VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Kunnille suunnatut digitaalisen turvallisuuden palvelut

26.8.2022

TIIVISTELMÄ

Haastattelujen perusteella kuntien digitaalisen turvallisuuden yhteisiin palveluihin liittyvät tarpeet ovat hyvin konkreettisia. Vain suurimmilla kaupungeilla on merkittävästi digitaalisen turvallisuuden asiantuntijoita ja asiantuntemusta, joten kunnat ulkoistavat digiturvapalveluitaan merkittävästi lopullisen vastuun jäädessä kuitenkin kunnalle itselleen. Kuntiin ja niiden toimialoille kohdistuu lainsäädännön tietosuojaan, tietoturvallisuuteen ja varautumisen vaatimuksia, eivätkä kaikki kunnat ole pystyneet toteuttamaan vaatimuksia kattavasti. Kunnissa kaivataan tätä varten tukea selkeiden toimeenpanosuunnitelmien laatimiseksi, tietoisuuden ja osaamisen kehittämistä päätöksenteon vahvistamiseksi sekä konkreettiset kuvaukset niistä tehtävistä, joiden avulla digitaalisen turvallisuuden hyväksyttävä minimitaso voidaan saavuttaa. Lainsäädännön kautta tapahtuvaa ohjausta pidetään tarpeellisena, koska nähdään sen lisäävän painetta digitaalisen turvallisuuden kehittämiseen, mutta toisaalta korostetaan autonomisen aseman säilyttämistä ja toimintamallia, joka sallisi joustavasti erilaisia toteutuksia.

Kuntien ja kuntayhtymien omistamat palvelutoimittajat toimivat yhteistoiminnan alueellisina vetureina erityisesti silloin, kun alueella ei ole yhtä suurta kuntaa, joka olisi ottanut tällaisen roolin. Alueellinen yhteistoiminta koetaan tärkeäksi osaamisen kehittämisen ja kokemusten vaihtamisen kannalta. Alueelliset palvelutoimittajat käyvät säännöllisesti keskusteluja omistajakuntien kanssa palvelutarpeiden kartoittamiseksi ja toiminnan kehittämiseksi. Nämä toimijat tuottavat palveluja omistaja-asiakkailleen näiden omien tarpeiden mukaisesti, mutta ne voivat myös tukea kuntia yhteishankintojen järjestämisessä tai tuottaa jaettuja ratkaisuja koko asiakaskuntansa tarpeisiin. Yhteisten tai yhteisesti hankittujen palvelujen avulla pienemmätkin kunnat voivat hyödyntää sellaisia ratkaisuja, jotka yksin hankittuna olisivat kunnalle liian kalliita tai vaikeita toteuttaa. Yhteisten palvelujen käyttäminen on myös alueellisten palveluntuottajien etu, koska asiakastuen ja -palvelun järjestäminen voidaan keskittää ja hankintoja voidaan tehostaa hankinnan koon kasvaessa.

Alueelliset palvelutoimittajat tekevät lisäksi yhteistyötä keskenään. Esimerkiksi SOC-palvelun tuottaminen edellyttää sekä vahvaa osaamista että taloudellisia resursseja. Palvelun tarve on tunnistettu laajasti, mutta pienillä tai edes keskisuurilla toimijoilla ei välttämättä ole tähän riittäviä resursseja käytettävissä. LapIT Oy tarjoaa Istekin tuottamaa SOC-palvelua omille asiakkailleen. Näin yhden toimijan palvelua voidaan hyödyntää useilla alueilla, mikä vahvistaa palvelun rahoituspohjaa ja kehitys- ja ylläpitotyöhön tarvittavia resursseja. Lisäksi alueellisten palveluyhtiöiden yhteistoimintaa on vahvistettu omistusjärjestelyissä, jossa LapIT, Istekki ja Joki ICT ovat toistensa osaomistajia.

Sisällys

1 JOHDANTO

1.1 Raportin lähtökohdat

Valtioneuvosto teki 8.4.2020 periaatepäätöksen Julkisen hallinnon digitaalisesta turvallisuudesta (VM 2020:33). Sen mukaan digitaalisen turvallisuuden viitekehykseen sisältyy riskienhallintaan, toiminnan jatkuvuudenhallintaan ja varautumiseen sekä kyberturvallisuuteen, tietoturvallisuuteen ja tietosuojaan liittyviä asioita. Periaatepäätöksessä on kuvattu julkisen hallinnon digitaalisen turvallisuuden kehittämisalueet ja kehittämisen periaatteet, sekä keskeisiä hallinnon toimintaa ja prosesseja tukevat digitaalisen turvallisuuden palvelut.

Valtioneuvoston periaatepäätöksen 8.4.2020 linjauksia toteuttaa Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelma 2020–2023 (Haukka) (VM 2020:33). Siinä kuhunkin digitaalisen turvallisuuden palveluun liittyen on valittu tehtäviä julkisen hallinnon digitaalisen turvallisuuden nykytilaselvityksen ja kansainvälisen vertailun perusteella. Tehtäville on asetettu tavoitteet ja aikataulu, sekä kuvattu tavoitteiden saavuttamiseksi tarvittavat toimenpiteet, niiden toteutumisen mittaaminen sekä arvioitu kustannuksia ja hyötyjä.

Yhtenä Haukka-toimeenpanosuunnitelman tehtävänä on ”Kuntien yhteiset digitaalisen turvallisuuden palvelut”. Tavoitteena on, että ”Valtiovarainministeriön ohjauksessa digi- ja väestötietovirasto yhdessä Kuntaliiton ja kuntien kanssa kokoaa työryhmän selvittämään kuntien yhteisten digitaalisen turvallisuuden kehittämishankkeiden tarvetta ja toteutusta.” Valtiovarainministeriön Haukka hankkeessa tehtävää toteuttamaan asetettiin 27.10.2021 koordinaatioryhmä. Sen tehtävänä on tuottaa yhteenveto kuntien yhteisistä digitaalisen turvallisuuden palveluiden tarpeista osana kuntien, valtion ja hyvinvointialueiden välistä yhteistoimintaa. Koordinaatioryhmän jäsenet ovat liitteessä 1.

1.2 Työn toteutus ja rajaukset

Työ toteutettiin haastattelemalla kunnille tarkoitettujen digitaalista turvallisuutta edistävien palveluiden koordinaatioryhmän jäseniä ja kuntien tai kuntayhtymien omistamia palveluntuottajia. Haastattelijoina toimi valtiovarainministeriön Haukka-projektiryhmän jäseniä. Haastatteluissa kartoitettiin kuntien digitaalisen turvallisuuden palveluiden tarpeita, niiden hankintaan ja käyttöönottoon liittyviä tarpeita sekä eri toimijoiden rooleja palvelujen tuottamisessa. Haastattelut toteutettiin helmikuun 2022 ja maaliskuun 2022 aikana. Haastatteluja oli yhteensä kuusi. Haastatellut organisaatiot ovat raportin liitteessä 2.

2 HAASTATTELUJEN HAVAINNOT

Haastatteluista kerätyt nyky- ja tavoitetilaa koskevat havainnot on koottu alla olevaan taulukkoon.

Palveluaihio	Haastatteluhavainnot
Digitaalisen turvallisuuden ohjaus	Kyberturvallisuusstrategia on haastattelujen perusteella toimiva pohja myös kunnille. Kuntatason kyberturvallisuusstrategiassa tulisi nostaa erityisesti mm. alueellinen yhteistyö, yhteiset hankkeet sekä yhteiset kyberturvallisuudet viitekehykset. Lisäksi koetaan tarvetta ryhmätoiminnalle kyberturvallisuuden kokonaisuuden minimitason määrittämiseksi ja sopivan kypsyystason varmistamiseksi.
Suositukset, ohjeet, vaatimukset ja työkalut	Perinteisten arviointien sijaan toivotaan digitaalisen turvallisuuden kriteeristöä tai mittaria riittävän kevyellä tasolla. Arviointiin tarvittaisiin myös konkreettisia arviointikehyksiä ja ohjeita. Valtiohallinnon tarjoamat tarkastus- ja valvontapalvelut voisivat toimia hyvänä motivointikeinona, ja kuntiin lähetettävillä ohjauskirjeillä on yleensä positiivinen vaikutus asioiden edistämiseen. Erilaisia yhteistyöelimiä on tunnistettu, mutta tietojen vaihto ei ole kovin tehokasta tällä hetkellä. Yhteinen palveluluettelo, jossa tiedot ja keskustelut ylläpidettäisiin keskitetysti, olisi hyödyllinen. Kunnat hyötyisivät myös digitaalisen turvallisuuden tiekartasta, jossa olisi määritelty selkeät askeleet vaatimusten mukaisen tietoturvatason saavuttamiseksi mukaan lukien turvallisuustekijöitä koskevat vaatimukset. Säädösten ja määräysten täsmällinen noudattaminen koetaan kunnissa haastavaksi. Esimerkiksi asiakastietolain ja tiedonhallintalain yhtäaikainen toteutus koetaan liian monimutkaiseksi ja toteutus jää helposti puutteelliseksi. Lisäksi eri hallinnonaloilta tuleva ohjeistus on epäyhtenäistä. Kansallinen malli tai vastaava kyberturvallisuusasiakirja selkeyttäisi prosessia, jossa on esitelty tarkemmat tehtävät lain näkökulmasta (esim. lokienhallinta, toipuminen) sekä määritelty minimitaso ja eri kypsyystasot eri kokoisille organisaatioille. Auditointi-, testaus- ja harjoittelutoiminta olisi hyvä toteuttaa kansallisesti, jolloin digitaalisen turvallisuuden ymmärryksen kasvattaminen olisi mahdollista toteuttaa laajemmin. Lisäksi todettiin, että kaikkia nykyisiäkään säädöksiä ei pystytä toteuttamaan varsinkaan pienemmissä kunnissa mm. resurssipuutteiden takia, eivätkä uudet säädökset siten paranna tilannetta. Toimeenpanoa

	varten tarvittaisiin ohjeistusta, joka pitäisi pystyä kiinnittämään konkreettisiin tehtäviin ja saavutettavat edut tai hyödyt tulisi pystyä kuvaamaan. Toimeenpanon ohjauksessa tarvitaan selkeitä ohjeita, joiden tulisi kuitenkin antaa kunnille riittävästi liikkumavaraa, jotta toteutus voidaan sovittaa kunnan tarpeisiin ja käytettävissä oleviin resursseihin. Koulutusalustoja on liian paljon ja tietoja on pirstaloitunut eri paikkoihin. eOppiva koetaan hyvänä koulutusportaalina. Yhteensä 19 kunnan ja kuntayhtymän digitaaliseen turvallisuuteen keskittyvässä DigiTyy-hankkeessa työstetään yhteistä riskirekisteriä. Uusille rekistereille tai järjestelmille ei nähdä tarvetta, vaan olemassa olevaa toimintaa pitää kehittää ja parantaa. Erillisiä työkaluja on hankala tuoda nykyisiin prosesseihin ja hankintaprosessia tulisi kehittää esimerkiksi siten, että ohjataan tekemään vaikutusarvio (BIA) ja tietosuojavaatimusten arviointi ensin. Kaupalliset toimijat tuovat lisäksi omia työkalujaan, mikä johtaa uusiin erillisratkaisuihin, mikä koetaan isona haasteena.
Digitaalisen turvallisuuden kehittämisen yhteistoiminta	Digitaalisen turvallisuuden tietoisuus, käsitys palvelutarpeesta ja keskeisistä hankinnoista on kunnilla usein yksittäisen henkilön vastuulla. Apuna voisi olla esimerkiksi työparimalli, jonka avulla henkilö saa vertaistukea ja sparrausta samassa tilanteessa olevien kanssa. Kuntien välinen yhteistyö nähdään osittain haasteelliseksi, mutta pienten kuntien osalta yhteistyö on nähty välttämättömäksi keinoksi asioiden toteuttamiseen ja asiaan suhtaudutaan myönteisesti. Yhteistyö muiden viranomaisten kanssa on kuitenkin vähäistä. On olemassa tietosuojavastaavien yhteistyöfoorumi, mutta hallinnollisen tietoturvan yhteistyö ei ole vielä konkretisoitunut kuntatasolla. Alueelliset palveluntuottajat tekevät sekä palveluyhteistyötä että strategien tason yhteistyötä toimijoiden roolien ja palvelujen kehittämiseksi. Tarkoituksena on saada perustettua alueellinen digiturvaryhmä, jona kautta syntyisi linkki kansallisiin foorumeihin. Tällaisen ryhmän vetäjänä voisi toimia esimerkiksi paikallinen, kuntien yhteisomistuksessa oleva palveluntuottaja. Kuntien ja kuntayhtymien omistamat palveluyritykset (esim. Istekki, LapIT ja JokiICT) tekevät yhteistyötä mm. tuottamalla palveluja, joita toisen yrityksen omistamat kunnat voivat hyödyntää. Esimerkiksi SOC-palvelun tuottaminen on kallista ja vaatii merkittävästi osaamista, joten edes kaikkien palveluyritysten ei kannata toteuttaa sellaista itse. Yhteistyössä hyödynnetään alueellista osaamista, jolloin

	kumppanit pääsevät tarjoamaan omille asiakkailleen ratkaisuja, joita eivät itse pysty tuottamaan.
Tutkimuksen koordinointi	Tutkimuksen koordinointi ei tuottanut haastatteluhavaintoja.
Taloudelliset resurssit	Kuntien taloudelliset resurssit ovat usein niukat. Resurssien kohdentumisesta digitaaliseen turvallisuuteen ei saatu haastatteluhavaintoja.
Digitaalisen turvallisuuden hankinnat ja hankkeet	Hankintaosaamisen puute koetaan ongelmaksi. Esimerkiksi teknisen toimialan järjestelmäkilpailutuksessa ei välttämättä osata huomioida esimerkiksi tietohallinnon tarpeita. Kuntien järjestelmien pitäisi olla yhteensopivia kansallisten tietovarantojen kanssa. Olisi myös tarvetta minimitason ohjeistukselle sekä helposti ymmärrettävälle asiakirjalle, jossa olisi kuvattu valmiiksi rakennetut palvelut eri vaihtoehtoineen ja yhteystietoineen eri tilanteisiin. Sote-uudistuksen myötä pienten kuntien suhteellinen lukumäärä käytännössä kasvaa, kun sosiaali- ja terveysasiat sekä pelastustoimi siirtyvät hyvinvointialueille ja kuntien tehtäväkenttä kapenee. Tämä lisää painetta yhteisten järjestelmien hankintaan, koska kuntien investointikyky heikkenee. Painetta tulee myös ohjelmistopuolelle, koska avoimet rajapinnat on huomioitava entistä paremmin. Yhteishankinnat nähdään kriittisenä onnistumistekijänä kuntien digitalisaatiossa tulevaisuudessa. Alueilla on tarpeita tehdä yhteishankkeita toimialoittain ja niitä tukemaan tarvittaisiin ulkopuolista arviointia. ja apua tiedonhallintamallin päivittämiseen. Alueellisesti omistetut palvelutoimittajat hankkivat tuotteita ja palveluja oman palvelunsa rakentamiseksi ja kehittämiseksi. Tämän lisäksi ne tekevät hankintoja, jossa valmis ratkaisu tarjotaan kaikkien omistajakuntien käyttöön. Mallista on saatu hyviä kokemuksia. Tällä hetkellä on käynnissä VM:n rahoittamana Digiturvallinen työkulttuuri ja -ympäristö -hanke, johon osallistuu 19 kuntaa JokiICT:n toimialueelta. Esiselvityksessä on käytetty Kyberturvallisuuskeskuksen kybermittaria ja myös toteutushankkeita on käynnissä.
Digitaalisen turvallisuuden palvelut	SOC-palvelu koetaan tarpeelliseksi ja se on resurssihaasteiden takia erittäin kysytty pienissä ja keskisuurissa kunnissa. Pienemmille kunnille tuotettuna palvelusta tulisi olla tarjolla nykyistä vielä kevyempi

	versio, jonka käyttö ja käyttöönotto olisi mahdollisimman yksinkertaista. Kunnissa on tunnistettu tarpeita riippumattomaan, ulkopuoliseen auditointiin. Auditointiin ja testaukseen löytyy osaamista kaupallisilta toimijoilta. Kunnissa voitaisiin kilpailuttaa näitä toimijoita osaamisen hyödyntämiseksi. Yhteisten palvelujen auditointi pitäisi toteuttaa kansallisesti (vrt. CE-merkintä). Tietoturvallisuuden teknisessä testauksessa toimitaan hybridimallilla, jossa osa tekijöistä on paikallisen, kuntaomisteisen yrityksen henkilöstöä ja osa ulkopuolisia kaupallisia toimijoita. Mallia pidetään hyvänä riskienhallinnankin näkökulmasta, kun osaajien joukko on laajempi. Auditointien perustana tulisi olla kansalliset vähimmäisvaatimukset ja hyvät käytänteet näiden toteuttamiseksi. Lisäksi tulisi määritellä, kuinka usein tarkastuksia tulisi tehdä ja mitkä ovat tarkastettavat kohteet. Perusasioiden pitää olla kunnossa, jotta turvallisuuden kehittämisen rakenne olisi kestävä. Riskienhallintaa ei välttämättä osata kytkeä kiinteäksi osaksi tietoturvallisuuden hallinnollista ja teknistä toteutusta. Kunnissa ei ole tunnistettu valmista riskien hallinnan ohjausmallia, jota voitaisiin soveltaa. Traficomin tietoturvaskannauspalvelu tunnistettiin osassa haastatteluista. Vielä sitä ei kuitenkaan tunnisteta yleisesti saatavilla olevaksi palveluksi. Toisaalta Traficomin mukaan palvelua ei ole mahdollista laajentaa ennen kuin kunnilta saadaan tietoja niiden käytössä olevista verkko-osoitteistoista.
Digitaalisen turvallisuuden osaaminen	Hallinnollisen tietoturvatietoisuuden kasvattamisessa on tunnistettu selkeä koulutustarve ja ulkopuolisen toimijan apua tarvitaan. Koulutusaihioita voisivat olla esimerkiksi yleinen digiturvallisuus, kuten koneiden lukitseminen, tiedon lähettäminen turvallisesti ja asiakirjojen luokittelu ja hallinta. Tietoturvavalmennus kaupunkien ja kuntien johdolle asiantuntemuksen ja ymmärryksen vahvistamiseksi olisi myös tarpeellista. Kunnilla ei ole välttämättä tietoa koulutuspalvelutarjonnasta tai sen saatavuudesta ja tähän kaivataan opastusta ja neuvontapalvelua. eOppivan opetusmateriaalit ja koulutukset ovat osoittautuneet erittäin hyödylliseksi. Kunnissa eOppiva tavoittaa kohdeyleisön hyvin ja kynnys käyttöönottoon on matala. Vastaavia tarpeeksi neutraaleja koulutusmateriaaleja pitäisi rakentaa lisää eri kokoisille organisaatioille ja toimijoille. Toisaalta erilaisten koulutuksellisten materiaalien katsotaan olevan liian hajallaan, mikä hankaloittaa niiden hyödyntämistä.

	Koulutuksellinen kypsyysanalyysi olisi hyvä, jotta myös pienemmät toimijat lähtisivät teettämään auditointeja ja pääsisivät näin hyödyntämään auditointien perusteella tehtyjä johtopäätöksiä. Digitaalisen turvallisuuden tietoisuuden lisäämiseksi jokin säätely voisi olla paikallaan. Varsinaiselle koulutukselle ja sen viestinnälle tulisi olla kansallinen malli sekä rahoitus.
Digitaalisen turvallisuuden harjoittelu	Alueellisia harjoituksia on järjestetty aktiivisesti. Jokainen kunta järjestää omia harjoituksia esimerkiksi pelastuslaitoksen kanssa. Yhteisesti johdetut valmiusharjoitukset koetaan hyödyllisiksi ja niitä toivotaan lisää. Myös kansainvälisiin kyberharjoituksiin olisi hyvä osallistua ja niihin voidaan osallistua Kyberturvallisuuskeskuksen kautta. Valtionhallinto (esim. ministeriö) nähdään luontevana järjestäjänä isommassa valmiusharjoituksessa, jossa olisivat mukana kunnat, tukipalveluiden tuottajat sekä muut viranomaiset. Harjoittelusta olisi myös hyvä rakentaa kansallinen malli. Yksittäisellä kunnalla tai toimijalla ei ole resursseja tuottaa ja ylläpitää vaadittavia rakenteita. Toivotaan, että valtionhallinto tuottaisi harjoitteluympäristön ja varmistaisi rahoituksen harjoittelulle.
Jatkuvuudenhallinta ja varautuminen	Tukea ja yksityiskohtaisempia ohjeita tarvittaisiin etenkin varautumisen hallintaan, varautumissuunnitelmien laatimiseen ja päivittämiseen sekä suunnitelmien testaukseen. Jatkuvuus- tai toipumissuunnitelma tulee yleensä ulkoa annettuna tietona, eikä suunnitelmien tekeminen ole välttämättä tuttua kuntasektorin toimijoille. Varautumista ei ole saatu jalkautettua hyvin kunnissa henkilöresurssihaasteen vuoksi. Auditoinnin avulla tulisi tunnistaa priorisoituja kehityskohteita. Turvallisuuden ja jatkuvuuden vähimmäisvaatimuksen määrittelystä olisi hyötyä, esimerkiksi hyödyntämällä kybermittaria. Vaatimuksen käyttöönoton mahdollistaminen vaatisi tietoisuuden lisäämistä ja harjoitusta (esim. Taisto-harjoitus). Myös kevyemmälle harjoitusten toteutukselle on tunnistettu tarve. Esimerkiksi virtuaalinen harjoitteluympäristö voisi toimia ratkaisuna, jossa keskeiset tahot pääsisivät harjoitukseen mukaan matalalla kynnyksellä.
Tilannekuva	Kyberturvallisuuskeskuksen viikoittainen raportti kyberturvallisuudentilanteesta koetaan erittäin hyödylliseksi. Tilannekuvien jakaminen kuntien kesken on tällä hetkellä yksi käytetyimmistä palveluista, ja tilannekuvapalvelujen ketjutusta ja jakamista tulisi vahvistaa julki-

	sen toimijoiden vahvuuksia yhdistämällä. Etenkin pienet kunnat tarvitsevat selkeää mallia tieto- ja kyberturvallisuuden tilannekuvan kartoittamiseksi. Esimerkiksi LapIT on parhaillaan tuotteistamassa mallia yhteistyössä Kyberturvallisuuskeskuksen kanssa. Tilannekuvan käsitettä voidaan pitää häilyvänä, koska aina ei ole täysine selvää, millaisesta tilannekuvasta kulloinkin puhutaan. Digitaalisen turvallisuuden osa-alueilla (esimerkiksi tietoturvallisuus tai tietosuoja) on omat tilannekuvansa, joihin tiedot voidaan koostaa erilaisista lähteistä ja toisistaan eroavissa sykleissä. Myös tilannekuvien kohderyhmät voivat poiketa toisistaan. Ei ole tunnistettu yleistä näkemystä siitä, mitkä tiedot muodostavat kunnan tilannekuvan, mistä tiedoista ja miten usein tilannekuva muodostetaan ja miten sitä hyödynnetään päätöksenteon tukena. Tilanteen johtamista ei voi ulkoistaa. Vaikka esimerkiksi tietosuojavastaavan tehtävä olisi hankittu ulkoistettuna palveluna, vastaa organisaatio silti tietosuojan toteutumisesta, tilannekuvan ajantasaisuuden varmistamisesta ja sisäisestä viestinnästä.
Häiriötilanteiden hallinta	Häiriö- ja kriisitilanteeseen liittyvät perinteisten ICT-palvelujen toimenpiteet hoidetaan sopimusten puitteissa. Jos häiriötilanne vaatii sovellusasiantuntijuutta (esim. potilastietojen hallinta), on häiriötilanteen hoitamisen vastuu järjestelmätoimittajalla. Toisaalta tilanteen johtamista ei voi ulkoistaa. Tarkempia vastuita ei ole määritelty monitoimittajaympäristön johtamisesta häiriötilanteessa eri organisaatioiden välillä. Muutoin häiriötilanteiden hallintakykyä varmistetaan auditoimalla palveluntuottajia ja kehittämällä palvelutoimintaa.

3 YHTEENVETO JA JOHTOPÄÄTÖKSET

Kunnille suunnattujen digitaalisen turvallisuuden palvelujen haastatteluissa nostettiin esiin useita samoja seikkoja, joita on tunnistettu Haukka-hankkeen yhteistoiminta- ja hallintamallin koordinaatioryhmänkin työssä. Pienten ja keskisuurtenkin kuntien taloudellisten resurssien niukkuus, digitaalisen turvallisuuden erityisosaamiseen liittyvät puutteet sekä monelta suunnalta kuntaa velvoittavat vaatimukset, määräykset ja ohjeet vaikuttavat siihen, että lakisääteisten velvoitteiden täyttäminen tuottaa ajoittain vaikeuksia.

Digitaalisen turvallisuuden parantamiseksi kunnat tarvitsevat selkeitä ohjeita vaatimusten toteuttamiseksi. Ohjeiden tulisi olla riittävän konkreettisia, jotta kunta voi niiden avulla laatia itselleen parhaiten soveltuvan toimintamallin. Toisaalta liian yksityiskohtaiset määräykset, ohjeet tai suositukset voivat jopa haitata toimeenpanon suunnittelua ja toteutusta. Esimerkkinä tarvittavasta ohjeistuksesta eräässä haastattelussa mainittiin Microsoft 365 –pilvipalvelun tietoturvallisen konfiguroinnin ohjeistus ja vastaavat yksityiskohtaiset ohjeet, joiden toisaalta ei pitäisi olla velvoittavia.

Yhteistoiminta- ja hallintamallin koordinaatioryhmän työssä käytännössä toimivaksi malliksi on tunnistettu rakenne, jossa yhden kunnan – tyypillisesti suuremman kaupungin – ympärille on muodostettu alueellista yhteistoimintaa toteuttava ryhmittymä. Yhteistoiminta ja sen avulla saavutettava suuruuden ekonomia sekä yhteiset ratkaisut ja toimintatavat toteutuvat haastattelujen perusteella hyvin myös kuntien ja kuntayhtymien omistamien alueellisten ICT-yhtiöiden toteuttamana. Koska nämä yhtiöt tekevät keskenään yhteistyötä esimerkiksi laajoja, erityisosaamista ja merkittäviä taloudellisia resursseja edellyttävissä hankkeissa, voidaan tällaista toimintamallia pitää varsin onnistuneena ja sen kehittämistä tulisikin tukea.

Hyvinvointialueiden perustamisen yhteydessä sosiaali- ja terveysalan toiminnot sekä pelastustoimi siirtyvät kunnilta hyvinvointialueille, mikä pienentää kuntien tehtäviä, henkilöstöä ja tuloja merkittävästi. Haastattelujen perusteella tämän johdosta kuntien investointikyvyn nähdään heikkenevän, mikä voi vaikeuttaa entisestään jopa lakisääteisten velvoitteiden täyttämistä varsinkin pienemmissä kunnissa. Yhteistyö, jaetut resurssit ja yhteiset ratkaisut nähdään välttämättöminä ratkaisuina tulevaisuudessa ja tätä tukemaan tulisi toteuttaa hyvinvointialueille, kunnille ja kuntien ICT-yhtiöille suunnattuja digitaalisen turvallisuuden kehittämisen yhteishankkeita. Kunnille suunnattu digitaalisen turvallisuuden edistämisen valtionapu hankkeiden tueksi voisi olla keino edistää vaatimustenmukaisuutta, parantaa kuntalaisten oikeuksien toteutumista ja varmistaa digitaalisen turvallisuuden vähimmäistavoitteiden saavuttaminen. Tätä raporttia kirjoittaessa onkin käynnissä kuusi valtionapua saanutta mm. digitaalista turvallisuutta kehittävää hanketta (lisätietoja: https://vm.fi/-/valtiovarainministerio-on-myontanyt-vuoden-2021-avustuksia-kuntien-digitalisaatiohankkeisiin).

LIITE 1: KOORDINAATIORYHMÄN JÄSENET

Niko Mäkilä, VM, puheenjohtaja
Tuija Kuusisto, VM
Ville-Veikko Ahonen, VM
Eelis Laine, VM
Rauli Paananen, LVM
Atte Pirttilä, DVV
Juha Ilkka, Traficom
Juha Matilainen, Kalajoki
Anssi Haapala, Porvoo
Pasi Kalevo, Turku
Jari Ylikoski, Kuntaliitto
Jarna Hartikainen, HVK
Peter Sund, FISC
Mikaiiro Laitinen, KPMG

LIITE 2: HAASTATTELUT

Osallistuja(t):
Kalajoen kaupunki
Porvoon kaupunki
Kymijoen ICT – Kaakkois-Suomen Tieto Oy
Joki ICT Oy
Istekki Oy
LapIT Oy