Finnish Information Security Cluster (FISC) – Kyberala ry

Lausunto

15.07.2022

Asia: VN/30823/2021-LVM-15

Lausuntopyyntö luonnoksesta hallituksen esitykseksi sähköisen viestinnän palveluista annetun lain, henkilötietojen käsittelystä Puolustusvoimissa annetun lain ja henkilötietojen käsittelystä poliisitoimessa annetun lain muuttamisesta

Yleiset kommentit viranomaisten toimintamahdollisuuksista tietoturvaloukkauksien selvittämiseksi

Yleisiä kommentteja esityksestä ja sen tavoitteista, ehdotetuista keinoista ja vaikutuksista

Teknologiateollisuus sekä Kyberala kiittävät mahdollisuudesta lausua asiasta. Finnish Information Security Cluster – Kyberala ry on Teknologiateollisuus ry:n toimialayhdistys ja edustaa Suomessa toimivaa kyber- ja tietoturvallisuusalaa. Lausunto on Teknologiateollisuuden ja Kyberalan yhteinen.

1. Ehdotuksen tavoitteet: esityksen jatkovalmistelussa tulisi tunnistaa ja tunnustaa viranomaisten ja yksityisen sektorin välisen tietojenvaihdon esteet, esittää keinot niiden poistamiseksi ja laatia korjaavat säännösehdotukset.

Kannatamme esityksen tavoitteita ja katsomme, että toimijoiden välinen tiedonvaihto on välttämätöntä tietoturvaloukkauksien havainnoinnissa, torjunnassa ja selvittämisessä. On tärkeää, että viranomaisilla on tehokkaat, nopeasti käyttöön otettavissa ja toteutettavissa olevat keinot toimia vakavissa häiriötilanteissa tai niiden selvästi uhatessa.

Nyt esitetyt muutokset eivät kuitenkaan yksinään ole riittäviä, erityisesti kun tavoitellaan tietoturvaloukkausten ja -uhkien ennalta ehkäisemistä (torjunta), mahdollisimman varhaista havaitsemista sekä haitallisten vaikutusten poistamista.

Muistutamme, että valtaosa yhteiskunnan toiminnan kannalta elintärkeän tieto- ja viestintäteknisen infrastruktuurin toiminnasta sekä siihen liittyvien ja sitä hyödyntävien palveluiden tarjonnasta on yksityisen sektorin vastuulla. Vaikka näillä toimijoilla onkin laajasti laissa asetettuja velvoitteita tietoturvaloukkauksista tai palveluhäiriöistä ilmoittamisesta vastuuviranomaiselle tai ylipäätään riskienhallintatoimista, ehdotuksessa ei ole käsitelty varsinaisiin torjuntatoimiin liittyviä

toimenpiteitä esim. yritysten oikeudesta saada tietoja, kun viranomainen on saanut niitä tiedonvaihtoon perustuen. On selvää, että ilman yksityisen sektorin toimijoiden aktiivista mukanaoloa tietoturvaloukkausten torjumista, havaitsemista ja selvittämistä koskevat tavoitteet jäävät vajaiksi.

On myös tärkeää, että elinkeinoelämä otetaan alusta lähtien mukaan nyt lausuttavana olevaan esitykseen liittymättömässä sisäministeriön ja puolustusministeriön käynnistämässä laajemmassa selvityshankkeessa (PLM003:00/2022), jossa arvioidaan tätä esitystä laajemmin viranomaisten toimintaedellytyksiä kansallisen kyberturvallisuuden varmistamisessa, kyberrikollisuuden torjunnassa ja kyberpuolustuksessa. On epäselvää, miten elinkeinoelämän osallisuutta on tähän mennessä huomioitu. Kunnes kokonaistavoitetta koskeva yhteisymmärrys on saavutettu, asiassa ei ole perusteltua vedota hallinnonalarajoihin ja -vastuisiin.

2. Ehdotuksen käsitteistö: Kansallisen turvallisuuden sekä yhteiskunnan kriittisiin toimintoihin tai toimijoihin tai kriittiseen infrastruktuuriin viittaavat määritelmät tulisi tarkentaa.

Luonnoksessa tai perustuslain 10 §:n muuttamisen yhteydessä käytetty kansallisen turvallisuuden käsite ei nähdäksemme välttämättä vastaa EU:n perussopimuksissa tai niiden nojalla annetuissa oikeudellisesti sitovissa säädöksissä (asetukset, direktiivit ja päätökset) käytettyä ja EU-tuomioistuimen vakiintuneeseen käytäntöön perustuvaa kansallisen turvallisuuden käsitettä. Korostamme asian tärkeyttä, koska sillä on merkitystä arvioitaessa ehdotusten yhteensopivuutta mm. EU:n tietosuojasääntelyn, verkko- ja tietoturvadirektiivin (NISD) ja sen päivityksen (NIS2D) sekä valmisteilla olevan rahoitusmarkkinoiden digitaalista häiriönsietokykyä koskevan asetuksen (DORA) kanssa.

Esityksen haasteena näemme myös jossain määrin esitetyn SVPL 319 a §:n määritelmän. Säännöksen tavoite on ymmärrettävä ja sinällään kannatettava. Esityksessä ei ole kyse poikkeusolojen lainsäädännöstä, vaan sillä luodaan normaaliaikoina viranomaisille valtuuksia poikkeuksellisissa tilanteissa käytettäväksi, joihin viranomaisilla ei normaalisti olisi mahdollisuutta. Koska tietojenvaihto säännöksen tarkoittamissa tilanteissa voi kohdistua myös mm. perustuslailla ja tietosuojalainsäädännöllä suojattuun yksityiselämän suojaan ja määritelmän täyttyminen laukaisee viranomaisten oikeuden antaa tietoja, määritelmältä on voitava edellyttää mahdollisimman suurta selkeyttä. Näemme haasteena sen, että lainsäädännössämme yhä useammin viitataan yhteiskunnan kriittisiin toimintoihin tai toimijoihin tai kriittiseen infrastruktuuriin, mutta näille termeille ei ole yhtä täysin vakiintunutta, kaikkialla lainsäädännössä tunnustettua tarkkarajaista sisältöä.

Tyypillisesti, kuten tässäkin esityksessä viitataan valtioneuvoston huoltovarmuuspäätökseen (1048/2018). Luonnoksen sivulla 40 todetaan: ”Yhteiskunnan kriittisellä infrastruktuurilla tarkoitetaan jokseenkin vastaavaa, mitä kriittisellä infrastruktuurilla on tarkoitettu valtioneuvoston huoltovarmuuspäätöksessä (1048/2018).” Myöhemmin esityksessä todetaan sivulla 42: ” Edellä mainittuihin kriittiseen infrastruktuuriin kuuluviin toimintoihin joko suoraan tai välillisesti vaikuttava tietoturvaloukkaus tai sellaisen uhka on omiaan vaikuttamaan laajasti koko yhteiskuntaan varsinkin, jos loukkauksen vaikutukset kohdistuisivat samanaikaisesti useammalle kuin yhdelle alueelle. Laajoista keskinäisriippuvuuksista johtuen vaikutukset voisivat ulottua varsinaista hyökkäyksen kohdetta laajemmalle.” Käytetyistä sanoista, mm. ”jokseenkin” ja ”tai välillisesti” seuraa väistämättä,

että tulkinta ei ole kovin tarkkarajainen sen suhteen, milloin säännöksen tarkoittama tilanne on käsillä.

Virka-apua koskevat ehdotukset

Lausunnonantajien näkemyksiä virka-apua koskevista ehdotuksista

3. Vakavien tietoturvaloukkausten ja -uhkien selvittämisessä ja niiden vaikutusten poistaminen: lisätään perusteluosio viranomaisten ja hyökkäyksen kohteeksi joutuneen toimijan yhteistyöstä.

Ehdotuksen mukaan ”tietoturvaloukkauksen tai sen uhan vaikutusten poistamisella tarkoitettaisiin niitä teknisiä tai muita toimia, joilla poistetaan, lievennetään tai torjutaan selvitetyn loukkauksen tai sen uhan aiheuttama vaara tai muu vaikutus tietoturvallisuudelle tai muulle viestinnän luottamuksellisuudelle. Vaikutuksien poistamisella tarkoitetaan erityisesti toimia, joilla varmistetaan, ettei tieto- turvaloukkauksesta tai sen uhkasta aiheudu haittaa tietojen luottamuksellisuudelle, eheydelle ja saatavuudelle. Vaikutusten poistamisen osalta on kuitenkin huomioitava, että useassa tilanteessa vastuu vaikutusten poistamisesta on hyökkäyksen kohteeksi joutuneella toimijalla itsellään tai tämän palveluntarjoajalla.”

Säädösehdotusta on perusteltu eritoten vakavien tietoturvaloukkausten ja -uhkien selvittämisen ja niiden vaikutusten poistamisen tavoitteilla. Ehdotuksessa todetaan kuitenkin, että vastuu vaikutusten poistamisessa on käytännössä yksityisellä, ellei tietoturvaloukkauksen kohde ole itse viranomainen, sillä Suomessa on pelkästään huoltovarmuuskriittisiä yrityksiä n. 1500 kappaletta ja yhteensä 85 000 työnantajayritystä. Ehdotuksessa ei selvitetä juuri lainkaan vaikutusten poistamista, kun toimet ovat yksityisten varassa. Ehdotuksessa tulisi tehdä ymmärrettäväksi, miten tiedonvaihto edesauttaisi vaikutusten poistamista eritoten, kun lisäperusteena ehdotuksessa on esitetty, että tiedonvaihtoa tarvitaan virnaomaisen ”päätöksentekokyvyn turvaamiseksi”. Millaisia päätöksiä viranomaiset tulisivat tekemään? Olisiko kyse tietoturvaloukkaustilanteen johtamisesta vai kenties selvittämistyön suuntaamisesta vai jostain muusta? Miten viranomaistoiminnalla voitaisiin edesauttaa vaikutusten poistamista?

4. Virka-apua koskevat ehdotukset: Lisätään virka-apua koskeva 1) rajoitusharkinta sekä (2) yksityisen avunanto säädöstasolle.

SVPL:n virka-apua koskevassa 309 §:ssä, tai muussa soveltuvassa säännöksessä tulisi määritellä virka-apua koskevassa harkinnassa käytettävät kriteerit (eikä pelkästään hallituksen esityksen tasolla), sillä näillä on suora yhteys siihen, minkälaisia tapauksia voidaan pitää merkittävinä ja seurauksiltaan vakavina tietoturvaloukkaustilanteina, ja jotka voivat siten laukaista oikeuden ehdotuksessa tarkoitettuun tiedonvaihtoon ja virka-apuun. On huomattava, että myös virka-aputilanteessa toisen viranomaisen henkilöstö saa tosiasiallisesti tietoa muutoin tiedonvaihtoa rajoittavien säännösten estämättä.

Säädökseen tulisikin siten kirjata merkittävän ja seurauksiltaan vakavan tietoturvaloukkaustilanteen asiallisen soveltamisalan (ks. yllä kohta 2 ja siinä viittaus 319 §) lisäksi tilanteen intensiivisyyttä ja merkittävyyttä koskevat kriteerit, kuten vaikutusten laajuus ja kesto, maantieteellinen levinneisyys sekä viestintäpalvelujen käytettävyys, eheys tai viestinnän luottamuksellisuus (ks. NIS-direktiivissäkin tarkoitettu tapa). Direktiiviviittausta ei voitane pitää suositeltavana johtuen ko. direktiivin kokonaisuudistushankkeen vireillä ollessa.

Lisäksi lakiin tulisi lisätä tarpeelliset säännökset yksityisen antamasta virka-apuun rinnastettavasta avustamisesta. Ehdotuksen sivulla 23 todetaan, että ”tietoturvan osalta korostuu myös henkilöstön osaaminen, mikä etenkin erityisissä teknistä osaamista vaativissa tapauksissa voi olla vain muutamilla henkilöillä Suomessa tai jopa koko maailmassa.” Koska merkittävän ja seurauksiltaan vakavan tietoturvaloukkaustilanteen havainnointi, torjunta ja selvittäminen voi vaatia käytännössä kaikkien relevanttien viranomaisten henkilöstön käyttämistä omiin päätehtäviinsä, tarvittavaa asiantuntemusta voidaan joutua hankkimaan muualta, eritoten elinkeinoelämän toimijoilta.

Tähän tarkoitukseen esimerkkinä voisivat olla esim. Poliisilakiin sisältyvät säännökset avustamistyöstä, joiden tarkoituksena on mahdollistaa poikkeuksellisissa tilanteista nopeasti tarkoitukseen sopivan ulkopuolisen avun käyttäminen. Tällöin säännöstasolla voitaisiin mahdollistaa Liikenne- ja viestintäviraston käyttää apunaan soveltuvaa henkilöä yksittäisessä havainnointi-, torjunta- ja selvittämistehtävissä, joihin ei sisälly merkittävää julkisen vallan käyttöä. Avustustyöhön osallistunut on oikeutettu saamaan valtion varoista työhön käytetyn ajan mukaan lasketun kohtuullisen palkkion. Avustustyöstä voidaan laatia sopimus joko henkilön tai soveltuvaa osaamista tarjoavan yrityksen kanssa.

Lisäksi, kuten ehdotuksessa asianmukaisesti todetaankin, että ”useassa tilanteessa vastuu vaikutusten poistamisesta on hyökkäyksen kohteeksi joutuneella toimijalla itsellään tai tämän palveluntarjoajalla” tarkoittaa käytännössä sitä, että hyökkäyksen kohteen kaikki omat resurssit voivat olla käytössä tai jopa ylityöllistyneinä pitkän aikaa. On kuitenkin perusteltua olettaa, että merkittävissä ja seurauksiltaan vakavissa tietoturvaloukkaustilanteissa esim. kohdeorganisaation asiakkaiden, yhteistyökumppanien, muiden osallisten tai muutoin vaikutusten alaisten tahojen oikeuksien turvaaminen voi ylittää vastuutahon tosiasiallisen kyvykkyyden ja siten edellyttää laajojakin viranomaisten koordinoimia lisätoimia.

Viranomaisten välinen tiedonvaihto

Lausunnonantajien näkemyksiä viranomaisten välistä tiedonvaihtoa koskevista ehdotuksista

5. Viranomaisten tiedonvaihto: Viranomaisten luovuttaessa yrityksiä koskevia tietoja vakavien tietoturvaloukkausten ja -uhkien selvittämis- ja vaikutusten poistamistarkoituksessa tulee niiden ilmoittaa tietojen luovuttamisesta tietojen alkuperää koskevalle yritykselle.

Ehdotamme, että SVPL:ään lisätään säännös, jossa viranomaisten luovuttaessa tietoja toisilleen, tulee niiden ilmoittaa sille yritykselle, jonka tietoja on luovutettu, mitä tietoa ja milloin on luovutettu ja kenelle.

Lisäksi ehdotamme, että SVPL 316 §:n 4 momentin mukaista tietojen hävittämistä koskevaa säännös ja velvoite tietojen hävittämisestä lisätään 319 a §:ään, kun tiedot eivät enää ole tarpeen pykälässä tarkoitettujen tehtävien hoitamiseksi tai niitä koskevan rikosasian käsittelemiseksi.

6. Tiedonvaihdon ja yhteistyön parantaminen: tieturvaloukkausten yhteisilmoitus useammalle toimivaltaiselle viranomaiselle kerralla.

Koska kyseisen ehdotuksen tavoitteena on viranomaisten aiempaa tehokkaampi yhteistyö, joka korostuu erityisesti vakavissa tietoturvaloukkaus- tilanteissa, joissa viranomaisten on toimittava nopeasti yhteisymmärryksessä tietoturvaloukkauksesta johtuvien vaikutusten poistamiseksi ja vahinkojen minimoimiseksi tulisi samalla varmistaa, ja tarvittaessa antaa tarvittavat säädökset siitä, että Liikenne- ja viestintäviraston (Kyberturvallisuuskeskuksen) ylläpitämän tietoturvaloukkausten ilmoituspalvelun ja muidenkin vapaaehtoisten tai lakiin perustuvien tietoturvailmoitusten yhteydessä ilmoittajan on mahdollista antaa suostumuksensa/pyytää ilmoituksen välittämistä myös esitutkintaviranomaiselle (esim. poliisi), tietosuojavaltuutetulle sekä NIS-viranomaiselle. On ilmeistä, että ehdotuksen tavoitteet vakavien tietoturvaloukkausten ja -uhkien selvittämisessä ja niiden vaikutusten poistamiselle edellyttävät nopean ja tehokkaan tietoturvaloukkausta (tai epäiltyä sellaista) koskevan ilmoituksen välittäminen kerralla useammalle toimivaltaiselle viranomaiselle.

Lisäksi, koska laajemman viranomaiskentän erityisosaamisen hyödyntäminen oletetaan parantavan tietoturvaloukkausten ja -uhkien hallintaa ja analysointia ja sen tarjoavan hyökkäyksen kohteena olevalle taholle (pääosin yritykset) paremmat edellytykset hankkia tilanteen korjaamiseksi tarvittavat palvelut, olisi ehdotetun palvelumallin kehittäminen perusteltua vähintään samassa yhteydessä muiden muutosten kanssa. Ilman tällaista palvelumallin muutosta eivät myöskään muut, huomattavasti merkittävimmät salassapidon avulla suojattavien oikeushyvien vähäisenkään heikentämiseen ole asianmukaisesti perusteltavissa.

Viestinnän välittäjän oikeus luovuttaa tietoja viesteistä ja välitystiedoista

Lausunnonantajan näkemyksiä viestinnän välittäjän oikeudesta luovuttaa tietoturvaloukkauksia koskevia tietoja Liikenne- ja viestintävirastolle

-

Muita havaintoja

Muita havaintoja ehdotuksen sisällöstä

-

Vaikutukset

Millaisia vaikutuksia ehdotuksella on lausunnonanatajan toimialalla?

-

Sund Peter
Finnish Information Security Cluster (FISC) – Kyberala ry -
Teknologiateollisuus ry.