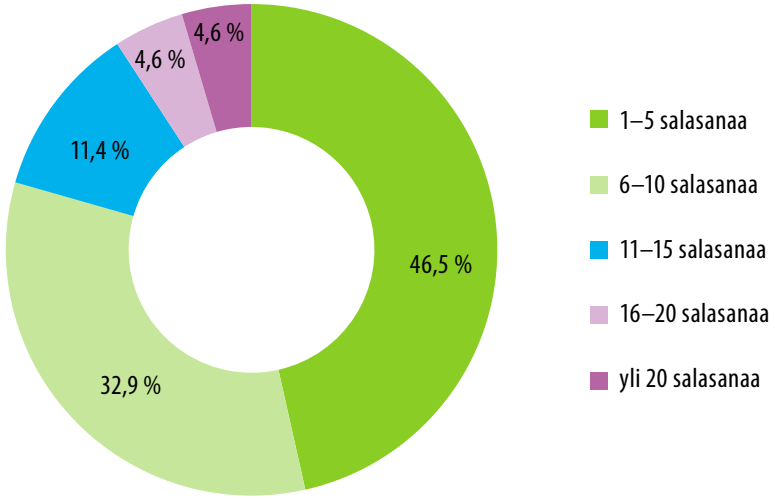
Tietoturvabarometrissa kysyttiin neljä kysymystä liittyen käyttäjätunnuksien ja salasanojen käyttöön työtehtävissä ja niihin liittyvissä palveluissa. Työtehtäviin liittyvillä palveluilla tarkoitettiin esimerkiksi vastaajan työsähköpostia, työantajan asianhallintajärjestelmiä, työajan kirjausjärjestelmä sekä talous- ja henkilöstöhallinnon järjestelmiä.

Salasanaksi laskettiin esimerkiksi salasana, jota käytetään työkoneelle kirjautuessa tai pin-koodia, jota käytetään työpuhelimen avaamiseksi. Jos vastaaja käytti samaa salasanaa tai salasanan hallintaohjelmaa eri palveluissa (esimerkiksi sama salasana työkoneelle kirjauduttaessa ja ulkopuolisen palveluntarjoajan järjestelmässä) laskettiin nämä kyselyssä eri salasanoiksi.

2.1.4.1 Vastaajien työtehtäviin liittyvien salasanojen määrä

Vastaajilla oli useimmiten (46,5 % vastaajista) käytössä 1-5 salasanaa työtehtävissään. Noin kolmanneksella oli käytössään 6-10 salasanaa. 11-15 salasanaa oli 11,4 % vastaajista. 4,6 % ilmoitti salasanojensa määräksi 16-20. Yli 20 salasanaa oli käytössä 4,6 % vastaajista.

Kuva 8. Vastaajien työtehtäviin liittyvien salasanojen määrä.



Valtiolla salasanoja vaikuttaa olevan käytössä keskimäärin enemmän kuin kunnissa. Valtiolla yleisin salasanojen määrä oli 6-10, kun taas kunnissa suurimmalla osalla oli käytössään 1-5 salasanaa. 1,8 %:lla vastaajista oli peräti yli 30 salasanaa käytössään työtehtävissä.

Taulukko 18. Vastaajien työtehtäviin liittyvien salasanojen määrä.

Salasanat	Kaikki	%	Valtio	%	Kunnat	%
1-5	6466	46,5 %	2286	34,4 %	4180	57,6 %
6-10	4582	32,9 %	2404	36,1 %	2178	30,0 %
11-15	1581	11,4 %	1035	15,6 %	546	7,5 %
16-20	643	4,6 %	433	6,5 %	209	2,9 %
21-25	276	2,0 %	204	3,1 %	72	1,0 %
26-30	111	0,8 %	81	1,2 %	30	0,4 %
Yli 30	250	1,8 %	208	3,1 %	42	0,6 %
Yhteensä	**13909**	**100,0 %**	**6651**	**100,0 %**	**7258**	**100,0 %**

2.1.4.2 Vastaajien käyttämät kirjautumistavat työtehtäviin liittyvissä palveluissa

Kysymyksessä, jossa kysyttiin vastaajien käyttämiä kirjautumistapoja, vastaajat saivat valita useamman vastausvaihtoehdon. Lähes kaikki vastaajat (96,8 %) käyttivät salasanoihin perustuvaa kirjautumista työtehtävissään. PIN-koodi tai PIN-koodeja oli käytössä 38,0 %:lla. Kertakirjautumista hyödynsi reilu kolmannes (34,1 %) ja virkakorttikirjautumista yli neljännes (27,4 %)

Kuntasektorilla hyödynnettiin enemmän salasanakirjautumista, kun taas kertakirjautuminen, virkakorttikirjautuminen ja PIN-koodilla kirjautuminen olivat valtionhallinnossa yleisempiä. Erityisen suuri ero oli kertakirjautumisen hyödyntämisessä (valtiolla 62,3 % ja kunnissa 8,3 %). Tätä selittänee virkamiehen kertakirjautumisratkaisu Virtun laaja käyttö valtionhallinnossa, ennen kaikkea talous- ja henkilöstöhallinnon palveluihin kirjautumisessa.

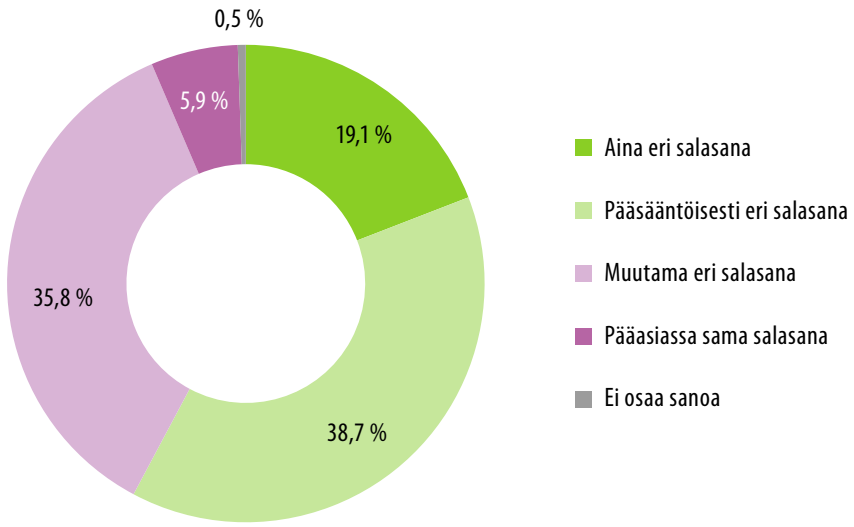
Taulukko 19. Työtehtäviin liittyvissä palveluissa käytetyt kirjautumistavat. Suluissa kysymykseen vastanneiden lukumäärä.

Kirjautumistavat	Kaikki (13909)	%	Valtio (6651)	%	Kunnat (7258)	%
Salasana	13469	96,8 %	6299	94,7 %	7169	98,7 %
Kertakirjautuminen	4750	34,1 %	4149	62,3 %	600	8,3 %
Virkakortti	3816	27,4 %	2850	42,8 %	965	13,3 %
PIN-koodi	**5289**	**38,0 %**	**3143**	**47,2 %**	**2145**	**29,5 %**

2.1.4.3 Salasanojen käyttö työtehtävissä

Seuraavaksi selvitettiin, kuinka salasanoja hyödynnetään työtehtävissä. Positiivista oli se, että pääsääntöisesti eri salasana (38,7 %) tai eri salasana jokaisessa palvelussa (19,1 %) oli käytössä yhteensä 57,8 %:lla vastaajista. Huolestuttavaa taas oli se, että 6,4 % prosenttia käyttäjistä käytti kaikissa palveluissa pääasiassa samaa salasanaa. Muutamaa eri salasanaa kaikissa palveluissa käytti reilu kolmannes 35,8 %.

Kuva 9. Eri salasanojen käyttö työtehtävissä (13 908 vastaajaa).



Valtionhallinnossa salasanojen käyttö oli hieman kuntia turvallisempaa. Erot olivat tosin hyvin pieniä.

Taulukko 20. Eri salasanojen käyttö työtehtävissä.

Salasanojen käyttö	Kaikki	%	Valtio	%	Kunnat	%
Pääasiassa sama salasana	821	5,9 %	326	4,9 %	495	6,8 %
Muutama eri salasana	4974	35,8 %	2187	32,9 %	2786	38,4 %
Pääsääntöisesti eri salasana	5379	38,7 %	2741	41,2 %	2638	36,4 %
Aina eri salasana	2659	19,1 %	1357	20,4 %	1302	17,9 %
Ei osaa sanoa	75	0,5 %	40	0,6 %	35	0,5 %
Yhteensä	**13908**	**100,0 %**	**6651**	**100,0 %**	**7256**	**100,0 %**

Jos käytössä on vain yksi tai muutama salasana, aiheuttaa se riskin. Jos yksi salasana murretaan, kaikissa muissakin palveluissa, joissa sama salasana on ollut käytössä, olevat tiedot ovat vaarassa. Riski on vielä suurempi, jos työtehtävissään käyttää samaa salasanaa kuin vapaa-ajan palveluissa, kuten sosiaalisessa mediassa. Kertakirjautumisen käyttäminen ei selitä tämän tutkimuksen antaman tuloksen perusteella sitä, miksi käytössä on pääsääntöisesti sama tai muutama eri salasana.

2.1.4.4 Salasanojen hallintaohjelmien käyttö työtehtävissä

Vastaajilla ei ollut yleensä käytössä salasanojen hallintaohjelmaa työtehtävissään (56,2 % vastaajista). Kunnissa salasanojen hallintaohjelmaa hyödynnettiin useammin työtehtävissä.

20,2 % käytti työnantajan asentamaa salasanojen hallintaohjelmaa ja 4,8 % itse asennettua salasanojen hallintaohjelmaa. Sekä työnantajan asentama että itse asennettu salasanojen hallintaohjelma oli käytössä 2,9 % vastaajista.

Tämä tarkoittaa, että yhteensä 7,7 % vastaajista käytti itse asennettua salasanojen hallintaohjelmaa työtehtävissään. Itse asennetun salasanojen hallintaohjelman käyttö työtehtävissä voi olla tietoturvariski. Tällöin ei voida tietää, onko käytössä oikeasti turvallinen ohjelma, onko se oikein ja oikeilla määrityksillä asennettu.

Taulukko 21. Salasanojen hallintaohjelmien käyttö.

Salasanojen hallintaohjelmat	Kaikki	%	Valtio	%	Kunnat	%
Ei käytössä	7810	56,2 %	4011	60,3 %	3799	52,4 %
Työnantajan asentama	2813	20,2 %	1243	18,7 %	1570	21,6 %
Itse asentama	674	4,8 %	324	4,9 %	350	4,8 %
Työnantajan sekä itse asentama	408	2,9 %	133	2,0 %	275	3,8 %
Ei osaa sanoa	2203	15,8 %	940	14,1 %	1262	17,4 %
Yhteensä	**13908**	**100,0 %**	**6651**	**100,0 %**	**7256**	**100,0 %**

Salasanojen käyttöön liittyen saadut tulokset ovat osin ristiriidassa salasana-asioihin saadun koulutuksen kanssa (taulukko 17). Riittävästi tai jonkin verran salasanojen käyttöön oli saanut koulutusta 80 % vastaajista. Kuitenkin aina eri salasana tai pääsääntöisesti eri salasana oli käytössä yhteensä vain 58,1 %:lla vastaajista (taulukko 20). Samoin itse asennettujen salasanojen hallintaohjelmien käyttö oli huolestuttavan yleistä.

2.1.5 Työtehtäviä hoitaessa huolestuttavat asiat ja uhkien toteutuminen

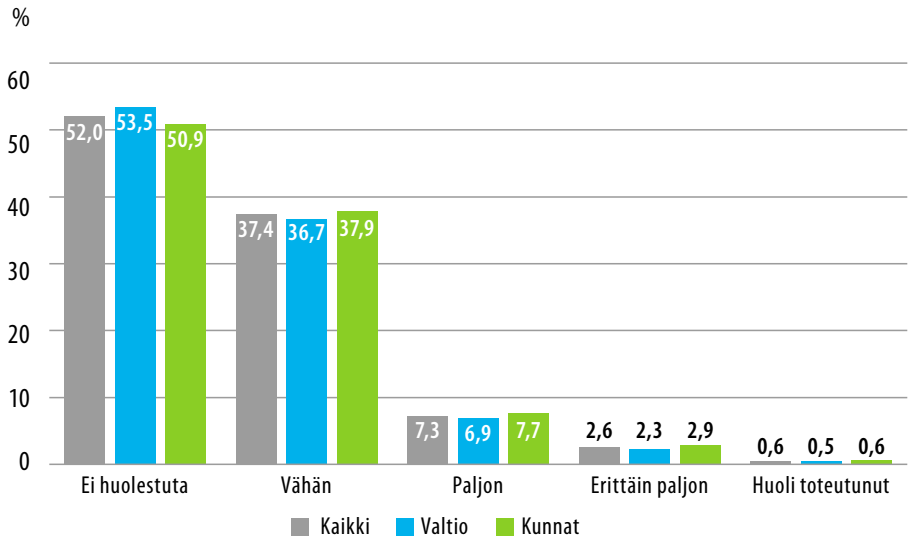
Viimeisessä käytännön arkea koskevassa kohdassa selvitettiin, mitkä sellaiset turvallisuuteen liittyvät asiat, jotka olivat vastaajille tärkeitä, huolestuttivat heitä työtehtävissä sekä sitä, oliko uhka toteutunut viimeisen kahden vuoden aikana. Huolen tai uhkan toteutumisella tarkoitettiin sitä, että työpaikalla oli tapahtunut tietoturvaan liittyvä yllättävä poikkeama tai muu kielteinen tapahtuma. Kaikkiin kysymyksen kohtiin, joita oli yhteensä 22, ei ollut pakko vastata, vaan ainoastaan tärkeäksi koettuihin. Huolestumista tai uhkan mahdollista toteutumista kysyttiin muun muassa henkilötietojen käsittelyyn, kuvallisiin henkilökortteihin ja nettihuijauksiin liittyen.

Eri kohtiin saatujen vastausten perusteella tärkeinä pidetyt tietoturvallisuuden osa-alueet eivät huolestuttaneet keskimäärin 52 % prosenttia vastaajista. 37,4 % oli keskimäärin vähän huolestuneita. 7,3 % huolestutti paljon ja 2,6 % erittäin paljon. Uhka tai huoli oli toteutunut keskimäärin 0,6 %:ssa tarkastelluista osa-alueista.

Tämän perusteella huolestuneisuus vastaajille tärkeistä tietoturvan osa-alueista on yleensä olematonta tai vähäistä. Havainto on yhteneväinen korkean turvallisuudentunteen kanssa (kohta 2.1.2). Alhaisen huolestuneisuuden, korkean turvallisuuden ja riittämättömän koulutuksen (kohta 2.1.3) välillä on kuitenkin ristiriita. Miten henkilöstön turvallisuudentunne on korkea ja huolestuneisuus vähäistä, kun koulutusta on saatu riittämättömästi?

Huolestuneisuus ei tarkoita samaa kuin uhkan toteutuminen. Huolessa on kyse loppujen lopuksi subjektiivisesta kokemuksesta. Tämä tarkoittaa toisaalta myös sitä, että osaa vastaajista ei välttämättä huolestuta jokin asia, vaikka ”faktat” tätä edellyttäisivät. Esimerkiksi toimitilaturvallisuus ei välttämättä huolestuta, vaikka työpaikalla on tapana jättää lukittavaksi tarkoitettuja ovia auki. Vastaavasti mobiililaitteiden käyttöön saatu riittämätön koulutus ei lisää huolestuneisuutta, jos siihen liittyviä tietoturvallisuusriskejä ei tunnisteta.

Kuva 10. Vastaajia huolestuttavat osa-alueet keskimäärin.



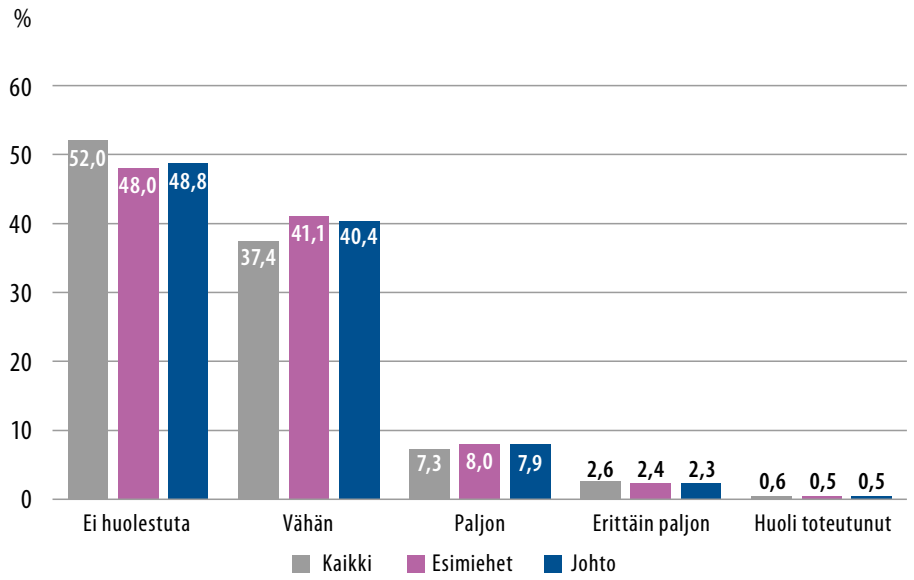
Vastauksia per kysymys tuli keskimäärin 13 245, joista valtiolta oli 6 322 ja kunnista 6 921. Kunnissa huolestuneiden osuus oli valtiota suurempi. Valtionhallinnon vastaajista keskimäärin 53,5 % ilmoitti, etteivät heitä huolestuttaneet heille tärkeät kohdat, kun taas kunnissa näin vastasi 50,9 %. Huolien ja uhkien toteutumisessa ei ollut suurta eroa valtionhallinnon ja kuntien välillä.

Taulukko 22. Vastaajia huolestuttavat osa-alueet keskimäärin.

Huolestuneisuus	Kaikki	%	Valtio	%	Kunnat	%
Ei huolestuta	6892	52,0 %	3380	53,5 %	3524	50,9 %
Vähän	4959	37,4 %	2323	36,7 %	2625	37,9 %
Paljon	971	7,3 %	438	6,9 %	531	7,7 %
Erittäin paljon	350	2,6 %	147	2,3 %	202	2,9 %
Huoli toteutunut	73	0,6 %	34	0,5 %	39	0,6 %
Yhteensä	**13245**	**100,0 %**	**6322**	**100,0 %**	**6921**	**100,0 %**

Kaikkien vastaajien, esimiesten ja johdon vastauksia vertailtaessa korostuu se, että esimiehet ja johto ovat hieman huolestuneempia eri uhista kuin kaikki vastaajat. Tämä voi johtua esimerkiksi siitä, että esimiehet ja johto kokivat saaneensa enemmän koulutusta ja ohjeistusta tietoturvallisuuteen. He siis osaavat olla huolissaan eri uhista.

Kuva 11. Eri vastaajatyyppejä huolestuttavat osa-alueet keskimäärin.



Eniten vastaajia huolestutti se, ettei heille tärkeä palvelu ole toiminnassa silloin, kun he tarvitsevat sitä. Kohtaan tuli toiseksi eniten vastauksia kaikista selvitetyistä osa-alueista. Ainoastaan 14,7 % kysymykseen vastanneesta 13481 henkilöstä ei ollut huolestunut asiasta. Tämä kertoo osaltaan siitä, kuinka tärkeä osa tietoturvallisuutta tiedon *saatavuus* on. Palveluiden ja tietojen tulisi olla käytössä aina esimerkiksi pelastustoimessa.

Toisaalta voidaan kysyä, huolestuttaako vastaajia palveluiden toimivuuteen liittyen useammin juuri tietoturvallisuus vai työtehtävien sujuvuus. Kun palvelu on alhaalla, moni saattaa

keskittyä työnsä sujumattomuuden tietoturvallisuuden pohtimisen sijasta. Työnteon sujuvuus on kuitenkin tässä tapauksessa yhteydessä tiedon saatavuuteen ja eheyteen. Kyseessä on siis sekä sujuvuus- että tietoturvallisuuskysymys.

Taulukko 23. Huolestuneisuus liittyen siihen, että tärkeä palvelu ei ole toiminnassa silloin, kun sitä tarvitaan.

Huolestuneisuus	Kaikki	%	Valtio	%	Kunnat	%
Ei huolestuta	1978	14,7 %	906	14,0 %	1072	15,3 %
Vähän	6265	46,5 %	3054	47,1 %	3211	45,9 %
Paljon	3319	24,6 %	1628	25,1 %	1691	24,1 %
Erittäin paljon	1168	8,7 %	528	8,2 %	640	9,1 %
Huoli toteutunut	751	5,6 %	362	5,6 %	389	5,6 %
Yhteensä	**13481**	**100,0 %**	**6478**	**100,0 %**	**7003**	**100,0 %**

Tekniikan toimivuus huolestutti vastaajia muutenkin. Haittaohjelmat (taulukko 24) ja laiterikko (taulukko 26) olivat molemmat varsin pelättyjä vastaajien joukossa. Haittaohjelmat eli virukset ja vastaavat huolestuttivat valtionhallinnossa huomattavasti kuntia enemmän. Tämä osa-alue koettiin myös kohdan tärkeimmäksi (13489 vastaajaa). Haittaohjelman iskeminen päätelaitteeseen huolestutti huomattavasti useammin kuin tietoturvapäivitysten ajantasaisuus (taulukko 25), vaikka tietoturvapäivitysten ajantasaisuus on tärkeä keino ehkäistä haittaohjelmien pääsemistä koneelle.

Taulukko 24. Huolestuneisuus liittyen siihen, että päätelaitteeseen iskee haittaohjelma.

Huolestuneisuus	Kaikki	%	Valtio	%	Kunnat	%
Ei huolestuta	3142	23,3 %	1439	22,2 %	3362	48,5 %
Vähän	8198	60,8 %	4008	61,9 %	3119	45,0 %
Paljon	1630	12,1 %	786	12,1 %	313	4,5 %
Erittäin paljon	463	3,4 %	209	3,2 %	133	1,9 %
Huoli toteutunut	56	0,4 %	31	0,5 %	9	0,1 %
Yhteensä	**13489**	**100,0 %**	**6473**	**100,0 %**	**6936**	**100,0 %**

Taulukko 25. Huolestuneisuus liittyen siihen, että päätelaitteen tietoturvapäivitykset eivät ole ajan tasalla.

Huolestuneisuus	Kaikki	%	Valtio	%	Kunnat	%
Ei huolestuta	7406	56,1 %	3580	56,7 %	3826	55,5 %
Vähän	4741	35,9 %	2228	35,3 %	2513	36,4 %
Paljon	742	5,6 %	352	5,6 %	390	5,7 %
Erittäin paljon	283	2,1 %	132	2,1 %	151	2,2 %
Huoli toteutunut	37	0,3 %	21	0,3 %	16	0,2 %
Yhteensä	**13209**	**100,0 %**	**6313**	**100,0 %**	**6896**	**100,0 %**

Taulukko 26. Huolestuneisuus liittyen siihen, että tärkeitä tietoja menetetään laiterikon takia.

Huolestuneisuus	Kaikki	%	Valtio	%	Kunnat	%
Ei huolestuta	3592	26,7 %	1749	27,1 %	1843	26,4 %
Vähän	6170	45,9 %	2973	46,0 %	3197	45,7 %
Paljon	2591	19,3 %	1251	19,4 %	1340	19,2 %
Erittäin paljon	981	7,3 %	428	6,6 %	553	7,9 %
Huoli toteutunut	122	0,9 %	63	1,0 %	59	0,8 %
Yhteensä	**13456**	**100,0 %**	**6464**	**100,0 %**	**6992**	**100,0 %**

Johdon riittämätön tuki tietoturvallisuudelle oli huolenaihe 55,5 %:lle vastaajista. Yleensä tuen puute huolestutti vähän, mutta joukossa oli runsaasti vastaajia, joita se huoletti paljon tai erittäin paljon. Kuntasektorilla huolestuneisuus oli valtionhallintoa suurempaa. Huoli on ymmärrettävää sen takia, että organisaation johto kantaa vastuun tietoturvallisuudesta. Samoin tämä voi heijastua siihen, miten johto toimii esimerkkinä tietoturvallisuuteen liittyvissä asioissa. Jos johdon tuki on vähäinen, saattaa se heijastua tietoturvallisuuteen liittyviin asenteisiin ja hitaaseen tietoturvakulttuurin muodostumiseen organisaatiossa.

Taulukko 27. Huolestuneisuus liittyen siihen, että johto ei tue riittävästi tietoturvallisuutta.

Huolestuneisuus	Kaikki	%	Valtio	%	Kunnat	%
Ei huolestuta	5917	44,5 %	3089	48,6 %	2827	40,6 %
Vähän	5819	43,7 %	2588	40,7 %	3231	46,5 %
Paljon	1027	7,7 %	439	6,9 %	588	8,5 %
Erittäin paljon	477	3,6 %	201	3,2 %	276	4,0 %
Huoli toteutunut	68	0,5 %	35	0,6 %	33	0,5 %
Yhteensä	**13308**	**100,0 %**	**6352**	**100,0 %**	**6955**	**100,0 %**

Vastaajia ei huolestuttanut heidän saamansa tietoturvallisuuskoulutuksen määrä. Paljon tai erittäin paljon tämä huolestutti yhteensä vain 13,2 %:a vastaajista. Tämä on mielenkiintoista, sillä kohdassa 3.1.3. läpi käyty vastaajien saama tietoturvallisuuskoulutus ja -ohjeistus eivät olleet yleensä riittävää (kuva 6). Vastaajat siis tunnistivat, että heitä ei ole koulutettu riittävästi, mutta tämä ei heitä huolestuta.

Taulukko 28. Huolestuneisuus liittyen siihen, että tietoturvallisuuteen ei ole koulutettu riittävästi.

Huolestuneisuus	Kaikki	%	Valtio	%	Kunnat	%
Ei huolestuta	4581	34,0 %	2482	38,6 %	2098	29,9 %
Vähän	7072	52,5 %	3266	50,8 %	3806	54,2 %
Paljon	1348	10,0 %	521	8,1 %	827	11,8 %
Erittäin paljon	427	3,2 %	151	2,3 %	276	3,9 %
Huoli toteutunut	30	0,2 %	9	0,1 %	21	0,3 %
Yhteensä	**13458**	**100,0 %**	**6429**	**100,0 %**	**7028**	**100,0 %**

Neljässä kohdassa selvitettiin vastaajien huolestuneisuutta heidän tietämykseensä liittyen. Vähiten huolestutti se, ettei vastaaja tiedä, kuinka henkilötietoja tulee käsitellä työtehtävissä (taulukko 29). Toiseksi vähiten se, ettei vastaaja tiedä, mitkä työtehtäviin liittyvät asiat ovat salassa pidettäviä (taulukko 30). Tietämys vastuista (taulukko 31) ja häiriötilanteissa toiminen (taulukko 32) huolestutti edellisiä enemmän.

Taulukko 29. Huolestuneisuus liittyen siihen, ettei tiedetä, kuinka henkilötietoja tulee käsitellä työtehtävissä.

Huolestuneisuus	Kaikki	%	Valtio	%	Kunnat	%
Ei huolestuta	8955	67,2 %	4259	67,1 %	4695	67,2 %
Vähän	3770	28,3 %	1809	28,5 %	1961	28,1 %
Paljon	468	3,5 %	215	3,4 %	253	3,6 %
Erittäin paljon	123	0,9 %	56	0,9 %	67	1,0 %
Huoli toteutunut	14	0,1 %	7	0,1 %	7	0,1 %
Yhteensä	**13330**	**100,0 %**	**6346**	**100,0 %**	**6983**	**100,0 %**

Taulukko 30. Huolestuneisuus liittyen siihen, ettei tiedetä, mitkä työtehtäviin liittyvät asiat ovat salassa pidettäviä.

Huolestuneisuus	Kaikki	%	Valtio	%	Kunnat	%
Ei huolestuta	8626	64,4 %	4105	64,3 %	4520	64,6 %
Vähän	3995	29,8 %	1946	30,5 %	2049	29,3 %
Paljon	583	4,4 %	257	4,0 %	326	4,7 %
Erittäin paljon	166	1,2 %	72	1,1 %	94	1,3 %
Huoli toteutunut	19	0,1 %	8	0,1 %	11	0,2 %
Yhteensä	**13389**	**100,0 %**	**6388**	**100,0 %**	**7000**	**100,0 %**

Taulukko 31. Huolestuneisuus liittyen siihen, ettei tiedetä vastuita tietoturvallisuuden osalta.

Huolestuneisuus	Kaikki	%	Valtio	%	Kunnat	%
Ei huolestuta	5359	40,1 %	2841	44,5 %	2517	36,0 %
Vähän	6227	46,5 %	2859	44,8 %	3368	48,2 %
Paljon	1371	10,2 %	527	8,3 %	844	12,1 %
Erittäin paljon	401	3,0 %	150	2,3 %	251	3,6 %
Huoli toteutunut	21	0,2 %	7	0,1 %	14	0,2 %
Yhteensä	**13379**	**100,0 %**	**6384**	**100,0 %**	**6994**	**100,0 %**

Taulukko 32. Huolestuneisuus liittyen siihen, ettei tiedetä, miten tulee toimia häiriötilanteissa.

Huolestuneisuus	Kaikki	%	Valtio	%	Kunnat	%
Ei huolestuta	5092	38,1 %	2720	42,7 %	2371	33,9 %
Vähän	6773	50,7 %	3095	48,6 %	3678	52,6 %
Paljon	1139	8,5 %	439	6,9 %	700	10,0 %
Erittäin paljon	303	2,3 %	94	1,5 %	209	3,0 %
Huoli toteutunut	50	0,4 %	19	0,3 %	31	0,4 %
Yhteensä	**13357**	**100,0 %**	**6367**	**100,0 %**	**6989**	**100,0 %**

Toimitilaturvallisuutta ja työn turvallisuutta työpaikan ulkopuolella selvitettiin neljässä kohdassa. Vähiten huolestutti se, ettei vastaajien toimipisteessä ole käytössä kuvallisia henkilökortteja (taulukko 33). Toimipaikan tilaturvallisuuden yleinen taso taas huoletti tätä enemmän (taulukko 34).

Se, että vastaaja joutuisi kuljettamaan ja käsittelemään salassa pidettäviä tietoja työpaikan ulkopuolella ei huolestuttanut kovinkaan paljon (taulukko 35). Etätyö huolestutti jonkin verran tätä enemmän (taulukko 36).

Taulukko 33. Huolestuneisuus liittyen siihen, että toimipisteessä ei ole käytössä kuvallisia henkilökortteja.

Huolestuneisuus	Kaikki	%	Valtio	%	Kunnat	%
Ei huolestuta	10459	80,2 %	5230	84,5 %	5229	76,2 %
Vähän	2021	15,5 %	748	12,1 %	1273	18,6 %
Paljon	340	2,6 %	128	2,1 %	212	3,1 %
Erittäin paljon	160	1,2 %	52	0,8 %	108	1,6 %
Huoli toteutunut	69	0,5 %	32	0,5 %	37	0,5 %
Yhteensä	**13049**	**100,0 %**	**6190**	**100,0 %**	**6859**	**100,0 %**

Taulukko 34. Huolestuneisuus liittyen siihen, että toimipaikan tilaturvallisuus ei ole riittävällä tasolla.

Huolestuneisuus	Kaikki	%	Valtio	%	Kunnat	%
Ei huolestuta	6506	48,9 %	3470	54,6 %	3035	43,7 %
Vähän	5206	39,2 %	2226	35,1 %	2980	42,9 %
Paljon	1042	7,8 %	432	6,8 %	610	8,8 %
Erittäin paljon	434	3,3 %	178	2,8 %	256	3,7 %
Huoli toteutunut	108	0,8 %	44	0,7 %	64	0,9 %
Yhteensä	**13296**	**100,0 %**	**6350**	**100,0 %**	**6945**	**100,0 %**

Taulukko 35. Huolestuneisuus liittyen siihen, että joudutaan kuljettamaan ja käsittelemään salassa pidettäviä tietoja työpaikan ulkopuolella.

Huolestuneisuus	Kaikki	%	Valtio	%	Kunnat	%
Ei huolestuta	9043	69,8 %	4462	72,4 %	4581	67,4 %
Vähän	3342	25,8 %	1501	24,3 %	1841	27,1 %
Paljon	402	3,1 %	141	2,3 %	261	3,8 %
Erittäin paljon	149	1,1 %	51	0,8 %	98	1,4 %
Huoli toteutunut	26	0,2 %	10	0,2 %	16	0,2 %
Yhteensä	**12962**	**100,0 %**	**6165**	**100,0 %**	**6797**	**100,0 %**

Taulukko 36. Huolestuneisuus liittyen siihen, että etätyöskentely ei ole turvallista työpaikan ulkopuolella.

Huolestuneisuus	Kaikki	%	Valtio	%	Kunnat	%
Ei huolestuta	7344	56,2 %	3481	55,8 %	3862	56,6 %
Vähän	4698	36,0 %	2313	37,1 %	2385	35,0 %
Paljon	762	5,8 %	335	5,4 %	427	6,3 %
Erittäin paljon	235	1,8 %	104	1,7 %	131	1,9 %
Huoli toteutunut	22	0,2 %	9	0,1 %	13	0,2 %
Yhteensä	**13061**	**100,0 %**	**6242**	**100,0 %**	**6818**	**100,0 %**

Tietoturvallisuuteen liittyvään rikollisuuteen ja tietojen päätymiseen vääriin käsiin liittyen vastaajat pääsivät arvioimaan peräti seitsemää kohtaa. Huolestuneisuus näihin liittyen on pääasiassa olematonta tai vähäistä. Eniten huolestutti se, että salassa pidettäviä tietoja päätyy henkilöille, joilla ei ole niihin oikeutta (taulukko 37) Vähiten vastaajia huolestutti se, että heitä uhkailtaisiin nettipalveluissa (taulukko 42)

Taulukko 37. Huolestuneisuus liittyen siihen, että salassa pidettäviä tietoja päätyy henkilöille, joilla ei ole niihin oikeutta.

Huolestuneisuus	Kaikki	%	Valtio	%	Kunnat	%
Ei huolestuta	5913	44,9 %	2953	47,2 %	2960	42,9 %
Vähän	6072	46,1 %	2808	44,9 %	3264	47,3 %
Paljon	838	6,4 %	365	5,8 %	473	6,8 %
Erittäin paljon	314	2,4 %	128	2,0 %	186	2,7 %
Huoli toteutunut	29	0,2 %	6	0,1 %	23	0,3 %
Yhteensä	**13166**	**100,0 %**	**6260**	**100,0 %**	**6906**	**100,0 %**

Taulukko 38. Huolestuneisuus liittyen siihen, että päätelaitteessa olevia salassa pidettäviä tietoja vuotaa ulkopuolisille.

Huolestuneisuus	Kaikki	%	Valtio	%	Kunnat	%
Ei huolestuta	6627	50,0 %	3265	51,7 %	3826	55,5 %
Vähän	5775	43,6 %	2656	42,1 %	2513	36,4 %
Paljon	591	4,5 %	278	4,4 %	390	5,7 %
Erittäin paljon	246	1,9 %	113	1,8 %	151	2,2 %
Huoli toteutunut	12	0,1 %	3	0,0 %	16	0,2 %
Yhteensä	**13251**	**100,0 %**	**6315**	**100,0 %**	**6896**	**100,0 %**

Taulukko 39. Huolestuneisuus liittyen siihen, että päätelaite päätyy vääriin käsiin.

Huolestuneisuus	Kaikki	%	Valtio	%	Kunnat	%
Ei huolestuta	6722	50,7 %	3163	49,9 %	1703	24,3 %
Vähän	5406	40,8 %	2659	42,0 %	4190	59,7 %
Paljon	805	6,1 %	379	6,0 %	844	12,0 %
Erittäin paljon	308	2,3 %	128	2,0 %	254	3,6 %
Huoli toteutunut	15	0,1 %	6	0,1 %	25	0,4 %
Yhteensä	**13256**	**100,0 %**	**6335**	**100,0 %**	**7016**	**100,0 %**

Taulukko 40. Huolestuneisuus liittyen siihen, että työtehtäviin liittyvä käyttäjätunnus ja salasana varastetaan.

Huolestuneisuus	Kaikki	%	Valtio	%	Kunnat	%
Ei huolestuta	7483	56,2 %	3664	57,7 %	3819	54,8 %
Vähän	5027	37,7 %	2318	36,5 %	2709	38,9 %
Paljon	556	4,2 %	259	4,1 %	297	4,3 %
Erittäin paljon	238	1,8 %	105	1,7 %	133	1,9 %
Huoli toteutunut	14	0,1 %	4	0,1 %	10	0,1 %
Yhteensä	**13318**	**100,0 %**	**6350**	**100,0 %**	**6968**	**100,0 %**

Taulukko 41. Huolestuneisuus liittyen siihen, että työtehtäviisi liittyviä tietoja yritetään urkkia tai vakoilla.

Huolestuneisuus	Kaikki	%	Valtio	%	Kunnat	%
Ei huolestuta	8357	63,3 %	3839	61,0 %	4518	65,5 %
Vähän	4051	30,7 %	2047	32,5 %	2004	29,0 %
Paljon	559	4,2 %	301	4,8 %	258	3,7 %
Erittäin paljon	196	1,5 %	91	1,4 %	105	1,5 %
Huoli toteutunut	29	0,2 %	13	0,2 %	16	0,2 %
Yhteensä	**13192**	**100,0 %**	**6291**	**100,0 %**	**6901**	**100,0 %**

Taulukko 42. Huolestuneisuus liittyen siihen, että joudutaan nettihuijauksen tai kiristyksen kohteeksi.

Huolestuneisuus	Kaikki	%	Valtio	%	Kunnat	%
Ei huolestuta	8614	66,2 %	4076	65,6 %	4538	66,8 %
Vähän	3646	28,0 %	1800	29,0 %	1846	27,2 %
Paljon	507	3,9 %	244	3,9 %	263	3,9 %
Erittäin paljon	226	1,7 %	89	1,4 %	137	2,0 %
Huoli toteutunut	10	0,1 %	3	0,0 %	7	0,1 %
Yhteensä	**13003**	**100,0 %**	**6212**	**100,0 %**	**6791**	**100,0 %**

Taulukko 43. Huolestuneisuus liittyen siihen, että nettipalveluissa uhkaillaan.

Huolestuneisuus	Kaikki	%	Valtio	%	Kunnat	%
Ei huolestuta	10726	82,3 %	5176	83,2 %	5550	81,5 %
Vähän	1878	14,4 %	858	13,8 %	1020	15,0 %
Paljon	251	1,9 %	116	1,9 %	135	2,0 %
Erittäin paljon	154	1,2 %	62	1,0 %	92	1,4 %
Huoli toteutunut	18	0,1 %	6	0,1 %	12	0,2 %
Yhteensä	**13027**	**100,0 %**	**6218**	**100,0 %**	**6809**	**100,0 %**

Se, että vastaajan työtehtävät edellyttävät tietoturvaohjeiden vastaista toimintaa, huoletti vastaajia suhteellisen harvoin. Valtionhallinnon ja kuntasektorin välillä ei ollut suuria eroja. 83 vastaajaa ilmoitti, että on joutunut toimimaan tietoturvaohjeiden vastaisesti. Huolimatta näiden vastaajien suhteellisesti pienestä osuudesta (0,6 % vastaajista) kyseessä on huolestuttava tulos.

Taulukko 44. Huolestuneisuus liittyen siihen, että työtehtävät edellyttävät tietoturvaohjeiden vastaista toimintaa.

Huolestuneisuus	Kaikki	%	Valtio	%	Kunnat	%
Ei huolestuta	9189	71,0 %	4412	71,5 %	4777	70,5 %
Vähän	2940	22,7 %	1353	21,9 %	1587	23,4 %
Paljon	492	3,8 %	243	3,9 %	249	3,7 %
Erittäin paljon	240	1,9 %	107	1,7 %	133	2,0 %
Huoli toteutunut	83	0,6 %	55	0,9 %	28	0,4 %
Yhteensä	**12944**	**100,0 %**	**6170**	**100,0 %**	**6774**	**100,0 %**

2.2 Tietoaineistojen luokittelu sekä luokittelua tukevat työvälineet ja palvelut

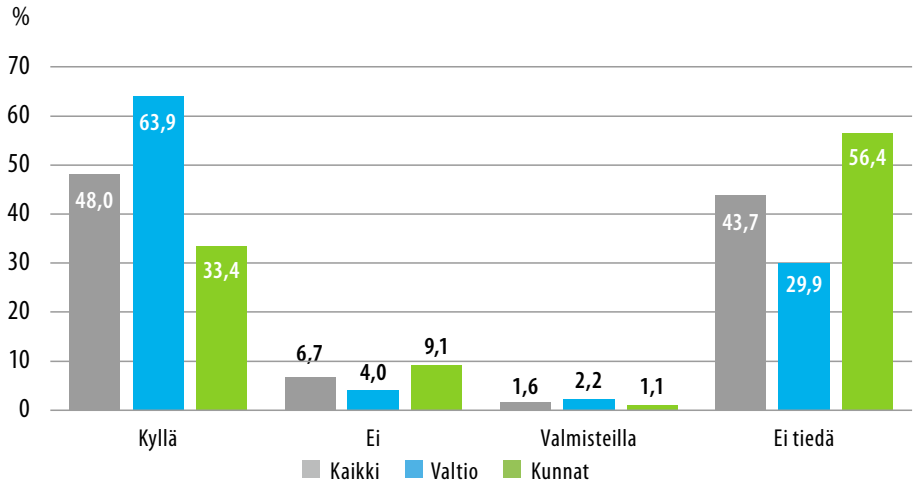
Tietoaineistojen luokitteluun sekä luokittelua tukeviin työvälineisiin ja palveluihin liittyen kysyttiin kaksi kysymystä. Lisäksi asiasta esitettiin kaksi alakysymystä, jotka aukesivat riippuen varsinaisessa kysymyksessä annetusta vastauksesta.

2.2.1 Ohjeistus salassa pidettävien tietojen luokitteluun

Ensin kysyttiin, oliko vastaajan organisaatiossa ohjeistus salassa pidettävien tietojen luokitteluun. Vastausohjeessa täsmennettiin, että ohjeistuksella tarkoitettiin kirjallista, konkreettista ohjetta, joka on olemassa organisaatiossa. Ohje voi perustua esimerkiksi julkisuuslakiin (621/1999). Kysymyksessä tarkoitetuksi ohjeistukseksi ei riittänyt, että vastaajaa oli koulutettu esimerkiksi lain sisällöstä, jos organisaatiokohtaisia ohjeita ei ollut saatavilla kirjallisesti.

Yleisin vastaus oli, että vastaajan organisaatiosta löytyy ohjeistus (48,0 %). Lähes yhtä usein vastaaja ei tiennyt, onko ohjeistusta olemassa (43,7 %). 6,7 % osasi sanoa, ettei ohjeistusta löydy ja 1,6 %, että sellainen on valmisteilla. Valtionhallinnon vastaajista peräti 63,9 % vastasi, että organisaatiosta löytyy ohjeet salassa pidettävien tietojen luokitteluun, kun kunnissa näin vastasi vain 33,4 % vastaajista. Tietämättömyys luokitteluohjeistuksien olemassaolosta oli molemmilla sektoreilla yllättävän yleistä.

Kuva 12. Luokitteluohjeistus vastaajien organisaatioissa (13913 vastaajaa).



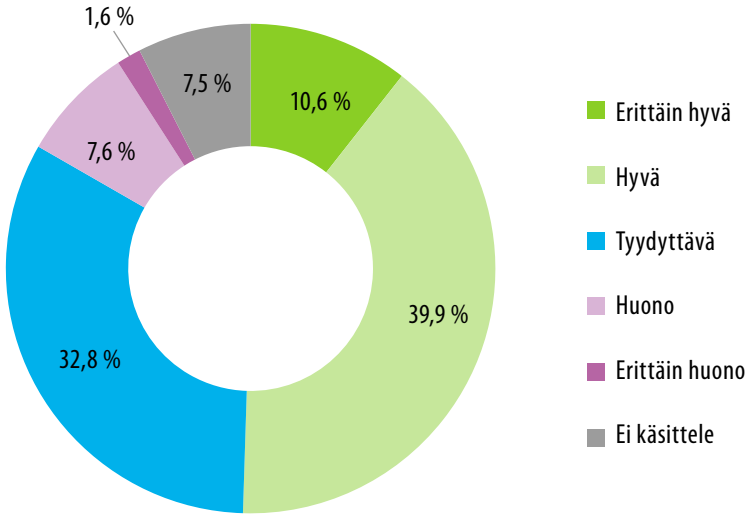
Taulukko 45. Luokitteluohjeistus vastaajien organisaatioissa.

Luokitteluohjeistus	Kaikki	%	Valtio	%	Kunnat	%
Kyllä	6677	48,0 %	4251	63,9 %	4251	33,4 %
Ei	930	6,7 %	266	4,0 %	266	9,1 %
Valmisteilla	223	1,6 %	145	2,2 %	145	1,1 %
Ei tiedä	6083	43,7 %	1990	29,9 %	1990	56,4 %
Yhteensä	**13913**	**100,0 %**	**6652**	**100,0 %**	**7260**	**100,0 %**

Niille vastaajille, jotka ilmoittivat, että heidän organisaatiossaan on olemassa ohjeistus salassa pidettävän tiedon luokitteluun, avautui lisäksi jatkokysymys, jossa selvitettiin, kuinka hyvin he osasivat käyttää tätä luokittelua. 10,6 % prosenttia vastaajista osasi käyttää luokittelua erittäin hyvin, 39,9 % hyvin, 32,8 % tyydyttävästi, 7,6 % huonosti ja 1,6 % erittäin huonosti. 7,5 % prosenttia ilmoitti, ettei käsittele salassa pidettävää tietoa. Kuntasektorilla luokitteluosaaminen oli jonkin verran valtionhallintoa parempaa.

Positiivista on se, että yhteensä alle kymmenesosa vastaajista ilmoitti, että heidän osaamisensa on huonoa tai erittäin huonoa ja peräti 83,3 % vastaajista osasi käyttää luokittelua erittäin hyvin, hyvin tai tyydyttävästi.

Kuva 13. Luokitteluosaaminen.



Kunnissa luokitteluosaaminen oli valtiota parempaa. Kunnissa osaamisensa koki erittäin hyväksi tai hyväksi yhteensä 49,5 %, kun valtiolla vastaava lukema oli 45,3 %. Tämä voi selittyä osittain kuntasektorin valtionhallintoa yksinkertaisemmalla, pääosin kaksitasoisella tietojen (julkinen / salainen) luokittelulla.[5]

Taulukko 46. Luokitteluosaaminen.

Luokitteluosaaminen	Kaikki	Valtio	Kunnat
Erittäin hyvä	10,6 %	8,0 %	15,1 %
Hyvä	39,9 %	37,3 %	44,4 %
Tyydyttävä	32,8 %	36,1 %	27,0 %
Huono	7,6 %	8,5 %	6,1 %
Erittäin huono	1,6 %	1,6 %	1,5 %
Ei käsittele	7,5 %	8,5 %	5,8 %
Yhteensä	**100,0 %**	**100,0 %**	**100,0 %**

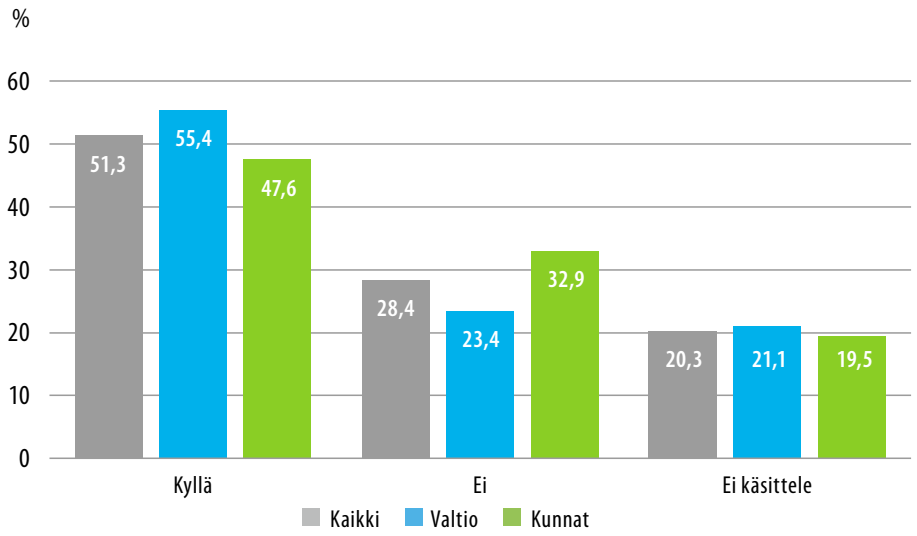
2.2.2 Palveluiden ja työkalujen käyttö salassa pidettävien tietojen käsittelyssä

Toiseksi haluttiin tietää, osasivatko vastaajat käyttää eri palveluita ja työkaluja salassa pidettävien tietojen käsittelyssä. Palveluilla ja työkaluilla tarkoitettiin esimerkiksi työkoneella tai verkossa olevia kansiota, sähköpostia sekä asianhallintajärjestelmiä. Käsittelyllä tarkoitettiin esimerkiksi salassa pidettävien tietojen lähettämistä ja tallentamista.

5 Ks. tietoturvallisuusasetuksen 681/2010 8 §

51,3 % tiesi, miten eri palveluita ja työkaluja tulee käyttää salassa pidettävien tietojen käsittelyssä, 28,4 % ilmoitti, ettei tiedä ja 20,3 % ilmoitti, ettei käsittele salassa pidettävää tietoa. Valtionhallinnossa työskentelevät osasivat käyttää palveluita ja työkaluja kuntasektorin vastaajia useammin. Tätä voi selittää se, että valtionhallinnossa on käytössä keskitetty palvelu turvallisen sähköpostin lähettämiseksi.

Kuva 14. Palveluiden käyttöosaaminen salassa pidettävien tietojen käsittelyssä (13913 vastaajaa).

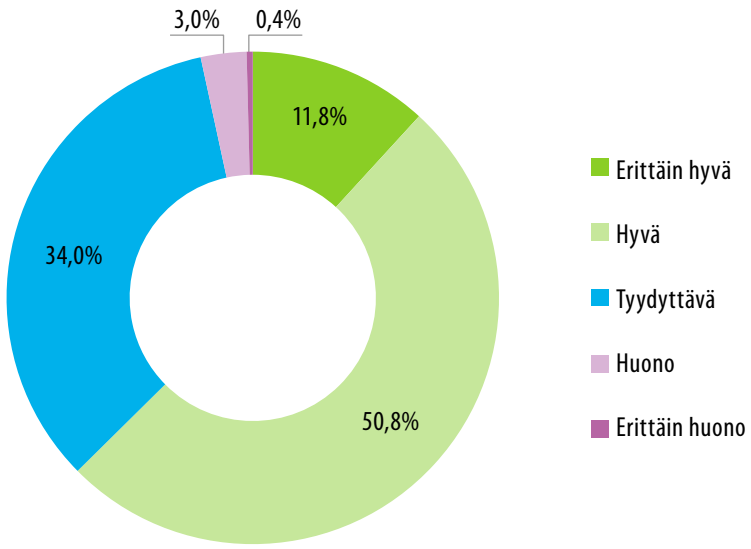


Taulukko 47. Palveluiden käyttöosaaminen salassa pidettävien tietojen käsittelyssä.

Osaaminen	Kaikki	%	Valtio	%	Kunnat	%
Kyllä	7141	51,3 %	3687	55,4 %	3453	47,6 %
Ei	3951	28,4 %	1559	23,4 %	2392	32,9 %
Ei käsittele	2821	20,3 %	1406	21,1 %	1415	19,5 %
Yhteensä	**13913**	**100,0 %**	**6652**	**100,0 %**	**7260**	**100,0 %**

Niiltä käyttäjiltä, jotka kokivat osaavansa käsitellä salassa pidettävää tietoa, kysyttiin jatkokysymyksenä, kuinka hyvä heidän osaamisensa oli. Erittäin hyvin salassa pidettävää tietoa osasi käsitellä 11,8 %, hyvin 50,8 %, tyydyttävästi 34,0 %, huonosti 3,0 % ja erittäin huonosi 0,4 %. Vaihtoehdon erittäin hyvin, hyvin tai tyydyttävästi valitsi yhteensä 96,6 % vastaajista. Ainoastaan 3,4 % koki osaavansa salassa pidettävän tiedon käsittelyn huonosti tai erittäin huonosti.

Kuva 15. Salassa pidettävän tiedon käsittelyosaaminen.



Valtionhallinnon ja kuntien väliset erot olivat hyvin pieniä. Kuntasektorilla käsittelyosaaminen oli jonkin verran valtiota korkeammalla tasolla.

Taulukko 48. Salassa pidettävän tiedon käsittelyosaaminen.

Käsittelyosaaminen	Kaikki	Valtio	Kunnat
Erittäin hyvä	11,8 %	10,8 %	12,9 %
Hyvä	50,8 %	50,4 %	51,2 %
Tyydyttävä	34,0 %	35,8 %	32,1 %
Huono	3,0 %	2,8 %	3,2 %
Erittäin huono	0,4 %	0,2 %	0,6 %
Yhteensä	**100,0 %**	**100,0 %**	**100,0 %**

2.3 Työskentely oman toimipaikan ulkopuolella

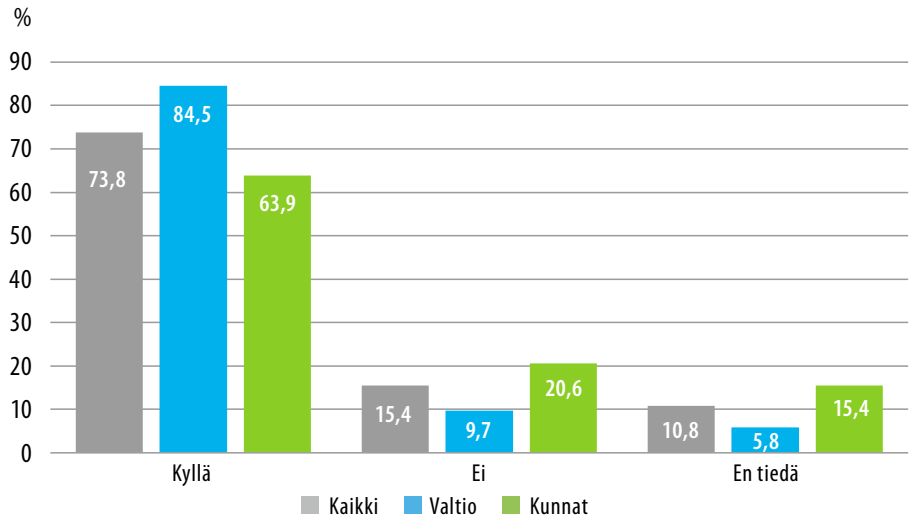
Työskentelyä oman toimipaikan ulkopuolella kartoitettiin erikseen kolmessa kysymyksessä. Kahdesta kysymyksestä avautui vastauksesta riippuen lisäksi jatkokysymys. Yksi kysymyksistä liittyi sähköpostin lukemiseen, jossa erityisenä mielenkiinnon kohteena oli sähköpostin lukeminen omilla vapaa-ajan laitteilla.

2.3.1 Mahdollisuus monipaikkaiseen työskentelyyn

Ensimmäiseksi kysyttiin sitä, salliko vastaajan organisaatio työskentelyn oman toimipaikan ulkopuolella. Työskentelyllä oman toimipaikan ulkopuolella tarkoitettiin niin sanottua monipaikkaista työskentelyä eli esimerkiksi etätyötä kotona, työskentelyä työmatkalla tai työtä oman työnantajan toisessa toimipisteessä.

Vastaajista 73,8 % prosenttia kertoi, että heidän organisaationsa salli työskentelyn oman toimipaikan ulkopuolella. 15,4 % prosenttia ei saanut työskennellä oman toimipaikan ulkopuolella ja 10,8 % prosenttia ei tiennyt, oliko monipaikkainen työskentely sallittua. Valtiolla (73,8 %) työskentely toimipaikalla oli useammin sallittua kuin kunnissa (63,9 %). Kunnissa oltiin epätietoisempia mahdollisuudesta työskennellä monipaikkaisesti.

Kuva 16. Monipaikkaisen työn salliminen vastaajien organisaatioissa.

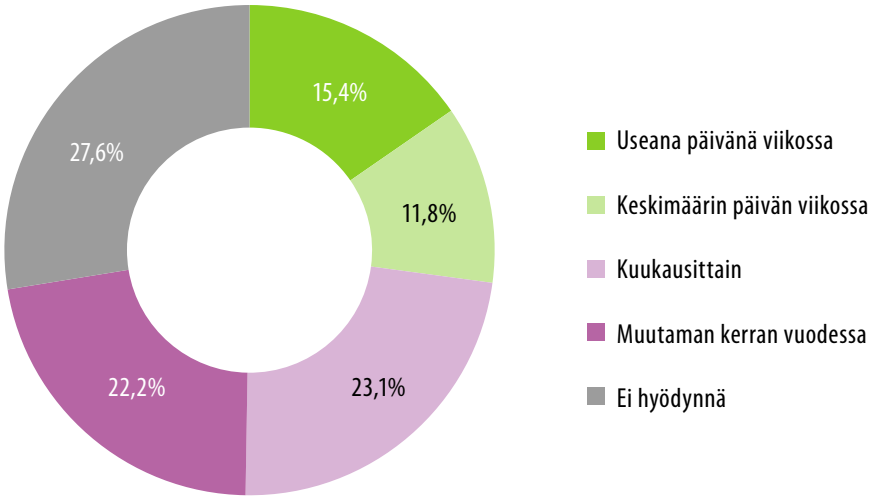


Taulukko 49. Monipaikkaisen työn salliminen vastaajien organisaatioissa.

Monipaikkainen työ	Kaikki	%	Valtio	%	Kunnat	%
Kyllä	10265	73,8 %	5624	84,5 %	4640	63,9 %
Ei	2140	15,4 %	642	9,7 %	1498	20,6 %
Ei tiedä	1507	10,8 %	386	5,8 %	1121	15,4 %
Yhteensä	**13912**	**100,0 %**	**6652**	**100,0 %**	**7259**	**100,0 %**

Niiltä vastaajilta, jotka saivat työskennellä oman toimipaikan ulkopuolella, selvitettiin vielä, kuinka usein he hyödynsivät tätä omassa työskentelyssään. Useana päivänä viikossa monipaikkaisesti työskenteli 15,4 %, keskimärin päivän viikossa 11,8 %, epäsäännöllisesti, mutta kuitenkin kuukausittain 23,1 % ja muutaman kerran vuodessa 22,2 %. 27,6 % ei työskennellyt oman toimipaikan ulkopuolella, vaikka tämä olisi ollut sallittua.

Kuva 17. Monipaikkaisen työn hyödyntäminen.



Niiden jatkokysymykseen vastanneiden vastaajien osuus, jotka työskentelivät monipaikkaisesti useana päivänä viikossa, oli suurempi kunnissa. Kunnissa työskentely oman toimipaikan ulkopuolella oli siis harvemmin sallittua, mutta silloin, kun se oli sallittua, sitä hyödynnettiin enemmän.

Taulukko 50. Monipaikkaisen työn hyödyntäminen.

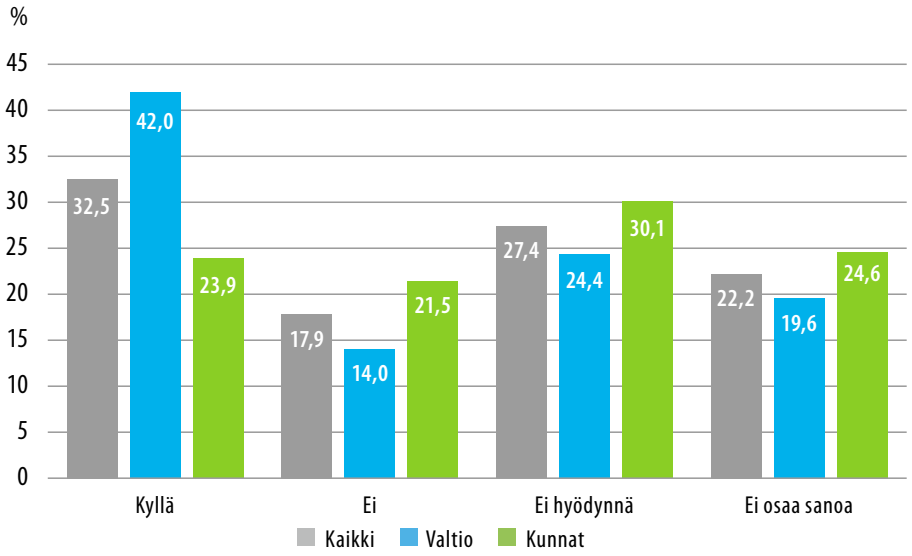
Hyödyntäminen	Kaikki	Valtio	Kunnat
Useana päivänä viikossa	15,4 %	11,9 %	19,6 %
Keskimäärin päivän viikossa	11,8 %	13,6 %	9,5 %
Kuukausittain	23,1 %	22,1 %	24,4 %
Muutaman kerran vuodessa	22,2 %	22,0 %	22,4 %
Ei hyödynnä	27,6 %	30,5 %	24,1 %
Yhteensä	**100,0 %**	**100,0 %**	**100,0 %**

2.3.2 Työskentelyn oman toimipaikan ulkopuolella ja tietoturvallisuuden huomioiminen

Seuraavaksi vastaajilta kysyttiin, oliko työskentelyä toimipaikan ulkopuolella ohjeistettu riittävästi myös tietoturvallisuuden näkökulmasta. Tällä tarkoitettiin, että vastaaja oli saanut ohjeistusta esimerkiksi päätelaitteiden ja salassa pidettävien tietoaineistojen käyttöön oman toimipaikan ulkopuolella.

32,5 % oli ohjeistettu riittävästi, 17,9 % prosenttia ei ollut ohjeistettu riittävästi, 27,4 % ilmoitti, ettei hyödynnä mahdollisuutta työskennellä toimipaikkansa ulkopuolella ja 22,2 % ei osannut sanoa. Valtionhallinnossa riittävä ohjeistus oli huomattavasti yleisempää kuin kuntasektorilla. Kunnissa oli myös paljon enemmän niitä, jotka eivät hyödyntäneet monipaikkaista työskentelyä.

Kuva 18. Riittävä ohjeistus toimipaikan ulkopuolella työskentelyyn.



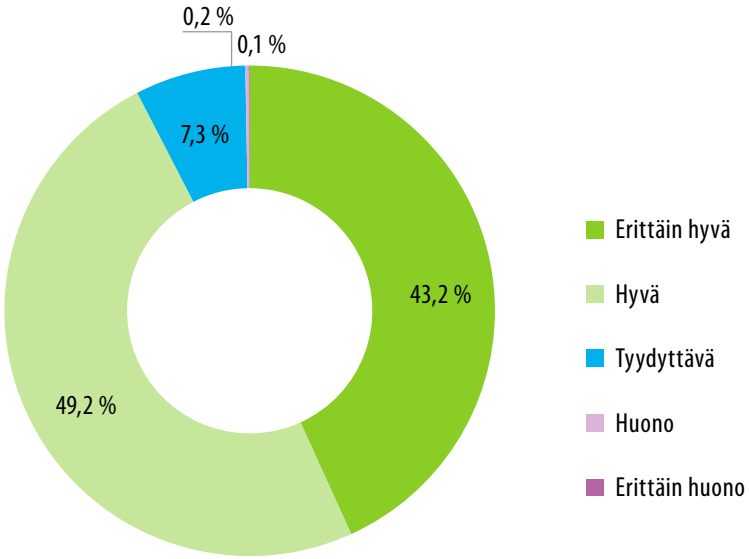
Taulukko 51. Riittävä ohjeistus toimipaikan ulkopuolella työskentelyyn.

Ohjeistus	Kaikki	%	Valtio	%	Kunnat	%
Kyllä	4528	32,5 %	2793	42,0 %	1735	23,9 %
Ei	2491	17,9 %	932	14,0 %	1559	21,5 %
Ei hyödynnä	3806	27,4 %	1623	24,4 %	2182	30,1 %
Ei osaa sanoa	3087	22,2 %	1304	19,6 %	1783	24,6 %
Yhteensä	**13912**	**100,0 %**	**6652**	**100,0 %**	**7259**	**100,0 %**

Niiden vastaajien, jotka vastasivat kyllä, tuli arvioida lisäksi, kuinka hyvin he pystyivät toimimaan saamansa ohjeistuksen perusteella. Eli ne vastaajat, jotka kokivat saaneensa riittävästi ohjeistusta, pääsivät arvioimaan *kykyään* toimia ohjeistuksen mukaisesti.

Erittäin hyvin toimimaan koki pystyvänsä 43,2 %, hyvin 49,2 %, tyydyttävästi 7,3 %, huonosti 0,2 % ja erittäin huonosti 0,1 % prosenttia kysymykseen vastanneista.

Kuva 19. Kyky toimia tietoturvaohjeistuksen mukaisesti.



Taulukko 52. Kyky toimia tietoturvaohjeistuksen mukaisesti.

Toimintakyky	Kaikki	Valtio	Kunnat
Erittäin hyvä	43,2 %	43,6 %	42,6 %
Hyvä	49,2 %	48,3 %	50,6 %
Tyydyttävä	7,3 %	7,7 %	6,6 %
Huono	0,2 %	0,3 %	0,1 %
Erittäin huono	0,1 %	0,0 %	0,1 %
Yhteensä	**100,0 %**	**100,0 %**	**100,0 %**

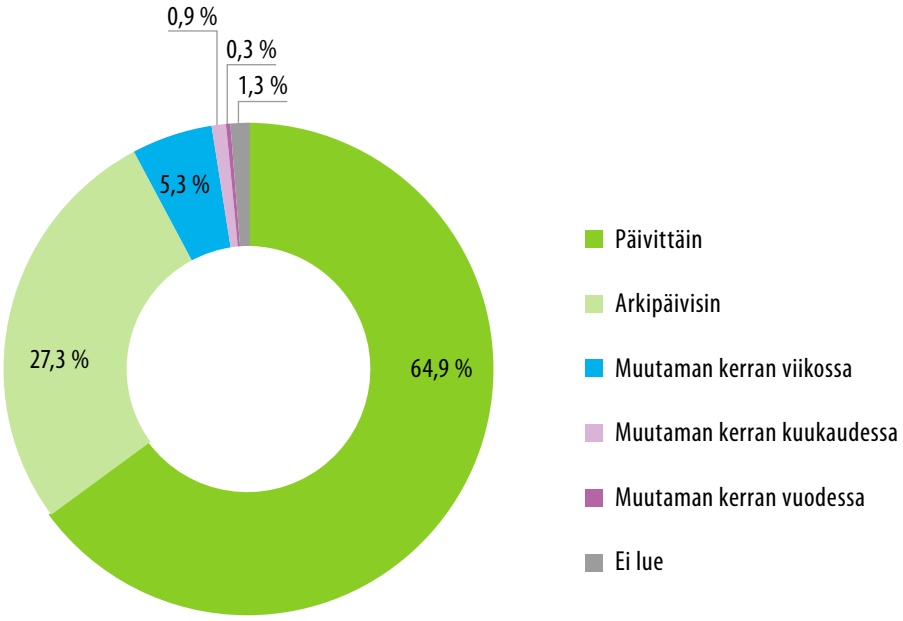
Kun ohjeistus on riittävää, pystytään yleensä toimimaan joko hyvin tai erittäin hyvin. Tosin riittäväkään ohjeistus ei riitä kaikissa tapauksissa siihen, että näin tapahtuisi. Tietoturva onkin viime kädessä kiinni niistä ihmisistä, jotka käytännön toiminnassaan toteuttavat tietoturvallisuutta.

2.3.3 Työsähköpostin lukeminen

Työskentelyyn oman toimipaikan ulkopuolella liittyen selvitettiin lisäksi, miten usein vastaajat lukivat työsähköpostia työvälineillä ja omilla vapaa-ajan laitteilla.

Työantajan antamilla välineillä organisaation sähköpostia luki päivittäin peräti 64,9 %, arkipäivisin 27,3 %, muutaman kerran viikossa 5,3 %, muutaman kerran kuukaudessa 0,9 % ja muutaman kerran vuodessa 0,3 % vastaajista. 1,3 prosenttia ilmoitti, ettei lue ollenkaan oman organisaationsa sähköpostia työnantajan välineillä

Kuva 20. Sähköpostin käyttö työnantajan laitteilla (13912 vastaajaa).



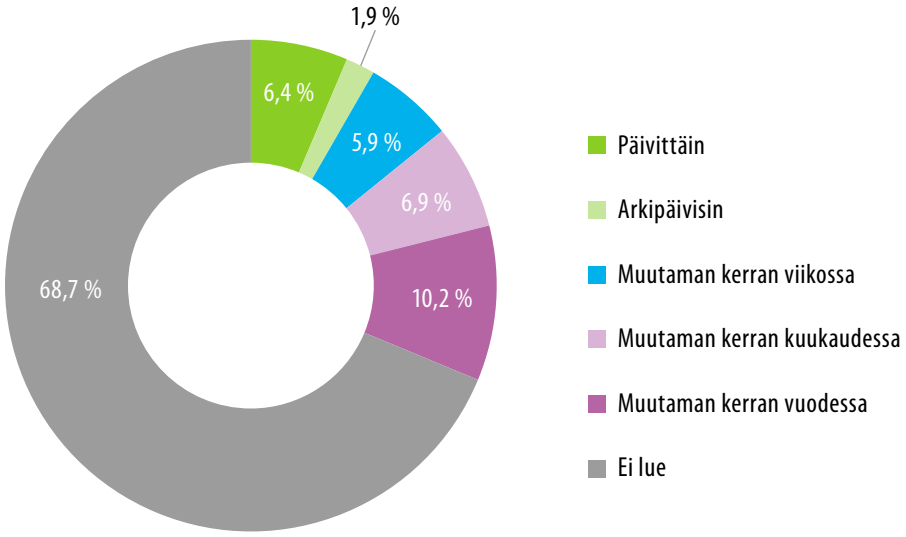
Valtiolla organisaation sähköpostia luettiin työantajan laitteilla jonkin verran enemmän kuin kunnissa.

Taulukko 53. Sähköpostin käyttö työnantajan laitteilla.

Työnantajan laitteilla	Kaikki	%	Valtio	%	Kunnat	%
Päivittäin	9032	64,9 %	4453	66,9 %	4578	63,1 %
Arkipäivisin	3796	27,3 %	1889	28,4 %	1907	26,3 %
Muutaman kerran viikossa	739	5,3 %	187	2,8 %	552	7,6 %
Muutaman kerran kuukaudessa	131	0,9 %	38	0,6 %	93	1,3 %
Muutaman kerran vuodessa	39	0,3 %	15	0,2 %	24	0,3 %
Ei lue	175	1,3 %	70	1,1 %	105	1,4 %
Yhteensä	**13912**	**100,0 %**	**6652**	**100,0 %**	**7259**	**100,0 %**

Omilla vapaa ajan laitteilla työsähköpostia luki päivittäin 6,4 %, arkipäivisin 1,9 %, muutaman kerran viikossa 5,9 %, muutaman kerran kuukaudessa 6,9 % ja muutaman kerran vuodessa 10,2 % vastaajissa. 68,7 prosenttia ilmoitti, ettei lue ollenkaan oman organisaationsa sähköpostia omilla laitteillaan.

Kuva 21. Työsähköpostin käyttö vapaa-ajan laitteilla (13912 vastaajaa).



Valtiolla omilla vapaa-ajan laitteilla organisaation sähköpostia luettiin paljon harvemmin kuin kunnissa. Valtionhallinnon vastaajista yhteensä 19,2 % ilmoitti lukevansa työsähköpostia omilla laitteilla, kun taas kunnissa vastaava luku oli 42,3 %.

Taulukko 54. Sähköpostin käyttö vapaa-ajan laitteilla (13912 vastaajaa).

Vapaa-ajan laitteilla	Kaikki	%	Valtio	%	Kunnat	%
Päivittäin	889	6,4 %	142	2,1 %	747	10,3 %
Arkipäivisin	267	1,9 %	42	0,6 %	225	3,1 %
Muutaman kerran viikossa	816	5,9 %	184	2,8 %	632	8,7 %
Muutaman kerran kuukaudessa	959	6,9 %	299	4,5 %	660	9,1 %
Muutaman kerran vuodessa	1418	10,2 %	611	9,2 %	807	11,1 %
Ei lue	9563	68,7 %	5374	80,8 %	4188	57,7 %
Yhteensä	**13912**	**100,0 %**	**6652**	**100,0 %**	**7259**	**100,0 %**

Se, että niinkin moni vastaaja käytti omia vapaa-ajan laitteitaan organisaationsa sähköpostin lukemiseen, on huolestuttavaa, koska se voi muodostaa tietoturvariskin. Tämä riippuu siitä, onko organisaatio sallinut sähköpostin lukemisen vapaa-ajan laitteilla. Jos näin on, on organisaatio myös tyypillisesti asettanut vaatimukset ja antanut ohjeet, kuinka vapaa-ajan laitteita tulee käyttää. Mikäli sähköpostin lukemista ei ole sallittu ja sitä luetaan siitä huolimatta, on mahdollista, että vapaa-ajan laitteille päätyy salassa pidettäviä tietoja, kuten arkaluonteisia henkilötietoja, joita sillä ei saisi käsitellä.

2.4 Tietoturvallisuuden merkitys ja toteuttaminen

Tietoturvabarometrin osallistujat pääsivät arvioimaan tietoturvallisuutta kahdessa kysymyksessä, joissa esitettiin neljä väittämää. Ensimmäisessä kysymyksessä selvitettiin tietoturvan merkitystä vastaajalle ja toisessa tietoturvan toteuttamista vastaajan organisaatiossa. Molemmissa kohdissa vastaajan tuli valita omasta mielestään sopivin väite tietoturvaan liittyen.

2.4.1 Tietoturvallisuuden merkitys – tietoturvallisuus on mahdollistaja

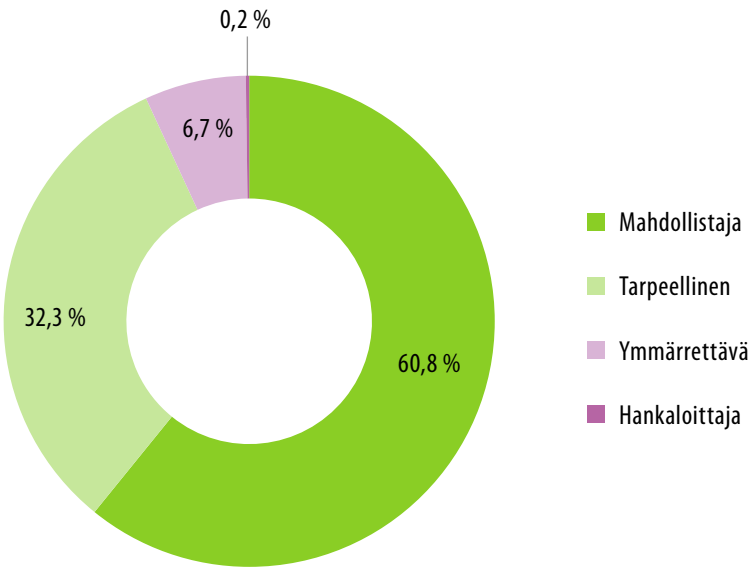
Ensimmäiseksi kysyttiin, millaisena vastaajat kokivat tietoturvallisuuden merkityksen. He saivat valita neljästä vaihtoehdosta sopivimman. Vaihtoehdot olivat:

1. ”Tietoturvallisuus mahdollistaa laadukkaan toiminnan ja antaa organisaatiostani luotettavan kuvan.”
2. ”Tietoturvallisuutta tarvitaan, jotta voin käsitellä työssä tarvitsemiani tietoja.”
3. ”Ymmärrän, miksi tietoturvallisuutta tarvitaan, mutta se aiheuttaa ylimääräistä työtä.”
4. ”Tietoturvallisuus on jatkuva riesa, en ymmärrä mihin sitä tarvitaan.”

Tietoturvallisuus koettiin *mahdollistajana*. Peräti 60,8 % vastaajista valitsi ensimmäisen vaihtoehdon. Vaihtoehdon 2 valitsi 32,3 %. Suurin osa niistä, jotka eivät valinneet ensimmäistä vaihtoehtoa, pitivät tietoturvallisuutta *tarpeellisena*. Vaihtoehdon 3 valitsi 6,7 %. Heille tietoturva oli *ymmärrettävä* asia, vaikka se aiheuttikin ylimääräistä työtä. Ainoastaan 0,2 % vastaajista valitsi vaihtoehdon 4. Näille vastaajille tietoturva oli toiminnan *hankaloittaja*.

Tietoturvallisuus nähdään siis julkishallinnon työntekijöiden keskuudessa varsin positiivisena asiana. Siihen kannattaa panostaa, jos haluaa mahdollistaa laadukkaan toiminnan ja antaa organisaatiostaan luotettavan kuvan. Samoin tämä heijastuu myös henkilöstön asenteeseen, joka vaikuttaa käytännön tasolla tietoturvallisuuden huomioimisena työskentelyssä.

Kuva 22. Tietoturvallisuuden merkitys (13913 vastaajaa).



Valtionhallinnon ja kuntasektorin vastauksien välillä oli vivahde-eroja. Valtionhallinnon vastaajat pitivät tietoturvallisuutta useammin mahdollistajana, kun kunnissa taas korostui sen tarpeellisuus.

Taulukko 55. Tietoturvallisuuden merkitys.

Merkitys	Kaikki	%	Valtio	%	Kunnat	%
Mahdollistaja	8465	60,8 %	4202	63,2 %	4263	58,7 %
Tarpeellinen	4488	32,3 %	1933	29,1 %	2554	35,2 %
Ymmärrettävä	930	6,7 %	510	7,7 %	420	5,8 %
Hankaloittaja	30	0,2 %	8	0,1 %	22	0,3 %
Yhteensä	**13913**	**100,0 %**	**6653**	**100,0 %**	**7259**	**100,0 %**

2.4.2 Tietoturvallisuuden toteuttaminen

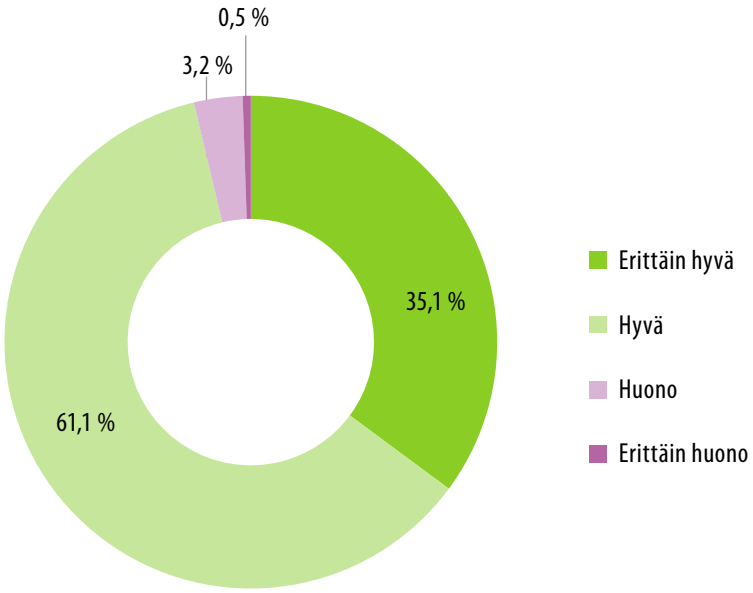
Toiseksi selvitettiin vastaajien kokemusta, tietoturvallisuuden toteuttamisesta organisaatioissa ja toteuttamisen vaikutuksesta työntekoon. Vastaajat saivat jälleen valita neljästä vaihtoehdosta sopivimman. Kysymys kuului: Miten koet, että tietoturvallisuus on toteutettu organisaatiossasi? Vaihtoehdot olivat:

1. ”Erittäin hyvin - työnteko ja palveluiden käyttö on sujuvaa ja vaivatonta”
2. ”Hyvin, mutta se saattaa satunnaisesti vaikeuttaa työntekoani”
3. ”Huonosti, koska se haittaa ja vaikeuttaa työntekoani usein”
4. ”Erittäin huonosti, koska se haittaa ja vaikeuttaa työntekoani jatkuvasti”

Tietoturvallisuus koki toteutuvan erittäin hyvin 35,1 %, jolloin työnteko ja palveluiden käyttö oli sujuvaa ja vaivatonta. 61,1 % vastaajista valitsi vaihtoehdon 2 eli tietoturvallisuus oli toteutettu heidän organisaatioissaan hyvin, mutta se saattoi satunnaisesti vaikeuttaa työntekoa. Tietoturvallisuuden koki toteutuvan huonosti 3,2 %, jolloin se haittasi vastaajan työntekoa usein. Ainoastaan 0,5 % koki, että tietoturvallisuus haittasi ja vaikeutti heidän työtään jatkuvasti.

Tietoturvallisuuden toteuttaminen on siis yleensä erittäin hyvää tai hyvää ja vain harvoin huonoa tai erittäin huonoa. 96,2 % vastaajista pitää tietoturvallisuuden toteuttamista omassa organisaatiossa erittäin hyvänä tai hyvänä. Tätä voidaan pitää erittäin tärkeänä havaintona. Vaikka usein kuullaan kielteistä palautetta siitä, että tietoturvallisuus hankaloittaa asioita, vain 3,7 % vastaajista kokee sen olevan toteutettu huonosti tai erittäin huonosti.

Kuva 23. Tietoturvallisuuden toteuttaminen vastaajien organisaatiossa.



Kuntasektorilla tietoturvallisuus toteutui useammin erittäin hyvin kuin valtionhallinnossa. Huonoksi tai erittäin huonoksi toteutuminen koettiin hivenen useammin valtionhallinnossa. Sekä valtiolla että kunnissa vastaukset olivat kuitenkin varsin samansuuntaisia.

Taulukko 56. Tietoturvallisuuden toteuttaminen vastaajien organisaatiossa

Toteutuminen	Kaikki	%	Valtio	%	Kunnat	%
Erittäin hyvä	4889	35,1 %	2247	33,8 %	2641	36,4 %
Hyvä	8505	61,1 %	4141	62,2 %	4364	60,1 %
Huono	444	3,2 %	232	3,5 %	212	2,9 %
Erittäin huono	74	0,5 %	33	0,5 %	41	0,6 %
Yhteensä	**13912**	**100,0 %**	**6653**	**100,0 %**	**7258**	**100,0 %**

Niiltä vastaajilta, jotka kokivat, että tietoturvallisuus toteutui huonosti tai erittäin huonosti eli niiltä, jotka valitsivat jommankumman kahdesta viimeisestä vastausvaihtoehdosta, kysyttiin lisäkysymyksenä, mikä erityisesti hankaloittaa heidän työntekoaan. Vastaajat saivat jättää tähän kohtaan avovastauksen. Avovastauksia tuli yhteensä 518.

Koulutuksen ja ohjeistuksen puute ja siihen liittyvä epätietoisuus olivat todella yleinen ongelma vastaajien keskuudessa. Monet joutuivat toimimaan itse hankittujen tietojen varassa. Tässäkin raportissa esitellyt tulokset riittävän koulutuksen ja ohjeistuksen puutteesta siis näkyvät joidenkin vastaajien arjessa.

> ”Koulutus on täysin riittämätöntä ja kollegojeni tiedot yksityisyydensuojasta ja tietoturvasta ovat viimevuotisen tutkimuksen mukaan heikolla tasolla. Pyysimme atk-vastaavien kanssa koulutusta tietoturvasta, mutta se evättiin henkilöstöltämme aika- ja rahapulaan vedoten.”

> ”Puutuvat ohjeet ja koulutus, toimin vanhoilla tiedoilla jotka olen itse joskus opiskellut”

> ”Ei ole ohjeistusta eikä tietojen luokittelua.”

> ”Minusta esimiehille tulisi kertoa/ opettaa mitä tietoja saa esim. lähettää sähköpostilla.”

Koulutukseenkin liittyvä organisointi ja tiedottaminen koettiin usein ongelmina tietoturvallisuuden suhteen. Vastaajat nostivat esille muun muassa asioiden tekemisen ”niin kuin on aina tehty” ja etätyön estämisen.

> ”Organisaatiossa tehdään paljon asioita, jossa tietoturvallisuus vaarantuu, kun tehdään niin kuin on aina tehty”

> ”Se, että etäyhteyttä ei myönnetä. Teen lähes 50 % työstä kaupungin netin ulkopuolella ja työntekoa vaikeuttaa, kun ei pääse tiedostoihin käsiksi.”

> ”Tietoturvallisuuteen ei yksinkertaisesti ole kiinnitetty riittävästi huomioita organisaatiossani. Ei se työntekoani vaikeuta; pikemminkin helpottaa.”

Avovastauksissa korostuivat myös salasanoihin liitetyt ongelmat. Salasanojen ja käyttäjätunnuksien määrä, muistaminen ja vaihtaminen aiheuttivat monelle vastaajalle päänvaivaa.

> ”Eri salasanat lukuisiin työssä tarvittaviin ohjelmiin, en voi muistaa niitä, niitä pitää päivittää toistuvasti ja eri rytmissä, ja ne pitää olla kirjoitettuna ylös”

> ”Lomien aikana vanhenevat salasanat. Koneelle kirjautumisen lisäksi joka kerta pitää naputella puolenkymmentä pitkää ja usein vaihdettavaa salasanaa vaikka salasanan takana olevaa pöytäkonettani ei käytä kukaan muu!”

Eräs vastaaja penäsi kuitenkin tiukempia salasanavaatimuksia, jotta tietoturvallisuus toteutuisi paremmin.

> ”Ei varsinaisesti hankaloita työntekoani, mutta minimisalasanavaatimukset saisi olla tiukemmat: nykyinen salasanasysteemi sallii hyvinkin yksinkertaiset salasanat.”

Monet olivat huolissaan sähköpostin toimimattomuudesta ja tietoturvallisuudesta. Esimerkiksi turvapostin puutetta ja roskapostia valiteltiin.

> ”Sähköpostin toimimattomuus haittaa erityisesti.”

> ”Työskentelisin paljon asiakkaiden ja verkostojen kanssa sähköpostitse mutta se ei ole salattu.”

> ”Sähköpostiin tulee jatkuvasti roskapostia, kaikista toimenpiteistä huolimatta”

Käytössä olevat ohjelmat aiheuttivat huolta ja ärtymystä. Monia olivat huolissaan puutteellisista päivityksistä, kun taas toisia harmitti, ettei ohjelmia saa asentaa itse.

> ”Ohjelmia ei päivitetä säännöllisesti, käytämme vanhentuneita ohjelmaversioita, jotka eivät välttämättä ole uusimpia ja turvallisuuden puolesta päivitetyimpiä.”

> ”Esimerkiksi työkoneelle en voi itse ladata tarvitsemiani ohjelmia.”

Ohjelmien välisten rajapintojen toimimattomuus koettiin varsin usein ongelmalliseksi.

> ”Tietojärjestelmiä on useita ja niihin kaikkiin on omat kirjautumistiedot. Niitä ei ole koottu hallittavaksi kokonaisuudeksi ja rajapinnat eri järjestelmien välillä ei toimi.”

> ”Työtehtävien pirstaleisuus, siis eri käyttöliittymät. Turhaa stressiä, kun kaikilla on jokin oma tunnuksensa jne. Sovellusergonomia vielä alkutekijöissään.”

Laitteiden toimimattomuus, puutteellisuus ja vanhentuneisuus oli myös yleinen huoli.

> ”Työhömme tarvittava laitteisto ja sovellukset saattavat olla toisinaan puutteellisia.”

Uhkien painottaminen toiminnan sujuvuuden kustannuksella harmitti erästä vastaajaa.

> ”Eri laitteita, eri salasanoja, eri ohjelmia, erimerkkisiä kaikkia. Toimitaan uhkien mahdollisuuden eikä todellisuuden mukaan.”

Se, että tietoturvallisuus on viime kädessä henkilöstöstä kiinni, nousi myös esiin.

> ”Tietoturvan puute huolestuttaa. suurin uhka aina tuolin ja näppäimistön välissä”

2.5 Johtoryhmään kuuluvien henkilöiden lisäkysymykset

Johtoryhmään kuuluneille vastaajille esitettiin kaksi lisäkysymystä. Ensimmäinen oli moniin alakohtiin jakautuva kysymys, jossa tuli arvioida esitettyjä osa-alueita kolmesta näkökulmasta ja toinen avokysymys. Näihin kysymyksiin tuli vastata, jos oli valinnut taustatiedot-kohdassa kuuluvansa organisaationsa johtoryhmään. Johdon kysymyksiin vastasi yhteensä 742 vastaajaa, joista valtionhallinnosta 344 ja kuntasektorilta 398.

2.5.1 Tietoturvallisuuden eri osa-alueiden toteutuminen omassa organisaatiossa

Ensimmäiseksi tuli vastata useampaa tietoturvallisuuden osa-aluetta koskevaan alakohtaan, ja arvioida esitettyjä väittämiä kolmesta näkökulmasta, jotka olivat *tärkeys, vaikeus ja toteutuminen*. Vastaajat pääsivät arvioimaan esimerkiksi riskienhallintaa, resursseja ja harjoittelua käsitelleitä väittämiä, joita oli yhteensä 15 näistä kolmesta näkökulmasta.

Eri osa-alueiden tärkeyttä arvioitiin asteikolla 0-4. Vaihtoehdot olivat seuraavat:

- 4 erittäin tärkeää
- 3 tärkeää
- 2 ei kovin tärkeää
- 1 ei lainkaan tärkeää
- 0 en osaa arvioida

Vaikeutta arvioitiin samoin asteikolla 0-4. Vaihtoehdot olivat seuraavat:

- 4 erittäin vaikeaa
- 3 melko vaikeaa
- 2 melko helppoa
- 1 erittäin helppoa
- 0 en osaa arvioida

Toteutumistakin arvioitiin asteikolla 0-4. Vaihtoehdot olivat seuraavat:

- 4 erittäin hyvin
- 3 melko hyvin
- 2 melko huonosti
- 1 erittäin huonosti
- 0 en osaa arvioida

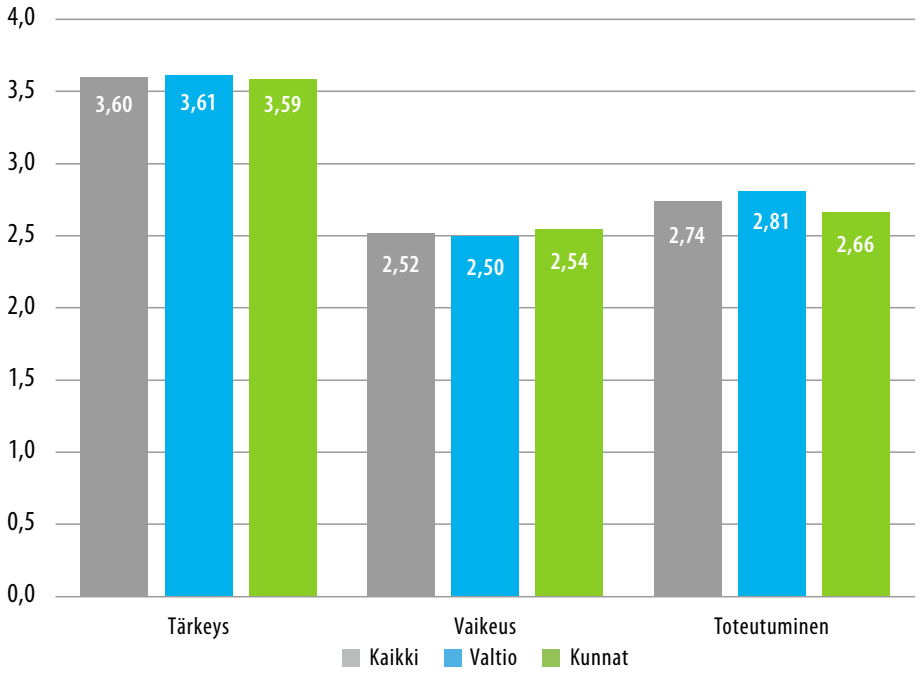
Kaikkien väittämien saamia keskiarvoja tarkastellessa korostuu se, että tietoturvallisuuden eri osa-alueita pidetään todella tärkeinä. Tärkeyden saama lukema on peräti 3,60, kun asteikko on 1-4. Tämä tarkoittaa, että eri osa-alueiden keskiarvo asettuu erittäin tärkeän ja tärkeän välimaastoon – kuitenkin lähemmäksi erittäin tärkeää. Kunnissa ja valtiolla tietoturvallisuuden osa-alueita pidetään keskimäärin suunnilleen yhtä tärkeinä.

Eri osa-alueiden toteuttamisen vaikeus asettuu asteikolla 1-4 lukemaan 2,52. Kuntasektorilla vaikeus on 0,05 yksikköä valtionhallintoa suurempaa. Kaiken kaikkiaan vaikeus asettuu keskimäärin melko helpon ja melko vaikean välimaastoon.

Toteutuminen käytännössä oli keskimäärin hieman melko hyvän alapuolella (2,74/4,00). Valtiolla eri osa-alueiden toteutuminen oli johtoryhmäläisten mielestä jonkin verran kuntia parempaa. Ero toteutumisessa valtionhallinnon ja kuntasektorin välillä oli keskimäärin 0,15 yksikköä.

Valtionhallinnon ja kuntasektorin vastausten välinen erotus on laskettu kaikkien osa-alueiden osalta, ja se esitetään kussakin taulukossa viimeisenä. Jos lukema on positiivinen, tarkoittaa se, että valtionhallinnon tulos on kuntasektoria korkeampi. Samoin, jos lukema on negatiivinen, kuntien vastauksissa on saatu korkeampi lukema.

Kuva 24. Kaikkien kohtien keskiarvo.



Johtoryhmän kysymyksistä saatujen tulosten mukaan tietoturvallisuus koetaan todella tärkeäksi, mutta toteutuminen jättää toivomisen varaa. Tämän perusteella voidaan todeta, että sekä kuntasektorilla että valtionhallinnossa on tarvetta edelleen lisätuelle, -koulutukselle ja -ohjeistukselle. Kunnissa tämä tarve on hieman valtiota suurempi. Onnistuneen koulutuksen myötä osa-alueiden toteuttamisen koettu vaikeuskin todennäköisesti laskisi.

Johtoryhmään kuuluvien vastaajien käsittelemät osa-alueet esitellään johtoryhmäläisten vastausten perusteella muodostetussa tärkeysjärjestyksessä. Tärkeimmäksi osa-alueeksi nostettiin se, että henkilöstö noudattaa olemassa olevia tietoturvaohjeita. Tämä toteutui kunnissa valtionhallintoa paremmin.

Taulukko 57. Henkilöstö noudattaa olemassa olevia tietoturvaohjeita.

Sektori	Tärkeys	Vaikeus	Toteutuminen
Kaikki	3,82	2,61	2,82
Valtio	3,85	2,64	2,79
Kunnat	3,80	2,58	2,85
Ero	0,05	0,06	-0,06

Sitoutumista tietoturvallisuuden toteuttamiseen johtoryhmän jäsenenä pidettiin heti henkilöstön toiminnan jälkeen toiseksi tärkeimpänä. Johtoryhmän sitoutuminen tietoturvallisuuteen nähtiin helpompana toteuttaa kuin se, että henkilöstö noudattaisi tietoturvaohjeita. Johtoryhmän sitoutumisen katsottiin myös toteutuvan henkilöstön toimintaa paremmin.

Taulukko 58. Sitoutuminen tietoturvallisuuden toteuttamiseen johtoryhmän jäsenenä.

Sektori	Tärkeys	Vaikeus	Toteutuminen
Kaikki	3,76	2,22	3,18
Valtio	3,76	2,23	3,21
Kunnat	3,75	2,21	3,16
Ero	0,01	0,02	0,05

Kolmas kohta käsitteli toimivaa tiedonkulkua organisaation sisällä. Tiedonkulku ja se, että organisaation ylin johto saa turvallisuudesta tarpeeksi tietoa koettiin varsin tärkeäksi, ei kovin vaikeaksi ja toteutumiseltaan hyväksi. Valtionhallinnossa tiedonkulkua pidettiin helpompana toteuttaa ja kunnissa sen koettiinkin toteutuvan huonommin.

Taulukko 59. Tiedonkulku organisaation sisällä toimii ja organisaation ylin johto saa turvallisuudesta tarpeeksi tietoa.

Sektori	Tärkeys	Vaikeus	Toteutuminen
Kaikki	3,73	2,45	2,86
Valtio	3,74	2,37	2,93
Kunnat	3,73	2,51	2,79
Ero	0,01	-0,14	0,14

Johtoryhmäläisten riittävä osaaminen oli valtiolla kuntia yleisempää (taulukko 59). Toisaalta organisaation tietoturvaosaaminen koettiin kuntasektorilla valtionhallintoa paremmaksi (taulukko 60).

Taulukko 60. Itselläni ja organisaationi muulla johdolla on tietoturvallisuuteen tarvittava osaaminen.

Sektori	Tärkeys	Vaikeus	Toteutuminen
Kaikki	3,72	2,54	2,92
Valtio	3,70	2,56	3,01
Kunnat	3,74	2,53	2,84
Ero	-0,03	0,03	0,17

Taulukko 61. Käytettävissä oleva organisaation tietoturvaosaaminen on riittävän korkeatasoista.

Sektori	Tärkeys	Vaikeus	Toteutuminen
Kaikki	3,72	2,61	2,90
Valtio	3,76	2,60	2,79
Kunnat	3,68	2,61	3,01
Ero	0,07	-0,01	-0,22

Riskienhallinnan toimivuutta pidettiin kunnissa valtiota tärkeämpänä. Sen myös koettiin toteutuvan kunnissa valtiota paremmin.

Taulukko 62. Riskienhallinta organisaation eri tasoilla on toimivaa.

Sektori	Tärkeys	Vaikeus	Toteutuminen
Kaikki	3,72	2,66	2,80
Valtio	3,67	2,74	2,76
Kunnat	3,77	2,60	2,84
Ero	-0,10	0,14	-0,07

Organisoinnin ja vastuutuksen toteutuminen vaatimusten mukaisesti koettiin valtionhallinnossa kuntia helpommaksi. Valtiolla se toteutuikin kuntia paremmin.

Taulukko 63. Tietoturvallisuuden organisointi ja vastuutus on toteutettu vaatimusten mukaisesti.

Sektori	Tärkeys	Vaikeus	Toteutuminen
Kaikki	3,68	2,48	2,88
Valtio	3,71	2,45	2,96
Kunnat	3,65	2,51	2,81
Ero	0,05	-0,07	0,15

Teknistä tietoturvallisuutta pidettiin valtionhallinnossa kuntia tärkeämpänä, vaikeampana ja paremmin toteutuvana.

Taulukko 64. Tekninen tietoturvallisuus on riittävä estämään keskeisimpien tietoturvauhkien toteutumisen.

Sektori	Tärkeys	Vaikeus	Toteutuminen
Kaikki	3,66	2,59	2,91
Valtio	3,70	2,64	2,96
Kunnat	3,63	2,54	2,86
Ero	0,07	0,10	0,10

Se, että sopimuksissa huomioidaan tietoturvallisuus ja toiminnan jatkuvuus on vaadittavalla tasolla, koettiin valtionhallinnossa vaikeammaksi, mutta toisaalta paremmin toteutuvaksi kuin kunnissa.

Taulukko 65. Sopimuksissa on huomioitu tietoturvallisuus ja toiminnan jatkuvuus vaadittavalla tasolla.

Sektori	Tärkeys	Vaikeus	Toteutuminen
Kaikki	3,64	2,49	2,85
Valtio	3,65	2,45	2,91
Kunnat	3,63	2,54	2,78
Ero	0,02	-0,08	0,13

Kunnissa koettiin, että tarvittavat talous- ja henkilöstöresurssit on vaikeampaa saada käyttöön kuin valtionhallinnossa. Valtionhallinnossa koettiinkin riittävän resursoinnin toteutuvan paremmin.

Taulukko 66. Käytössä on tietoturvallisuuteen tarvittavat talous- ja henkilöstöresurssit.

Sektori	Tärkeys	Vaikeus	Toteutuminen
Kaikki	3,62	2,66	2,69
Valtio	3,62	2,63	2,74
Kunnat	3,62	2,70	2,65
Ero	0,00	-0,07	0,10

Tietoturvapoikkeamien ja häiriötilanteiden toimintamallin kuvaaminen ja käyttöönotto oli toteutunut valtiolla kuntasektoria paremmin.

Taulukko 67. Tietoturvapoikkeamien ja häiriötilanteiden toimintamalli on kuvattu ja käytössä.

Sektori	Tärkeys	Vaikeus	Toteutuminen
Kaikki	3,55	2,58	2,54
Valtio	3,58	2,54	2,62
Kunnat	3,53	2,62	2,46
Ero	0,05	-0,09	0,16

Valtionhallinnossa pidettiin tietoturvapoikkeamista ilmoittamista Viestintävirastossa toimivalle Kyberturvallisuuskeskukselle kuntasektoria tärkeämpänä ja huomattavasti helpompana. Osa-alue toteutuikin valtionhallinnossa kuntia paljon paremmin.

Taulukko 68. Tietoturvapoikkeamista ilmoitetaan Viestintävirastossa toimivalle Kyberturvallisuuskeskukselle.

Sektori	Tärkeys	Vaikeus	Toteutuminen
Kaikki	3,42	2,40	2,59
Valtio	3,49	2,23	2,86
Kunnat	3,35	2,57	2,27
Ero	0,14	-0,35	0,59

Tietoturva-auditointeja pidettiin hieman tärkeämpinä kunnissa, mutta ne toteutuivat valtionhallinnossa paremmin.

Taulukko 69. Tietoturva-auditointeja ja muita tarkastuksia tehdään tai teetetään säännöllisesti.

Sektori	Tärkeys	Vaikeus	Toteutuminen
Kaikki	3,35	2,49	2,51
Valtio	3,34	2,43	2,67
Kunnat	3,36	2,56	2,32
Ero	-0,02	-0,13	0,35

Sitä, että johto käsittelee tietoturvatilannetta säännöllisesti, pidettiin monia muita kohtia vähemmän tärkeänä. Toteutuminen oli valtionhallinnossa jonkin verran kuntia parempaa.

Taulukko 70. Johto käsittelee tietoturvatilannetta säännöllisesti.

Sektori	Tärkeys	Vaikeus	Toteutuminen
Kaikki	3,31	2,31	2,53
Valtio	3,33	2,26	2,67
Kunnat	3,30	2,36	2,40
Ero	0,04	-0,10	0,27

Vähiten tärkeimpänä pidettiin häiriötilanteiden hallinnan riittävää harjoittelua. Kohdan tärkeydeksi arvioitiin kuitenkin peräti 3,30 asteikolla 1-4. Tämä kertoo siitä, että kaikkia tietoturvallisuuteen liittyviä osa-alueita pidetään varsin tärkeinä julkishallinnon johtoryhmäläisten keskuudessa. Kohdan toteutuminen oli johtoryhmän vastaajien mukaan melko huonolla tasolla.

Taulukko 71. Häiriötilanteiden hallintaa harjoitellaan riittävästi

Sektori	Tärkeys	Vaikeus	Toteutuminen
Kaikki	3,30	2,70	2,07
Valtio	3,29	2,68	2,21
Kunnat	3,31	2,71	1,93
Ero	-0,02	-0,03	0,28

2.5.2 Keskitetyn tuen tarve tietoturvan kehittämisessä

Tietoturvallisuuden eri osa-alueiden arvioimisen jälkeen johtoryhmiin kuuluneet vastaajat pääsivät arvioimaan avovastauksena, millaista keskitettyä tukea he haluaisivat julkishallinnon tietoturvan kehittämiseen. Vastaajat saivat arvioida kysymystä sekä oman organisaation että koko julkishallinnon näkökulmasta.

Johtoryhmän vastauksissa resurssit nousivat esille enemmän kuin kaikkia vastaajia avovastauskohdissa. Resurssien vähyyttä valiteltiin.

> ”Resurssit ovat liian tiukalla tähän asiaan paneutumiseen. Ja tietoa organisaatioissa aivan liian vähän.”

Koulutus ja ohjeistus nousivat esille myös johtoryhmäläisten avovastauksissa. He kaipasivat käytännön koulutuksen ja tiedon jakamisen ohella selkeyttä ohjeistuksiin.

”Ett aktivare grepp gällande dessa frågor, utbildning och informationspridning. Eftersom vi har ett intranät så borde man kunde utnyttja det mer för den här typen av information.”

”Informaatiota tietoturvan tavallisimmista epäonnistumisista ja syistä epäonnistumisiin (mitä pahikset tavallisesti tekevät). Keinot suojautumiseen käytännön elämässä (kuinka pahikset torjutaan).”

”Tukea/ohjeita toimintamallien kertaukseen, häiriötilanteiden harjoitteluun. Tarvitaanko tuotantoyksikkökohtaisia ohjeita?”

”Lähiesimiehille suunnattua koulutusta.”

Ohjeistukseen liittyvään tietoturvallisuuden organisointiin, vastuihin ja rooleihin liittyen tarvitaan myös paljon tukea.

”Selkeät ohjeistukset ja vastuut - tällä hetkellä on todella vaikea sanoa, että mitä keneltäkin odotetaan ja kuka tietoturvasta vastaa.”

”Ohjeistusta eri tasoille, toiminnan keskeiset roolit ja organisointi.”

Eräs vastaaja painotti tietoturvatestaamisen merkitystä.

”Tietoturvatestit määrävälein ovat tärkeitä kertauskursseja.”

Koulutuksen ja ohjeistuksen lisäksi kaivattiin ajantasaista tiedottamista.

”Uhkamuutoksista tiedottamista”

”Jos kyberuhkaa on ilmassa, siitä valtionhallinnon sisäistä tiedottamista.”

Toimivat tietojärjestelmät ja laitteet saivat myös joitain mainintoja.

”Toimivat tietojärjestelmät 24/7”

”Mobiililaitteiden käytön turvallisuus ja sosiaalisen median riskit/hyödynnettävyys (siis ihan konkreettiset toimet)”

Loppujen lopuksi on siis kyse pienistä teoista, jotka kuitenkin saattavat olla vaikeita toteuttaa. Eräs johtoryhmän vastaaja kiteytti keskitetyn tuen tarpeen seuraavanalaisesti:

”Ihan perusasioita”

2.6 Oman organisaation turvallisuuden kehittämistarpeet – ei harjaa oven väliin

Kyselyn lopussa vastaajat saivat arvioida vapaamuotoisesti turvallisuuden kehittämiseen liittyviä tarpeita omassa organisaatiossaan. Avokysymys koski kaikkia vastaajia – myös johtoryhmiin kuuluvia. Vastauksia annettiin runsaasti ja niissä korostuivat jälleen konkreettiset perusasiat.

> ”Miten kannattaisi määritellä turvallinen salasana ja kuinka usein sitä pitäisi vaihtaa? Mitä sivustoja kannattaisi työtehtävissä välttää (listaus)?”

Toimitilaturvallisuuteen kiinnitettiin huomiota aiempia kohtia enemmän. Eräässä organisaatiossa oli ongelmana lukittuna pidettäväksi tarkoitetun oven auki pitäminen harjaa käyttäen.

> ”Lukittuna pidettävän ulko- oven väliin ei laiteta esim. harjaa.”

Muita koettuja ongelmia toimitilaturvallisuuteen liittyen olivat muun muassa hälytysjärjestelmät, vartijat ja yksityisyys työtehtäviä hoidettaessa.

> ”Hälyttimet, vartijat ym. tällaisen toiminnan edellyttämälle tasolle. Tätä tosin onkin kehitetty siihen suuntaan ja jatkossa ilmeisesti entistä enemmänkin.”

> ”Henkilökorttien käyttöönotto”

> ”Työtilassa käyvien ulkopuolisten ihmisten näkyvillä ja kuulolla ei ole asioita.”

> ”Asiakaspalvelupisteet turvallisemmiksi = asiakas ei pääse samaan tilaan asiakaspalvelijan kanssa, vaan palvelu tapahtuu luukulta”

Vastaajat nostivat useasti esiin erilaiset tietoturvallisuuteen liittyvät vastuut ja roolit.

> ”Nimeämällä vastuuhenkilö, joka sopivassa vaiheessa käy tietoturva-asiat läpi henkilöstönsä kanssa.”

> ”Henkilöstörekisterit - kenen vastuulla ja kuinka laajasti ko. tietojen katseluoikeutta jaetaan.”

> ”Terveystietojen käsittelijät nimettävä”

Esimiestyöskentelyssä nähtiin kehittämistarpeita, esimerkiksi salassa pidettäviin tietoihin liittyen. Lisäksi oltiin huolissaan esimiesten osaamisesta. Esimiesten roolia korostaneet vastaajat kuuluivat yleensä henkilöstöön.

> ”Koulutusta voisi olla enemmän. Salassa pidettävien tietojen osalta kaipaisin suurempaa vastuuta esimiehiltä”

> ”Esimerkiksi salassa pidettävien henkilötietojen käsittelyn oikeellisuudesta vastuussa olevan johdon ja esimiesten pitäisi ymmärtää syvällisemmin ja toteuttaa määrämuotoisemmin suunnittelu- ja valvontavastuuseen kuuluvat asiat.”

> ”Esimiesten osaamisen ylläpitäminen ja päivittäminen tulisi muistaa.”

Tekniseen tietoturvaan liittyvät laitteet, ohjelmat ja päivitykset mainittiin usein vastauksissa. Erityisesti korostui laitteiston ja ohjelmien ajantasaisuus.

> ”Att man har någotlunda moderna datorer och system som inte är föråldrade”

> ”Että voisi luottaa siihen, että tehdyt, salassapitovelvollisuuden alaisuudessa olevat kirjaukset eivät päädy vääriin käsiin esim. ohjelman epäluotettavuuden takia. ”

> ”Jag önskar att antivirusprogrammen alltid är aktuella.”

Aiemmissakin kohdissa korostunutta koulutusta ja ohjeistustakaan ei unohdettu oman organisaation tietoturvallisuuden kehittämistarpeita lueteltaessa. Eräs vastaaja ei ollut saanut vielä ollenkaan tietoturvallisuuskoulutusta. Toinen taas kaipasi säännöllisiä tietoturvatenttejä, kun kolmas painotti selkeän ohjeistuksen merkitystä.

> ”Olen ollut vain vähän aikaa talossa; en ole saanut vielä minkäänlaista koulutusta ko. asiasta. Olen kyllä lukenut aihetta koskevat kirjalliset ohjeet, mutta toivottavasti saan myöhemmin koulutusta asian tiimoilta. Ja henkilökunnan koulutus ylipäätään on avainsana näinä muuttuvina aikoina.”

> ”Jokaisen täytyisi suorittaa tietoturvatentti hyväksytyin väliajoin. Perehdyttämisessä tulisi entistä enemmän korostaa näitä asioita.”

> ”Koko henkilöstölle on hyvä kertoa tietoturvariskeistä, hyvistä toimintatavoista ja tulevaisuuden uhkakuvista, vaikka kaikki eivät henkilötietoja tai muita yksityisyystietoja käsittelisikään työssään.”

3 VAHTI-tietoturvabarometri tulevaisuudessa

Osana valtiovarainministeriön asettaman VAHTIn tietoturvallisuuden kehittämistyötä vuonna 2016 toteutettu henkilöstön ja johdon tietoturvabarometri on tarkoitus toteuttaa myös vastaisuudessa. Tätä silmällä pitäen tämän vuoden kyselystä sai antaa kehittämisehdotuksia, risuja ja ruusuja liittyen esimerkiksi käsiteltyihin teemoihin ja kysymyksenasetteluun erityisessä palaute-kohdassa. Palautetta saatiin lähes 2000 vastaajalta ja sitä on käyty läpi kyselyn kehittämiseksi. Lisäksi palautetta kyselystä on saatu ja saadaan edelleen sähköpostitse, kokouksissa ja muissa tilaisuuksissa.

Palautteessa korostui se, että kyselyn järjestämistä pidettiin hyvänä asiana.

> ”Hyvä, että tällaista selvitetään jolloin tulee yleiskuva siitä, että missä mennään ja mitä asioita pitää kehittää.”

Kysymyksenasettelusta saatiin myös palautetta. Osa vastaajista piti kysymyksenasettelua onnistuneena, kun toiset taas näkivät kehittämiskohteita.

> ”Kiitos, erittäin monipuolisesti laadittu ja jäsennelty ajankohtainen kysely.”

> ”Joihinkin kohtiin olisi voinut olla avovastausmahdollisuus, koska muutamiin kysymyksiin ei ollut yksiselitteistä vastausta.”

Useat vastaajat toivoivat, että oman aseman tai tehtävänkuvan voisi valita, jotta eri ryhmiä voitaisiin vertailla paremmin keskenään. Tulevissa kyselyissä tähän tullaan kiinnittämään huomiota.

> ”Oikein hyvä kysely, hyvä että tällaisia on. Kohderyhmät olisi hyvä voida asettaa yrityskohtaisesti (esim. johto, hallinto, työnjohto, työntekijät), jolloin saataisiin samalla kyselyllä tieto myös siitä eroavatko henkilöstöryhmät merkittävästi toisistaan”

VAHTIn historian ensimmäistä henkilöstön ja johdon tietoturvabarometria pidettiin tarpeellisena ja sille toivottiin jatkoa. Eräs vastaaja korosti tulevien kyselyiden vastausten vertailua nyt toteutetun kyselyn kanssa.

> ”Erittäin tarpeellinen kysely. Toivottavasti tehdään uudestaan 1-2 vuoden päästä, jotta organisaatiot voivat seurata, onko asiassa tapahtunut muutoksia”

Vastaajilta saatu palaute otetaan siis huomioon mahdollisten tulevien kyselyjen suunnittelussa. Muun muassa kysymyksenasetteluun, vastausvaihtoehtoihin ja kysymysten määrään tullaan kiinnittämään runsaasti huomiota. Lisäksi oman aseman tai tehtävänkuvan tai molemmat voi valita tarkemmin seuraavissa kyselyissä. Tulevien kyselyiden vastauksia voidaan vertailla nyt toteutettuun kyselyyn soveltuvin osin riippuen muutoksien suuruudesta.

Salasanojen käytettävyys ja turvallisuus olivat monelle vastaajalle tärkeä teema ja niihin liittyen esitettiin monta kysymystä. Salasanaturvallisuus oli osin huolestuttavalla tolalla. Tähän liittyen olisi mielenkiintoista kysyä esimerkiksi, käyttävätkö vastaajat samoja salasanoja vapaa-ajalla ja työtehtävissä. Kysymyksiä tullaankin kohdentamaan tarkemmin tulevissa kyselyissä.

Kyselyn vastaajakuntaakin tulee pohtia. Voitaisiinko kyselyä tarjota myös sellaisilla organisaatioille, jotka eivät sen piirissä tällä kertaa olleet? Esimerkiksi pelastustoimi, seurakuntayhtymät ja työttömyyskassat hoitavat julkisia tehtäviä, ja niille voisi olla hyötyä kyselyyn vastaamisessa. Maakuntauudistuksen myötä myös maakunnat voisivat tulla kyselyn piiriin.

Palautteen perusteella voidaan todeta, että VAHTIn henkilöstön ja johdon tietoturvabarometri on konsepti, jota kannattaa kehittää edelleen eteenpäin ja hyödyntää vastaisuudessakin. Kysely on tärkeä keino julkishallinnon tietoturvallisuuden kehittämisessä ja tietoturvallisuustyön vaikuttavuuden parantamisessa. Vastaajaorganisaatiot, valtiovarainministeriössä toimiva VAHTI sekä muut yhteiskunnalliset toimijat saavat käyttöönsä arvokasta tietoa vahvuuksistaan ja kehittämiskohteistaan.

Päätöksen seuraavasta VAHTI-tietoturvabarometrista tekee uusi vuoden 2017 alussa aloittava VAHTI-johtoryhmä. Mikäli se toteutetaan, kaikkien tämän vuoden kyselyssä mukana olleiden organisaatioiden kannattaa osallistua tietoturvabarometriin ensi vuonnakin. Lisäksi VAHTI kannustaa myös niitä organisaatioita, jotka syystä tai toisesta eivät tänä vuonna osallistuneet henkilöstön ja johdon tietoturvabarometriin, osallistumaan tuleviin kyselyihin. Vastaajaorganisaatioiden lisäksi koko julkishallinto ja sen piirissä tehtävä tietoturvallisuustyö hyötyy jokaisesta uudesta vastaajasta.

LIITE 1. KYSELYN TOTEUTUS

Valtiovarainministeriön asettama VAHTI-johtoryhmä päätti syyskuussa 2015 osana vuosien 2015-2016 toimintasuunnitelmaansa toteuttaa ensimmäisen henkilöstön ja johdon tietoturvabarometrin. Kyselyä valmisteli eri hallinnonalojen edustajista ja palveluntarjoajista koottu ryhmä, joka kehitti kyselyn teemoja ja kysymyksenasettelua vaiheittain. Tietoturvabarometria pilotoitiin testikäyttäjillä ennen sen julkaisua. Valmis kysely oli siis pitkän kehitystyön tulos.

Kyselystä lähetettiin kunta- ja uudistusministeri Anu Vehviläisen allekirjoittama saate sekä ohjeet kyselyyn osallistumiseen kaikille kunnille, valtionhallinnon kirjanpitoyksiköille sekä sairaanhoitopiireille. Osallistuminen oli vapaaehtoista.

Kysely muodostui yhteensä 17 varsinaisesta kysymyksestä, viidestä jatkokysymyksestä ja kahdesta johtoryhmän lisäkysymyksestä. Kyselyyn sai valita vastauskieleksi joko suomen tai ruotsin. Vastaajaorganisaatioiden ja vastaajien tueksi tuotettiin molemmilla kielillä kattavat vastausohjeet, joissa neuvottiin tarkemmin kysymyksiin vastaamisessa. Kyselystä tiedottaminen henkilöstölle ja johdolle oli kunkin vastaajaorganisaation vastuulla ja vastaaminen vapaaehtoista.

Kysely toteutettiin Valtion tieto- ja viestintätekniikkakeskus Valtorin tarjoaman Vyvin viestintäratkaisupalvelun yhteydessä olevaa tietoturvallisen vastaamisen mahdollistavaa kyselypalvelua käyttäen aikavälillä 9.9. -14.10.2016. Samaa palvelua on käytetty aikaisemmin muun muassa VAHTIn vuosittaisen organisaatiokyselyn yhteydessä ja sitä voidaan käyttää myös tulevissa VAHTIn tietoturvabarometreissä.

Saatujen vastausten kokonaismäärä vaihtelee hieman kohdittain, sillä kaikki vastaajat eivät ole jostain syystä vastanneet kaikkiin kohtiin. Taustalla voi olla esimerkiksi jokin kyselyn toteutuksen liittyvä tekninen seikka tai tulosten analyysissa tapahtunut poikkeama, mikä on luonnollista tämän kokoluokan kyselyssä.

Valtiovarainministeriö on käsitellyt vastaukset luottamuksellisesti ja tuottanut tämän yhteenvetoraportin, joka sisältää keskeiset havainnot kyselystä ja suosituksia tietoturvallisuuden kehittämiseksi. Lisäksi valtiovarainministeriö on tuottanut vastaajaorganisaatiokohtaiset raportit organisaatioiden omaa käyttöä ja tietoturvallisuuden kehittämistä varten. Ministeriö on arvioinut tapauskohtaisesti, mitä tietoja se on voinut luovuttaa vastaajaorganisaatioille.

VALTIOVARAINMINISTERIÖ
Snellmaninkatu 1 A
PL 28, 00023 VALTIONEUVOSTO
Puhelin 0295 160 01
Telefaksi 09 160 33123
www.vm.fi

ISSN 1798-0860 (pdf)
ISBN 978-952-251-812-5 (pdf)

Joulukuu 2016