HEL 2021-002756

Valtioneuvoston periaatepäätös tietoturvan ja tietosuojan parantamiseksi kriittisillä toimialoilla; lausunto

Lausuntopyynnön diaarinumero: VN/3501/2021

LAUSUNTOKOHTA 1: Ehdotukset poliittisiksi linjauksiksi, kommentit:

Liikenne- ja viestintäministeriö on pyytänyt (VN/3501/2021) Helsingin kaupungilta lausuntoa Valtioneuvoston periaatepäätöksestä tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla.

Linjaus 5. Selvitetään viranomaisten tarpeet teknologisille ratkaisuille salassa pidettävän ja turvaluokitellut tiedon vaihtamiseen. Selvityksen kohteena ovat viranomaisten yhdenmukainen salattu sähköpostiviestintä, turvalliset neuvotteluyhteydet ja - palvelut sekä turvallinen tiedonsiirtopalvelu.

Helsingin kaupunki toteaa, että esimerkiksi sosiaali- ja terveydenhuollon käytettävissä on jo turvallisia tiedonsiirtopalveluja, mutta toimialaa koskeva erityislainsäädäntö aiheuttaa epäselvyyttä siitä, millä tavoin ja missä laajuudessa tietojen vaihtaminen niiden avulla on mahdollista. Sosiaali- ja terveydenhuollon erityislainsäädäntö on nimittäin viranomaisen tiedonsaantioikeutta koskien monilta osin vanhentunutta ottaen huomioon, että tarve tietojen vaihtoon on jokapäiväistä.

Sosiaali- ja terveydenhuollon erityislainsäädäntö on säädetty pääosin aikana, jolloin toimialat olivat erilliset ja näin ollen henkilötietojen käsittelyä koskevat säännökset poikkeavat monilta osin toisistaan toimialojen välillä. Sosiaali- ja terveydenhuolto järjestetään nykypäivänä kaikissa kunnissa kuitenkin yhdessä, eikä toimialoja voi enää erottaa samaan tapaan toisistaan. Sosiaali- ja terveydenhuollon erityislainsäädäntöä ei ole kaikilta myöskään päivitetty vastaamaan EU:n yleistä tietosuoja- asetusta.

Edellä kuvattu johtaa käytännön elämässä tietoturvan ja tietosuojan kannalta ei-toivottuihin ratkaisuihin tietojen jakamisen keinoina, esimerkiksi faksin käyttöön tietojärjestelmässä tapahtuvan tietojen käsittelyn sijasta. Tiedonhallintalain mukaan tietojen luovuttaminen teknisen käyttöyhteyden avulla tai katseluyhteyden avaamisella avulla edellyttää, että tiedot vastaanottavalla viranomaisella on luovutettaviin tietoihin laissa säädetty tiedonsaantioikeus.

Edellä lausutuista syistä Helsingin kaupunki katsoo, että hallinnonalojen erityislainsäädännön päivittäminen vastaamaan EU:n yleistä tietosuoja-asetusta on tehtävä samassa yhteydessä, kun selvitetään tarve teknologisille ratkaisuille tiedon vaihtamiseen. Tämän lisäksi on selvitettävä, onko viranomaisille turvattu erityislainsäädännössä riittävä tiedonsaantioikeus laissa säädettyjen tehtävien hoitamista varten. Mikäli viranomaisella ei ole laissa säädettyä tiedonsaantioikeutta, ei tietojen vaihtaminen teknologisten ratkaisujen, kuten katseluyhteyden ja teknisen rajapinnan avulla, välttämättä ole mahdollista.

Linjaus 9. Liikenne- ja viestintäviraston Kyberturvallisuuskeskus laatii ennakollisen ohjeen yleisistä tietoturvavaatimuksissa huomioitavista asioista. (Kommentti koskee myös linjauksia 8 ja 31)

Helsingin kaupunki kiinnittää huomiota siihen, että ehdotetuissa poliittisissa linjauksissa on vahvasti erotettu tietosuojan ja tietoturvan viranomaisvalvonta ja –ohjaustehtävät. Sellaisten toimialojen kohdalla, joilla henkilötietojen käsittely on vähäistä ja suojattava tieto on luonteeltaan muuta kuin henkilötietoa, tällainen erottelu voi sinänsä olla perusteltua. Tietosuojavaatimukset toteutetaan kuitenkin useimmiten tietoturvan keinoin ja tästä syystä tietosuojan ja tietoturvan erottelu ei useimmiten ole perusteltua eikä palvele tarkoitustaan etenkään sellaisilla toimialoilla, joissa henkilötiedot muodostavat valtaosan suojattavasta tiedosta. Valtaosalle ihmisistä ei ole selvää, mitä eroa tietosuojalla ja tietoturvalla on ja tästä syystä näiden valvonta- ja ohjaustehtävien erottaminen on omiaan lisäämään epätietoisuutta siitä, keneltä asiassa voi pyytää neuvontaa ja ohjausta.

Näin ollen linjauksissa mainittu ohjeistus tietoturvavaatimuksissa huomioitavista asioista olisi syytä laatia yhteistyössä Tietosuojavaltuutetun toimiston kanssa. Yleisemminkin poliittisissa linjauksissa olisi syytä korostaa Kyberturvallisuuskeskuksen ja Tietosuojavaltuutetun toimiston yhteistyötä ohjaus- ja neuvontatehtävissä.

Linjaus 11. Kriittisille toimialoille säädetään velvoite säännöllisesti auditoida kriittiset tieto- ja tietoliikennetekniset prosessit ja toiminnot. Auditointimalli määräytyy laissa riskiperusteisesti sen mukaan, kuinka kriittistä tietoa sisältävästä järjestelmästä tai prosessista tai toiminta ohjaavasta on kyse. Määrittelyssä huomioidaan taloudelliset vaikutukset. (Kommentti koskee myös linjauksia 26 ja 29)

Helsingin kaupunki toteaa, että useilla kunnilla on käytössä samat tietojärjestelmät tai muutoin toisiaan vastaavat tieto- ja tietoliikennetekniset prosessit ja toiminnot. Säännöllisestä auditointivaatimuksesta seuraa mahdollisesti merkittävät kustannusvaikutukset. Tästä syystä poliittisissa linjauksissa olisi aiheellista kiinnittää huomiota julkisten toimijoiden mahdollisuuteen tehdä yhteistyötä ja jakaa tietoa tehokkaasti tietoturvaa ja tietosuojaa koskevassa työssä, esimerkiksi tietoturva-auditointien ja tietosuojan vaikutustenarviointien tekemisessä, päällekkäisten kustannusten välttämiseksi. Erityisesti tämä korostuu kunnissa ja tulevilla sote-hyvinvointialueilla, joilla eri toimijoilla on paljon samoja tietojärjestelmiä käytössään. Uudenmaan alueella on jo kokemusta yhteisestä vaikutustenarviointityöstä. Yhteistyöllä lasketaan paitsi menettelyiden kustannuksia, vahvistetaan myös merkittävästi osaamista.

Helsingin kaupunki kiinnittää samassa yhteydessä huomiota siihen, että valtakunnallisesti ei ole saatavissa tietoa jo tehdyistä tietosuojan vaikutustenarvioinneista. Tämän seurauksena on mahdollista, että useat rekisterinpitäjät tekevät erillään vaikutustenarvioinnin esimerkiksi

samasta tietojärjestelmästä. Kustannustehokkainta olisi tehdä vaikutustenarviointi rekisterinpitäjien yhteistyönä tai hyödyntää myöhemmin tehtävässä arvioinnissa aiemman arvioinnin tuloksia. Jatkotyössä olisi syytä pohtia, millä tavalla tietoa jo tehdyistä vaikutustenarvioinneista saataisiin laajemmin käytettäväksi ja rekisterinpitäjien yhteistyötä lisättyä.

Linjaus 12. Kriittisten toimialojen merkittävimpien toimijoiden tulee osoittaa käyttävänsä tietoturvallisuuden hallintajärjestelmää ISO 27001 -sertifioinnilla vuoden 2024 loppuun mennessä.

Väliraportissa todetaan, että kriittisten toimialojen sertifiointivelvoitteessa on hyvä tarkastella toimijoiden kykyä hankkia sertifikaatteja. Väliraporin mukaan ISO 27001 –tietoturvasertifikaatin hankkimisen kokonaiskustannuksiksi on arvioitu 76 480 euroa.

Helsingin kaupunki toteaa, että jatkotyössä on selvitettävä, millaisia toiminnanmuutoksia ja lisäresursointia tietoturvasertifikaatin hankkiminen kriittisiltä toimialoilta vaatii ja mitkä sen todelliset kokonaiskustannukset ovat. Väliraportista ei käy ilmi, onko tarvittavista toiminnanmuutoksista ja esimerkiksi järjestelmäkehittämisestä aiheutuvat kustannukset huomioitu esitetyssä ISO 27001 –tietoturvasertifikaatin hankkimisen kokonaiskustannuksessa. Kaupunki toteaa lisäksi, että jatkotyössä on tarkkaan arvioitava, mitkä tahot olisivat velvollisia hankkimaan tietoturvasertifikaatin.

Kuten väliraportissa todetaan, on mahdollista, että pienemmät toimijat poistuvat markkinoilta, koska niillä ei ole taloudellista mahdollisuutta tietoturvasertifikaatin hankkimiseen. Tällöin on mahdollista, että yksittäisille toimijoille muodostuu markkina-asema, jonka kautta ne voivat vaikuttaa hintatasoon. Viranomaisen asettamilla sertifiointivelvoitteilla on siis merkittävä vaikutus markkinatoimintaan. Jatkotyössä on näin ollen selvitettävä, millaista hyötyä sertifiointivelvoite tuo sen mahdollisesti aiheuttamaan kilpailua vääristävään vaikutukseen nähden ja onko hyöty hyväksyttävä suhteessa haittaan. Sertifiointivelvoitteen tulisi olla oikeassa suhteessa tavoiteltuun päämäärään nähden ja lainsäätäjän olisi varmistuttava, että sertifiointivelvoitteen asettaminen on hyväksyttyä muun muassa Euroopan unionin kilpailusääntely huomioiden.

Linjaus 27. Selvitetään Suomen 15 suurimman kunnan tietoturvan ja tietosuojan taso terveydenhuollossa, energiahuollossa ja vesihuollossa.

Helsingin kaupunki toteaa, että linjauksissa esitetty rajaus terveydenhuoltoon ei ole tarkoituksenmukainen, vaan selvityksessä tulisi huomioida myös sosiaalihuolto. Myös sosiaalihuollossa käsitellään merkittävässä määrin esimerkiksi terveyttä koskevia tietoja ja muita julkisuuslain mukaan salassa pidettäviä tietoja.

Perusterveydenhuollon, sosiaalihuollon ja erikoissairaanhoidon palvelut muodostavat kokonaisuuden ja terveydenhuollon palveluja järjestetään usein yhdessä sosiaalihuollon palvelujen kanssa. Esimerkiksi sosiaalihuollon asumispalveluissa toteutetaan tyypillisesti myös terveydenhuoltoa, kuten haavanhoitoa ja lääkkeiden määräämistä. Näin ollen rajanveto sosiaali- ja terveydenhuollon palveluiden välillä on nykypäivänä keinotekoinen, erityisesti sellaisten henkilöiden kohdalla, jotka käyttävät runsaasti kyseisiä palveluita.

Sosiaali- ja terveydenhuollon palvelujen yhteyttä korostaa se, että eri toimijat ovat hankkineet näille palveluille yhteisiä tietojärjestelmiä. Esimerkiksi Uudellamaalla on jo osittain käytössä sosiaali- ja terveydenhuollon yhteinen Apotti- asiakas- ja potilastietojärjestelmä. Myös muilla alueilla ollaan hankkimassa sosiaali- ja terveydenhuollon yhteistä asiakas- ja potilastietojärjestelmää, esimerkiksi Keski-Suomessa kilpailutus on päättynyt ja yhteisen tietojärjestelmän käyttöönotto on tarkoitus alkaa vuonna 2023. Näin ollen kokonaiskuvan

saamiseksi on tärkeää selvittää tietoturvan ja tietosuojan taso terveydenhuollon lisäksi sosiaalihuollossa.

Linjaus 29. Kriittisten toimialojen rekisterinpitäjien on varmistettava vuoden 2021 loppuun mennessä, että tietosuojaa koskevat vaikutusarvioinnit on yleisen tietosuoja-asetuksen mukaisesti tehty siltä osin, kun käsittely todennäköisesti aiheuttaa korkean riskin ihmisten oikeuksille ja vapauksille.

Helsingin kaupunki huomauttaa, että EU:n yleisen tietosuoja-asetuksen vaikutustenarvioinnin tekemistä koskevat vaatimukset koskevat myös ennen 25.5.2018 käynnissä olleita käsittelytoimia.
Linjauksesta ei kuitenkaan käy ilmi, koskeeko esitetty aikataulu pelkästään EU:n yleisen tietosuoja-asetuksen voimaantulon jälkeen alkaneita käsittelytoimia, vai myös ennen 25.5.2018 alkanutta käsittelyä. Kaupunki kiinnittää huomiota siihen, että yhteiskunnan kriittisillä toimialoilla toimivilla rekisterinpitäjillä on käytössään useita kymmeniä, ellei jopa satoja, tietojärjestelmiä, joissa käsitellään laajamittaisesti henkilötietoja. Monet näistä järjestelmistä on otettu käyttöön huomattavasti ennen EU:n yleisen tietosuoja-asetuksen voimaantuloa. Lisäksi ennen EU:n yleisen tietosuoja-asetuksen voimaantuloa käynnissä on ollut lukuisia muitakin käsittelytoimia, jotka edellyttävät tietosuojan vaikutustenarviointia. Kriittisillä toimialoilla toimivilla rekisterinpitäjillä on käytössään rajalliset resurssit vaikutustenarviointien tekemiseen. Tämä tulisi huomioida linjauksissa esitetyssä aikataulussa.

Helsingin kaupunki kiinnittää huomiota myös siihen, että huolimatta aikataulusta, rekisterinpitäjät tarvitsevat Tietosuojavaltuutetun toimistolta kattavampaa ohjeistusta vaikutustenarvioinnin tekemiseen. Yhteiskunnan kriittisillä toimialoilla toimivat rekisterinpitäjät tarvitsevat kaupungin arvion mukaan ohjausta erityisesti tietoturvavaatimusten huomioimisesta vaikutustenarvioinnissa. Tältä osin Helsingin kaupunki viittaa jäljempänä linjauksen 33 kohdalla lausuttuun Tietosuojavaltuutetun toimiston resurssien määrästä ja kohdentamisesta.

Linjaus 33. Varmistetaan Tietosuojavaltuutetun toimistolla riittävät resurssit valvoa sektoreita tehokkaasti ja puuttua henkilötietojen tietoturvaloukkauksiin.

Helsingin kaupunki toteaa, että poliittisissa linjauksissa olisi syytä painottaa ennaltaehkäiseviä toimia. Resurssien varaaminen pääasiassa valvontatehtäviin ei ole tarkoituksenmukaista, koska kuten väliraportissa todetaan, mikään määrä valvontaa ei yksin riitä tekemään yhteiskunnasta ja sen kriittisisät toiminnoista turvallisia. Tietoturvan ja tietosuojan on oltava sisäänrakennettuna kriittisten toimialojen toimintakulttuuriin.

Näin ollen ensisijainen keino varmistaa linjausten toteutuminen on varata Tietosuojavaltuutetun toimistolle riittävät resurssit viranomaisen ohjaus- ja neuvontavelvollisuuden täyttämiseksi. Rekisteröidyn näkökulmasta on olennaisempaa, että rekisterinpitäjillä on riittävä tietosuojan ja tietoturvan osaaminen ja että tietosuojavaatimukset toteutuvat kaikessa toiminnassa, kuin että viranomaisvalvonnalla puututaan jälkikäteen esimerkiksi puutteisiin tietosuojan toteuttamisessa. Kaupunki korostaa, että Tietosuojavaltuutetun toimistolle on linjauksen mukaisesti varattava riittävät resurssit myös valvontatehtävien hoitamiseksi. Painopiste resurssien varaamisessa tulisi kuitenkin kohdistua ennaltaehkäiseviin toimiin ja yhteiskunnan kriittisillä toimialoilla toimivien rekisterinpitäjien tietosuojaosaamisen lisäämiseen.

Linjaus 34. Seurataan tietosuojalain mukaisen seuraamusjärjestelmän soveltamista ja toimivuutta.

Helsingin kaupunki kannattaa ehdotusta. Samalla kaupunki kiinnittää huomiota siihen, että Tietosuojavaltuutetun toimiston ratkaisukäytäntöä tulisi julkaista nykyistä laajemmin. Finlex-palvelussa julkaistujen ratkaisujen määrä on huomattavan pieni suhteessa

Tietosuojavaltuutetun toimiston vuosittain antamien päätösten määrään. Ratkaisukäytännön laajempi julkaiseminen olisi omiaan lisäämään rekisterinpitäjien tietosuojaosaamista ja täydentämään viranomaisen ohjaus- ja neuvontavelvollisuutta.

Linjaus 35. Kehitetään yksityishenkilöille ja organisaatioiden edustajille mobiilipäätelaitteeseen asennettava sovellus, jonka kautta on mahdollista saada kohdennetusti ajankohtaista tietoa tietoturvauhkista ja -loukkauksista ja tietoturvallisuutta koskevista ohjeista sekä ilmoittaa tietoturvauhkista ja -loukkauksista Kyberturvallisuuskeskukselle, kriittisen toimialan valvovalle viranomaiselle ja/tai poliisille. Lisäksi sovelluksesta voisi ilmoittaa henkilötietojen tietoturvaloukkauksesta Tietosuojavaltuutetun toimistolle. Palvelu, mukaan lukien sovellus ja palveluun liittyvät järjestelmät, toteutetaan turvallisen ohjelmistokehityksen sekä hyvän tietoturvan ja -suojan periaatteita noudattaen.

Helsingin kaupunki pitää ehdotusta lähtökohtaisesti kannatettavana. Asian valmistelussa on kuitenkin ratkaistava monia kysymyksiä erityisesti koskien rekisterinpitäjän asemaa henkilötietojen tietoturvaloukkaustilanteissa. Jos yksityishenkilö voi ilmoittaa henkilötietojen tietoturvaloukkauksista suoraan Tietosuojavaltuutetun toimistolle rekisterinpitäjän sijasta, ei tieto välity välttämättä rekisterinpitäjälle riittävän nopeasti. On myös huomattava, että rekisterinpitäjällä on lakisääteinen velvollisuus ilmoittaa tapahtuneista henkilötietojen tietoturvaloukkauksista.

Helsingin kaupungin strategiaosasto lausuu lisäksi seuraavaa

Helsingin kaupungin toimintaan liittyviltä osin tässä väliraportissa esitetyt linjaukset kohdennettuna yhteiskunnan kriittisille toimijoille ovat pääasiassa kannatettavia.

(Linjaus 12) Kriittisten toimialojen merkittävimpien toimijoiden sertifiointivelvoite on mahdollista hyväksyä varsin rajatulle toimijajoukolle. Markkinatoimijat voivat saavuttaa laatusertifikaatteja kustannustehokkaastikin, ja standardien noudattaminen voi tuoda markkinointietua ICT-palveluiden myymisessä. Aikaraja 2024 voi olla mahdollinen ainakin niille toimijoille, joiden toiminta on jo jonkin laatujärjestelmän mukaista.

Julkisen sektorin merkityksen tunnistaminen ja huomioiminen kriittisenä toimialana on tärkeää. (Linjaus 27) Suurimpien kuntien tietoturvan ja tietosuojan tason selvittäminen terveydenhuollossa, energiahuollossa ja vesihuollossa on kannatettavaa. Tätä tukee tietoturvan arviointilaitosten määrän lisääminen (linjaus 13).

(Linjaus 29) Vaikkakin kriittisillä toimialoilla toimivilla rekisterinpitäjillä on käytössään rajalliset resurssit vaikutustenarviointien tekemiseen, niin jos käsittely todennäköisesti aiheuttaa korkean riskin ihmisten oikeuksille ja vapauksille, viranomaisen voi odottaa kohdentavan käytössään olevia resurssejaan vaikutusten arvioinnin tekemiseen. Tällöin myös tulee harkituksi mikä on mahdollisesti syntyvä korkea riski.

Yleisenä huomiona suurten kaupunkien palvelutoiminnan kannalta on erilaiset mahdollisuudet ja haasteet hallinnoida kyberturvaa hajautetusti tai keskitetysti. Kyberturvakeskuksen ja tietosuojavaltuutetun tietosuojan- ja turvan yhteisohjaus voi muodostua monimutkaiseksi ja aiheuttaa enemmän haasteita kuin mahdollisuuksia.

Julkishallinnolle hyödyllisintä saattaisi olla Kyberturvallisuuskeskuksen keskittyminen vauhdittamaan julkishallinnon yhteisten teknisten standardien ja käytäntöjen aikaan saamista. Tietosuojavaltuutettu katsoo kyberturvallisuutta enemmän yksilöiden oikeuksien näkökulmasta.

Suurilla organisaatioilla, kuten suurimmilla kaupungeilla, on mahdollisuus hankkia riittävää asiantuntijuutta kaikille tarvittaville digitaalisen turvallisuuden osa-alueille kuten tietosuoja ja kyberturva.

Helsingin kaupungin sosiaali- ja terveystoimiala lausuu lisäksi seuraavaa

Kaikilla kriittisillä toimialoilla pitää olla lakisääteiset tietoturvavaatimukset sekä toimintojen että järjestelmien suhteen, ja näitä vaatimuksia pitää arvioida säännöllisesti.

Kriittisille toimialoille säädetään velvoite säännöllisesti auditoida kriittiset tieto- ja tietoliikennetekniset prosessit ja toiminnot sekä järjestelmät.

Tietoturvallisuuden hallintajärjestelmän ISO 27001 -sertifiointivaatimus ja tarkastusmahdollisuus ovat hyviä kannustimia.

Tärkeä asia, että Suomen 15 suurimman kunnan tietoturvan ja tietosuojan tason selvityksessä hyödynnetään Kyberturvallisuuskeskuksen tarjoamaan tietoturvallisuuden kartoituspalvelua.

Linjauksissa kriittisten toimialojen erityispiirteisiin voitaisiin terveydenhuollon osalta lisätä myös kaikkien terveydenhuollon tietojärjestelmien rekisteröinti Valviran rekisteriin (A- ja B-luokat).

Nämä poliittiset linjaukset ovat hyviä ja tarpeellisia linjauksia myös terveydenhuollon palveluille.

LAUSUNTOKOHTA 2: Väliraportin muut osat, kommentit:

Helsingin kaupunki katsoo tietoturvassa ja tietosuojassa onnistumisen liittyvän laajasti kunnan toimintaan, sillä yhteiskunnan kriittisiksi toimialoiksi voidaan lukea merkittävä osa kunnan toimintaa. Tietoturvassa onnistuminen on nykyaikaisessa julkishallinnon toimintaympäristössä välttämätöntä. Tuki tietoturvatoiminnassa kehittymiselle on tärkeämpää kuin sanktiot tai pelotteet.

Linjausten lähtökohtana tulisi olla välttää lisävelvoitteiden syntymistä ja taloudellisten rasitteiden kasvua. Niiden sijaan linjausten tulee tukea tietoturvatoiminnassa kehittymistä ja osaamisen kasvamista.

Linjauksissa tulisi esittää julkishallinnon tietoturvaan liittyvän harjoittelun järjestämisvastuu sekä tuki julkishallinnon laajalle osallistumiselle. Kuntien tietoturvan osalta olisi merkityksellistä, että julkishallinnon tietoturvaan liittyvään harjoitteluun saa osallistua myös kuntien palvelutoimittajat.

Tietoturvan osaamisen lisäämiseksi tulisi linjata julkishallinnon eritasoisten tietoturvan koulutusohjelmien toteuttaminen. Koulutusohjelmat tulisi olla joustavasti suoritettavia koko julkishallinnon henkilöstölle, tukeutuen verkkokoulutusjärjestelyihin. Kunnan tietoturvassa onnistuminen edellyttää aiempaa enemmän ja aiempaa useammalta tietoturvan osaamista.

Tietoturvaan osoitettavista henkilövoimavaroista tulisi linjata kuten esimerkiksi tietosuoja- tai työsuojelutoiminnassa on jo velvoitteita käytettävissä olevalle henkilöstölle. Suhteutettuna kunnan kokoon tulisi kunnalla olla käytettävissään omaa tietoturvahenkilöstöä tietty minimimäärä. Sillä jos tietoturvatyötä tehdään vain oman työn ohella, niin tietoturvakyvykkyys ei voi vastata nykyaikaisen julkishallinnon organisaation tarpeita.

Varsinaisten sertifiointien sijaan tulisi linjata organisaation omavalvonnan järjestämisestä siten, että julkishallinnon tietoturvavelvoitteiden toteutumista voidaan arvioida suhteessa julkishallinnossa käytettävään arviointikehikkoon. Julkishallinnon tietoturvan arviointikehikko

tulisi laatia ja linjata Suomen julkishallinnon tietoturvan kypsyysmalliksi. Tämän laadinnassa voitaisiin hyödyntää jo olemassa olevia kansallisia kriteeristöjä kuten kansallinen turvallisuusarviointikriteeristö, pilviturvallisuuskriteeristö sekä VAHTI-ohjeet (tiedonhallintalautakunnan suositukset).

Linjauksissa voitaisiin esittää kuinka vertaisarviointiin perustuva julkishallinnon tietoturvatoiminnan laadun arvioiminen tulisi järjestää Suomen julkishallinnon tietoturvan kypsyysmallia käyttäen. Malli tulee laatia sellaiseksi, että sitä voi soveltaa myös pk-yrityksissä. Silloin nämä linjaukset ja malli tukevat laajasti kansallista tietoturvassa kehittymistä.

Suomen julkishallinnon tietoturvan kypsyysmallin laatiminen tukisi siihen perustuvan paikallisen tietoturvaliiketoiminnan kehittymistä. Kun kypsyysmalli laaditaan ottaen huomioon kansallinen tietoturvan lähtötaso ja sovitetaan realistisesti saavutettaviksi yksinkertaisiksi kyvykkyysportaiksi, niin mahdollistetaan julkishallinnon tosiasiallinen tietoturvassa onnistumisen kehittyminen käytännössä.

Erityisen keskeisenä kuntien teknisessä tietoturvassa onnistumiselle Helsinki pitää sitä, että julkishallinnolle olisi tarjolla tietoturvan ja tietosuojan kannalta riittävän laadukkaat tieto- ja viestintätekniset palvelut ja ratkaisut valmiiksi kilpailutetuista palvelutarjoomista. Nykytilanteessa kuntien voimavaroja kuluu tarpeettoman paljon paikalliseen selvitystyöhön sekä riittämättömiin ratkaisuihin. Kuntien tarvitsemat tieto- ja viestintätekniset palvelut ja ratkaisut ovat kuitenkin pääasiassa samankaltaisia läpi koko kuntakentän.

Valmiiksi kilpailutettu ja laatuvarmistettu palvelutarjooma toisi sekä toiminnallista että taloudellista etua kaikille osallisille.

Helsingin kaupungin sosiaali- ja terveystoimiala lausuu lisäksi seuraavaa

4. Nykytilan arviointi

Valvira valvoo sosiaali- ja terveydenhuollon asiakas- ja potilastietojen käsittelyyn tarkoitettujen tietojärjestelmien olennaisten vaatimusten toteutumista:
https://www.valvira.fi/terveydenhuolto/sosiaali-ja-terveydenhuollon-tietojarjestelmat

Valviralle ilmoitettujen tietojärjestelmien tiedot tallennetaan Excel-muotoiseen rekisteriin, josta löytyy tällä hetkellä A-luokan järjestelmiä 82 kpl ja B-luokan järjestelmiä 260 kpl (katso oheinen linkki).

Valmistajan on ilmoitettava tuotantokäyttöön otettavasta tietojärjestelmästä Valviralle, mutta valitettavasti kaikki tietojärjestelmät eivät löydy edellä mainitusta rekisteristä (A- tai B-luokista).

Tietoturvavaatimuksia koskeva sääntely terveydenhuollon toimialalla (katso raportin liite) ei ole kattavaa:

o THL:n Määräys 1/2015: A-luokkaan kuuluvien sosiaali- ja terveydenhuollon tietojärjestelmien olennaiset tietoturvavaatimukset

o THL:n Määräys 2/2015: Omavalvontasuunnitelmaan sisällytettävät selvitykset ja vaatimukset

o Findatan Määräys 1/2020: Määräys muiden palveluntarjoajien tietoturvallisille käyttöympäristöille asetettavat vaatimukset

Tarvitaan yksityiskohtaisemmat tietoturvavaatimukset sekä A- että B-luokan järjestelmiin, samoin myös näiden tietoturva-auditointi.

Sertifiointivaatimus myös tietosuojan puolella on erinomainen tapa osoittaa, että tietosuoja-asetusta ja erityisesti käsittelyn turvallisuuteen liittyviä vaatimuksia noudatetaan.

6. Arvio keskeisistä vaikutuksista

Taulukosta 3 voidaan todeta, että terveydenhuollossa on 18364 yritystä ja näistä on lähes 95% prosenttia alle kymmenen hengen toimijoita. Pienille yrityksille ISO 27001 –tietoturvasertifikaatin hankkiminen (kokonaiskustannuksiksi on arvioitu 76480 euroa) on mahdoton tehtävä, mutta isommille toimijoille tämä lienee mahdollista.

Valmistelija

Aaro Hallikainen
Tietoturva-asiantuntija
Kaupunginkanslia