VALTIOVARAINMINISTERIÖ

Haukka-hankkeen vaikuttavuuden arviointi

Raportti

31.12.2023

Sisällys

TIIVISTELMÄ

Julkisen hallinnon digitaalisen turvallisuuden tavoitteena on valtioneuvoston vuoden 2020 periaatepäätöksen (VM 2020:23) mukaan kokonaisturvallisuuden viitekehyksessä suojata kansalaisia, yhteisöjä ja yhteiskuntaa niiltä riskeiltä ja uhkilta, jotka voivat kohdistua tietoihin, palveluihin ja yhteiskunnan toimintaan digitaalisessa toimintaympäristössä. Julkisiin palveluihin ja niissä käsiteltäviin tietoihin kohdistuu jatkuvasti tietoturvaloukkauksia ja niiden yrityksiä. Ne vaarantavat julkisten palvelujen toimintaa sekä tietojen salassapitoa, saatavuutta ja eheyttä. Julkisia palveluja ja tietoja on siten suojattava sekä tahalliselta haitalliselta toiminnalta että vahingoilta ja onnettomuuksilta. Julkisten palvelujen turvallisuuteen ja jatkuvuudenhallintaan on investoitava resursseja tasapainoisesti digitaalisten palvelujen ensisijaisuuden edistämisen rinnalla.

Arvioidaan, että optimaalinen julkisten palvelujen kehittämisen ja niiden turvallisuuden edistämisen tasapainoinen resursointi saavutetaan investoimalla turvallisuusuuteen jopa noin 37 % julkisten palvelujen mahdollisten tietoturvaloukkausten menetysten odotusarvosta. Julkisten palveluiden turvallisuuden kustannustehokkaan varmistamisen lähtökohtana on se, että mahdollisten tietoturvaloukkausten aiheuttamat menetykset on tunnistettu ja niitä hallitaan. Tämä toteutuu arvioimalla ja hallitsemalla merkittävimpiä digiriskejä ja niiden vaikutuksia sekä digiriskien mahdollisen toteutumisen aiheuttamia kustannuksia ja toteuttamalla turvallisuusinvestointeja riskiarviointien perusteella. Pyrkimyksenä on vähentää tietoturvaloukkausten mahdollisesti aiheuttamia menetyksiä siten, että julkisten palvelujen toiminnan jatkuvuus ja luotettavuus on turvattu.

Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelmassa 2020–2023 (VM 2020:33) kuvattu valtiovarainministeriön (VM) Haukka-hanke oli yksi yhteiskunnan turvallisuusinvestoinneista. Se toimeenpani valtioneuvoston vuoden 2020 periaatepäätöstä julkisen hallinnon digitaalisesta turvallisuudesta. Haukka-toimeenpanosuunnitelma valmisteltiin valtiovarainministeriön asettamassa poikkihallinnollisessa koordinaatioryhmässä. Suunnitelmalla tuettiin myös kyberturvallisuusstrategian 2019 kehittämisohjelman valmistelua ja toteuttamista sekä pantiin osaltaan täytäntöön valtioneuvoston päätöstä huoltovarmuuden tavoitteista (1048/2018). Haukka-hanketta toteutettiin VM:n lisäksi Digi- ja väestötietovirastossa (DVV) ja Liikenne- ja viestintävirastossa (Traficom). Toteuttamiseen osallistui henkilöitä laajasti myös muista ministeriöistä ja virastoista sekä alue- ja paikallishallinnosta, Huoltovarmuuskeskuksesta (HVK), Kuntaliitosta, HAUS koulutuskeskus Oy:stä ja FISTECistä. Lisäksi lukuisissa sidosryhmätilaisuuksissa vaihdettiin näkemyksiä julkisen hallinnon, yritysten ja kolmannen sektorin edustajien kanssa.

Tässä asiakirjassa kuvattu Haukka-hankkeen vaikuttavuuden arviointi on toteutettu useisiin lähdeaineistoihin perustuvana itsearviointina. Lähdeaineistoja ovat olleet Haukka-hankkeen tehtävät ja tuotokset; Suomen digitaalisen kompassin (VN 2022:65) Kokonaisturvalliset julkiset palvelut -tavoitteen avaintulosten edistäminen; Viron ylläpitämän National Cyber Security Index (NCSI) mittarin tiedot hankkeen ajalta; DVV:n ylläpitämästä digiturvan kokonaiskuvapalvelusta poimitut vertailutiedot; haastattelut, joissa hankkeeseen eri organisaatioista osallistuneet henkilöt ovat arvioineet Haukka- toimeenpanosuunnitelman tehtävien toteutumista; verkkokyselyt ja ryhmäkeskustelu, joissa julkisen hallinnon toimijat ovat arvioineet valittujen hankkeen tuotosten vaikuttavuutta; DVV:n ja HAUS koulutuskeskus Oy:n digiturvatilaisuuksista, harjoituksista ja verkkokoulutuksista keräämä

palaute; DVV:n digiturvapalveluista kerätty palaute; ja Traficomin Haukka-hankkeessa toteuttamista palvelupiloteista kerätty palaute.

Haukka-hankkeen tuotoksia arvioitiin Suomen digitaalisen kompassin Kokonaisturvalliset julkiset palvelut -tavoitteen avaintulosten edistämisen näkökulmasta sekä kansainvälisen NCSI-mittarin ja DVV:n kansallisten digiturvan kokonaiskuvapalvelun indikaattorien ja tuotoksista kerätyn palautteen perusteella. Täten muodostettiin laadullinen kokonaisarvio hankkeen vaikutuksista julkisen hallinnon digitaaliseen turvallisuuteen ja yleisemminkin digitaalisen turvallisuuden kehittymiseen Suomessa hankkeen aikana.

Haukka-hankkeen tuotoksia ovat julkisen hallinnon digiturvan digipalvelut: Traficomin toteuttamat kuntien haavoittuvuusskannausten (Hyöky) ja HAVARO-käyttöpilotit sekä Hyöky-palvelu kunnille, DVV:n Julkri-arviointikriteeristön työkalu, kriittisyysluokittelutyökalu, digiturvan kokonaiskuvapalvelu ja strategisten digiriskien arviointi- ja hallintapalvelu sekä DVV:n verkkosivuilla ja eOppivassa tarjolla olevat digiturvamateriaalit. Tilannetietoisuutta ja tiedolla johtamista on parannettu digiturvan strategisen johtoryhmän toiminnalla, toteuttamalla strategisten digiriskien hallintaympäristö, kehittämällä DVV:n digiturvan kokonaiskuvapalvelun tietosisältöä ja hyödyntämistä, laatimalla kuntien digiturvapalveluiden tiekartta palvelujen kehittämisen ohjaamisen tueksi sekä valmistelemalla kansainvälisiä, päätöksenteossa hyödynnettyjä vertailuja. Digiturvaosaamista edistäviä hankkeen tuotoksia ovat Digiturvan avoimet verkkokoulutukset ja -tilaisuudet, TAISTO-harjoitusympäristön vakiinnuttaminen, VAHTI hyvät käytännöt -tukimateriaalit, VAHTI riskienhallintasanasto, digiturvan arkkitehtuurikuvaus ja Digiturvakompassi-podcastit. Säädösvalmistelun esiselvityksiä ja toimintamallikuvauksia ovat selvitys digitaalisen turvallisuuden arvioinnin kehitystarpeista, selvitys digitaalisen turvallisuuden kansainvälisestä arviointilainsäädännöstä, julkisen hallinnon digitaalisen turvallisuuden yhteistoiminta- ja hallintamalliselvitys (VM 2022:76) sekä digitaalisen turvallisuuden yhteistoiminta- ja hallintamallien kansainvälinen vertailu. Niitä on hyödynnetty valmisteltaessa VM:n Arviomuistiota julkisen hallinnon tietojärjestelmien sääntelyn nykytilasta ja kehittämistarpeista (2021:54), hallituksen esitystä eduskunnalle julkisen hallinnon automaattista päätöksentekoa koskevaksi lainsäädännöksi (145/2022), VM:n virkamiespuheenvuoroa (2022:77) ja Suomen digitaalista kompassia (VN 2022:65).

Valtioneuvoston selonteossa Suomen digitaalisesta kompassista yhtenä tavoitteena on Kokonaisturvalliset julkiset palvelut eli julkisten palvelujen tuottaminen kokonaisturvallisuuden mallin mukaisesti. Haukka-hanke sijoittuu Kokonaisturvalliset julkiset palvelut -tavoitteen alueelle. Hankkeen tuotokset ovat luoneet pohjaa ja edistäneet Kokonaisturvalliset julkiset palvelut -tavoitteen seuraavia avaintuloksia: valtion, hyvinvointialueiden ja kuntien digitaalinen turvallisuus on parantunut, julkisen hallinnon digitaalisen turvallisuuden ennakointia käytetään toiminnan ja talouden suunnittelussa, julkisten digipalvelujen digiturvaratkaisut tukevat informaatiovaikuttamisen ja disinformaation tunnistamista ja hallintaa sekä julkisille digipalveluille on asetettu riskiperustaisesti digiturvavaatimukset ja niiden toteutumista arvioidaan ja valvotaan jatkuvasti.

Yksi Suomen kyberturvallisuutta mittaava kansainvälinen indeksi on Viron ylläpitämä, kansainväliseen vertailuun perustuva National Cyber Security Index (NCSI). Sen tuloksissa Suomen sijoitus on hankkeen aikana laskenut vuoden 2020 seitsemänneltä sijalta tuoreimman marraskuun 2023 tiedon mukaan kolmannelletoista sijalle. Suomi on päivittänyt NCSI:hin tietoja viimeksi marraskuussa 2020.

Suomen sijoittumisesta vertailussa ei siten voida päätellä kyberturvallisuuden kehittymistä Haukka-hankkeen aikana. Sijoittumisen lasku kertoo enemmän kyberturvallisuuden parantamisesta verrokkivaltioissa. Indikaattoreista Suomella oli eniten puutteita elintärkeiden palvelujen turvaamisessa. Suomen tietojen seuraava päivitys alkuvuodesta 2024 on valmistelussa.

DVV:n digiturvan kokonaiskuvapalvelu kertoo Suomen julkisen hallinnon digiturvan tilasta. Sen johtamisen, riskienhallinnan, toiminnan jatkuvuuden ja varautumisen, tietoturvallisuuden, tietosuojan sekä kyberturvallisuuden vertailutietojen perusteella digiturvan taso julkisessa hallinnossa on säilynyt lähes ennallaan vuosina 2021–2023. Digiturvan tasotietonsa ilmoittaneiden julkisen hallinnon organisaatioiden määrä oli vuonna 2021 128, 2022 118 ja 2023 194 organisaatiota.

Suomen Digitaalisen kompassin Kokonaisturvalliset julkiset palvelut avaintulosten edistymisen arvioinnin sekä Haukka-hankkeen tuotoksista kerätyn palautteen perusteella Haukka-hankkeen vaikutukset julkisen hallinnon digitaaliseen turvallisuuteen ja sen kehittymiseen ovat olleet myönteisiä. Voidaankin perustellusti sanoa, että hanke on ollut oleellisesti mukana vaikuttamassa julkisen hallinnon digitaalisen turvallisuuden parantumiseen. Haukka-hanketta on useissa eri sidosryhmien edustajien haastatteluissa ja keskusteluissa pidetty merkittävänä digitaalisen turvallisuuden kehittymisen edistäjänä ja vastaavan kaltaiselle, pitkäaikaiselle ja jatkuvalle digiturvan kehittämiselle nähdään tarvetta myös tulevaisuudessa.

Haukka-toimeenpanosuunnitelman tehtävät kattavat laajasti julkisen hallinnon toimintaa ja toimijoita. Siten Haukka-hankkeen tuotokset on suunniteltu ja toteutettu kattavasti julkisen hallinnon käyttöön. Tuotosten avulla on pystytty parantamaan digitaalista turvallisuutta ja laatimaan edelleen jatkokehityssuunnitelmia. Julkinen hallinto on kuitenkin heterogeeninen, joten tuotosten hyödyntämisen tilanne vaihtelee organisaatioittain. Jatkossa tulee kiinnittää enemmän huomiota digitaalisen turvallisuuden kehittämistehtävien tarkempaan ryhmittelyyn ja fokusointiin. Hankkeessa kehitettyjen digiturvan digipalveluiden käyttöaste on vielä matalahko. Digiturvapalveluiden markkinointia uusille julkisen hallinnon käyttäjäorganisaatioille tulee siten edelleen jatkaa. NIS2-direktiivin kansallinen täytäntöönpano koskee hankkeessakin selvitettyjä, pilotoituja ja toteutettuja asioita: kyberturvallisuustietojen vapaaehtoisia jakamisjärjestelyjä sekä tietoturvaloukkausten havainnointia ja haavoittuvuuskartoituksia. Haukka-hankkeen voidaan siten katsoa edistäneen myös NIS2-direktiivin kansallisen täytäntöönpanon edellytyksiä.

1 JOHDANTO

Suomalaisen yhteiskunnan digitalisaatio on edennyt nopeasti ja digitaalisten palvelujen määrä kasvaa jatkuvasti. Julkisen hallinnon digitaaliset palvelut samoin kuin verkkopankit ja -kaupat ovat jo arkipäivää. Terveydenhuollon digitaalisiin palveluihin panostetaan koko ajan enemmän. Tekoälypohjaisiin ratkaisuihin, kuten ChatGPT-avusteinen työnteko tai koneoppivat järjestelmät automaattisessa teknisessä valvonnassa, kohdistuu osaamisen kehittämiseen, työhön ja jopa yhteiskunnan rakenteisiin liittyviä odotuksia.

Fyysisen maailman turvallisuusmekanismeihin verrattuna digitaalisen toimintaympäristön turvallisuus koostuu aineettomista ja usein hankalammin hahmotettavista, abstrakteista tekijöistä. Kuten julkisuudessakin olleet tietomurrot, tietovuodot, identiteettivarkaudet, tietoverkkojen toiminnan häirintä ja kybervakoilutapaukset osoittavat, kohdistuu digitaalisiin palveluihin vakavia uhkia, joihin tulee pystyä varautumaan, joita pitää kyetä torjumaan ja joista on voitava toipua mahdollisimman vähin vaurioin. Digitaalisen toimintaympäristön tärkeintä elementtiä, tietoa ja sen käsittelyä, on voitava suojata niin tahalliselta, haitalliselta toiminnalta kuin vahingoiltakin. Tämän vuoksi turvallisuuden kehittämiseen digitaalisessa toimintaympäristössä on investoitava resursseja samaan tapaan kuin turvallisuuteen panostetaan fyysisessäkin toimintaympäristössä.

Digitaalinen toimintaympäristö muuttuu nopeasti, joten uhkat ja riskitkin muuttuvat jatkuvasti. Näin ollen digitaalista turvallisuutta tulee parantaa jatkuvasti, jotta digitaalisten palvelujen ensisijaisuutta voidaan edistää turvallisesti. Laki julkisen hallinnon tiedonhallinnasta (906/2019, tiedonhallintalaki) edellyttää tietoturvallisuustoimenpiteiden mitoittamista riskien arvioinnin perusteella. Merkittävänä näkökulmana riskienhallinnassa on kustannustehokkuus. Haukka-hankkeessa valmistelussa kustannus-vaikuttavuuden arviointiraportissa viitatun Gordon & Loeb (2002)[1] mallin mukaan tietoturvallisuuden parantamiseen voidaan optimaalisesti investoida jopa noin 37 % mahdollisten menetysten odotusarvosta[2]. Julkisten palveluiden turvallisuuden kustannustehokas varmistaminen siten edellyttää, että mahdollisten tietoturvaloukkausten aiheuttamat menetykset on tunnistettu ja niitä hallitaan. Tämä toteutuu arvioimalla ja hallitsemalla merkittävimpiä digiriskejä ja niiden vaikutuksia sekä digiriskien mahdollisen toteutumisen aiheuttamia vuosittaisia kustannuksia ja toteuttamalla turvallisuusinvestointeja jatkuvasti riskiarviointien perusteella. Pyrkimyksenä on vähentää tietoturvaloukkausten mahdollisesti aiheuttamia menetyksiä siten, että julkisten palvelujen toiminnan jatkuvuus ja luotettavuus on turvattu.

1.1 Haukka-toimeenpanosuunnitelmasta

Valtioneuvoston periaatepäätöksessä julkisen hallinnon digitaalisesta turvallisuudesta (VM 2020:23) määritetään kehittämisen periaatteet ja keskeiset palvelut turvallisuuden edistämiseksi digitaalisessa toimintaympäristössä. Digitaalisen turvallisuuden viitekehykseen katsotaan sisältyvän riskienhallinnan, toiminnan jatkuvuuden ja varautumisen sekä kyberturvallisuuden, tietoturvallisuuden ja tieto-

[1] Gordon, L. & Loeb, M. (2002). The economics of information security investment.
[2] Digitaalisen turvallisuuden kustannus-vaikuttavuusarviointi julkisessa hallinnossa. Selvitystyön raportti 1.6.2020.

suojan asioita. Periaatepäätöksessä on kuvattu julkisen hallinnon digitaalisen turvallisuuden kehittämisalueet ja kehittämisen periaatteet, sekä keskeisiä hallinnon toimintaa ja prosesseja tukevia digitaalisen turvallisuuden palveluita.

Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelma 2020–2023 (Haukka) (VM 2020:33) toteutti valtioneuvoston periaatepäätöstä digitaalisesta turvallisuudesta. Toimeenpanosuunnitelmaan on kirjattu julkisen hallinnon digitaalisen turvallisuuden nykytilaselvityksen ja kansainvälisen vertailun perusteella 19 tehtävää. Toimeenpanosuunnitelmaa laadittaessa tehtäville asetettiin tavoitteet ja alustava aikataulu sekä arvioita toteutuskustannuksista ja tavoitelluista hyödyistä. Tehtävien toteutumisen arvioinnin tueksi toimeenpanosuunnitelmassa on kuvattu myös tehtävien toteutumisen mittaaminen.

Tässä Haukka-ohjelman vaikuttavuuden arviointiraportissa kuvataan, mitä toimeenpanosuunnitelman toteutus on vaikuttanut julkisen hallinnon digitaalisen turvallisuuden kehittymiseen. Digitaalisen turvallisuuden käsitteen määritelmä on edelleen vakiintumaton. Siten ei ole yksityiskohtaista digitaalisen turvallisuuden lähtötasoa, johon nykyistä tasoa voisi verrata. Näin ollen merkittävää ja pysyvää digitaalisen turvallisuuden parantumista on vaikea osoittaa kiistattomasti. Osa hankkeen vaikutuksista ei välttämättä näy lyhyellä aikavälillä, vaan esimerkiksi koulutusten ja harjoitusten, yhteistoimintamallin ja säädösvalmistelutyön tulokset vaikuttavat vasta myöhemmin.

Haukka-toimeenpanosuunnitelma julkaistiin 22.4.2020, jolloin koronapandemia oli jo käynnissä. Venäjän hyökkäys Ukrainaan helmikuussa 2022 on muuttanut geopoliittista tilannetta niin Euroopassa kuin maailmanlaajuisestikin. Informaatiovaikuttaminen on lisääntynyt entisestään, ja varautumisen merkitys kriittisen infrastruktuurin suojaamisessa ja yhteiskunnan toimivuuden varmistamisessa on korostunut. Pandemian ja sodan kaltaiset mullistukset ovat muuttaneet turvallisuusympäristöä ja siten myös digitaalisen turvallisuuden kehittämistä. Kehittämistehtävien painopisteitä ja tarkempia sisältöjä on jouduttu tarkastelemaan uudelleentoimintaympäristön muutoksia vastaaviksi.

Toimintaympäristön merkittävien muutosten takia Haukka-toimeenpanosuunnitelman tehtävien ja painotusten sisältöjä päivitettiin tehtävien yksityiskohtaisemmassa suunnittelussa vastaamaan paremmin toimintaympäristön muutoksia. Toimeenpanosuunnitelman tehtäviä tarkennettiin VM:n, DVV:n ja Traficomin hankesuunnitelmissa. Tarkennettuja suunnitelmia ja niiden edistymistä käsiteltiin VM:n Julkisen hallinnon ICT-osaston (JulkICT) hallitusohjelmahankkeiden seurannan käytänteiden mukaisesti neljännesvuosittain hankesalkussa ja VM:n JulkICT-osaston johtoryhmän kokouksissa. Lisäksi DVV:n ja Traficomin hankesuunnitelmien toteutumista seurattiin säännöllisesti kokoontuneessa DVV:n Haukka-tehtäviä toteuttaneen JUDO-hankkeen ohjausryhmässä, jossa suunnitelmiin perustuneet tarkemmat tehtäväsuunnitelmat ja hankinnat hyväksyttiin.

Tämä Haukka-hankkeen vaikuttavuuden arviointiraportti on valmisteltu työryhmässä, johon ovat kuulunet tietohallintoneuvos Tuija Kuusisto ja neuvotteleva virkamies Niko Mäkilä valtiovarainministeriöstä sekä työtä tukeneet KPMG:n konsultit.

1.2 Yhteenveto hankkeen keskeisistä tuotoksista

Haukka-hanke on tuottanut monipuolisesti sekä strategisia että operatiivisia tuotoksia julkisen hallinnon käyttöön. Hankkeen tuotoksia ovat Traficomin ja DVV:n tarjoamat digiturvan digipalvelut; VM:ssä, DVV:ssä ja Traficomissa valmistellut tilannekuvaukset ja uudet tiedolla johtamisen prosessit, jotka on toteutettu ja toiminnassa; DVV:n valmistelemat sekä DVV:n yhdessä HAUS koulutuskeskus Oy:n kanssa valmistelemat digiturvaosaamista edistävät tuotokset ja VM:ssä laajassa yhteistyössä eri toimijoiden kanssa valmistellut säädösvalmistelun esiselvitykset, toimintamalli- ja jatkovalmisteluehdotukset. Hankkeessa julkaistuja tuotoksia on lueteltu liitteessä A. Esimerkkejä hankkeessa tai sen aikana laadituista keskeisistä tuotoksista ovat:

- poikkihallinnollisen digitaalisen turvallisuuden strategisen johtoryhmän perustaminen ja johtoryhmän toiminta
- julkisen hallinnon digiturvan tilannekuvan ja vertailutiedon tuottamiseen kehitetty kokonaiskuvapalvelu
- strategisten digiriskien hallintaympäristön toteutus
- digiturvan avoimet verkkokoulutukset, -tilaisuudet
- julkiselle hallinnolle suunnatut tietosuoja- ja tietoturvaloukkauksien hallinnan harjoitukset
- tieto- ja kyberturvahavainnointia kehittävien palvelujen toteuttaminen
- yhteisen digiturva-arkkitehtuurin laatiminen.

Hankkeen tuotoksia laadittiin julkisessa hallinnossa virkavalmisteluna. Tehtävissä hyödynnettiin kansainvälistä ja kansallista laajaa yhteistoimintaa, vuorovaikutusta ja tietoja sekä yksityiseltä sektorilta kilpailutettuja resursseja.

Digitaalisen turvallisuuden strategisen johtoryhmän toiminta

Valtiovarainministeriö asetti digitaalisen turvallisuuden strategisen johtoryhmän toimikaudeksi 1.1.2020–31.12.2024. Johtoryhmän tehtäviä olivat mm. julkisen hallinnon digitaalisen turvallisuuden strategisen riskiarvion koordinointi, digitaalisen turvallisuuden kansallisen strategisen tason yhteistoimintamallin luonti ja koordinointi sekä keskeisten kehitettävien digitaalisen turvallisuuden palvelujen arviointi, ohjaus, koordinointi ja valvonta. Johtoryhmä on kokoontunut toimikautensa aikana 4–5 kertaa vuosittain, ja se on arvioinut toteuttaneensa hyvin sille asetetut tehtävät.

VM:ssä edistettiin julkisen hallinnon digitaalisen turvallisuuden strategista riskiarviota toteuttamalla Haukka-hankkeessa syksyllä 2020 strategisen tason riskikysely kuntien digitaalisesta turvallisuudesta. DVV ja VM selvittivät yhteistyössä syksyn 2021 aikana julkishallinnon digitaalisen turvallisuuden merkittävimmiksi arvioituja riskejä osana julkisen hallinnon digitaalisen turvallisuuden strategisen riskiarviomallin pilotointia. Vuonna 2022 DVV valmisteli riskiennakointiraportin. Digitaalisen turvallisuuden strateginen johtoryhmä päätti Haukka-hankkeessa toteutetuista toimenpiteistä vuosien 2020–2022 riskikyselyjen perusteella. DVV julkaisi vuonna 2022 kuvauksen[3] julkisen hallinnon digitaalisen turvallisuuden strategisesta riskienhallintamallista. Mallin tavoitteena on ”mahdollistaa poikkihallinnollisten ja laajojen jaettujen riskien tunnistaminen hajautettuun rakenteeseen perustu-

[3] Julkisen hallinnon digitaalisen turvallisuuden strateginen riskienhallinta - Riskienhallintamallin rakenne - 15.12.2022

vassa julkishallinnossa, sekä niiden arviointi ja käsittelyyn ohjaus sekä hallintatoimien tehostaminen". Standardeihin perustuva riskienhallintamenettely perustuu organisaatiokohtaiseen riskienhallintaan, eikä sellaisenaan huomioi esimerkiksi yhteiskunnallista näkökulmaa. Strateginen riskienhallintamalli luo uusia edellytyksiä digiriskien laaja-alaiseen, poikkihallinnolliseen tunnistamiseen, arviointiin ja käsittelyyn. Lisäksi sen kautta voidaan tehostaa käsittelyn ohjausta ja hallintakeinojen toteutusta sekä tarjota parempi digiriskien jaettu tilannekuva. DVV rekrytoi vuonna 2023 henkilön toteuttamaan mallia ja julkaisi riskitilannekatsauksen keväällä 2023. Tilannekatsaus toimii pohjatietona Digikompassin Kokonaisturvalliset julkiset palvelut -tavoitteen kehittämistoimenpiteiden suunnittelussa.

Kansalliseen strategisen tason yhteistoimintamalliin liittyen Haukka-hankkeessa valmisteltiin digitaalisen turvallisuuden yhteistoiminta- ja hallintamallien kansainvälinen vertailu. Siinä arvioitiin Suomeen verrattuna digitaalisen turvallisuuden organisoitumista ja keskitettyjä tehtäviä Alankomaissa, Australiassa, Iso-Britanniassa, Israelissa, Ruotsissa, Saksassa, Venäjällä ja Virossa. Kansallisen strategisen tason yhteistoimintamalli on kuvattu hankkeessa valmistelussa digitaalisen turvallisuuden yhteistoiminta- ja hallintamalliselvityksessä (VM 2022:76). Malli on toteutuksessa ja sitä kehitetään edelleen digitoimistossa, ministeriöissä, DVV:ssä ja Traficomissa. Mallin kehittämiseen vaikuttanee Orpon hallitusohjelman s. 168 kirjaus kokonais- ja kyberturvallisuuden johtamisrakenteen uudistamisesta hallituskauden aikana. Mallin toteutumisesta tulisi järjestää jatkotarkastelu vuonna 2025.

DVV:n digiturvan kokonaiskuvapalvelu

DVV on toteuttanut Organisaation Digiturvakyselyä saman sisältöisenä vuodesta 2021 alkaen ja vuonna 2022 otettiin käyttöön viraston kehittämä Kokonaiskuvapalvelu. Palvelun tavoitteena on tarjota julkisen hallinnon organisaatioille vertailutietoa muista julkisen hallinnon organisaatioista ja tuottaa jatkuvasti käytettävää, ajantasaista digiturvan tilannekuvaa. Digiturvan kokonaiskuvapalveluun on koottu tietoa kaikista digiturvan osa-alueista: johtaminen, riskienhallinta, toiminnan jatkuvuus ja varautuminen, tietoturva, tietosuoja sekä kyberturvallisuus. Palvelun käyttäjien määrä on ollut vuonna 2021 128, 2022 118 ja 2023 194 organisaatiota ja sen käyttöä pyritään edelleen laajentamaan mahdollisimman kattavan ja todenmukaisen tilannekuvan ja vertailutietojen varmistamiseksi. DVV on antanut kokonaiskuvapalvelun sisällön ylläpidon ja kehittämisen tehtäväksi digiturvahenkilöstölleen.

HAUSin digiturvan avoimet verkkokoulutukset

HAUS Koulutuskeskus Oy on yhdessä DVV:n ja muiden toimijoiden kanssa toteuttanut digiturvan verkkokursseja. Ne käsittelevät tietosuojaa, tieto- ja kyberturvallisuutta, riskienhallintaa sekä digiturvan häiriötilanteissa toimimista. Kurssitarjontaa on laajennettu ja kurssien sisältöjä päivitetty vuosittain. Vuonna 2023 tarjolla on yksitoista digiturvallisuuteen liittyvää verkkokurssia, jotka ovat liitteessä C.1. Kurssien suoritusmäärät vuosittain ovat korkeita: vuonna 2022 digiturvakursseja suoritettiin yli 50 000 kertaa ja vuoden 2023 suorituksia on kirjattu 24.10.2023 mennessä yli 31 000.

DVV:n TAISTO-harjoitusympäristön vakiinnuttaminen

DVV:n TAISTO-harjoituksissa julkisen hallinnon organisaatiot kehittävät tietosuoja- ja tietoturvaloukkausten hallinnan, johtamisen sekä viestinnän prosesseja ja toimintatapoja annetussa kuvitteelli-

sessa tilanteessa. TAISTO-harjoituksia on järjestetty jo vuodesta 2018 lähtien. Harjoituksiin osallistuneiden organisaatioiden lukumäärä on kasvanut vuoden 2021 250:stä vuoden 2022 375:een ja osallistuneiden henkilöiden määrä 2400 henkilöstä lähes 3400 henkilöön. DVV on julkaissut harjoituksista vuosittain yhteenvetoraportin.

Hanselin digiturvan dynaamiset hankintajärjestelyt

Hansel toteutti VM:n osana Haukka-hanketta ohjaamana Tiedonhallinnan ja digiturvallisuuden asiantuntijapalveluiden 2021–2026 sekä Tietoturvallisuuden arviointilaitosten arviointipalvelujen 2021–2026 dynaamiset hankintajärjestelyt.

Traficomin Hyöky- ja HAVARO-käyttöpilottiprojektit

Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus kartoitti kunnille suunnatussa pilottihankkeessa kyberturvallisuushaavoittuvuuksia ja kuntien kyberturvallisuuden hyökkäyspinta-alaa. Tavoitteena oli mm. selvittää, havaittiinko pilottien avulla haavoittuvuuksia, joita ei muuten olisi ollut organisaation tiedossa, mitä konkreettisia toimenpiteitä tulosten perusteella on voitu käynnistää sekä ovatko pilottien tulokset kasvattaneet organisaatioiden tietoisuutta hyökkäyspinta-alastaan. Haavoittuvuuksien kartoituspalvelu Hyöky on julkaistu Kyberturvallisuuskeskuksen palveluvalikoimaan 13.9.2023 ja tulee kunnille tilattavaksi syksyn 2023 aikana.

Traficomin HAVARO-palvelu on otettavissa käyttöön Hanselin toteuttaman digitaalisen turvallisuuden dynaamisen hankintajärjestelyn kautta. Traficomin kunnille suunnatussa pilottihankkeessa toteutettiin helposti käyttöönotettava, kustannustehokas, virtuaalisiin havainnointisensoreihin perustuva HAVARO-käyttöpilotti. Palvelu antaa käyttäjilleen tietoa organisaatioon kohdistuvasta, vakaviin tietoturvauhkiin liittyvästä kybertoiminnasta ja tuottaa varoituksia, joiden perusteella organisaatio voi reagoida tilanteeseen mahdollisimman aikaisessa vaiheessa. Palvelua on pilotoitu ja kehitetty edelleen vuoden 2023 aikana.

1.3 Haukka-hankkeen suunniteltu ja toteutunut rahoitus

Haukka-toimeenpanosuunnitelman kehitystehtäviin oli alun perin arvioitu tarvittavan 3 660 000 euroa VM:n, DVV:n ja Traficomin tehtäviin. Kustannusarvion ulkopuolelle rajattiin muun muassa valtion ja kuntien havainnointi- ja reagointikyvyn kasvattamisen palveluiden käyttöönoton ja käytön kustannukset sekä kuntien kyberhäiriöiden valvomotoiminteen kustannukset.

VM, DVV ja Traficom ovat seuranneet suunniteltujen tehtävien tarkentumisen vaikutuksia kustannusten määrään ja niiden kohdentamiseen. Hankkeen aikana DVV:n ja Traficomin toteuttamiin, pääosin alun perin suunnitellun rahoituksen ulkopuolelle jääneisiin kuntien digitaalisen turvallisuuden parantamisen tehtäviin sekä Traficomin hyökkäyspinta-alan kartoitustehtäviin ja Havaro-pilottiin osoitettiin lisää rahoitusta. Hankkeen kustannukset olivat 4 495 000 euroa. Hanketta on myös toteutettu virkavalmisteluna, jonka kustannukset eivät sisälly kustannusarvioon.

2 HANKKEEN VAIKUTTAVUUDEN ARVIOINNIN TOTEUTTAMINEN

Haukka-hankkeen vaikuttavuuden arviointi on toteutettu useisiin lähdeaineistoihin perustuvana itsearvioitina. Lähdeaineistoja ovat olleet Haukka-hankkeen tehtävät ja tuotokset; Suomen digitaalisen kompassin (VN 2022:65) Kokonaisturvalliset julkiset palvelut -tavoitteen avaintulosten edistäminen; Viron ylläpitämän National Cyber Security Index (NCSI) mittarin tiedot hankkeen ajalta; DVV:n ylläpitämästä digiturvan kokonaiskuvapalvelusta poimitut vertailutiedot; haastattelut, joissa hankkeeseen eri organisaatioista osallistuneet henkilöt ovat arvioineet Haukka- toimeenpanosuunnitelman tehtävien toteutumista; verkkokyselyt ja ryhmäkeskustelu, joissa julkisen hallinnon toimijat ovat arvioineet valittujen hankkeen tuotosten vaikuttavuutta; DVV:n ja HAUS koulutuskeskus Oy:n digiturvatilaisuuksista, harjoituksista ja verkkokoulutuksista keräämä palaute; DVV:n digiturvapalveluista kerätty palaute; ja Traficomin Haukka-hankkeessa toteuttamista palvelupiloteista kerätty palaute.

Hankkeen vaikuttavuutta arvioitaessa tarkasteltiin hankkeen tuotoksia ja niiden vaikutuksia julkisen hallinnon digitaalisen turvallisuuden parantumiseen. Pyrittiin huomioimaan, miten kattava hankkeen tuotosten kohderyhmä kokonaisuudessaan on ollut ja millaisia toiminnallisia tai rakenteellisia muutoksia tuotosten avulla on toteutettu. Hankkeen tuotosten käyttötarkoitus, käyttötapa ja kohdeyleisö vaihtelevat. Siten hankkeen kokonaisvaikuttavuus muodostuu erilaisista osista. Esimerkiksi digiturvaosaaminen ja -tietoisuus parantavat organisaatioiden kykyä toimia muuttuvassa digiturvaympäristössä, strateginen tilannetietoisuus tukee vaikuttavaa päätöksentekoa ja digiturvan digipalvelut tehostavat organisaatioiden operatiivista digiturvatyötä. Pilottihankkeiden kautta organisaatiot saivat suoria ja konkreettisia tuloksia digiturvan kehittämiseksi. Erilaisia kirjallisia tuotoksia voidaan hyödyntää säädösvalmistelussa, julkisen hallinnon digiturvatyön perustan vahvistamisessa sekä digiturvan jatkokehittämistoimenpiteiden tukemisessa.

2.1 Vaikuttavuuden arvioinnin mittarit

Haukka-hankkeen tuotoksia arvioitiin Valtioneuvoston selonteon Suomen digitaalisesta kompassista (VN 2022:65) Kokonaisturvalliset julkiset palvelut -tavoitteen avaintulosten edistämisen näkökulmasta sekä kansainvälisen Viron ylläpitämän NCSI-mittarin ja DVV:n kansallisten digiturvan kokonaiskuvapalvelun indikaattorien, VM:n JulkICT-osaston tavoitetilan 2025 mittareiden saavuttamisen sekä hankkeen tuotoksia koskevan palautteen perusteella. Täten muodostettiin laadullinen kokonaisarvio hankkeen vaikutuksista julkisen hallinnon digitaaliseen turvallisuuteen ja yleisemminkin digitaalisen turvallisuuden kehittymiseen Suomessa hankkeen aikana.

Suomen digitaalisen kompassin yhtenä tavoitteena on Kokonaisturvalliset julkiset palvelut eli julkisten palvelujen tuottaminen kokonaisturvallisuuden mallin mukaisesti. Haukka-hanke sijoittuu Kokonaisturvalliset julkiset palvelut -tavoitteen alueelle. Hankkeen tuotoksia arvioitiin tämän tavoitteen **avaintulosten edistämisen** näkökulmasta. Avaintulokset ovat:

- Toimintavarma ja häiriösietoinen viestintäinfrastruktuuri on saatavilla kansalaisille ja viranomaisille.
- Valtion, hyvinvointialueiden ja kuntien digitaalinen turvallisuus on parantunut.

- Julkisen hallinnon digitaalisen turvallisuuden ennakointia käytetään toiminnan ja talouden suunnittelussa.
- Julkisten digipalvelujen digiturvaratkaisut tukevat informaatiovaikuttamisen ja disinformaation tunnistamista ja hallintaa.
- Julkisille digipalveluille on asetettu riskiperustaisesti digiturvavaatimukset ja niiden toteutumista arvioidaan ja valvotaan jatkuvasti.

Valtioneuvoston TEAS-raportissa Kyberturvallisuuden strateginen johtaminen Suomessa (TEAS 28/2018[4]) on vertailtu erilaisia kyberturvallisuuden kansallisen tason mittareita. Raportissa todetaan, että Viron ylläpitämän kansainväliseen vertailuun perustuva **National Cyber Security Index** (NCSI)-mittarin ”arvioidaan soveltuvan parhaiten Suomen kansalliseksi kyberturvallisuuden kyvykkyyttä osoittavaksi mittariksi”. NCSI[5]-mittarin valikoituja indikaattoreita sekä DVV:n digiturvan kokonaiskuvapalvelun indikaattoreita on alustavasti suunniteltu Suomen digitaalisen kompassin Kokonaisturvalliset julkiset palvelut-tavoitteen avaintulosten mittareiksi. NCSI:n sovellettavia indikaattoreita ei ole vielä valittu. **Kokonaiskuvapalvelun digiturvan tason indikaattoreina** on tarkoitus käyttää johtamista, riskienhallintaa, toiminnan jatkuvuutta ja varautumista, tietoturvallisuutta, tietosuojaa sekä kyberturvallisuutta. Haukka-hankkeen vaikutusta Suomen digitaalisen turvallisuuden edistämiseen arvioitiin NCSI-mittarin ja DVV:n kokonaiskuvapalvelun indikaattorien avulla.

Haukka-hanketta arvioitiin myös VM:n **JulkICT-osaston vuoden 2025 tavoitetilan[6]** mittareiden saavuttamisen perusteella. Tavoitetilan saavuttamista tukevia strategisia painopistealueita oli määritetty kahdeksan. Yksi niistä oli ”Digiturvariskit hallinnassa”. Se määritettiin seuraavasti: ”Mahdollistamme digiturvallisuuden riskienhallinnalla julkisen hallinnon toimintakykyä ja joustavuutta (resilienssiä) ja arvioimme vaikuttavuutta tavoitteiden toteutumisen ja strategiassa asetettujen digiturvaa koskevien avaintulosten ja mittareiden perusteella.” Kriittisimmäksi kehityskohteeksi oli määritetty: ”digiturvariskienhallinta on osa normaalia VN controllerin ohjeistamaa ja virastojen soveltamaa riskienhallintaprosessia.” Tavoitteeksi vuoteen 2025 asetettiin se, että ”digiturvallisuuden osa-alueen huomioiminen on normaali osa organisaatioiden toimintaa ja riskienhallintaa.”

JulkICT-osaston tavoitetilan 2025 saavuttamiseksi laadittiin polutus ja priorisoitiin tavoitteet. Digiturvaa koskeviksi priorisoiduiksi tavoitteiksi asetettiin 1.4.2021 seuraavat:

1) Julkisen hallinnon digiturvan arviointikriteeristö on käytössä, 1-6/2022.
2) Julkisen hallinnon digiturvan riskienhallinta osana VN controllerin ohjeistusta, 7-12/2022.
3) Jokaisen kunnan digiturvan maturiteettitaso vähintään 3 asteikolla 1-5, 7-12/2023.

Haukka-hankkeen tuotosten vaikuttavuuden arvioinnissa käytettiin lisäksi seuraavia **tuotoksista kerättyjä palautteita**:

1) Haukka-toimeenpanosuunnitelman toteutuminen

[4] https://urn.fi/URN:ISBN:978-952-287-532-7
[5] https://ncsi.ega.ee/ncsi-index/?order=rank
[6] VM (2020). Tavoitetila 2025. JulkICT-osaston visio, missio ja strategiset painopistealueet. 4.12.2020. Julkaisematon.

Tehtäviä toteuttaneiden toimijoiden: VM:n, DVV:n ja Traficomin sekä toteutukseen osallistuneiden toimijoiden: ulkoministeriön (UM), Kuntaliiton ja Huoltovarmuuskeskuksen (HVK) edustajien haastatteluissa antamien tietojen perusteella muodostettu näkemys hankkeen toteuttamisen vaikutuksista julkisen hallinnon digitaaliseen turvallisuuteen. KPMG:n konsultit toteuttivat haastattelut ilman VM:n virkamiesten osallistumista niihin.

4) Digitaalisen turvallisuuden strategisen johtoryhmän näkemykset
   Digitaalisen turvallisuuden strategisen johtoryhmän näkemykset digiturvan kehittymisestä Haukka-hankkeen aikana. KPMG keräsi näkemykset johtoryhmän kokouksen yhteydessä järjestetyssä pyöreän pöydän keskustelussa 10.2.2023.

5) Haukka-hankkeessa laadittujen kirjallisten tuotosten selkeys
   KPMG toteutti hankkeessa julkaistujen tuotosten teksteille yksinkertaisen sana-analyysin, jossa teksteistä etsittiin kapulakielisyyteen viittaavia sanoja.

6) Digiturvan eOppiva-koulutuksista kerätty palaute
   Digiturvaosaamisen kehittymistä hankkeen aikana arvioitiin HAUSin yhdessä DVV:n kanssa järjestämien eOppiva-kurssien suoritusten määrän ja numeerisen kurssipalautteen perusteella.

7) DVV:n digiturvatilaisuuksista kerätty palaute
   DVV:n järjestämien digiturvatilaisuuksien vaikuttavuutta digitaalisen turvallisuuden tietoisuuden ja osaamisen lisääjänä arvioitiin DVV:n tilaisuuksiin osallistuneilta keräämän määrällisen palautteen perusteella.

8) Kuntien digiturvavalmennuksesta kerätty palaute
   DVV:n kymmenelle kunnalle järjestämän digiturvavalmennuksen vaikuttavuutta arviointiin DVV:n kunnilta keräämän määrällisen palautteen perusteella.

9) Haukka-hankkeen valituista tuotoksista kerätty palaute
   Haukka-hankkeen tuotosten vaikuttavuutta arvioitiin valitsemalla kuusi tuotosta ja selvittämällä niiden tunnettuutta ja soveltamisen perusteella saavutettuja hyötyjä. KPMG toteutti selvityksen keräämällä määrällistä palautetta julkisen hallinnon organisaatioille lähetetyn verkkokyselyn avulla.

10) TAISTO-harjoituksista kerätty palaute
    DVV:n järjestämien TAISTO-harjoitusten vaikuttavuutta toiminnan jatkuvuuden ja varautumisen kehittymiseen arvioitiin DVV:n harjoituksiin osallistuneilta keräämän määrällisen palautteen perusteella.

11) Traficomin pilottihankkeista kerätty palaute
    Traficomin haavoittuvuuspinta-alakartoituksen (Hyöky) pilottikunnista ja HAVARO-käyttöpilotin kuntasektorin pilottikäyttäjiltä vuoden 2023 aikana kerätty palaute.

Haukka-hankkeen tuotoksista kerätystä palautteesta määrällisiä tietoja saatiin Haukka-hankkeessa laadittujen kirjallisten tuotosten selkeydestä, eOppiva-kursseista, DVV:n digiturvatilaisuuksista, kuntien digiturvavalmennuksista, TAISTO-harjoituksista sekä Haukka-hankkeen tuotosten tunnettuutta ja soveltamisen perusteella saavutettuja hyötyjä koskevasta selvityksestä. Haukka-toimeenpanosuunnitelman toteutumisen arviointi, digitaalisen turvallisuuden strategisen johtoryhmän näkemykset sekä Traficomin Hyöky- ja HAVARO-käyttöpilotoinnin hyötyjä koskeva selvitykset perustuivat laadullisiin tietoihin digitaalisen turvallisuuden tasosta ja sen muutoksista.

Lisäksi vaikuttavuuden arvioinnissa hyödynnettiin DVV:n toteuttamia digiturvapalvelujen käyttäjille suunnattuja palautekyselyjä. Ensimmäinen DVV:n vuoden 2019 digiturvatoimintaa koskenut kysely toteutettiin tammikuussa 2020. Vuosia 2020–2021 koskenut kysely digiturvapalveluista toteutettiin marraskuussa 2021. Vuosia 2022–2023 koskenut, edellisiä hiukan laajempi kysely toteutettiin syys-lokakuussa 2023.

2.2 Vaikuttavuuden arvioinnin haasteita

Koronapandemia ja Venäjän hyökkäys Ukrainaan ovat muuttaneet toimintaympäristöä niin kansallisesti kuin maailmanlaajuisestikin. Etätyöskentelyn ja etäpalvelujen tarve kasvoi, kun fyysisiä kontakteja rajoitettiin tautitilanteen takia. Sodan vaikutukset ovat näkyneet kybertoimintaympäristönkin uhkien kasvuna. Toiminnan jatkuvuuden, varautumisen ja valmiuden merkitys on korostunut muuttuvassa turvallisuustilanteessa ja erilaiset hybridi- ja informaatiovaikuttamisen keinot vaikuttavat lisääntyneen sodan jatkuessa.

Digitaalisen turvallisuuden (myös digiturva) määritelmä on edelleen vakiintumaton. Se on määritelty VAHTI riskienhallintasanastossa[7], mutta termiä ei löydy esimerkiksi TEPA-termipankista. OECD on hankkeen aikana päivittänyt digitaalisen turvallisuuden määritelmäänsä. OECD määritteli vuonna 2022 digitaalisen turvallisuuden kyberturvallisuuden osa-alueena, johon kuuluvat kyberturvallisuuden taloudelliset ja sosiaaliset näkökulmat[8]. Haukka-hankkeessa ja siten tässä vaikuttavuudenarviointiraportissa digitaalinen turvallisuus ymmärretään riskienhallinnan, varautumisen ja toiminnan jatkuvuuden varmistamisen, tietoturvan, tietosuojan sekä kyberturvallisuuden kattava käsitteenä. Digiturva-termin merkityserojen vuoksi ei ole käytettävissä selkeää vertailukohtaa, johon digiturvan kehittämisellä saavutettuja tuloksia voisi verrata. Ei siis ole aina selvää, onko digiturva kehittynyt, onko kehittyminen ollut merkittävää tai onko kehittymisestä seurannut digiturvan ja sen kypsyystason pysyvä parantuminen, vaikka intuitiivisesti näin vaikuttaisikin olevan.

Digiturvan osa-alueiksi nimettyjä riskienhallintaa, tietoturvaa, tietosuojaa, toiminnan jatkuvuutta ja varautumista sekä kyberturvallisuutta kehitetään julkisessa hallinnossa jatkuvasti niin päivittäisessä linjatyössä kuin kansallisissa hankkeissa. Näitä hankkeita ovat valtioneuvoston periaatepäätös tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla (Titukri)[9], Suomen kyberturvallisuusstrategia 2019 (valtioneuvoston periaatepäätös PLM/2019/52)[10] ja sen toimeenpano, Huoltovarmuuskeskuksen yhteiskunnan sietokykyä kyberhäiriöitä vastaan parantava Digiturva2030-ohjelman[11] sekä Kyberturvallisuusdirektiivin eli ns. NIS2-direktiivin[12] kansallinen täytäntöönpano[13].

[7] VAHTI-riskienhallintasanasto digitaaliseen toimintaympäristöön – esittely ja johdatusta riskiviestintään VAHTI Hyvät Käytännöt -tukimateriaali 15.11.2022
[8] OECD (2022), OECD Policy Framework on Digital Security, OECD Publishing Paris, https://doi.org/10.1787/a69df866-en
[9] https://valtioneuvosto.fi/hanke?tunnus=LVM012:00/2021
[10] https://valtioneuvosto.fi/paatokset/paatos?decisionId=0900908f80655af5
[11] https://www.huoltovarmuuskeskus.fi/huoltovarmuusorganisaatio/huoltovarmuuskeskus/4962-2/digitaalinen-turvallisuus-2030
[12] https://eur-lex.europa.eu/eli/dir/2022/2555
[13] https://valtioneuvosto.fi/hanke?tunnus=LVM044:00/2022

Näin ollen Haukka-hankkeen ja muidenkin digitaalista turvallisuutta edistävien hankkeiden vaikuttavuus näkyy siinä, miten digiturvaa saadaan edistettyä yhden kehittämissyklin aikana, mutta vaikutukset voivat näkyä käytännössä vasta selvästi hankkeiden päättymisen jälkeen.

Haukka-hankkeeseen kuuluvien tehtävien toteutumista ei aina voi selkeästi erottaa virkatyöstä ja rinnakkaishankkeista. Oleellisempaa kuin yksittäisten tehtävien osoittaminen jollekin tietylle toimijalle on kuitenkin digiturvan johdonmukainen edistäminen koko julkisessa hallinnossa. Siten toimeenpanosuunnitelman tehtävien ja digiturva parantumisen välille ei ainakaan lyhyellä aikavälillä voi aina osoittaa selkeää syy-seuraussuhdetta. Digiturva on voinut parantua hankkeen tuloksena tai muusta syystä hankkeen aikana. Toisaalta Haukka-hankkeessa on esimerkiksi tehty digiturvan ja sen arvioinnin säädösvalmistelun taustatyötä sekä laadittu uusia yhteistoiminnan toimintamalleja, joiden vaikutukset näkyvät vasta myöhemmin. Haukka-hankkeen tavoitteen toteutumista arvioidessa on painotettu digiturvan kehittymistä ja parantumista riippumatta siitä, perustuuko mahdollinen myönteinen kehitys Haukka-toimeenpanosuunnitelmaan suoraan vai välillisesti ja milloin vaikutukset alkavat konkreettisesti muotoutua.

Haukka-hankkeen vaikuttavuuden arvioinnissa edellä kuvattuja haasteita on pyritty hallitsemaan luomalla määrällisiä ja laadullisia mittareita Haukka-hankkeen tuotosten arviointiin sekä hyödyntämällä Suomen Digitaalisen kompassin Kokonaisturvalliset julkiset palvelut avaintulosten edistymisen arviointia, kansainvälistä NCSI-mittaria ja kansallisen DVV:n digiturvan kokonaiskuvapalvelun indikaattoreita. Käytettyjen mittareiden ja näkökulmien on yhdessä arvioitu kuvaavan Haukka-hankkeen vaikuttavuutta riittävän kattavasti.

2.3 Rajaukset

Tässä vaikuttavuudenarvioinnissa käytetyt vaikuttavuuden arvioinnin mittarit on pyritty suunnittelemaan siten, että ne täydentävät toisiaan. Mittarit ovat laajuudeltaan erilaisia, eivätkä ne kata kaikkia Haukka-hankkeen mukaisia tehtäviä. Yksittäisen mittarin tuloksia ei ole siten merkittävästi painotettu. Hankkeen vaikuttavuutta on arvioitu eri mittareiden tuottaman yleiskuvan perusteella. Arvioinnissa on oletettu, että jos useat eri mittarit tuottavat keskenään ristiriitaisia tuloksia julkisen hallinnon digitaalisen turvallisuuden kehittymisestä, ei kehitys ole ollut ainakaan merkittävää. Jos toisaalta kaikkien mittareiden tulokset viittaavat siihen, että digiturva on parantunut, on positiivista kehitystä pidetty uskottavana. Koska tarkoituksena oli muodostaa kokonaiskuva hankkeen vaikutuksista julkisen hallinnon digiturvan kehittymiseen, ei raportissa ole arvioitu yksittäisten tehtävien toteuttamista, toteutumista tai onnistumista, tehtävissä saavutettujen tulosten laatua eikä yksittäisten organisaatioiden toimintaa hankkeen aikana.

3 VAIKUTTAVUUDEN ARVIOINNIN TULOKSET

Vaikuttavuuden arvioinnissa pyrittiin selvittämään Haukka-hankkeen vaikuttavuutta. Yksittäisten mittausten tuloksista arvioitiin yleisesti vaikuttavuutta julkisen hallinnon digitaalisen turvallisuuden kehittymiseen Haukka-hankkeen aikana. Toteutetut mittaukset ja arvioinnit näyttävät osoittavan, että hankkeen vaikutus julkisen hallinnon digitaaliseen turvallisuuteen ja sen kehittymiseen on ollut myönteistä. Hanketta on useissa eri sidosryhmien edustajien haastatteluissa ja keskusteluissa pidetty merkittävänä digiturvan kehittymisen edistäjänä ja vastaavan kaltaiselle, pitkäaikaiselle ja jatkuvalle digiturvan kehittämiselle on nähty tarvetta myös tulevaisuudessa.

3.1 Digikompassin kokonaisturvalliset julkiset palvelut avaintulosten edistyminen

Valtioneuvoston selonteossa Suomen digitaalisesta kompassista (VN 2022:65) Kokonaisturvalliset julkiset palvelut tavoitteelle on määritelty viisi avaintulosta. Haukka-hankkeen tuotosten arvioitiin luoneen pohjaa ja edistäneen näistä neljää. Nämä avaintulokset sekä niitä edistäneet Haukka-hankkeen tuotokset on lueteltu alla olevassa taulukossa.

Kokonaisturvalliset julkiset palvelut – avaintulokset	**Avaintulosta edistäneet Haukka-hankkeen tuotokset**
Valtion, hyvinvointialueiden ja kuntien digitaalinen turvallisuus on parantunut	*Digiturvan digipalvelut* • Traficom: Hyöky- ja HAVARO-käyttöpilottihankkeet, Hyöky-palvelu • DVV: Julkri-työkalu ja kriittisyysluokittelutyökalu sekä niiden ohjeistus • DVV: kokonaiskuvapalvelu, strategisten digiriskien arviointi- ja hallintapalvelu • DVV: DVV:n verkkosivuilla ja eOppivassa tarjolla olevat digiturvamateriaalit *Digiturvan tiedolla johtaminen* • Digitaalisen turvallisuuden strategisen johtoryhmän toiminta • VM&DVV: Julkisen hallinnon strateginen digiriskienhallinta ja sen toimeenpano • VM: Ohjeiden ja suositusten vaikuttavuuden arvioinnin pilotointi • DVV: Digiturvan kokonaiskuvapalvelu • DVV: Kuntien digiturvapalveluiden tiekartta • DVV: Julkisen hallinnon digitaalisen turvallisuuden kansallisen harjoitustoiminnan tavoitteet ja toimenpiteet 2021–2022 • Haukka-hankkeeseen sisältyneet DVV:n JUDO-hankkeen ja Traficomin julkisen hallinnon digiturvapalveluiden hankesuunnitelmat ja niiden toimeenpanon ohjaus *Digiturvan tilannekuva* • DVV: Digiturvabarometrit • DVV: Kunnille suunnatut digitaalisen turvallisuuden palvelut -selvitys • DVV: Julkisen hallinnon digitaalisen turvallisuuden nykytilan selvitys • DVV: Kuntien digitaalisen turvallisuuden selvitys • DVV: Raportti - versio 1.10. – Koronaviruspandemian vaikutukset digitaaliseen turvallisuuteen

	• DVV: Julkishallinnon digitaalisen turvallisuuden kansallisen harjoitustoiminnan nykytilan kuvaus • DVV: Selvitys harjoitustoiminnan vaikuttavuudesta, luonnos 2023 • DVV: Kuinka johto varmistaa organisaation toiminnan jatkuvuuden ja luottamuksen säilymisen 2020-luvulla? – Kyselyn yhteenveto • DVV: Turvalliset teknologiat –selvitys • VM: Koneoppiminen digitaalisen turvallisuuden teknisessä valvonnassa *Digiturvan säädösvalmistelun esiselvitykset* • VM: Selvitys organisaation tietoturvatehtävistä ja niiden organisoimisesta • VM: Julkisen hallinnon digitaalisen turvallisuuden yhteistoiminta- ja hallintamalliselvitys • VM: Digitaalisen turvallisuuden yhteistoiminta- ja hallintamallien kansainvälinen vertailu • VM: Digitaalisen turvallisuuden kunta-valtio yhteistoimintamallin esiselvitys *Digiturvan osaamisen kehittäminen* • VM&DVV: Digiturvakompassi-podcast-sarja • DVV: TAISTO-harjoitukset • DVV: Digiturvan avoimet verkkokoulutukset ja -tilaisuudet • DVV: VAHTI-verkosto • DVV: VAHTI hyvät käytännöt tukimateriaalit, 21 julkaisua • DVV: Julkishallinnon digitaalisen turvallisuuden arkkitehtuurikuvaus • DVV: Jatkuvuudenhallintamallin prosessikuvaus • DVV: Opas digitaalisen turvallisuuden harjoitusohjelman ja -toiminnan suunnitteluun • DVV: Turvallisen tekoälykehittämisen opas • DVV: Turvallisen sovelluskehityksen käsikirja
Julkisen hallinnon digitaalisen turvallisuuden ennakointia käytetään toiminnan ja talouden suunnittelussa	*Digiturvan digipalvelut* • DVV: strategisten digiriskien arviointi- ja hallintapalvelu *Digiturvan tiedolla johtaminen* • VM: Digitaalisen turvallisuuden strategisen johtoryhmän toiminta • VM: Digitaalisen turvallisuuden strategisen johtoryhmän näkemyksiä digitaalisen turvallisuuden edistämisestä • VM&DVV: Julkisen hallinnon digitaalisen turvallisuuden strateginen riskienhallinta ja sen toimeenpano • VM: Digitaalisen turvallisuuden kustannus-vaikuttavuusarviointi julkisessa hallinnossa – Selvitystyön raportti • DVV: Kustannus-vaikuttavuus-malli digitaalisen turvallisuuden riskienhallintaan, valmistuu 2023 aikana
Julkisten digipalveluiden digiturvaratkaisut tukevat informaatiovaikuttamisen ja disinformaation tunnistamista ja hallintaa	*Digiturvan tiedolla johtaminen* VM: Näkökulmia julkisten digipalveluiden ja tiedonhallinnan informaatioturvallisuuteen-raportti *Digiturvan osaamisen kehittäminen* • DVV: TAISTO-harjoitukset • DVV: VAHTI hyvät käytännöt - tietosuoja pilvipalveluissa • DVV: VAHTI hyvät käytännöt - Digitaalisen turvallisuuden havainnoinnin kehittäminen

Julkisille digipalveluille on asetettu riskiperustaisesti digiturvavaatimukset ja niiden toteutumista arvioidaan ja valvotaan jatkuvasti	*Digiturvan digipalvelut* • DVV: Julkri-työkalu ja kriittisyysluokittelutyökalu • Traficom: Hyöky- ja HAVARO-käyttöpilottihankkeet, Hyöky-palvelu • DVV: Tietosuojaliite – Henkilötietojen käsittelytoimien kuvaus *Digiturvan tiedolla johtaminen* • VM&DVV: Digitaalisen toimintaympäristön tietovaranto -selvitykset • DVV: Kuntien tietoturvavalvomoiden toimintamallit -selvitys *Digiturvan säädösvalmistelun esiselvitys* • VM: Selvitys digitaalisen turvallisuuden arvioinnin kehitystarpeista • VM: Selvitys digitaalisen turvallisuuden kansainvälisestä arviointilainsäädännöstä • VM: Esityö julkisen hallinnon digitaalisen turvallisuuden arviointikriteeristön luomiseksi *Digiturvaosaamisen kehittäminen* • DVV: VAHTI hyvät käytännöt –tukimateriaalit 10 kpl • DVV: Keinoja ja suosituksia turvata kriittisiä tietovarantoja, tietopalveluita ja tietojärjestelmiä • DVV: Tekoälyn hyödyntäminen – huoneentaulut ja tarkistuslistat • DVV: Kriittisten kohteiden luokittelun menetelmäkuvaus

Avaintuloksia edistäneet Haukka-hankkeen tuotokset on jaoteltu viiteen kokonaisuuteen. Hankkeen tuotoksista lukumääräisesti selkeästi eniten on digiturvan **osaamisen kehittämisen** aineistoa: digiturvatilaisuuksia ja -verkkokoulutuksia sekä oikeudellisesti sitomattomia ohjeita ja oppaita. Varsinaisia **digiturvan digipalveluita** on seitsemän. Niukka digipalveluiden määrä johtuu siitä, että digiturvan digipalveluiden kehittämisen ja käytön kustannukset rajattiin hankkeen käynnistyessä Haukka-hankkeen rahoituksen ulkopuolelle. Traficomin digiturvan digipalveluiden ja DVV:n kuntien digiturvapalveluiden kehittämiseen osoitettiin myöhemmin rahoitusta hankkeen aikana.

Tiedolla johtamisen tuotoksia on kohtalaisesti. Ne ovat tuotoksia, joissa on jalostettu ja hyödynnetty tietoa päätöksenteossa. Koska julkisen hallinnon keskeisimpiin tehtäviin kuuluu koko yhteiskuntaa koskevien päätösten valmistelu, toteutus ja toimeenpano, tulisi jatkossa julkisten palvelujen turvallisuuden johtamista painottaa enemmän. Tällöin päätöksenteon tueksi saadaan hyvin analysoitua ja ajantasaista tietoa. **Digiturvan tilannekuvaa** koostaneita selvityksiä laadittiin melko paljon. Niitä hyödynnettiin muodostettaessa tarkempaa näkemystä julkisen hallinnon ja erityisesti kuntien digiturvan nykytilasta ja kehitystarpeista sekä suunniteltaessa ja toteutettaessa digiturvapalveluita hankkeen aikana. Lisäksi tuotoksia hyödynnettiin hankkeen ulkopuolisessa säädösvalmistelussa. **Säädösvalmistelun esiselvityksiä** on niukasti. Alkuperäisessä Haukka-toimeenpanosuunnitelmassa niitä oli tarkoitus käyttää hankkeessa toteutettavassa säädösvalmistelussa. Hankkeen aikana säädösvalmistelutehtävät rajattiin hankkeen ulkopuolelle VM:n JulkICT-osaston säädösvalmistelusuunnitelmassa.

Haukka-hankkeen tuotoksissa keskeisenä näkyy digitaalisen turvallisuuden strategisen johtoryhmän toiminta. Se on vaikuttanut kaikkiin avaintuloksiin. Avaintuloksista laajin on **valtion, hyvinvointialueiden ja kuntien digitaalinen turvallisuus on parantunut**, mikä selittää tuotosten painottumista tälle avaintulokselle. Avaintulokselle **Julkisen hallinnon digitaalisen turvallisuuden ennakointia käytetään toiminnan ja talouden suunnittelussa** osuvat Haukka-hankkeen digiturvan kustannus-

vaikuttavuutta sekä strategista riskienhallintaa selvittäneet valtiovarainministeriön raportit. Raporteihin kerättyjen tietojen pohjalta DVV:ssä on suunniteltu ja toteutuksessa tiedolla johtamista: strategisten digiriskien hallinta ja hallintaympäristö sekä digiriskienhallinnan kustannus-vaikuttavuusarviointi.

Selkeästi vähiten hankkeen tuotoksia on avaintulokselle **Julkisten digipalveluiden digiturvaratkaisut tukevat informaatiovaikuttamisen ja disinformaation tunnistamista ja hallintaa**. Tähän avaintulokseen liittyviä tehtäviä ei sisältynyt alkuperäiseen Haukka-toimeenpanosuunnitelmaan, mutta Haukka-hankkeeseen lisättiin yksi selvitystehtävä informaatiovaikuttamisesta toimintaympäristön muutosten johdosta. Selvitystehtävä toteutettiin osana digitaalisen turvallisuuden strategisen johtoryhmän toimintaa.

Haukka-tuotoksista DVV:n Julkri- ja kriittisyysluokittelutyökalut, Traficomin pilottihankkeiden perusteella julkaistu Hyöky-palvelu sekä HAVARO-palvelun edelleen kehittäminen ovat keskeisiä **Julkisille digipalveluille on asetettu riskiperustaisesti digiturvavaatimukset ja niiden toteutumista arvioidaan ja valvotaan jatkuvasti** -avaintuloksen tuotoksia. Näiden palveluiden tarjoamista julkiselle hallinnolle on perusteltua jatkaa myös hankkeen jälkeen: Hyöky-palvelu auttaa asiakasorganisaatioita tunnistamaan haavoittuvuuksia ja HAVARO-palvelut auttavat Traficomia tunnistamaan vakavan, vihamielisen, ulkopuolisen kybertoiminnan ja varoittamaan asiakasorganisaatioita niistä. Avaintuloksen tiedolla johtamisen tuotokset ja säädösvalmistelun esiselvitykset valmistuivat, mutta varsinainen säädösvalmistelu rajattiin myöhemmillä päätöksillä hankkeen ulkopuolelle. Tuloksia on hyödynnetty valmisteltaessa VM:n Arviomuistiota julkisen hallinnon tietojärjestelmien sääntelyn nykytilasta ja kehittämistarpeista (2021:54), hallituksen esitystä eduskunnalle julkisen hallinnon automaattista päätöksentekoa koskevaksi lainsäädännöksi (145/2022), VM:n virkamiespuheenvuoroa (2022:77) ja Suomen digitaalista kompassia (VN 2022:65).

3.2 Haukka-hanke keskeisten kyber- ja digiturvamittareiden näkökulmasta

Suomen sijoitus Viron NCSI-mittarissa on Haukka-hankkeen aikana laskenut vuoden 2020 seitsemänneltä sijalta tuoreimman lokakuun 2023 tiedon mukaan kolmannelletoista sijalle[14]. Suomi on päivittänyt NCSI:hin tietoja viimeksi marraskuussa 2020. Suomen sijoittumisesta vertailussa ei siten voida päätellä kyberturvallisuuden kehittymistä Haukka-hankkeen aikana. Suomen sijoituksen laskua selittävät ainakin digi- ja kyberturvan parantamiseksi verrokkivaltioissa tehdyt investoinnit, jotka ovat nostaneet useiden valtioiden sijoitusta indeksissä: esimerkiksi Belgia, Romania ja Iso-Britannia. Näin ollen voi sanoa, että Suomen digi- ja kyberturvan taso ei ole heikentynyt, mutta verrokkivaltioissa panostukset digiturvan kehittämiseen ovat olleet Suomea vahvempia.

Indikaattoreista Suomella oli eniten puutteita elintärkeiden palvelujen (essential services) turvaamisessa. Neljän indikaattorin yhteensä kuudesta kriteeristä Suomi ei ollut viimeksi toimitettujen tietojen perusteella toteuttanut yhtään. Lisäksi kyberkriisien hallinnassa Suomi oli toteuttanut neljän indikaattorin yhteensä viidestä kriteeristä ainoastaan kolme. Suomen tietojen seuraava päivitys alkuvuodesta 2024 on valmistelussa.

[14] Finland_2020-11-17_ncsi.ega.ee.pdf

DVV on toteuttanut Organisaation Digiturvakyselyä saman sisältöisenä vuosina 2021–2023. Hankkeen aikana Organisaation Digiturvakysely siirrettiin osaksi hankkeessa tuotettua DVV:n digiturvan kokonaiskuvapalvelua. Viimeisimmät tulokset on julkaistu raporttina 30.5.2023. Kyselyyn vastanneiden organisaatioiden lukumäärä on ollut vuonna 2021 128, 2022 118 ja 2023 194 organisaatiota. Osa-aluekohtaiset tulokset vuosina 2021–2023 ovat alla olevassa taulukossa.

	2023	**2022**	**2021**
Koko kysely	**0,70**	**0,69**	**0,71**
Johtaminen	0,65	0,65	0,65
Riskienhallinta	0,68	0,70	0,68
Toiminnan jatkuvuus ja varautuminen	0,66	0,67	0,67
Tietoturvallisuus	0,75	0,75	0,78
Tietosuoja	0,78	0,77	0,81
Kyberturvallisuus	0,61	0,59	0,59

Lähde: Organisaation Digiturvakysely – Raportti ja keskeiset havainnot, 30.5.2023, Digi- ja väestötietovirasto

Digiturvan kokonaiskuvapalvelun vuoden 2023 yhteenvetotietojen perusteella digitaalinen turvallisuus julkisessa hallinnossa on kokonaisuutena varsin hyvä. Kyselyn osa-alueiden tunnusluvut olivat melko korkeita. Tunnusluvut ovat vaihdelleet vuosittain, mutta muutokset ovat olleet vähäisiä. Vastaajien lukumäärän kasvu on voinut lisätä tuloksiin hajontaa, joka voi lisääntyä jatkossakin. Toisaalta kattavampi vastaajien joukko antaisi tarkemman kuvan julkisen hallinnon digiturvan yleisestä tasosta varsinkin, jos aineistosta laskettaisiin keskiarvojen lisäksi hajontaa kuvaavia tunnuslukuja. Kattavampi vastaajien joukko myös vähentäisi yksittäisen vastauksen vaikutusten ylikorostumista.

DVV:n digiturvan kokonaiskuvapalvelun indikaattoreiden perusteella Suomen digitaalinen turvallisuus on Haukka-hankkeen aikana säilynyt lähes ennallaan. Toimintaympäristön ja digipalveluissa käytettyjen teknologioiden jatkuvassa muutoksessa tätä voi pitää tyydyttävänä saavutuksena. Digiturvan kokonaiskuvapalvelua ja sen tuloksia on esitelty yksityiskohtaisemmin liitteessä B.

3.3 VM:n JulkICT-osaston tavoitetilan 2025 digiturvatavoitteiden toteutuminen

VM:n JulkICT-osaston tavoitetilan 2025 saavuttamiseksi laadittujen digiturvaa koskevien priorisoitujen tavoitteiden toteuma on seuraava:

1) Julkisen hallinnon digiturvan arviointikriteeristö on käytössä, 1-6/2022.
   Toteuma: Haukka-hankkeessa valmisteltiin 11.5.2021 julkaistu asiakirja ”Esityö julkisen hallinnon digitaalisen turvallisuuden arviointikriteeristön luomiseksi”. Tämän jälkeen kriteeristön valmistelu siirrettiin JulkICT-osaston päätöksellä tiedonhallinalautakunnan tehtäväksi. Tiedonhallintalautakunta julkaisi 2.6.2022 suosituksen ”Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri) : Suositus ja kriteeristö (VM 2022:43) sekä päivityksen (VM 2023:46) 12.6.2023.

   Tavoite saavutettiin ja Haukka-hanke osaltaan tuki tavoitteen saavuttamista.

2) Julkisen hallinnon digiturvan riskienhallinta osana VN controllerin ohjeistusta, 7-12/2022.
   Toteuma: Strategisten digiriskien hallintamalli valmisteltiin DVV:n JUDO-hankkeessa yhteistyössä VN controller -toiminnan kanssa. JUDO-ohjausryhmä hyväksyi strategisten digiriskien hallintamallin 8.9.2022. DVV julkaisi ”VAHTI riskienhallintasanasto digitaaliseen toimintaympäristöön” -hyvät käytänteet tukimateriaalin 9.6.2022. VM julkaisi 17.8.2023 Riskienhallinnan käsikirjan valtionhallinnon toimijoille (VM 2023:54). Digitaalisen toiminnan riskienhallinnan todetaan käsikirjassa sisältyvän riskienhallintaan. Siinä myös viitataan VAHTI riskienhallintasanastoon digitaaliseen toimintaympäristöön -asiakirjaan sekä VAHTI-verkoston materiaaleihin ja Haukka-hankkeessa valmisteltuihin raportteihin ja selvityksiin.

   Tavoite saavutettiin vaikkakin noin puoli vuotta myöhemmin kuin oli tavoitteena ja Haukka-hanke osaltaan tuki tavoitteen saavuttamista.

3) Jokaisen kunnan digiturvan maturiteettitaso vähintään 3, 7-12/2023.
   Toteuma: DVV:n digiturvan kokonaiskuvapalveluun antoi vuonna 2023 tietoja yhteensä 121 kuntaa ja kuntayhtymää. Kaikkien digiturvan eri osa-alueiden keskiarvot olivat yli 0,5, minkä voi katsoa vastaavan arvoa 3 asteikolla 1–5. Johtamisen keskiarvo oli 0,62, riskienhallinnan 0,66, toiminnan jatkuvuuden ja varautumisen 0,64, tietoturvallisuuden 0,74, tietosuojan 0,76 ja kyberturvallisuuden 0,59. Vuoden 2021 tuloksiin verrattuna osa-alueittain on tapahtunut pieniä muutoksia. Johtamisen tulos on pysynyt samana, riskienhallinnan tulos on laskenut 0,02, toiminnan jatkuvuuden ja varautumisen tulos on laskenut 0,04, tietoturvallisuuden tulos on laskenut 0,01, tietosuojan tulos on laskenut 0,03. Kyberturvallisuuden tulos on noussut 0,06. On syytä huomioida, että kunta- ja kuntayhtymävastaajien yhteenlaskettu lukumäärä on vuoden 2021 tuloksista lähtien lähes kolminkertaistunut. Keskiarvot on laskettu vastaajien lukumäärällä painotettuina, koska kuntavastaajia on ollut huomattavasti kuntayhtymävastaajia enemmän.

   DVV järjesti kymmenelle kunnalle digiturvavalmennusta vuosina 2021 ja 2022. Palautekyselyyn vastanneet viisi kuntaa arvioivat digiturvansa parantuneen kaikilla digiturvan osa-alueilla[15]. Osa-alueittain kuntien keskiarvot paranivat seuraavasti: johtamisen keskiarvo kasvoi 0,18, riskienhallinnan 0,16, toiminnan jatkuvuuden ja varautumisen 0,25, tietoturvallisuuden 0,03, tietosuojan 0,05 ja kyberturvallisuuden 0,05. Valmennuksesta kerätyn palautteen tuloksia on käsitelty liitteessä E.

   Tavoitetta ei täysin saavutettu, mutta Haukka-hanke osaltaan tuki tavoitteen saavuttamista.

3.4 Haukka-hankkeen tuotosten vaikuttavuuden arvioinnista kerätty palaute

3.4.1 Haukka-toimeenpanosuunnitelman toteutuminen

KPMG toteutti Haukka-toimeenpanosuunnitelman toteutumisen arvioinnin haastattelemalla DVV:n, Traficomin ja Kuntaliiton asiantuntijoita sekä tutustumalla hankkeessa julkaistuihin selvityksiin ja raportteihin. Haastattelut toteutettiin marraskuussa 2022 ja dokumentaatioon tutustuminen marras-joulukuussa 2022. Lisäksi sähköpostitse kysyttiin tehtävien valmistumisesta ulkoministeriöstä ja

[15] Kuntien digiturvavalmennukset 2022 - Kartoitusten yhteenveto.pdf

Huoltovarmuuskeskuksesta. Lopuksi arvioitiin VM:n vastuulla olevien tehtävien toteuttamisen vaikutuksia julkaisujen ja muiden kirjallisten lähteiden sekä VM:n asiantuntijoiden kanssa toteutettujen keskustelun avulla.

Haastattelujen ja lähdeaineiston perusteella Haukka-toimeenpanosuunnitelman tehtäviä on toteutettu kattavasti. Toimeenpanosuunnitelman tehtävää 4 Digitaalisen identiteetin hallinta on edistetty Haukka-hankkeen alusta lähtien omana erillisenä hankkeena, joten sen toteutumisen vaikutuksia ei arvioitu. Hankkeessa julkaistut tuotokset ovat liitteessä A. Tuotoksia on käsitelty VM:n digitaalisen turvallisuuden strategisessa johtoryhmässä ja JulkICT-osaston johtoryhmässä sekä DVV:n VAHTI-johtoryhmässä, JUDO-hankkeen ohjausryhmässä ja digiturvatilaisuuksissa.

Vaikuttavuuden arvioinnin kannalta Haukka-toimeenpanosuunnitelman tehtävien jatkuvaa päivittämistä voi pitää myönteisenä seikkana: riittävän joustavaksi laadittu toimeenpanosuunnitelma ja sen toteutuksen ohjaus on mahdollistanut resurssien kohdistamisen tarkoituksenmukaisesti. Siten ei ollut tarkoituksenmukaista arvioida, ovatko suunnitelmaan kirjatut yksittäiset kehitystehtävät toteutuneet alkuperäisen suunnitelman mukaisesti. Arviointi on kohdistettu Haukka-toimeenpanosuunnitelman vaikuttavuuteen julkisen hallinnon digitaalisen turvallisuuden kehittymiseen kokonaisuutena.

Haukka-hankkeessa on toteutettu useita merkittäviä, digitaalista turvallisuutta parantavia toimenpiteitä. Hankkeen tuotosten katsottiin vaikuttaneen positiivisesti digiturvan digipalvelujen sekä uusien digiturvamallien ja -prosessien käyttöönottoon ja käyttöön, digiturvatietoisuuden ja -osaamisen lisääntymiseen sekä julkisen hallinnon digiturvan sääntelyn edistämiseen. Haukka-toimeenpanosuunnitelman toteutumisen arvioinnin perusteella Haukka-hankkeen vaikutus julkisen hallinnon digitaaliseen turvallisuuteen on siten ollut myönteinen.

3.4.2 Digiturvan strategisen johtoryhmän näkemykset

Digiturvan strategisen johtoryhmän keskustelun perusteella Haukka-hankkeen vaikuttavuuden mittaamista ja yksityiskohtaista analysointia pidettiin haastavana ja erityisesti heterogeenisen kuntasektorin arviointia vaikeana. Johtoryhmä tunnisti kuitenkin yhteistoiminnassa, harjoittelussa ja tietoisuuden lisäämisessä saavutettuja merkittäviä tavoitteita, kuten esimerkiksi TAISTO-harjoitukset ja Traficomin pilottihankkeet.

Todettiin, että hankkeessa on toteutettu toimivaa ohjausmallia, jossa ensin on valmisteltu valtioneuvoston periaatepäätös ja sitten periaatepäätöstä toimeenpanevat kehittämistoimenpiteet. Toimintamalli on tukenut laaja-alaista kehittämistä hyvin. Digiturvatekemistä on voitu edistää pitkäaikaisella, keskitetyllä rahoituksella. Laajojen kehittämistoimenpiteiden katsottiin edellyttävän pitkäaikaista rahoitusta, hyvää yhteistyötä ja selkeää koordinointia.

3.4.3 Haukka-hankkeessa laadittujen kirjallisten tuotosten selkeys

Haukka-hankkeen vaikuttavuuden kannalta on tärkeää, että hankkeen tuotoksia on julkaistu ja niistä on viestitty sekä eri johto- ja ohjausryhmien kokouksissa että eri digiturvatilaisuuksissa. Tuotosten

selkeys ja ymmärrettävyys kuitenkin vaikuttavat niiden hyödyntämiseen käytännön digiturvatyössä. Tähän tulisi kiinnittää jatkossa yhä enemmän huomiota.

Tuotosten selkeyden ja ymmärrettävyyden arvioimiseksi tarkasteltiin 15 tekstimuotoisten hankkeen julkaisun kielellisestä laadusta laskettua kahta tunnuslukua. Ne olivat julkaisujen virkkeiden sanamäärät sekä niiden virkkeiden osuudet, jotka sisältävät ns. kapulakielisiä sanoja. Verrokkiaineistoina käytettiin yhtä Kotimaisen kielen tutkimuskeskuksen (Kotus) ja yhtä Kielikello-lehden verkkoartikkelia.

Hankkeen tarkasteltujen julkaisujen virkkeiden keskimääräinen pituus oli 11–17 sanaa. Tämä vastaa verrokkiaineistojen keskimääräistä virkkeen sanamäärää. Kapulakielisten virkkeiden määrä oli noin 7 % kaikista virkkeistä. Tämä on lähellä verrokkiaineistoja. Virkkeiden sanamäärien ja kapulakielisten sanojen määrien perusteella hankkeen julkaisuja voidaan pitää ainakin kohtuullisen selkeinä.

Tarkastellut tunnusluvut kertovat Haukka-hankkeen vaikuttavuudesta vain välillisesti. Niiden perusteella ei voi vielä tehdä kovin pitkälle meneviä johtopäätöksiä hankkeen vaikuttavuudesta.

3.4.4 Digiturvan eOppiva-koulutuksista kerätty palaute

HAUS Koulutuskeskus Oy:n yhdessä DVV:n ja muiden toimijoiden kanssa toteuttamien digiturvan verkkokurssien suoritusten määrä on kasvanut vuosittain jatkuvasti. Vuonna 2020 erilaisia digiturvakursseja oli viisi ja suorituksia näissä yhteensä noin 10 000. Vuonna 2022 kursseja oli julkaistu yksitoista ja suorituksia niissä oli yhteensä lähes 51 000. Tätä kirjoitettaessa (24.10.2023) suorituksia on ollut hieman yli 31 000. Tämä kertoo siitä, että digiturva-asioiden ja osaamisen kehittämisen merkitys on tunnistettu laajasti. Julkiselle hallinnolle tuotetaan useampia kursseja kuin avoimelle puolelle ja lisäksi osa kursseista on suunnattu tietyille henkilöryhmille, kuten Digiturvallisuus kuntien luottamushenkilöille ja Digiturvallisuus hyvinvointialueiden luottamushenkilöille.

Suoritusmäärien kasvu ja vahvasti positiivinen palaute osoittavat, että digiturvan tietoisuuden ja osaamisen kasvattaminen koetaan tärkeäksi. Koulutuksista on annettu palautetta vuosina 2021–2023 yli 40 000 kertaa ja arvosanat ovat pysyneet jatkuvasti korkeina. Koulutusten arviointia varten osallistujia on pyydetty arvioimaan koulutusta kahdentoista tekijän perusteella. Koulutusten toteutuksesta, sisällöstä ja hyödyllisyydestä annetut arvosanat ovat olleet viisiportaisella asteikolla vuosittain vähintään 4,2 ja kokemusten jakamisesta kollegoiden kanssakin annetut arvosanat ovat olleet vähintään 3,3. Palautteen korkeat arvosanat kertovat siitä, että digiturvan verkkokoulutukset vaikuttavat merkittävästi ja pysyvästi digiturvan osaamisen ja tietoisuuden parantumiseen.

Haukka-hankkeen vaikutus digitaalisen turvallisuuden osaamisen kehittymiseen on siten ollut myönteinen. Mittaria ja sen tuloksia on esitelty yksityiskohtaisemmin liitteessä C.

3.4.5 DVV:n digiturvatilaisuuksista kerätty palaute

Digiturvaosaamiselle ja -tietoisuudelle on DVV:n digiturvatilaisuuksista kerättyjen palautteiden perusteella runsaasti kysyntää niin julkisessa hallinnossa, yksityisellä sektorilla kuin kansalaistenkin

joukossa. Digiturvatilaisuuksien osallistujamäärät ovat säilyneet varsin korkeina ja voidaankin arvioida, että tilaisuuksilla on ollut tavoitellun kaltainen vaikutus eri kohderyhmien digiturvatietoisuuden lisääntymiseen.

DVV:n digiturvatilaisuuksista kerätyn palautteen perusteella Haukka-hankkeen vaikutus julkisen hallinnon digitaaliseen turvallisuuteen on ollut myönteinen. Mittaria ja sen tuloksia on esitelty yksityiskohtaisemmin liitteessä D.

3.4.6 Kuntien digiturvavalmennuksesta kerätty palaute

DVV järjesti kymmenelle kunnalle digiturvavalmennusta vuosina 2021 ja 2022 ja näistä puolet vastasi valmennuksen palautekyselyyn. Vastaajat olivat kokeneet digiturvan parantuneen kaikilla digiturvan osa-alueilla. Niiden yhteenlaskettu keskiarvo nousi noin 22 %. Siten valmennus oli ollut vaikuttavaa.

Toisaalta digiturvavalmennukseen osallistui vain kymmenen kuntaa. Palautekyselyn tuloksiin on siten suhtauduttava varauksella. Voidaan kuitenkin olettaa, että vastaavalle valmennukselle on tarvetta jatkossakin.

Kuntien digiturvavalmennuksesta kerätyn palautteen perusteella sen vaikutus kuntien ja siten koko julkisen hallinnon digitaaliseen turvallisuuteen on ollut myönteinen. Mittaria ja sen tuloksia on esitelty yksityiskohtaisemmin liitteessä E.

3.4.7 Haukka-hankkeen tuotosten vaikuttavuutta koskeva kysely

VM lähetti Haukka-hankkeen tuotosten vaikuttavuutta koskevan kyselyn yli seitsemäänsataan julkisen hallinnon organisaation kirjaamoon sähköpostitse. Vastauksia saatiin yhteensä 106, eli vastausprosentti oli noin 15. Vastaajista 28 edusti valtionhallintoa, 6 aluehallintoa (sis. hyvinvointi- ja yhteistoiminta-alueet), 53 kuntia ja kuntayhtymiä, 14 korkeakouluja ja 5 muita vastaajia.

Hankkeen tuotoksista kyselyyn valittiin arvioitavaksi sellaisia tuotoksia, joiden kohderyhmä olisi mahdollisimman laaja, joita oletettiin toteutetun monissa organisaatioissa ja joiden käyttötarkoitukset olivat erilaisia. Arvioitavien kohteiden lukumäärä rajattiin kuuteen, jotta arviointikysely ei muodostuisi liian raskaaksi. Arvioitaviksi valitut tuotokset olivat VM:n yhteistoiminta- ja hallintamalliselvitys (VM 2022:76), VM:n tietoturvavastaavan roolikuvaus, DVV:n digiturvakatsaukset ja digiturvavartti, DVV:n kriittisyysluokittelun työkalu ja menetelmäkuvaus, VAHTI riskienhallintasanasto sekä DVV:n digiturvan arkkitehtuurikuvaus -wiki.

Kyselyssä vastaajia pyydettiin kertomaan näkemyksiä siitä, miten hyvin tuotokset tunnettiin, oliko organisaatio suorittanut tuotosten aihepiiriin kuuluvia tehtäviä viimeksi kuluneen kahdentoista kuukauden aikana ja miten tuotoksia oli näissä tehtävissä hyödynnetty. Lisäksi kysyttiin, miten merkittäviä vaikutuksia tuotosten hyödyntämisellä oli koettu olevan organisaatioiden digiturvatyössä.

Hankkeen tuotosten tunnettuus vaihteli vastausten perusteella melko paljon. Tuotoksista parhaiten tunnettu oli DVV:n digiturvakatsaukset ja digiturvavartti, jonka kohderyhmäkin on laajin. Vastaajista noin 80 % tunsi niitä ainakin jonkin verran. Vastaajista noin 60 % tunsi ainakin jonkin VM:n tietoturvavastaavan roolikuvausta, VAHTI riskienhallintasanastoa ja DVV:n kriittisyysluokittelun työkalua ja menetelmäkuvausta sekä arkkitehtuurikuvausta. VM:n yhteistoiminta- ja hallintamalliselvitys oli vähiten tunnettu: noin puolet vastaajista tunsi sitä ainakin jonkin verran.

Tuotoksiin liittyviä tehtäviä oli vastaajaorganisaatiossa tehty kyselyä edeltäneiden kahdentoista kuukauden aikana odotettua vähemmän. Parhaiten tunnettuun digiturvakatsauksiin ja digiturvavarttiin liittyviä tehtäviä oli tehty useimmin, noin 75 %:ssa vastanneista organisaatioista. Noin 60 %:ssa vastanneista organisaatioista oli tehty muihin tuotoksiin liittyviä tehtäviä. Yhteistoiminta- ja hallintamalliselvitykseen liittyviä tehtäviä oli tehty noin joka toisessa organisaatioissa. Vaikuttaisi siltä, että erityisesti digiturvan yhteistoimintaa olisi perusteltua kasvattaa. Toisaalta vastausten perusteella kriittisyysluokittelun, digiturva-arkkitehtuurin tai tietoturvatehtävien organisoinnin tehtäviä ei ollut tehty lainkaan yli 40 %:ssa kaikista vastanneista organisaatioista. Se ei välttämättä edusta kattavasti todellista tilannetta julkisessa hallinnossa. Kuitenkin kunnat ja kuntayhtymät -ryhmässä tuotoksiin liittyvien tehtävien tekeminen oli muita ryhmiä vähäisempää. Tehtäviä suorittaneiden organisaatioiden osuus tässä vastaajaryhmässä oli selvästi keskiarvoja alempi kaikilla tuotoksilla.

Tuotosten hyödyntämisestä kysyttiin tarkemmin vain niiltä vastaajilta, jotka olivat suorittaneet näihin tuotoksiin liittyviä tehtäviä. Parhaiten tunnettuja tuotoksia oli hyödynnetty useimmin: tuotosten tunnettuuden ja niiden hyödyntämisen korrelaatiokerroin oli noin 1. Parhaiten tunnetut tuotokset arvioitiin myös vaikuttavimmiksi. Vastaajista noin 60 % oli hyödyntänyt DVV:n digiturvakatsauksia ja digiturvavarttia sekä noin 50 % VAHTI riskienhallintasanastoa ja VM:n tietoturvavastaavan roolikuvausta. Niiden vaikuttavuudeksi arvioitiin noin 2 asteikolla 1–3. Noin 30–40 % oli hyödyntänyt kolmea muuta arvioitua tuotosta. Niistä vaikuttavimmaksi arvioitiin kriittisyysluokittelun työkalu ja menetelmäkuvaus. Tuotosten hyödyntämiseen vaikuttivat siten eniten niiden tunnettuus sekä mahdollisesti niiden soveltuvuus vastauksen antaneen henkilön digiturvavastuisiin tai -tehtäviin.

Tehtävien suorittamista ja tuotosten hyödyntämistä koskeviin kysymyksiin toivottiin palautteessa vastausvaihtoehdoiksi ”en tiedä” tai ”en osaa sanoa”. Tämän perusteella arvioidaan, että kysely ei ollut tavoittanut kaikissa tapauksissa henkilöä, jonka tehtäviin digiturva-asiat kuuluisivat. Kaikissa vastaajaorganisaatioissa ei ehkä myöskään tunneta yleisiä digiturvatehtäviä. Jatkossa tulisi pohtia sekä kyselyn kohdistamista että digiturvaosaamisen kehittämistä. Kysely tulisi saada osoitettua aiempaa tarkemmin niille henkilöille, jota toteuttavat digiturvatehtäviä organisaatiossa tai sen lukuun. Lisäksi organisaatioiden tulisi pohtia, miten digiturvaosaamista olisi mahdollista edelleen lisätä.

Kyselyyn vastanneet arvioivat kyselyn mittaavan Haukka-toimeenpanosuunnitelman vaikuttavuutta melko hyvin: arvioiden keskiarvo oli 3,2 asteikolla 1–5. Myös jokaisen Haukka-hankkeen tuotoksen arvioinnin koettiin mittaavan toimeenpanosuunnitelman vaikuttavuutta melko hyvin: vastausten keskiarvo oli yli 3 asteikolla 1–5. Kyselyn toteuttamisessa onnistuttiin siten hyvin.

Vaikka kyselyn vastausprosentti oli melko alhainen, voi tuotoksiin liittyvien tehtävien suorittamisen ja niissä tuotoksia hyödyntäneiden organisaatioiden osuuksia pitää varsin vähäisinä. Digiturvan arkkitehtuurin määrittäminen, tietoturvavastuiden organisointi ja toimintojen kriittisyysluokittelu ovat

keskeisiä digiturvatyön tehtäviä, joita olisi pitänyt toteuttaa lähes kaikissa organisaatioissa. Vastausten perusteella digiturvan kehittämistoimenpiteistä ja niiden tuotoksista viestimiseen tulisi jatkossa kiinnittää enemmän huomiota. Tehokkaampi viestintä parantaisi todennäköisesti tuotosten tunnettuutta, mikä kyselyn tulosten perusteella tehostaisi niiden hyödyntämistä digiturvatyössä. Toisaalta melko alhainen vastausprosentti viittaa siihen, että vastaavan kaltaisia kyselyjä tulee organisaatioihin niin paljon, ettei niihin ehditä paneutua. Mittaria ja sen tuloksia on esitelty yksityiskohtaisemmin erillisessä liitteessä[16].

3.4.8 TAISTO-harjoituksista kerätty palaute

Harjoitusten merkitys digiturvaosaamisen kehittämisen keinona on kirjattu Haukka-toimeenpanosuunnitelmaan. TAISTO-harjoituksista kootun palautteen [17, 18, 19] perusteella harjoittelua häiriötilanteissa toimimisen varalle pidetään hyvin tärkeänä. Harjoituksiin osallistuneiden organisaatioiden lukumäärä on kasvanut vuoden 2021 250:stä vuoden 2022 375:een ja osallistuneiden henkilöiden määrä 2400 henkilöstä lähes 3400 henkilöön. Haukka-hankkeesta vuosina 2020–2023 rahoitetut TAISTO-harjoitukset ovat kasvattaneet suosiotaan jatkuvasti. Harjoituksiin osallistujilta saadun palautteen perusteella harjoituksista on saatu hyötyä niin organisaatioille kuin osallistujille ja yleisarvosanat harjoitusten sisällöstä, ajankohtaisuudesta ja toteutuksesta ovat jatkuvasti olleet erittäin hyviä. Lähes kaikki palautekyselyyn vastaajat (vähintään 98 % vuosittain) ovat pitäneet harjoituksia hyödyllisinä, yli 85 % on arvioinut oman osaamisensa kehittyneen ja yli 90 % vastaajista on antanut harjoituksen yleiskuvalle erinomaisen tai hyvän arvosanan. Vuosien 2020 ja 2021 harjoitusten oli arvioitu parantaneen organisaation toimintaa (4,54 asteikolla 1–5) ja vuoden 2022 harjoituksessa 96 % vastaajista oli samaa mieltä toiminnan kehittymisestä.

TAISTO-harjoituksista kerätyn palautteen perusteella harjoittelun vaikutus julkisen hallinnon digitaaliseen turvallisuuteen on ollut myönteinen. Mittaria ja sen tuloksia on esitelty yksityiskohtaisemmin liitteessä F.

3.4.9 Traficomin pilottihankkeista kerätty palaute

Traficom toteutti erityisesti kunnille ja kunnallisille palvelutoimijoille suunnatut hyökkäyspinnan kartoituspalvelun (Hyöky) ja havainnoinnin kehittämisen (HAVARO-käyttöpilotti) pilottihankkeet. Hyöky- ja HAVARO-pilottihankkeista saadut tulokset auttoivat osallistujia toteuttamaan konkreettisia digiturvan teknisiä kehitys- ja korjaustoimenpiteitä. Pilottihankkeet ovat lisänneet julkisen hallinnon organisaatioiden tietoisuutta kyberturvallisuutensa tilasta, tarjonneet ohjeita tunnistettujen haavoittuvuuksien korjaamiseen sekä parantaneet julkisen hallinnon kyber- ja tietoturvallisuuden tilannekuvaa. Pilottihankkeista kerätyn palautteen perusteella niiden vaikutus julkisen hallinnon digitaaliseen turvallisuuteen on ollut myönteinen.

[16] Haukka-tehtävien arvioinnin tulokset.pdf
[17] TAISTO20 loppuraportti
[18] TAISTO21 loppuraportti
[19] TAISTO22 loppuraportti

Hyöky-pilottiin osallistui vuosina 2020–2021 yhteensä 49 organisaatiota, joista palautetta antoi 14 organisaatiota[20]. Skannaus koettiin hyödylliseksi ja se auttoi organisaatioita tunnistamaan haavoittuvuuksia, joita ne eivät olleet aiemmin tunnistaneet. Skannausten koettiin lisäävän vaikuttavuutta ja tuottamaan tarvittavaa lisätietoa palveluntuottajien toiminnan ohjaukseen ja sopimusvelvoitteiden tarkasteluun.

HAVARO-käyttöpilotointi jatkui vuoden 2023 loppuun asti. Pilotista ei ole vielä kerätty julkaistavissa olevaa palautetta, mutta yleisesti pilottiin osallistuneilta organisaatioilta saatu laadullinen palaute on ollut positiivista, ja organisaatiot ovat kokeneet pilottipalvelun hyödylliseksi. Mittaria ja sen tuloksia on esitelty yksityiskohtaisemmin liitteessä G.

3.5 DVV:n digiturvapalveluiden palautekyselyiden tuloksia

DVV:n vuonna 2021 toteuttamassa kyselyssä vastaajat arvioivat JUDO-hanketta. Kyselyyn saatiin 153 vastausta. JUDO-hankkeen kokonaistyytyväisyyttä kuvaava keskiarvo oli 3,81 (asteikolla 1–5).

Vuosia 2020–2021 koskeneessa kyselyssä vuonna 2021 sekä vuosia 2022–2023 koskeneessa kyselyssä vuonna 2023 kartoitettiin kaikkien digiturvapalveluiden tilannetta. Vuoden 2021 kyselyyn saatiin 130 vastausta. Kysymykseen ”Minkä arvosanan annat DVV:n digiturvapalveluiden onnistumiselle kokonaisuudessaan vuonna 2021?” saatiin kokonaiskeskiarvoksi 4,24. Viestinnän onnistumisen arvosanojen keskiarvo oli 4,16. Lähes kaikilla yksittäisillä osa-alueilla keskiarvo ylitti tavoitteeksi asetetun 4 (asteikolla 1–5).

Vuoden 2023 kyselyyn saatiin 152 vastausta. Siinä digiturvapalveluiden onnistumiselle annettu arvosana oli 4,22 ja viestinnän onnistumiselle annettu arvosana 4,08. Vastaajien antamat arviot DVV:n toiminnan vaikutuksesta kunkin vastaajan organisaation digiturvan kehittymiseen ovat alla. Arviointiasteikko: 3 = paljon, 2 = melko paljon, 1=jonkin verran, 0 = ei lainkaan. Suluissa on vuoden 2021 tulos.

- Digiturvan johtamista 1,68 (1,37)
- Riskienhallintaa 1,62 (1,26)
- Jatkuvuuden hallintaa ja varautumista 1,64 (1,24)
- Tietosuojan hallintaa 1,80 (1,52)
- Hallinnollista tietoturvallisuutta (ohjeet, koulutukset) 1,78 (1,54)
- Teknistä tietoturvallisuutta 1,44 (-)

Lisäksi vastaajat arvioivat vuonna 2023 kuinka paljon DVV:n tuottamat digiturvapalvelut ja -materiaalit olivat säästäneet organisaation työaikaa. Osa arvioi, että säästöä ei ole tullut, mutta vastauksissa oli myös kymmeniä toteamuksia ajan säästöstä, kuten jonkin verran, aika paljon, paljon, erittäin paljon, merkittävästi. Perusteluina säästyneelle työajalle olivat mm. hyvät materiaalit, osaamisen karttuminen sekä tuki omille näkemyksille. Vastaajilta saatiin myös joitakin arvioita rahallisista säästöistä, kuten jonkin verran, paljon, merkittävästi sekä määrällisesti 5000–10000€. Tuloksia on esitelty yksityiskohtaisemmin JUDO-hankkeen loppuraportissa[21].

[20] v1-HAUKKA_-_Skannauspalvelun_valmisteluselvityksen_(pilotti)_loppuraportti.pdf
[21] JUDO loppuraportti 2019-2023.docx

4 JOHTOPÄÄTÖKSET

Haukka-hankkeen tuotoksia arvioitiin Suomen digitaalisen kompassin Kokonaisturvalliset julkiset palvelut -tavoitteen avaintulosten edistämisen näkökulmasta sekä kansainvälisen NCSI-mittarin ja DVV:n kansallisten digiturvan kokonaiskuvapalvelun indikaattorien, VM:n JulkICT-osaston tavoitetilan 2025 mittareiden saavuttamisen sekä tuotoksista kerätyn palautteen perusteella. Täten muodostettiin laadullinen kokonaisarvio hankkeen vaikutuksista julkisen hallinnon digitaaliseen turvallisuuteen ja yleisemminkin digitaalisen turvallisuuden kehittymiseen Suomessa hankkeen aikana.

Monivuotisen hankkeen toimeenpanosuunnitelman toteutumista sellaisenaan voi pitää epärealistisena. Toimintaympäristön sisäisten ja ulkoisten muutosten takia tehtävien sisältöjä, laajuutta, kustannuksia ja vastuutahoja on tarkennettava jatkuvasti, jotta suunnitelma säilyy merkityksellisenä. Hankkeen vaikuttavuutta tuleekin arvioida suhteessa valmistumisajankohdan toimintaympäristöön, eikä niinkään alkuperäiseen toimeenpanosuunnitelmaan. Haukka-hankkeen toimeenpanosuunnitelmaa voi pitää kokonaisuutena tarkasteltuna onnistuneena, koska se on ollut riittävän väljä ja sitä on voitu joustavasti sovittaa muuttuviin tarpeisiin.

Vaikuttavuuden arvioinnissa käytettyjen mittarien tulokset eivät sellaisenaan kerro hankkeen vaikuttavuudesta. Lisäksi on huomattava, että käytettyjen palaute- ja arviointikyselyiden vastaajamäärät olivat usein melko alhaisia. Tarkemman kuvan saaminen digiturvan tasosta edellyttäisi kattavampaa vastaajien joukkoa. Tällöin kuvaavien tunnuslukujen tuottamiseksi ja analysoimiseksi olisi mahdollista tehdä vahvempaa tilastollista tarkastelua.

Kansainvälinen NCSI-mittari antaa perustiedot digiturvan tasosta Suomessa Haukka-hankkeen alkaessa vuonna 2020 ja kansallinen DVV:n digiturvan kokonaiskuva kertoo digiturvan kehittymisestä hankkeen aikana. Nämä tiedot eivät kuitenkaan riitä Haukka-hankkeen onnistumisen suoraviivaiseksi määrittämiseksi. Kun lisäksi hankkeen vaikutukset toteutuvat osittain vasta tulevaisuudessa, on vaikuttavuudesta vaikea raportoida täsmällisesti. Vaikuttavuuden arvioinnissa toteutettujen mittausten perusteella hankkeen vaikuttavuutta on pidetty hyvänä, mihin viittaa sekin, että Haukka-hankkeen kaltaista digiturvan pitkäkestoista ja laaja-alaista kehittämistä on pidetty tarpeellisena myös tulevaisuudessa.

Vaikka tämän raportin tarkoituksena onkin arvioida nimenomaan Haukka-hankkeen vaikuttavuutta, tulisi digitaalisen turvallisuuden kehittymistä julkisessa hallinnossa tarkastella kokonaisuutena riippumatta siitä, missä hankkeessa tehtäviä on toteutunut tai mikä organisaatio niitä toteuttaa. Haukka-hanketta voi siten pitää sekä vaikutuksia itse tuottavana hankkeena että katalyyttina, jonka aikana tehty suunnittelutyö on edistänyt digiturvan kehittymistä laajemminkin. Voidaankin perustellusti sanoa, että hanke on ollut oleellisesti mukana vaikuttamassa julkisen hallinnon digiturvan parantumiseen.

Haukka-hankkeen tuotosten vaikuttavuuden arvioinnin perusteella hankkeen voi katsoa onnistuneen varsin hyvin. Digitaalinen turvallisuus edellyttää kuitenkin jatkuvaa parantamista ja toimintamallien kehittämistä uusien ja muuttuvien uhkien varalle. Keskustelu julkisen hallinnon digiturvasta on Haukka-hankkeen kuluessa lisääntynyt, minkä voi katsoa lisänneen tietoisuutta digiturvasta, sen ke-

hittämisen merkityksestä ja kehitystarpeista. Tunnistamalla uusia kehityskohteita, käynnistämällä kehityskohteiden parantamiseksi tehokkaasti vaikuttavia toimenpiteitä, seuraamalla toimenpiteiden vaikuttavuutta ja mittaamalla tuloksia saadaan edistettyä koko yhteiskunnan digitaalista turvallisuutta.

Julkisen hallinnon digiturvaosaamisen kehittämistä pidetään tärkeänä. Digiturvaosaamista edistäviin tapahtumiin osallistumisella nähdään olevan positiivisia vaikutuksia niin henkilökohtaiseen kuin organisaatioidenkin digiturvan kehittymiseen. Vaikka Haukka-toimeenpanosuunnitelman toteuttaminen ei välttämättä ole vaikuttanut suoraan kaikkeen digiturvaosaamisen kehittämiseen ja kehittymiseen, ovat toimeenpanosuunnitelman osaamisen kehittämisen tavoitteet kuitenkin toteutuneet varsin kattavasti.

Digiturvan ajantasaisen tilannekuvan muodostaminen, digiturvaan liittyvien säännösten kehittäminen ja päätöksenteon tueksi tuotetut analysoidut tiedot ovat digiturvakokonaisuuden kehittämisen tärkeitä tukipilareita. Pilottihankkeet ja tuotteistuksessa olevat yhteiset digiturvan ratkaisut ja palvelut auttavat julkisen hallinnon organisaatioita parantamaan digiturvaansa ja tarkentavat julkisen hallinnon digiturvan tilannekuvaa. Yhdistämällä tasapainoisesti uusien palvelujen ja teknisten digipalvelujen tarjoamaa konkretiaa sekä hallinnollista digiturvaa tukevia tuotoksia lisätään monivuotisten digiturvahankkeiden vaikuttavuutta ja parannetaan digiturvan kokonaisuutta koko julkisessa hallinnossa.

Haukka-hankkeessa on julkiselle hallinnolle tuotettu välineitä digiturvan kehittämistyöhön, mutta tuotosten tunnettuudessa ja niiden hyödyntämisessä on vielä parantamisen varaa. Vaikuttaa siltä, että julkaistuja ohjeita, apuvälineitä ja digiturvapalveluita olisi mahdollista hyödyntää tehokkaamminkin digiturvan edistämisessä. Siksi valmistuneita tuotoksia tulisi markkinoida julkisessa hallinnossa aiempaa enemmän tuotosten tunnettuuden, käytettävyyden ja hyödynnettävyyden parantamiseksi sekä digiturvan tason kohottamiseksi. Jatkossakin tulisi harkita, mitkä ovat sellaisia kehitystoimenpiteitä, joilla parannetaan merkittävästi digiturvan tasoa, kenen vastuulla tällaisten toimenpiteiden toteuttamisen pitäisi olla ja miten eri toimijoiden digiturvatyötä koordinoidaan yhteisten tavoitteiden saavuttamiseksi.

Suomen Digitaalisen kompassin Kokonaisturvalliset julkiset palvelut avaintulosten edistymisen arvioinnin sekä Haukka-hankkeen tuotoksista kerätyn palautteen perusteella Haukka-hankkeen vaikutukset julkisen hallinnon digitaaliseen turvallisuuteen ja sen kehittymiseen ovat olleet myönteisiä. Voidaankin perustellusti sanoa, että hanke on ollut oleellisesti mukana vaikuttamassa julkisen hallinnon digitaalisen turvallisuuden parantumiseen. Haukka-hanketta on useissa eri sidosryhmien edustajien haastatteluissa ja keskusteluissa pidetty merkittävänä digitaalisen turvallisuuden kehittymisen edistäjänä ja vastaavan kaltaiselle, pitkäaikaiselle ja jatkuvalle digiturvan kehittämiselle nähdään tarvetta myös tulevaisuudessa.

Haukka-toimeenpanosuunnitelman tehtävät kattavat laajasti julkisen hallinnon toimintaa ja toimijoita. Siten myös Haukka-hankkeen tuotokset on suunniteltu ja toteutettu kattavasti julkisen hallinnon käyttöön. Tuotosten avulla on pystytty parantamaan digitaalista turvallisuutta ja laatimaan edelleen jatkokehityssuunnitelmia. Julkinen hallinto on kuitenkin heterogeeninen, joten tulokset voivat vaihdella organisaatioittain. Jatkossa tulee kiinnittää enemmän huomiota digitaalisen turvallisuuden kehittämistehtävien tarkempaan ryhmittelyyn ja fokusointiin sekä vaikuttavuuden arviointiin. Mittareita

asetettaessa on kuitenkin huomioitava, että julkisen hallinnon organisaatiot ovat heterogeenisiä, eikä kaikille ole mielekästä asettaa samanlaisia digiturvan kypsyystason tavoitteita.

NIS2-direktiivin kansallinen täytäntöönpano vuoden 2024 marraskuusta sisältää hankkeessakin selvitettyä, pilotoitua ja toteutettua kyberturvallisuustietojen vapaaehtoisia jakamisjärjestelyjä sekä tietoturvaloukkausten havainnointipalvelua ja haavoittuvuuskartoituksia. Haukka-hankkeen voidaan siten katsoa edistäneen myös NIS2-direktiivin kansallisen täytäntöönpanon edellytyksiä.

LIITE A: HAUKKA-HANKKEESSA JULKAISTUT TUOTOKSET

Asiakirja	Päiväys	Julkisuus
Digitaalisen turvallisuuden kustannus-vaikuttavuusarviointi julkisessa hallinnossa – Selvitystyön raportti	1.6.2020	julkinen www.vm.fi
Digitaalisen turvallisuuden strateginen riskiarviomalli – Haastatteluiden yhteenveto	31.8.2020	TL IV
Kuntien digitaalisen turvallisuuden riskikyselyn tulokset	8.2.2021	julkinen www.vm.fi
Selvitys digitaalisen turvallisuuden arvioinnin kehitystarpeista	10.5.2021	julkinen www.vm.fi
Esityö julkisen hallinnon digitaalisen turvallisuuden arviointikriteeristön luomiseksi	11.5.2021	julkinen www.vm.fi
Digitaalisen turvallisuuden kunta-valtio yhteistoimintamallin esiselvitys	11.6.2021	julkinen www.vm.fi
Julkishallinnon digitaalisen turvallisuuden arkkitehtuuri – Haukka-hanke	11.6.2021	julkinen www.vm.fi
Digitaalisen turvallisuuden strategisen johtoryhmän näkemyksiä digitaalisen turvallisuuden edistämisestä	16.8.2021	salassa pidettävä
Yhteenveto Digiturvakompassi-podcasteista	24.8.2021	julkinen www.vm.fi
Selvitys digitaalisen turvallisuuden kansainvälisestä arviointilainsäädännöstä	3.9.2021	julkinen www.vm.fi
JUDO-hankkeen palvelut kunnille	21.1.2022	julkinen www.vm.fi
Selvitys organisaation tietoturvatehtävistä ja niiden organisoimisesta	9.3.2022	julkinen www.vm.fi
Digitaalisen turvallisuuden yhteistoiminta- ja hallintamallien kansainvälinen vertailu – Muistio	25.4.2022	julkinen www.vm.fi
Haukka Ohjeiden ja suositusten vaikuttavuuden arvioinnin pilotointi	21.4.2022	julkinen www.vm.fi
Kunnille suunnatut digitaalisen turvallisuuden palvelut	26.8.2022	julkinen www.vm.fi
Esiselvitys julkisen hallinnon digitaalisen toimintaympäristön tietovarannosta	15.11.2022	julkinen www.vm.fi
Julkisen hallinnon digitaalisen turvallisuuden yhteistoiminta- ja hallintamalliselvitys	1.12.2022	julkinen VM 2020:76
Näkökulmia julkisten digipalveluiden ja tiedonhallinnan informaatioturvallisuuteen	27.10.2022	TL IV

Digiturvakompassi-podcast	13.2.2020 – 20.2.2023	julkinen www.vm.fi
NIS2-selvitysraportti	5.4.2023	ei julkaistu
Koneoppiminen digitaalisen turvallisuuden teknisessä valvonnassa	8.6.2023	ei julkaistu
Opas digitaalisen turvallisuuden harjoitusohjelman ja -toiminnan suunnitteluun	6.3.2020	julkinen ww.dvv.fi
Kuinka johto varmistaa organisaation toiminnan jatkuvuuden ja luottamuksen säilymisen 2020-luvulla? – Kyselyn yhteenveto	11.5.2020	julkinen www.dvv.fi
Julkishallinnon digitaalisen turvallisuuden kansallisen harjoitustoiminnan nykytilan kuvaus	28.9.2020	julkinen www.dvv.fi
Digiturvabarometri – Keskeiset tulokset ja havainnot	22.10.2020	julkinen www.dvv.fi
Digiturvan hyvät käytännöt johdolle ja ICT:n sekä digiturvan asiantuntijoille – tarkistuslista	26.10.2020	julkinen www.dvv.fi
Raportti - versio 1.10. – Koronaviruspandemian vaikutukset digitaaliseen turvallisuuteen	29.11.2020	julkinen www.dvv.fi
Julkisen hallinnon digitaalisen turvallisuuden kansallisen harjoitustoiminnan tavoitteet ja toimenpiteet 2021 – 2022	5.3.2021	julkinen www.dvv.fi
Julkisen hallinnon digitaalisen turvallisuuden nykytilan selvitys	25.3.2021	julkinen www.dvv.fi
Kuntien digitaalisen turvallisuuden selvitys	25.3.2021	julkinen www.dvv.fi
TTTT-malli digiturvalliseen työskentelyyn – VAHTI-hyvät käytännöt tukimateriaali	19.5.2021	julkinen www.dvv.fi
Digiturvabarometri – Keskeiset tulokset ja havainnot – kesäkuu 2021	21.6.2021	julkinen www.dvv.fi
Digiturvallisuuden riskikyselyn tuloksia, syksy 2021	syksy 2021	julkinen www.dvv.fi
Organisaation Digiturvakysely – Raportti ja kehittämiskohteet	18.8.2021	julkinen www.dvv.fi
Digiturvan usein kysytyt kysymykset – VAHTI-hyvät käytännöt tukimateriaali	31.8.2021	julkinen www.dvv.fi
Sisäänrakennetun ja oletusarvioisen tietosuojan periaatteiden läpikäynti hankinnoissa - VAHTI-hyvät käytännöt tukimateriaali	5.11.2021	julkinen www.dvv.fi
Hankinnan muistilista tietosuoja-asioissa – VAHTI-hyvät käytännöt tukimateriaali	5.11.2021	julkinen www.dvv.fi
Tietosuoja-asetuksen itsearviointi – Digiturvan hyvät käytännöt tukimateriaali	5.11.2021	julkinen www.dvv.fi

Tietosuoja - vaikutustenarviointi – alkukartoitus – VAHTI-hyvät käytännöt tukimateriaali	5.11.2021	julkinen www.dvv.fi
Tietosuoja – vaikutustenarviointi – VAHTI-hyvät käytännöt tukimateriaali	5.11.2021	julkinen www.dvv.fi
Tietosuojatyön vuosikello – VAHTI Digiturvan hyvät käytännöt tukimateriaali	5.11.2021	julkinen www.dvv.fi
Tietotilinpäätös – malli – VAHTI-hyvät käytännöt tukimateriaali	5.11.2021	julkinen www.dvv.fi
Digiturvallisuuden käytännön vinkit – VAHTI-hyvät käytännöt tukimateriaali	1.12.2021	julkinen www.dvv.fi
Digiturvallisuuden hallinta – VAHTI hyvät käytännöt tukimateriaali	1.12.2021	julkinen www.dvv.fi
JUDO-hanke, Väliraportti 2019-2021	25.1.2022	julkinen www.dvv.fi
Kriittisten kohteiden luokittelu – VAHTI-hyvät käytännöt tukimateriaali	11.3.2022	julkinen www.dvvi
Kriittisten kohteiden luokittelu, työkalun käyttöohje – VAHTI-hyvät käytännöt tukimateriaali	11.3.2022	julkinen www.dvv.fi
Kriittisten kohteiden luokittelutyökalu	14.3.2022	julkinen www.dvv.fi
Jatkuvuudenhallintamalli	18.3.2022	julkinen www.dvv.fi
VAHTI-hyvät käytännöt: Varautumiskoulutus henkilöstölle	9.5.2022	julkinen www.dvv.fi
Digiturvan kokonaiskuvapalvelun käyttövaltuuksien määrittely	1.8.2022	julkinen www.dvv.fi
Digiturvan kokonaiskuvapalvelu – ohje työkalun käyttäjälle	1.8.2022	julkinen www.dvv.fi
Digiturvan kokonaiskuvapalvelu − infotilaisuus 16.8.2022	16.8.2022	julkinen www.dvv.fi
Digiturvabarometrin tulokset herättävät huolen suomalaisten digiturvaosaamisen tasosta – “Nyt tarvitaan koulutusta”	10.10.2022	julkinen www.dvv.fi
Tietosuoja pilvipalveluissa – VAHTI hyvät käytännöt tukimateriaali	9.11.2022	julkinen www.dvv.fi
VAHTI-riskienhallintasanasto digitaaliseen toimintaympäristöön – esittely ja johdatusta riskiviestintään – VAHTI Hyvät Käytännöt -tukimateriaali	15.11.2022	julkinen www.dvv.fi
Digitaalisen turvallisuuden arkkitehtuuri (Confluence-sivusto)	12.12.2022	julkinen www.dvv.fi
Digitaalisen turvallisuuden havainnoinnin kehittäminen – VAHTI hyvät käytännöt tukimateriaali	12.12.2022	julkinen www.dvv.fi

Julkisen hallinnon digitaalisen turvallisuuden strateginen riskienhallinta – Riskienhallintamallin rakenne	15.12.2022	julkinen www.dvv.fi
Keinoja ja suosituksia turvata kriittisiä tietovarantoja, tietopalveluita ja tietojärjestelmiä – Tukimateriaali; toteutettu osana JUDO-hanketta ja kyberturvallisuusstrategian kehittämisohjelmaa	20.12.2022	julkinen www.dvv.fi
Digitaalisen turvallisuuden havainnoinnin kehittäminen – VAHTI hyvät käytännöt -tukimateriaali	16.1.2023	julkinen www.dvv.fi
Julkisen hallinnon digitaalisen turvallisuuden strateginen riskienhallinta – Yleinen riskitilannekatsaus, syksy 2022	23.1.2023	julkinen www.dvv.fi
Julkri-työkalu – ohje käyttäjälle	24.1.2023	julkinen www.dvv.fi
Julkisen hallinnon arviointikriteeristö (Julkri) -työkalun käyttövaltuuksien määrittely	24.1.2023	julkinen www.dvv.fi
Digiturmajahti –VAHTI hyvät käytännöt -tukimateriaali	6.2.2023	julkinen www.dvv.fi
Julkisen hallinnon digitaalisen turvallisuuden strateginen riskienhallinta – Yleinen riskitilannekatsaus, kevät 2023	29.5.2023	julkinen www.dvv.fi
Tietosuojaliite – Henkilötietojen käsittelytoimien kuvaus	29.5.2023	julkinen www.dvv.fi
Organisaation Digiturvakysely – Raportti ja keskeiset havainnot	30.5.2023	julkinen www.dvv.fi
Turvallisen kehittämisen opas – Tekoälyjärjestelmien kehittäminen	9.6.2023	julkinen www.dvv.fi
Turvallisen sovelluskehityksen käsikirja (Confluence-sivusto)	12.6.2023	julkinen www.dvv.fi
Tekoälyn hyödyntäminen – huoneentaulut ja tarkistuslistat – VAHTI hyvät käytännöt -tukimateriaali	12.9.2023	julkinen www.dvv.fi
Vinkkejä tekoälypalveluiden hyödyntämiseen –VAHTI hyvät käytännöt -tukimateriaali	12.9.2023	julkinen www.dvv.fi
VAHTI-webinaari: Tekoälyn ohjeistaminen ja VAHTI hyvät käytännöt tukimateriaalin julkistaminen – VAHTI Tekoälyn huoneentaulut	12.9.2023	julkinen www.dvv.fi
Tietoturvavalvomon (SOC) käyttöönoton tarkastuslista – VAHTI hyvät käytännöt 10/2023	2.10.2023 kommenttiversio	julkinen www.dvv.fi
Kuntien tietoturvavalvomot -selvitys	27.11.2023	julkinen www.dvv.fi

Julkisen hallinnon digitaalisen toimintaympäristön tietovaranto -selvitys	lopullinen luonnosversio 10/2023	DVV:n sisäistä valmisteluaineistoa
Turvalliset teknologiat -selvitys	30.10.2023	julkinen www.dvv.fi
Kustannus-vaikuttavuus-malli digitaalisen turvallisuuden riskienhallintaan	julkaisu vuoden 2023 aikana	julkinen
Selvitys harjoitustoiminnan vaikuttavuudesta	luonnosversio 12/2023	DVV:n sisäistä valmisteluaineistoa

LIITE B: DVV:N DIGITURVAN KOKONAISKUVAPALVELUSTA POIMITUT VERTAILUTIEDOT

Kokonaiskuvapalvelu on DVV:n hallinnoima, julkisen hallinnon organisaatioille tarkoitettu työkalu digitaalisen turvallisuuden arviointiin, seurantaan ja raportointiin [22]. Kokonaiskuvapalvelu on otettu käyttöön vuonna 2022. Sen sisältämiä tietoja on aiemmin kerätty DVV:n toteuttamilla Digiturvakyselyillä. Kokonaiskuvapalvelusta saatavien tunnuslukujen ja vertailutietojen perusteella arvioidaan digitaalisen turvallisuuden kehittymistä julkisella sektorilla Haukka-hankkeen aikana. Kokonaiskuvapalvelussa on tietoja julkisen hallinnon digitaalisen turvallisuuden tilasta eri osa-alueilla ja eri sektoreilla, joita ovat mm. valtio, kunnat ja sairaanhoitopiirit sekä vuoden 2023 alusta toimintansa aloittaneet hyvinvointialueet.

Kokonaiskuvapalveluun vastauksia antaneiden toimijoiden joukko on vaihdellut tarkastelujakson eli vuosien 2021–2023 aikana. Kokonaiskuvapalvelun käyttäjien lukumäärää pyritään jatkuvasti laajentamaan houkuttelemalla mukaan yhä uusia julkisen hallinnon organisaatioita. Vastaajien määrän lisääntyessä tuloksiin saattaa tulla yhä enemmän vaihtelua, mutta toisaalta parempi kattavuus tuottaisi tarkemman kuvan digiturvan kehittymisestä ja kehitystarpeista. Vastaajien lukumäärä ja kattavuus huomioitiin, kun arvioitiin, miten hyvin vastaukset kuvaavat julkisen hallinnon digiturvan kehittymistä Haukka-hankkeen aikana ja siten osaltaan hankkeen vaikuttavuutta.

Kokonaiskuvapalvelun digiturvakyselyjen perusteella tehty vaikuttavuuden arviointi perustuu DVV:n laatimiin yhteenvetoihin vuosilta 2021 ja 2022 sekä 30.5.2023 julkaistuun organisaation digiturvakyselyn raporttiin[23]. Kyselyssä vastaajat olivat arvioineet digiturvan osa-alueisiin (riskienhallinta, toiminnan jatkuvuus ja varautuminen, tietoturva, tietosuoja sekä kyberturvallisuus) ja digiturvan johtamiseen liittyviä väittämiä kolmiportaisella asteikolla (0=ei toteudu, 0,5=toteutuu osittain, 1=toteutuu). Lisäksi kyselyissä oli selvitetty digiturvan havainnointia. Pyyntö vastata digiturvan kokonaiskuvapalvelun kyselyyn oli lähetetty kaikkiin julkisen hallinnon kirjaamoihin (lähes seitsemänsataa vastaanottajaa), mutta vastaajien osuudet olivat selvästi alle 20 %.

Kokonaiskuvapalvelun digiturvakyselyn perusteella vaikuttaa siltä, ettei julkisen hallinnon digitaalisen turvallisuuden kokonaisuus ole muuttunut paljonkaan vuotta 2022 koskevaan kyselyyn mennessä, ja julkisen hallinnon organisaatioiden hallinnollinen turvallisuuden kokonaisuus on pysynyt lähes muuttumattomana. Vastaajaryhmien kesken tuloksissa on pientä vaihtelua. Sote-toimijoiden tulokset ovat muita vastaajaryhmiä alempia, mutta erot ovat melko vähäisiä ja niitä saattaa osittain selittää sote-toimijoiden vastaajien melko pieni lukumäärä. Digiturvan osa-alueittain tarkasteltuna arviot tietosuojan ja tietoturvan tasosta olivat muita osa-alueita paremmat, kun taas kyberturvallisuuden arviot olivat osa-alueista alhaisimmat. Erityisesti resursointiin ja osaamiseen sekä kriittisten palvelujen riskiarviointia koskeviin kysymyksiin annettiin matalat arviot.

Jokaisen arvioidun osion sisältämien yksittäisten arviointikysymysten tuloksissa oli huomattavaa vaihtelua. Parhaimmillaan yksittäisten kysymysten keskiarvot olivat selvästi yli 0,7 (asteikolla 0–1)

[22] Suomi.fi/Digiturvan kokonaiskuvapalvelu, https://www.suomi.fi/palvelut/digiturvan-kokonaiskuvapalvelu-digi-ja-vaestotietovirasto/1b38df61-ca48-41b4-a238-da5ab1baaf27
[23] Organisaation Digiturvakysely - Raportti ja keskeiset havainnot - 30.5.2023

ja yksittäisissä tapauksissa yli 0,9. Jokaisessa osiossa oli kuitenkin kysymyksiä, joissa keskiarvot jäivät useimmilla vastaajaryhmillä alle 0,5, mikä tarkoittaa, että huomattava osa vastaajista koki, että väite toteutui organisaatiossa enintään osittain. Tällaisia kohtia olivat esimerkiksi:

- digiturvaosaajien riittävyys ja digiturvan mittaaminen (johtaminen)
- jäännösriskien käsittely (riskienhallinta)
- jatkuvuusriskien arviointi ja jatkuvuussuunnitelmat (toiminnan jatkuvuus ja varautuminen)
- henkilöiden taustatarkastuksen menettelyt, varmuuskopiointi ja auditoinnit (tietoturvallisuus)
- rakenteettoman tiedon hallinta (tietosuoja)
- resursointi ja osaaminen, riskien arviointi sekä informaatiovaikuttaminen (kyberturvallisuus).

Organisaatioiden digiturvankyselyjen perusteella on vuonna 2021 kehityskohteiksi nostettu 19 toimenpidettä, joita on edistetty. Seurannan perusteella vain etäkäyttöön liittyvässä kehityskohteessa oli saavutettu selvästi edistymistä. Muissa kehityskohteissa oli saavutettu pieniä parannuksia, mutta ei merkittävää kehittymistä. Vuodelle 2023 oli nimetty kahdeksan uutta kehittämiskohdetta.

Kokonaiskuvapalvelun digiturvakyselyn yhteenvetotietojen perusteella digitaalinen turvallisuus julkisessa hallinnossa on keskimäärin varsin hyvä, vaikka vastaajaryhmien, arvioitujen osioiden sekä osioiden sisältämien kysymysten välillä on vaihtelua. Tarkemman kuvan saaminen digitaalisen turvallisuuden tasosta edellyttäisi kattavampaa vastaajien joukkoa. Lisäksi luotettavien tunnuslukujen tuottaminen ja analysointi edellyttäisi vahvempaa tilastollista tarkastelua ja riittävän pitkää tarkastelun aikajaksoa. Haukka-hankkeen vaikuttavuuden kannalta on positiivista, että kehityskohteita on asetettu ja niiden edistymistä on seurattu. Digiturvan osa-alueiden parantuminen on kuitenkin ollut useimmissa tapauksissa vähäistä. Tulosten perusteella voidaan arvioida, että digiturvan parantaminen julkisessa hallinnossa edellyttää kehitystoimenpiteiden tarkoituksenmukaista valintaa ja kohdentamista, riittävää resursointia sekä tarkkaa seurantaa.

LIITE C: DIGITURVAN EOPPIVA-KOULUTUKSISTA KERÄTTY PALAUTE

Valtioneuvoston periaatepäätöksen (VM 2020:23) yhdeksi kehittämisen periaatteeksi on nostettu kansalaisten ja henkilöstön digitaalisen turvallisuuden osaamisen kehittäminen. Yhdeksi osaamisen kehittämisen ja sen vaikuttavuuden mittariksi valittiin eOppiva-koulutusalustan digitaalista turvallisuutta käsittelevien verkkokurssien suorituksista saadut tiedot.

HAUS koulutuskeskus Oy (HAUS) on VM:n hallinnonalaan kuuluva yhtiö, joka tuottaa julkiselle hallinnolle koulutus- ja kehityspalveluja. Palvelujen osana on eOppiva-koulutusalusta, joka sisältää verkkokoulutuksia digitaalisen turvallisuuden osa-alueille. Kurssit sisältävät sekä julkiselle hallinnolle suunnattuja että kaikille avoimia koulutuksia. Tässä vaikuttavuuden arvioinnissa mukana olleet kurssit suoritusvuosittain ovat liitteessä C.1. Erilaisten kurssien lukumäärä on kasvanut vuosittain. Vuonna 2022 toteutetuista kymmenestä digiturvakurssista kolme käsitteli tietosuojaa ja neljä digiturvaa. Kyberturvallisuutta, riskienhallintaa ja varautumista käsitteleviä kursseja oli yksi kutakin.

HAUS kokoaa suoritetuista kursseista lukumäärätietoja[24]. Kurssin suorittajat saattoivat halutessaan vastata palautelomakkeen kyselyyn, jossa vastaaja arvioi väitteitä kurssin toteutuksesta ja sen vaikutuksista. Lisäksi vastaaja voi antaa kurssiin liittyvää avointa palautetta. Eri koulutuksia koskevat palautteet ovat melko yhdenmukaisia ja poikkeavat toisistaan vain vähän. Palautteiden yhteenveto on esitetty liitteessä C.2.

Digiturvan verkkokurssien suoritusten määrä on kasvanut vuosien aikana, mikä kertoo siitä, että digiturva-asioiden ja osaamisen kehittämisen merkitys tunnistetaan laajasti. Julkiselle hallinnolle tuotetaan useampia kursseja kuin avoimelle puolelle ja lisäksi osa kursseista on suunnattu tietyille henkilöryhmille, kuten Digiturvallisuus kuntien luottamushenkilöille ja Digiturvallisuus hyvinvointialueiden luottamushenkilöille.

Digiturvan osa-alueittain tarkasteltuna tietosuoja erottuu muista kursseista suoritusmäärien perusteella. Vuoden 2022 suorituksia oli lähes kaksi kertaa niin paljon kuin kaikkia muita yhteensä ja näistä suorituksista noin kolme neljännestä oli avoimen puolen suorituksia. Toiseksi eniten suorituksia on kertynyt yleistä digitaalista turvallisuutta ja tietoturvaa käsittelevistä koulutuksista, joiden määrä oli vuonna 2022 lähes kaksinkertainen kahteen edelliseen vuoteen verrattuna.

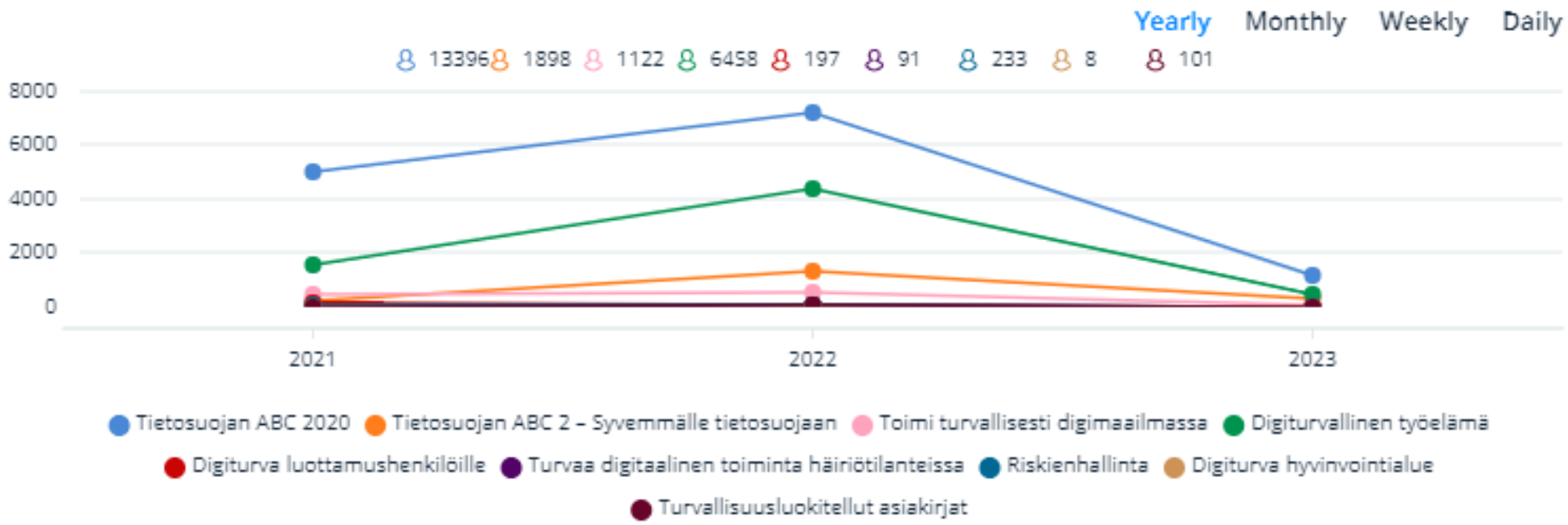
Palautteesta nähdään, että toteutuksen ja sisällön arvosanat ovat korkeita ja koulutukset ovat siten hyvin onnistuneita ja niiden sisältö on ollut oppijoille hyödyllistä. Verkkokursseista kerättyä palautetta ei ollut mahdollista ryhmitellä.

Suoritusmäärien kasvu ja vahvasti positiivinen palaute osoittavat, että digiturvan tietoisuuden ja osaamisen kasvattaminen koetaan tärkeäksi. Sekä koulutusten toteutuksesta että niiden vaikuttavuudesta on annettu korkeat arvosanat kertovat siitä, että digiturvan verkkokoulutukset vaikuttavat merkittävästi ja pysyvästi digiturvan osaamisen ja tietoisuuden kehittymiseen.

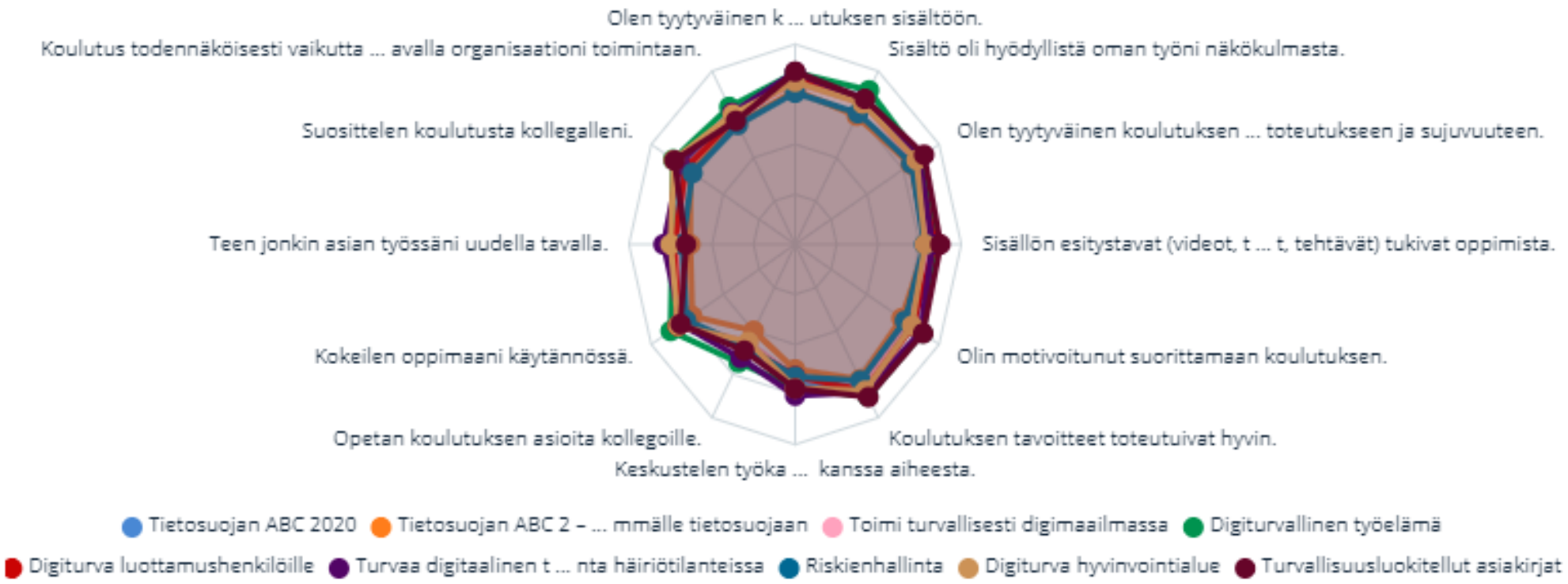
eOppiva-koulutukset 2020–2023

[24] eOppiva suoritukset 20230423.pdf

Suoritus-vuosi	Kurssin nimi	Digiturvan osa-alue
2020	Digiturvallinen työelämä	Tietoturva
	Riskienhallinta digimaailmassa	Riskienhallinta
	Tietosuojan ABC	Tietosuoja
	Tietosuojan ABC julkishallinnon henkilöstölle	Tietosuoja
	Toimi turvallisesti digimaailmassa	Tietoturva
	Turvaa digitaalinen toiminta häiriötilanteissa	Varautuminen
2021	Digiturvallinen työelämä	Tietoturva
	Digiturvallisuus kuntien luottamushenkilöille	Tietoturva
	Riskienhallinta digimaailmassa	Riskienhallinta
	Tietosuojan ABC	Tietosuoja
	Tietosuojan ABC 2 - Syvemmälle tietosuojaan	Tietosuoja
	Tietosuojan ABC julkishallinnon henkilöstölle	Tietosuoja
	Toimi turvallisesti digimaailmassa	Tietoturva
	Turvaa digitaalinen toiminta häiriötilanteissa	Varautuminen
2022	Digitaalinen turvallisuus järjestykseen arkkitehtuurin avulla	Kyberturvallisuus
	Digiturvallinen työelämä	Tietoturva
	Digiturvallisuus hyvinvointialueiden luottamushenkilöille	Tietoturva
	Digiturvallisuus kuntien luottamushenkilöille	Tietoturva
	Riskienhallinta digimaailmassa	Riskienhallinta
	Tietosuojan ABC	Tietosuoja
	Tietosuojan ABC 2 - Syvemmälle tietosuojaan	Tietosuoja
	Tietosuojan ABC julkishallinnon henkilöstölle	Tietosuoja
	Toimi turvallisesti digimaailmassa	Tietoturva
	Turvaa digitaalinen toiminta häiriötilanteissa	Varautuminen
2023	Digitaalinen turvallisuus järjestykseen arkkitehtuurin avulla	Kyberturvallisuus
	Digiturvallinen elämä -testi	Tietoturva, kyberturvallisuus
	Digiturvallinen työelämä	Tietoturva
	Digiturvallisuus hyvinvointialueiden luottamushenkilöille	Tietoturva
	Digiturvallisuus kuntien luottamushenkilöille	Tietoturva
	Riskienhallinta digimaailmassa	Riskienhallinta
	Tietosuojan ABC 2 - Syvemmälle tietosuojaan	Tietosuoja
	Tietosuojan ABC julkishallinnon henkilöstölle	Tietosuoja
	Toimi turvallisesti digimaailmassa	Tietoturva
	Turvaa digitaalinen toiminta häiriötilanteissa	Varautuminen
	Turvallisuusluokitellut asiakirjat	Tietoturva


Yearly
Monthly
Weekly
Daily
13396
1898
1122
6458
197
91
233
8
101
8000
6000
4000
2000
0
2021
2022
2023
Tietosuojan ABC 2020
Tietosuojan ABC 2 – Syvemmälle tietosuojaan
Toimi turvallisesti digimaailmassa
Digiturvallinen työelämä
Digiturva luottamushenkilöille
Turvaa digitaalinen toiminta häiriötilanteissa
Riskienhallinta
Digiturva hyvinvointialue
Turvallisuusluokitellut asiakirjat

eOppiva-koulutuspalautteet



LIITE D: DVV:N DIGITURVATILAISUUKSISTA KERÄTTY PALAUTE

DVV on järjestänyt digiturvaviikon vuosittain vuodesta 2020 alkaen. Viikon tarkoituksena on lisätä tietoisuutta digitaalisesta turvallisuudesta ja aktivoida organisaatioita digiturva-asioissa. Jokaisella digiturvaviikon päivällä on ollut oma teemansa. Vuosina 2020 ja 2021 digiturvaviikolle ilmoittautui 300 ja vuonna 2022 217 pientä ja suurta organisaatiota sekä julkiselta että yksityiseltä sektorilta. Mukana oli myös organisaatioita jotka eivät olleet ilmoittautuneet. Ilmoittautuneiden organisaatioiden laajuutta voidaan arvioida niiden yhteenlasketun henkilöstömäärän mukaan, joka vuonna 2020 oli yhteensä 248 000, vuonna 2021 253 000 ja vuonna 2022 230 000 henkilöä. Organisaatioiden ennakkoilmoittautumista ei toteutettu vuoden 2023 digiturvaviikolle. [25, 26]

Vuonna 2020 digiturvaviikon livelähetysten katsojamäärä oli noin 11 000, vuonna 2021 noin 13 000, vuonna 2022 noin 9000 ja vuonna 2023 noin 7400 henkilöä. Vuoden 2023 alhaista katsojamäärää saattaa selittää viikon aikana järjestetty kaksipäiväinen Nordic Business Forum -tapahtuma, johon osa digiturvaviikon kohderyhmästä on todennäköisesti osallistunut. Digiturvaviikon tallenteita katsottiin vuonna 2022 digiturvaviikon aikana ja neljänä päivänä sen jälkeen yhteensä noin 10 000 kertaa ja vuonna 2023 digiturvaviikon aikana ja 11 päivänä sen jälkeen noin 8500 kertaa. Digiturvaviikon kohderyhmään tavoiteltiin vuosina 2022 ja 2023 aiemmista vuosista poiketen laajemmin osallistujia myös kansalaisista ja eri alojen työntekijöistä laajentamalla tilaisuuksissa käsiteltäviä aiheita. Myös ennakkomainontaa ja mediajulkaisuja kohdennettiin useille eri kohderyhmille käyttäen monipuolisesti sosiaalisen median kanavia: X (aiemmin Twitter), LinkedIn ja Instagram. Katsojamäärien laskun perusteella digiturvaviikon kohderyhmän laajentaminen ei ole onnistunut tavoitellusti.

Kerätyn palautteen perusteella yli 70 % piti vuoden 2022 Digiturvaviikkoa joko hyvänä tai erittäin hyvänä ja 60 % piti sitä hyödyllisenä tai erittäin hyödyllisenä. Digiturvaviikkojen ennakkomainonnan, verkkolähetysten, mediajulkaisujen ja julkisten esiintymisten avulla tapahtumat ovat saaneet merkittävästi huomiota niin toimituksellisessa kuin sosiaalisessakin mediassa. Suurin osa digiturvaviikkojen sosiaalisen median keskusteluista on käyty Twitterissä, jossa näyttökerrat kasvoivat vuoden 2021 noin puolesta miljoonasta vuoden 2022 yli miljoonaan näyttökertaan. X:ssä vuonna 2023 näyttökertoja oli ainoastaan 166 000. Digiturvaviikon verkkosivustolle siirtyi Twitter-keskusteluista vuonna 2021 455 henkilöä ja vuonna 2022 70 000 henkilöä. Vuonna 2023 X-keskusteluista siirtyi digiturvaviikon verkkosivuille vain 201 henkilöä.

DVV on järjestänyt vuosina 2019–2023 säännöllisiä kuukausittaisia verkkolähetyksiä, jotka suunnattiin kohderyhmittäin organisaatioiden henkilöstölle, johdolle ja asiantuntijoille. Verkkolähetysten materiaalit on tekstitetty ja tallenteet ovat saatavilla DVV:n verkkosivuilta[27]. DVV:n verkkolähetyksistä keräämän palautteen perusteella verkkolähetysten katsojamäärä vuonna 2023 on ollut tyypillisesti noin 800 katsojaa/verkkolähetys, yhteensä lokakuun 2023 loppuun mennessä noin 9000 katsojaa. Verkkolähetysten sisällöstä ja teknisestä toteutuksesta annettujen arvioiden keskiarvot ovat olleet varsin korkeat. Sisällöstä annetun palautteen keskiarvo on vuonna 2023 ollut 4,58 ja teknisestä toteu-

[25] VALTI_0212_2022_Digiturvaviikko_raportti_2022.pdf
[26] Digiturvaviikko loppuraportti 2023.pdf
[27] DVV:n digiturvatilaisuudet, https://www.mediaserver.fi/live/digiturva

tuksesta 4,62 viisiportaisella asteikolla. Palautteita tilaisuuksista on kuitenkin annettu vähän. Tyypillisesti tilaisuuksista on saatu kymmenkunta palautetta. Sanallisessa palautteessa positiivisina seikkoina oli nostettu esiin esitysten laaja-alaisuus, ajankohtaisuus ja kohderyhmien huomiointi. Kehityskohteina oli toivottu uusia ja monimuotoisempia esiintyjiä, enemmän konkretiaa, pienten organisaatioiden näkökulmaa, teknisestä tietoturvasta puhumista sekä yksityisen ja julkisen sektorin vuorovaikutusta.

Digiturvakatsausten lisäksi DVV toteutti vuonna 2023 kuusi webinaaria, jotka oli suunnattu ainoastaan VAHTI-verkostolle. Webinaareissa käsiteltiin mm. tietoturvaa ja jatkuvuutta, työasema- ja palvelinympäristöjen suojaamista sekä Microsoftin pilvipalveluja. Webinaareilla oli yhteensä noin 220 katsojaa.

DVV:n digiturvatilaisuuksista koottu palaute osoittaa, että digiturvatietoisuudelle on runsaasti kysyntää niin julkisessa hallinnossa, yksityisellä sektorilla kuin kansalaistenkin joukossa. Digiturvatilaisuuksien katselijamäärät ovat säilyneet varsin korkeina ja voidaankin arvioida, että tilaisuuksilla on ollut tavoitellun kaltainen positiivinen vaikutus eri kohderyhmien digiturvatietoisuuden ja -osaamisen lisääntymiseen.[28]

[28] Digiturvaviikko 2023_kampanjan analyysi.pdf

LIITE E: KUNTIEN DIGITURVAVALMENNUKSESTA KERÄTTY PALAUTE

DVV järjesti kymmenelle kunnalle digiturvavalmennusta vuosina 2021 ja 2022 ja näistä puolet vastasi valmennuksen palautekyselyyn. Kyselyssä valmennukseen osallistujat vastasivat kuuden osa-alueen (tietosuojan, tietoturvallisuuden, riskienhallinnan, johtamisen, toiminnan jatkuvuuden sekä kyberturvallisuuden) kehittymistä väittämien perusteella. Väittämien vastaukset olivat asteikolla 0=ei toteudu, 0,5=toteutuu osittain, 1=toteutuu täysin.

DVV:n tuottaman erillisen yhteenvedon perusteella kaikki valmennukseen kuuluneet osa-alueet kehittyivät kunnissa positiivisesti. Kaikkien osa-alueiden yhteenlaskettu keskiarvo nousi noin 22 %. On kuitenkin huomioitava, että vastauksia oli melko vähän. Lisäksi toimijoiden digiturvan eri osa-alueiden lähtötasot olivat erilaisia. Vuonna 2021 toimijoiden arvioiden keskiarvo tietosuojan toteutumisesta oli korkea 0,75. Sen sijaan toimijoiden arvioiden keskiarvo toiminnan jatkuvuuden toteutumisesta oli matala 0,39.

Niissä digiturvan osa-alueissa, joissa lähtötaso oli alempi, oli prosentuaalinen arvion muutos vuoteen 2022 verrattuna suurempi. Toiminnan jatkuvuuden, johtamisen ja riskienhallinnan osa-alueissa muutokset olivat +64 %, +38 % ja +32 % vastaavasti. Kyberturvallisuuden osa-alueen toteutuminen oli kuitenkin kasvanut vain 0,43:sta 0,48:aan (noin 12 %). Toisaalta, kun arvion lähtötaso oli korkea, on luonnollista, ettei kasvu ollut yhtä suurta. Korkea lähtötaso kertoo tilanteen olevan jo varsin hyvä, eikä vähenevän rajahyödyn periaatteen mukaisesti lisäpanostuksilla saavuteta välttämättä enää suuria parannuksia. Jokainen osa-alue oli kuitenkin kehittynyt positiivisesti.

Valmennuksen osa-alueita mittaavia väittämiä tarkasteltaessa nähdään, että useimpien väittämien toteutuminen oli parantunut. Jokaisessa osa-alueessa oli kuitenkin yksittäisiä väittämiä, joissa arviot toteutumisesta olivat laskeneet. Johtamisessa katsottiin, että organisaatioissa on vähemmän osaavaa henkilöstöä digiturvan osa-alueilla (-25 %). Riskienhallinnassa jäännösriskien käsittelyn taso oli laskenut (-25 %). Toiminnan jatkuvuudessa huomattiin, että palvelutasovaatimuksia ei huomioida niin hyvin sopimuksissa, eikä jatkuvuusriskejä arvioida niin säännöllisesti (kummassakin -17 %). Tietoturvassa tietoturvavaatimusten vieminen sopimuksiin oli heikentynyt (-29 %) ja käyttövaltuuksien ajantasaisuuden seuranta heikentynyt (-40 %). Tietosuojassa yhteisrekisterinpitäjyyden vastuut ovat epäselvemmät (-33 %), henkilötietojen siirrossa kolmansiin maihin on enemmän epäselvyyksiä (-24 %) eikä rakenteetonta tietoa tunnisteta ja kuvata riittävästi (-20 %). Kyberturvallisuudessa heikentyneitä kohtia olivat toimintaympäristön ilmiöiden seuranta (-25 %), palveluihin liittyvien riskien arviointi (-17 %) ja kriittisten palveluiden tunnistaminen (-14 %).

Koska digiturvavalmennukseen osallistui vain kymmenen kuntaa, on palautekyselyn tuloksiin suhtauduttava varauksella. Positiivista on, että vastaajat ovat kokeneet digiturvan parantuneen kaikilla osa-alueilla, joten valmennuksella on ollut positiivinen vaikutus. Toisaalta syitä yksittäisten väittämien arvioiden negatiivisiin muutoksiin on aineiston perusteella vaikea osoittaa. Jos osaavaa henkilöstöä ei ole riittävästi (johtamisen osa-alueen väittämä), voi se vaikuttaa digiturvatehtävien hoitamiseen yleisemminkin. Kun kuitenkin muissa väittämissä havaittiin positiivista kehitystä, ei henkilöstön määrä näytä olevan ainoa syy. Voidaankin tulkita, että osaamisen ja tietoisuuden lisääntyminen tuotti

realistisempia arvioita, mikä näkyy erikoistunutta osaamista edellyttävien tehtävien arvioiden heikentymisenä.

Valmennuksella on ollut suotuisia vaikutuksia kuntien ja siten koko julkisen hallinnon organisaatioiden digiturvaan. Voidaan olettaa, että vastaavalle valmennukselle on tarvetta jatkossakin.

LIITE F: TAISTO-HARJOITUKSISTA KERÄTTY PALAUTE

Digi- ja väestötietovirasto (DVV) järjestää julkisen sektorin organisaatioille ja niiden sidosryhmille TAISTO-harjoituksia, joissa organisaatiot harjoittelevat, testaavat ja kehittävät digiturvan toimintamallejaan kuvitteellisissa häiriötilanteissa. Harjoitusten yleisenä tavoitteena on testata organisaatioiden tietoturvallisuuden hallintaa, johtamista ja viestintää tietoturvaloukkaustilanteissa. Harjoituksia on järjestetty vuodesta 2019 alkaen vuosittain. Harjoituksista kerätyn palautteen perusteella arvioitiin julkisen hallinnon toiminnan jatkuvuuden ja varautumisen osa-alueen kehittymistä.

DVV on julkaissut vuosittaisen yhteenvetoraportin TAISTO-harjoituksen tuloksista[29,30,31]. Raporteista nähdään, että harjoituksiin osallistuneiden organisaatioiden ja henkilöiden määrät ovat kasvaneet vuosittain. Vuonna 2020 osallistuvia organisaatioita oli 250 ja henkilöitä yli 2400. Seuraavina vuosina organisaatioita osallistui 315 ja 375 ja osallistuvien henkilöiden määrä kasvoi noin 20 % kumpanakin vuonna. Vuoden 2023 Taisto-harjoitus oli meneillään tätä kirjoitettaessa, joten siitä ei ole vielä loppuraporttia saatavilla.

Harjoitusten palautekyselyssä vastaajia oli pyydetty arvioimaan mm. yleistä tunnelmaa, harjoituksen hyödyllisyyttä sekä osaamisen kehittymistä harjoituksen tuloksena. Yleisen tunnelman arviointiasteikko oli vuonna 2020 viisiportainen (erinomainen, hyvä, ok, ei niin hyvä, huono), mutta seuraavina vuosina vaihtoehto ”OK” oli jätetty pois, joten asteikko oli neliportainen. Hyödyllisyyttä ja osaamisen kehittymistä arvioitiin kolmiportaisella asteikolla (kyllä, ei, en osaa sanoa). Lisäksi palautekyselyissä oli kartoitettu tarkemmin harjoituksen sisältöön ja tuloksiin liittyviä kysymyksiä.

Yleinen tunnelma oli kaikissa harjoituksissa ollut erittäin hyvä. Erittäin hyvän tai hyvän arvosanan oli antanut selvästi yli 90 % vastaajista ja osuudet ovat pysyneet toisiaan vastaavina kaikissa tarkastelluissa harjoituksissa (pl. vuosi 2020, jolloin arvosteluasteikko oli erilainen). TAISTO-harjoituksia on pidetty jokaisena vuonna lähes yksimielisesti hyödyllisinä: vain noin 2 % vastaajista ei ole pitänyt harjoituksia hyödyllisinä tai ei ole osannut sanoa mielipidettään. Myös osaamisen kehittymistä arvioivat luvut ovat pysytelleet lähes samoina vuosittain: noin 85 % vastaajista katsoi osaamisensa kehittyneen, 6–8 %:lla kehittymistä ei tunnistettu ja 6–8 % ei osannut sanoa, olivatko harjoitukset kehittäneet osaamista.

Harjoitusten ajankohtaisuutta ja realistisuutta pidettiin erittäin hyvänä ja useimmat organisaatiot olivat tunnistaneet harjoitusten perusteella kehitettäviä kohteita omassa toiminnassaan. Vaikka kehityskohteita oli tunnistettu, niistä vain osa oli toimenpiteiksi aikataulutettu ja vastuutettu vuosittain noin 40 %. Toteutettujen ja toimintaan vietyjen muutosten osuuksissa oli melko paljon vuosittaista vaihtelua (2020: 27 %, 2021: 16 % ja 2022: 55 %). Keskeneräisten kehitystoimenpiteidenkin osuuksissa vuosittaista vaihtelua esiintyi selvästi (2020: 44 %, 2021: 64 % ja 2022: 39 %).

TAISTO-harjoituksista kootun palautteen perusteella harjoittelua häiriötilanteissa toimimisen varalle pidetään tärkeänä. Harjoituksiin osallistuvien organisaatioiden ja henkilöiden määrät ovat kasvaneet

[29] TAISTO20 loppuraportti
[30] TAISTO21 loppuraportti
[31] TAISTO22 loppuraportti

vuosittain ja arviot harjoituksen sisällöstä ja toteutuksesta ovat pysyneet erittäin korkeina. Harjoittelijat ovat kokeneet osaamisensa kasvavan, mikä viittaa henkilökohtaiseen vaikuttavuuden kokemukseen. Osallistuvat organisaatiot ovat tunnistaneet harjoitusten perusteella kehitettäviä kohteita, mutta niistä vain osa on toteutettu ja viety osaksi organisaation toimintaa. Tämä on luonnollista, koska kehitystoimenpiteitä joudutaan aina priorisoimaan käytettävissä olevien resurssien ja erilaisten sisäisten ja ulkoisten tarpeiden perusteella. Organisaatioiden tulisi kuitenkin varmistua siitä, että digiturvan taso vähintäänkin säilyy riittävänä ja sen vuoksi kehitystoimenpiteiden edistymistä ja toimintaympäristön muutoksia tulisi aktiivisesti seurata.

Ensimmäiset TAISTO-harjoitukset järjestettiin jo ennen Haukka-toimeenpanosuunnitelman täytäntöönpanoa, mutta vuodesta 2020 lähtien harjoituksia on rahoitettu Haukka-hankkeesta. Koska harjoitusten merkitys on kirjattu toimeenpanosuunnitelmassa huomioitavaksi tehtäväksi, voidaan Haukka-hankkeen toimeenpanosuunnitelman katsoa onnistuneen vaikuttamaan erittäin hyvin julkisen hallinnon digiturvan kehittymiseen.

LIITE G: TRAFICOMIN PILOTTIHANKKEISTA KERÄTTY PALAUTE

Kuntien haavoittuvuusskannaus (Hyöky)

Osana valtiovarainministeriön Haukka-hanketta Traficomin Kyberturvallisuuskeskus toteutti erityisesti kuntasektorille suunnatun hyökkäyspinta-alan kartoituksen pilotin vuosina 2020–2021. Hankkeen tarkoituksena oli selvittää mm. sitä, tuottaisiko pilotti havaintoja sellaisista haavoittuvuuksista, joita ei muuten havaittaisi, millaisia konkreettisia kehitystoimenpiteitä pilotin perusteella voitaisiin käynnistää, sekä miten osallistujien oma käsitys hyökkäyspinta-alastaan vastaisi skannauksesta saatuja tuloksia.

Pilottiin osallistui yhteensä 49 kuntaa ja siinä toteutettiin haavoittuvuusskannaus kolme kertaa noin puolen vuoden välein. Pilottihankkeen lopuksi osallistujille lähetetyn kyselyn avulla selvitettiin pilotin vaikuttavuutta sekä osallistujien kokemuksia. Palautekyselyyn vastasi 14 osallistujaa eli hieman alle 30 % osallistujista.

Kerätyn palautteen perusteella noin puolet palautekyselyyn vastanneista osallistujista oli saanut uusia havaintoja skannauksen tuloksista. Tulokset koskivat aiemmin tunnistamattomia haavoittuvuuksia, internetiin avoinna olevia palveluita ja hyökkäyspinta-alaa, riskiprotokollia ja TLS-varmenteita sekä salatun yhteyden pakottamista. Lisäksi ulkopuolisen toimijan tuottamaa, riippumatonta yleiskuvaa arvostettiin. Yksityiskohtaisten havaintojen perusteella osallistujat olivat käynnistäneet lisäselvityksiä ja tehneet teknisiä parannuksia ja korjauksia. Pilotti osoitti, että toistuvat skannaukset ja havaintojen perusteella tehdyt korjaukset vähensivät haavoittuvuuksien lukumääriä ja siten paransivat pilottiin osallistuneiden organisaatioiden digiturvaa.

Pilotin jälkeen skannauspalvelua on kehitetty edelleen ja kehitystyön tuloksena esimerkiksi raportointi tuottaa palvelun käyttäjille ohjeistavaa tietoa kehittämisen tueksi, minkä käyttäjät ovat kokeneet tärkeäksi. Skannaukset hyödyttävät palvelun käyttäjiä auttamalla tunnistamaan haavoittuvuuksia, joita ne eivät ehkä muuten tunnistaisi. Tunnistettuihin haavoittuvuuksiin voidaan siten valmistella korjaustoimia ja vastakeinoja etukäteen. Pilotin jälkeen palvelusta on saatu lisää palautetta osallistuneilta kunnilta. Tuloksia ei ole vielä julkistettu, mutta palaute on Kyberturvallisuuskeskuksen mukaan samansuuntaista kuin pilottihankkeen loppuraportissa[32].

Pilottihankkeen ja sen jatkokehityksen vaiheen käyttäjät ovat kokeneet palvelun hyödylliseksi ja kokeneet palvelulle olevan tarvetta jatkossakin. Palvelu on julkaistu 13.9.2023 osaksi Kyberturvallisuuskeskuksen palveluvalikoimaa ja syksyn 2023 kuluessa palvelu on tarkoitus saattaa kaikkien kuntien tilattavaksi. Pilotin ja sen jatkokehityksen menestymisen mahdollisuuksia on arvioitu vähäisiksi ilman Haukka-hankkeesta saatua rahoitusta.

Kuntien havainnointikyvyn kehittäminen (HAVARO-käyttöpilotti)

[32] v1-HAUKKA_-_Skannauspalvelun_valmisteluselvityksen_(pilotti)_loppuraportti.pdf

Kyberturvallisuuskeskus on toteuttanut tietoturvauhkien havainnointiin ja niistä varoittamiseen kehitetystä HAVARO-palvelusta helpommin käyttöönotettavan ja kustannustehokkaan version (HAVARO-käyttöpilotti). Palvelusta saatavia kokemuksia on kerätty vuoden 2023 loppuun kestäneessä pilottihankkeessa. Päätökset mahdollisesta palvelun tuotteistamisesta osaksi HAVARO-tuoteperhettä tehdään myöhemmin.

Pilotin pääasiallisena kohderyhmänä ovat kunnat ja kunnalliset huoltovarmuuskriittiset toimijat, ja pilottiin on saatu mukaan kuntia ja kuntayhtiöitä. Pilottihankkeen tavoitteena on lisätä tietoisuutta siitä, kuinka laajalti erilaiset tietoturvauhat koskettavat julkisen hallinnon organisaatioita sekä parantaa erityisesti kuntasektorin tieto- ja kyberturvallisuuden tilannekuvaa tuomalla palvelun piiriin lisää havainnointisensoreita.

HAVARO-käyttöpilotti, kuten muutkin HAVARO-palvelut, auttavat Kyberturvallisuuskeskusta tunnistamaan vakavan, vihamielisen, ulkopuolisen kybertoiminnan ja varoittamaan asiakasorganisaatioita niistä. Havaintojen ja varoitusten perusteella voidaan esimerkiksi estää kiristyshaittaohjelman leviäminen organisaatioon tai toteuttaa muita hallintakeinoja. HAVARO-käyttöpilotti täydentää siten Hyöky-palvelua ja valvomopalveluita.

Käynnissä olevasta pilottihankkeesta ei ole vielä julkaistu määrällisiä tai laadullisia tuloksia. Arvioidaan kuitenkin, että havainnointiin on saatu mukaan merkittävästi uusia organisaatioita, vaikka pilotista kertyneiden havaintojen määrä onkin pienempi kuin fyysisiin sensoreihin perustuvassa HAVARO-palvelussa. Osallistujilta kerätään palautetta, jota seurataan ja jonka perusteella palvelua kehitetään edelleen.

Pilotista kerättyjen tietojen perusteella arvioidaan, että erityisesti kuntasektorin kyber- ja tietoturvallisuuden tilannekuva on parantunut. Edelleen palautteiden perusteella vaikuttaa siltä, että palvelulle on tarvetta jatkossa varsinkin kuntasektorilla. Mahdollisimman kattava havainnointisensorien verkosto tuottaa koko julkista hallintoa hyödyttävää tilannekuvatietoa.