Digi- ja väestötietovirasto

Lausunto

05.01.2021 DVV/78/2021

Asia: VN/24348/2020

Selvitys tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla; työryhmän väliraportti

Lausunnonantajan lausunto

Ehdotukset poliittisiksi linjauksiksi, kommentit:

Työryhmä on esittänyt kattavasti linjausehdotuksia tietoturvan ja tietosuojan parantamista useilla eri kriittisiksi toimialoiksi katsotuilla sektoreilla ja ehdottanut että julkinen sektori tunnistettaisiin kriittiseksi toimialaksi. Väliraportin esittämät poliittiset linjaukset luovat pohjan konkreettisille kehittämistoimenpiteille yhteiskunnan kriittisten palveluiden ja ne mahdollistavan infrastruktuurin suojaamiseksi, ja molempien osalta on tunnustettu digitaalisen toimintatavan kasvava merkitys.

Digi- ja väestötietovirasto ja pitää ehdotusta osin 1 kannatettavana. Viranomaisten välinen yhteistyö on jo nyt merkittävässä roolissa sekä tietoturvaloukkaustilanteiden ehkäisemisessä että niiden selvittämisessä. Erityisesti tietoturvaloukkaustilanteiden ehkäisemiseen keskittyvässä yhteistyössä myös Digi- ja väestötietoviraston VAHTI toiminnolla on myös keskeinen rooli julkisen hallinnon digitaalisen toimintaympäristön turvaamisen osalta. Linjauksen 1 osata tulisi tehdä tarkempi arvio, miten säädöspohjaa kehitettäisiin siten, että jo olemassa olevia toimivaksi todettuja yhteistyömenettelyjä voidaan hyödyntää ehkäisevässä työssä ja toisaalta tietoturvaloukkaustilanteiden toipumisessa ja selvittämisessä voitaisiin tarjota mahdollisimman tehokkaasti keskitetty palvelu loukkauksen kohteena olevalle toimijalle sekä sen asiakkaille. Toimeenpanon tueksi tulisi tehdä myös riittävä arviointi osallistuvien toimialojen resursoinnista sekä uusien että jo olemassa olevien tehtävien osalta, jotta nämä tehtävät on mahdollista suorittaa linjausten esittämällä tavalla. Riittävän resursoinnin varmistamiseksi sekä viranomaistoiminnassa että siihen kytkeytyvässä yksityisessä palvelutuotannon ekosysteemissä tulee tehdä tarkempaa vaikutuksenarviointia. Ehdotusten 2 ja 3 osalta pätevät samat kommentit olemassa olevien rakenteiden huomioimisesta sekä toiminnan riittävä resursointi myös niiden kohteena olevissa toimijoissa. Lisäksi erityisesti ehdotuksen 3 osalta tulisi tarkastella ehdotetun koulutuksen suhde Digi- ja väestötietoviraston JUDO-hankkeessa tuottamaan koulutukseen, joka on kaikkien julkisen hallinnon toimijoiden saatavilla eOppiva.fi-oppimisalustalla.

Ehdotuksen 4 osalta vaikuttaa aiheelliselta tarkentaa muotoilua. Nykyinen muotoilu kertoo palvelun kyvystä auttaa tietoturvahaavoittuvuuksien korjaamisessa. Käytännössä haavoittuvuuksien korjaaminen kuulunee kuitenkin palvelun omistajan ja/tai sen tuottajan vastuulle. Näin ollen myös jälkimmäisten osalta tulisi varmistaa riittävä resursointi löydöksiin reagoimiseksi.

Ehdotukset 5-6 ovat kannatettavia. Viranomaisten yhteisen turvallisen tiedonsiirtopalvelun osalta DVV nostaa esiin Suomi.fi-palveluväylän, joka tarjoaa tietoturvallisen tiedonsiirtokanavan sekä viranomaisille että yksityisen sektorin käyttöön. Suomi.fi-palveluväylä tarjoaa teknisen tiedonsiirtokanavan lisäksi merkittävän luottamusinfra-struktuurin, johon liittyneet toimijat voivat luottaa tiedonvaihdon kohteena olevan osa-puolen organisaatioidentiteettiin ja joka omaa lukuisia mekanismeja mm. tietorajapintojen luvitusten hallitsemiseksi sekä lokitietojen hallinnoimiseksi. Lisäksi viranomainen voi tietoturvallisesti välittää Suomi.fi-viestit palvelun avulla viestejä kansalaisille ja viranomaisille. Digi- ja väestötietoviraston hallinnoima varmennepalveluinfrastruktuuri muodostaa laajasti käytetyn luottamuksen perustan viranomaisten turvalliseen tietojenkäsittelyyn.

Ehdotukset 7-13 koskevat tärkeitä aihealueita. Näiden linjauksien jatkovalmistelu ja toimeenpano tulisi suorittaa laajassa yhteistyössä osallistuvien viranomaisten kesken. Ehdotuksissa esitetään tietoturvasäännösten määrittämistä laintasoisesti, kun EU:n tietosuoja-asetus asettaa vastuun tietoturvallisuustoimenpiteiden riskiperusteisesta määrittämisestä rekisterinpitäjälle. Tämän osalta tarvittaneen jalkauttamisen tueksi selkeää ja tarkentavaa ohjeistusta sekä seurantaa linjausten mukaisten tavoiteltujen vaikutus-ten toteutumisen varmistamiseksi. Ehdotus 8 vaikuttaa päällekkäiseltä tiedonhallinta-lain (906/2019) 9 §:n mukaisen lausuntopyyntömenettelyn kanssa, joka kattaa myös tietoturvallisuutta koskevat kysymykset. Tällaista päällekkäistä lausuntomenettelyä tulisi välttää hallinnollisen taakan minimoimiseksi ja samalla ehdotettujen säädösten suhde tiedonhallintalakiin tulisi tarkentaa, jottei syntyisi päällekkäistä säätelyä ja soveltamisohjeita. Ehdotuksessa 10 nostetaan esiin lainsäädäntötasoinen määrittely kriittisten tietojen ja tietoaineistojen osalta sekä kriittisten tieto- ja tietoliikenneteknisen prosessien ja toimintojen osalta. Tämän määrittelyn toteuttaminen lainsäädäntötasolla vaatisi myös riittävän resursoinnin lainsäätäjille. Nopeasti kehittyvässä digitaalisessa toimintaympäristössä on myös haastavaa pitää lainsäädäntö ennakoitavana mutta riittävän ajantasaisena kehittyvä uhkaympäristö huomioiden. Ehdotuksen 12 mukainen ISO 27001 sertifioinnin edellyttäminen vaikuttaa selkeältä, DVV:llä ja sen edeltäjävirasto VRK:lla on ollut vastaava sertifiointi yhtäjaksoisesti vuodesta 2002 alkaen. Tämä vaikuttaa kuitenkin laajamittaisesti velvoittavana käytännön kannalta mahdollisesti erittäin haastavasti toteutettavissa olevalta sekä raskaalta toimenpiteeltä. Mikäli sertifiointia odotettaisiin kriittisten toimialojen toimijoilta, tulisi toimijat määritellä tar-kasti sekä linjata riittävän tarkasti, miten sertifiointi ulotetaan myös ko. toimijan alihankkijoita koskevaksi. Ehdotuksessa 13 esiin nostettu tavoite arviointilaitosten määrän lisäämisestä voi johtaa niiden hyväksymismenettelyn tason laskuun, joka ei välttämättä edistä tietoturvan tasoa. Arviointilaitoksia koskeva sääntely on verrattain vakiintunutta, jolloin arviointilaitosten määrä voidaan katsoa vakiintuneen niiden markkinakysyntää vastaavaksi. Määrä voisi nousta nykyiselläkin hyväksymismenettelyllä, jos tämän väli-raportin toimenpiteet nostavat niiden palveluiden kysyntää.

Ehdotuksissa 14-21 esitetään linjattavaksi useita yksittäisten kriittisten toimialojen velvoitteita. Ehdotukset ovat sinänsä kannatettavia, mutta samalla on huomioitava näidenkin toimialojen

riippuvuudet sekä toisistaan että riippuvuus yhteiseen digitaalisen palveluinfrastruktuurin. Näiden riippuvuuksien vuoksi asetetut vaatimukset ulottuvat myös niihin palveluihin, jotka ovat ko. palvelutuotannolle välttämätöntä. Riippuvuuksien tunnistamisessa avoin tiedonjako, yhteistyö ja etukäteisohjaus ovat osoittautuneet toimiviksi mekanismeiksi, joiden soveltaminen muuttuvaan toimintaympäristöön olisi joustavampaa kuin säädöspohjan uudelleen säätäminen.

Ehdotuksissa 22-27 esitetään linjattavaksi useita erityisesti julkista sektoria koskevia toimenpiteitä. Ehdotuksen mukaisesti Digi- ja väestötietovirasto pitää kannatettavana, että julkinen sektori tunnistetaan kriittiseksi toimialaksi. Digi- ja väestötietovirasto on eräs viranomainen, joka tuottaa yhteiskunnan digitaalisten palveluiden jatkuvuuden ja varautumisen kannalta keskeisiä digitaalisia palveluita käyttäen Valtorin tuottamia ICT-käyttöpalveluita. Ehdotus näiden palveluiden minimitason takaamisesta on kannatettava, mutta siihen liittyy seuraavia edelleen tarkemmin arvioitavia seikkoja. Ehdotuksen 22 mukaiset Valtorin järjestelmät ja prosessit vaikuttaisi kattavan vain Valtorin tuottamat ICT-käyttöpalvelut, sen sijaan niiden avulla tuotetut digitaaliset palvelut kuten hallinnon yhteiset Suomi.fi-palvelut tai muut viranomaisen tuottamat palvelut ja erityisesti niiden käyttäjien eli kansalaisten henkilötiedot ovat ko. palvelua tuottavan viranomaisen vastuulla. Tämän vuoksi substanssijärjestelmien käsittelemän tiedon tietoturvan ja tietosuojan lisääminen vaatisi tosiasiallisesti resursointia myös näiden substanssijärjestelmien sovellustason järjestelmien ja prosessien auditointiin. Ehdotuksessa 23 esitetään vaatimukseksi täyttää Katakri TL IV tason vaatimukset, tällaisten vaatimusten määrittäminen jälkikäteisesti jo olemassa oleville järjestelmille vaikuttaa haastavalta ja voi olla jopa mahdotonta valmisohjelmistojen tapauksessa. Ehdotuksessa 35 esitetään kehitettäväksi yksityishenkilöille ja organisaatioiden edustajille sovellus, jonka kautta on mahdollista saada tietoa ajankohtaisista uhkista sekä viestiä havainnoista viranomaisille. Suomi.fi-viestit mobiilisovellus on tällaiseen käyttötarkoitukseen sopiva tietoturvallinen kahdensuuntainen viestintäsovellus. Suomi.fi-viestit sovelluksen hyödyntäminen tähän tarkoitukseen olisi myös käyttäjäystävällistä, kun käyttäjän ei tarvitsisi asentaa tarpeettoman montaa sovellusta mobiililaitteisiinsa viestiäkseen valtion toimijoiden kanssa.

Linjausehdotuksille yhteisenä haasteena korostuu vaikeus määrittää yleistä kriteeristöä, miten määriteltäisiin järjestelmien kriittisyys ja onko järjestelmien kriittisyys lopulta kuinka tarkasti sidoksissa lausunnon taustatiedoissa mainittuun tavoitteeseen ”kansa-laisten tiedot olisivat nykyistä paremmin suojatut”. Digi- ja väestötietoviraston näkökulmasta keskeinen kansalaisten tietoja sisältävä tietovaranto on Väestötietojärjestelmä, jonka sisältämiä tietoja käytetään laajasti julkisella, yksityisellä ja kolmannella sektorilla palvelutuotantoon. Väestötietojärjestelmästä on rajattavissa henkilötietoja eri laajuisin ja käyttötarkoituksen perusteella rajattaviin käyttötarpeisiin. Näiden käyttötarpeiden mahdollistaminen tietoturva ja tietosuoja huomioiden on onnistunut monimuotoisessa palveluekosysteemissä menestyksekkäästi hyödyntäen olemassa olevaa säätelyä ja riskiperustaista tietoturvaperusteiden määrittämistä. Jos tällaiseen kokonaisuuteen lähdettäisiin soveltamaan kaavamaisesti esimerkiksi väliraportissa mainittuja ISO 27 001 tai Katakri TL IV kriteeristöjä voisivat vaikutukset toimijoiden tietoturvavaatimuksiin olla kohtuuttomia ja vaikeuttaa ajantasaisen henkilötiedon käyttöä palvelujen tuottamisessa, millä osaltaan turvataan henkilöiden oikeusturvan toteutumista. Myös muut Digi- ja väestötietoviraston tuottamat palvelut, kuten Suomi.fi-palvelut ja varmennepalvelut käsittelevät ja välittävät henkilöiden tietoja laajasti käyttäjäorganisaatioihin, jolloin osin samat havainnot koskevat myös näitä palveluita. Toisaalta raportin nykyisellä sanoituksella osa vaatimuksista on kovin yleisellä tasolla, esimerkiksi

linjausehdotuksessa 23 esitetty vaatimus PiTuKri-vaatimusten hyödyntämisestä on tulkittavissa huomattavasti lievemmäksi vaatimukseksi kuin vaatimus ko. kriteeristön täyttämisestä. Tällainen tulkinnanvaraisuus yhdistettynä varsin laajaan toimenpiteiden joukkoon aiheuttaa riskin siitä, että tietoturvan ja tietosuojan parantamiseksi tehtävien toimenpiteiden valinta ja kohdentaminen on entistä haastavampaa resurssien ollessa rajalliset.

Väliraportin muut osat, kommentit:

Väliraportin selvitysosassa esitetään linjausehdotuksen 12 mukaisen ISO 27 001 tieto-turvallisuuden hallintajärjestelmän käyttöönoton kustannukseksi 76 480 euroa. Tällaisen yksittäisen tai edes keskimääräisen arvion löytäminen on vaikeata, sillä organisaation lähtötaso hallintajärjestelmän käyttöönotossa voi vaihdella suuresti ja niilläkin organisaatioilla, joilla hallintajärjestelmä kattaa osan palveluista voi olla tarkoituksenmukaista ja oikeasuhtaista soveltaa hallintajärjestelmää vain osaan palveluistaan. Täten velvoittavien linjausehdotuksien tueksi vaikuttaisi tarpeelliselta tehdä edelleen tarkentava kustannusvaikutusten arviointia.

Lausuttavana oleva väliraportti nostaa esiin vuonna 2019 valmistuneen Suomen kyberturvallisuusstrategian ja sen vuonna 2021 valmistuvan toimeenpano-ohjelman. Väliraportissa todetaan, että toimeenpano-ohjelman ja väliraportit toimenpiteet muodostavat yhdenmukaisen ja toisiaan tukevan kokonaisuuden. Digi- ja väestötietovirasto nostaa edelleen tarpeelliseksi arvioida tämän kokonaisuuden suhdetta edellä mainittuihin, VAHTI-toimintaan sekä JUDO-hankkeeseen ja Haukka-toimeenpano-ohjelmaan.

Salovaara Timo
Digi- ja väestötietovirasto

Pitkänen Mikko
Digi- ja väestötietovirasto