Finnish Information Security Cluster – Kyberala ry

Lausunto

05.01.2021

Asia: VN/24348/2020

Selvitys tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla; työryhmän väliraportti

Lausunnonantajan lausunto

Ehdotukset poliittisiksi linjauksiksi, kommentit:

Finnish Information Security Cluster – Kyberala ry (jäljempänä Kyberala) kiittää mahdollisuudesta lausua tietoturvan ja tietosuojan parantamiseksi yhteiskunnan eri sektoreilla koskevasta väliraportista. Kyberala pitää hyvänä, että liikenne- ja viestintäministeriö (LVM) on käynnistänyt otsikossa mainitun selvityshankkeen, sillä yhteiskunnan kyberturvallisuuden parantaminen sekä siihen liittyvään yhteistyöhön panostaminen on ensiarvoisen tärkeää Suomen menestymisen kannalta.

Ehdotukset poliittisiksi linjauksiksi

Viranomaisten yhteistyö (linjaukset 1–6)

Viranomaisten yhtenäisen tietoturvallisuusloukkaustilanteita koskevan säädöspohjan kehittäminen on tervetullutta ja perusteltua. Sitä luotaessa on kuitenkin muistettava, että myös yhteistyö ja tiedonvaihto yritysten kanssa on keskeinen osa kansallisen kyvykkyyden kehittämistä. Kyky nopeaan reagointiin yhdessä yrityskentän kanssa on tehokkain keino rajoittaa tietoturvaloukkauksesta aiheutuvia vahinkoja.

Liikenne- ja viestintäviraston Kyberturvallisuuskeskus on ollut erittäin hyvin toimiva kriittisten toimialojen yhteistyötä mahdollistanut viranomainen, ja yritykset ovat ilmoittaneet sinne havainnoistaan aktiivisesti. On jatkossakin huolehdittava, että viranomaisten tiedonvaihtoa kehitettäessä tämä onnistunut yhteistyö voidaan turvata ilman, että yritysten halukkuus tietojen ilmoittamiseen Kyberturvallisuuskeskukseen vähenisi.

Tietoturvallisuusloukkausten ehkäisy, selvittäminen ja hallinta edellyttävät poikkeuksetta sujuvaa yhteistyötä erityisesti kyberalan yritysten kanssa. Sen vuoksi on erittäin tärkeää, että alan kokemuksia ja olemassa olevia hyviä käytänteitä hyödynnetään, eikä sääntelyllä ainakaan muodosteta esteitä jo toimivien yhteistyötapojen käytölle.

Kyberturvallisuuskeskuksen resurssien kasvattaminen digitalisoituvassa yhteiskunnassa on perusteltua, mutta samalla on huomioitava, että kyberalan yritykset kärsivät tällä hetkellä merkittävästä osaajapulasta. On vältettävä tilanne, jossa julkisen sektorin henkilöresurssien lisääminen aiheuttaa kilpailun rajallisesta työvoimasta sekä syö samalla kasvu- ja kehittymispohjaa alan teollisuudelta. Viranomaisresurssien ja kyvykkyyksien kasvattamisen tulee sen vuoksi tapahtua pitkäjänteisesti ja asteittain korkeimpien riskien aloja priorisoiden sekä tarvittaessa olemassa olevia markkinoilta hankittavia palveluita hyödyntäen.

Kyberala ei pidä tietoturvallisuuden kartoituspalvelun tarjoamista viranomaistoimintona perusteluna tai tarpeellisena. Kyberturvallisuusala tarjoaa jo nykyisin runsaasti laadukkaita tietoturvallisuuden arviointi- ja kartoituspalveluja. Markkinat toimivat tällä hetkellä hyvin, tarjolla on useita erikoistuneita palveluita eri toimialoille ja kilpailutilanne on todettu toimivaksi. Viranomaisten ei tule ryhtyä tarjoamaan julkisin varoin ja resurssein tuotettavia palveluita, koska seurauksena olisi alan teollisuuden kehitystä heikentävä ja haitallinen markkinahäiriö. Erityisenä haasteena koetaan myös tilanne, jossa yksityinen sektori joutuu kilpailemaan kasvavasti julkisen sektorin kanssa alan väistämättä rajallisesta työvoimasta.

Vaatimukset (linjaukset 7–9)

Teknologian jatkuva nopea kehitys sekä siihen liittyvät kyberuhat muuttuvat nopeudella, joka on haastava tietoturvallisuutta ja tietosuojaa koskevan lainsäädännön näkökulmasta. Liian tarkkarajainen sääntely myös voi monesti myös olla vanhentunutta jo voimaan tullessaan. Samaan aikaan lakisääteisten tietoturvallisuusvelvoitteiden tulisi olla selkeitä, oikeasuhtaisia sekä Suomea koskevien EU- ja kansainvälisten velvoitteiden mukaisia.

Digitaalinen maailma riskeineen on moniulotteinen kansainvälinen kokonaisuus. Sen vuoksi myös ratkaisujen tulee mahdollistaa monimuotoisuus ja useat erilaiset tavat päästä turvallista ja kestävää toimintaa tukeviin tavoitteisiin. Kokemusten perusteella voidaan sanoa, että kovin yksityiskohtainen sääntely ja vaatimusmäärittely vaikeuttavat tietoturvan ylläpitämistä ja sen kokonaisvaltaista tehokasta kehittämistä. Samoin tiukka sääntely voi haitata organisaatioiden omien tietoturvakyvykkyyksien jatkuvaa riskiperusteista parantamista sekä heikentää väistämättä rajallisten turvallisuusinvestointien panos-tuotos-suhdetta.

Toimialojen tietoturvavaatimuksissa tulisi lähtökohtaisesti hyödyntää laajasti tunnustettuja kansainvälisiä standardeja, jotta kilpailukykyyn heikentävästi vaikuttavat mahdolliset kansalliset erityisvaatimukset eivät aiheuta suomalaisyrityksille markkinaongelmia. Hyvä tapa kehittää teknistä sääntelyä on myös tiivis osallistuminen ja vaikuttaminen kansainväliseen standardointiin.

Arvioinnit (linjaukset 10–13)

Tiedonhallintalainsäädäntö ja NIS-direktiivin luomat vaatimukset tarjoavat tällä hetkellä kehyksen kriittisten toimijoiden prosessien ja toimintojen määrittelylle. Erityisesti on huomioitava, että niistä poikkeavien kansallisten vaatimusten kehittäminen ja velvoittamaksi määritteleminen voi aiheuttaa arvaamattomia haitallisia seurauksia yritysten kilpailukyvylle. Samalla tietoturvallisuuden positiivinen mahdollistava ja edistävä ulottuvuus voisi jäädä monilta toimijoilta saavuttamatta.

Prosessien ja toimintojen tietoturvallisuuden laaja arviointi voi muodostua hyödylliseksi tavaksi tietoturvallisuuden kehittämiseen. Tässä on kuitenkin hyödynnettävä yleisesti tunnustettuja malleja sekä tarjolla olevia palveluita, ei kehittää erillistä julkista arviointipalvelua tai kansallisia erityisvaatimuksia.

Arviointien määrä huomioiden niiden toteuttaminen olisi myös lähtökohtaisesti mahdotonta pelkästään viranomaistoimin. Sen vuoksi mukaan arviointityöhön tarvitaan mittava joukko sertifiointilaitoksia, joilla on kansainvälisesti tunnustettu akkreditointi esimerkiksi mainittuihin ISO-standardeihin. Tällöin on kuitenkin muistettava, että sertifioinnin kustannukset voivat olla suuria ja jäädä siten joidenkin toimijoiden tavoittamattomiin. Laadukkaita arviointeja voidaan tehdä organisaatioissa myös itsenäisesti alan ammattilaisten avustamina. Tällaisissa tapauksissa voitaisiin hyödyntää esimerkiksi tietoturvasetelin kaltaista kannustetta tietoturvan ulkopuoliseen riippumattomaan arviointiin ja kehittämiseen.

Toimialojen erityispiirteet (linjaukset 14–21)

Kaikkiaan toimialakohtaisten erityispiirteiden tunnistaminen ja huomioiminen on tarpeellista, koska toimialojen tietoturvataso vaihtelee merkittävästi. Samojen toimien edellyttäminen kaikilta ei välttämättä johda hyvään lopputulokseen.

NIS-direktiivin uudistamistyöhön vaikuttaminen on perustelua.

On myös tärkeää, että poliisilla on resursseja tietoverkkorikostorjuntaan ja niiden ennalta estämiseen. On huomioitava, että verkkorikosten selvittäminen mahdollistuu monesti kyberalan

yritysten erityisosaamista hyödyntäen. Sen vuoksi on hyvin tärkeää, että pakkokeinolainsäädäntöä kehitettäessä yritysten näkökulmat otetaan tarkasti huomioon, eikä niille aseteta kohtuuttomia vaatimuksia, vaan rikostorjunnassa tehtävä yhteistyö perustuu molemminpuoliseen hyötyyn ja koko yhteiskunnan etuun.

Julkinen sektori kriittisenä toimijana (linjaukset 22–27)

Julkishallinnon on perusteltua panostaa aiempaa vahvemmin tietoturvallisuuden ja tietosuojan kehittämiseen erityisesti yhteiskunnan kriittisen palveluntuotannon jatkuvuuden ja sietokyvyn parantamiseksi. Valtaosa tästä tuotannosta toteutetaan käytännössä yksityisissä yrityksissä. Tämä luonnollisesti edellyttää julkisilta toimijoilta hyvää hankintapolitiikkaa ja -osaamista sekä uusien yhteistyömallien hyödyntämistä aiempaa rohkeammin.

Merkittävä osa tästä voidaan toteuttaa virkatyönä olemassa olevin henkilöstövoimavaroihin tukeutuen ja olemassa olevaa sääntelyä noudattaen sekä hyödyntämällä jo valmiiksi tarjolla olevia palveluita ja tuotteita entistä laajemmin ja tehokkaammin. Esimerkiksi tietosuojan tai tietoturvan tason selvittämiseksi palvelut voidaan hankkia sujuvasti alan yrityksiltä. Näin voidaan toimia tehokkaasti, luotettavasti ja kokonaistaloudellisesti.

Tietosuojasääntelyn kehittäminen (linjaukset 28–34)

Tietosuojan osalta on huomioitava, että sitä ohjaa EU:n yleinen tietosuoja-asetus GDPR, joka velvoittaa jo nykyisellään sekä yrityksiä että viranomaisia. Tähän liittyen tietosuojavaltuutetun toimiston perusvoimavaroja on syytä vahvistaa, jotta se kykenee tarjoamaan yrityksille nykyistä konkreettisempaa ohjeistusta asiasta.

Erilaisia tietosuoja-arviointeja toteutetaan yrityksissä nykyisin säännöllisesti. Samoin tietosuojan sertifiointiin on olemassa tunnustettuja kehyksiä (esimerkkinä ISO27701) ja kypsyysmalleja kehitetään jatkuvasti. Mikäli väliraportissa esitetyillä toimenpiteillä tarkoitetaan uuden kansallisen tietosuojasertifikaatin kehittämistä, siihen tulee suhtauta hyvin varovasti huomioiden, että tietosuojan sääntelykehys on koko EU:n laajuinen ja ainoastaan kansallisen lisäkuormitusta tuottavan sertifikaatin luominen ei ole perusteltua. Huomioiden kansainvälisten mallien perusperiaatteet, linjausten pohjalta jää varsin epäselväksi, miten eteneminen tietosuojan sertifioinnissa käytännössä toteutuisi.

Uudet toimintatavat (linjaus 35)

Uudet ja helppokäyttöiset toimintatavat sekä sovellukset ovat tervetulleita tietoturvallisuuden kehittämisessä. Suomessa on runsas joukko yrityksiä, jotka kykenevät kehittämään raportissa kuvatun mobiilisovelluksen. Sovellusta kehitettäessä on tärkeää, että ilmoittaminen viranomaisille voisi tapahtua yhteen yhteyspisteeseen, mutta tarvittaessa myös valikoiden mille viranomaiselle ilmoituksen haluaa tehdä.

Väliraportin muut osat, kommentit:

Keskeisimmät havainnot ja esitykset jatkotyöhön:

1) Työryhmän jatkotyöhön tarvitaan mukaan yritysten ja elinkeinoelämän edustajia. Kaikki tietojärjestelmät, niiden tietoturvallisuus, ylläpito ja kehittäminen tehdään lähes poikkeuksetta yrityksissä. Valmistelussa tulee siksi arvioida huolellisesti ehdotusten vaikutukset tietoturvallisuustuotteita ja -palveluita tarjoaviin kyberalan yrityksiin ja niiden kilpailumahdollisuuksiin sekä laajemmin eri elinkeinoelämän toimijoihin. Annetussa aikataulussa vaikutusarviointi on hyvin haastavaa ja siksi jatkotyössä olisi huolella arvioitava eri toimenpiteiden ja linjausten yhteisvaikutuksia.

2) Viranomaisten kyberturvallisuuteen osoitettujen resurssien parantaminen on perusteltua, mutta viranomaisten ei tule rakentaa alan yritysten palveluiden kanssa kilpailevaa julkisin varoin rahoitettua palvelutuotantoa. Viranomaisen tulee keskittyä edistämään ja mahdollistamaan yhteiskunnan kriittisten toimijoiden käyttämien palveluntarjoajien toimintaa, ei rakentamaan yritysten palveluiden kanssa kilpailevaa julkista palvelutarjontaa ja kilpailemaan rajallisesta osaavasta työvoimasta.

3) Väliraportin ehdotukset valvonnan, tarkastusten ja sertifiointien osalta edellyttävät suuria taloudellisia panostuksia sekä viranomaisilta että yrityksiltä. Merkittävimmät panostukset tulisi kuitenkin suunnata varsinaisiin tietoturvallisuustoimenpiteisiin, ei vaatimusten määrittelyyn ja niiden valvontaan. Sen vuoksi on ensiarvoisen tärkeää luoda uusia turvallisuusinvestointeihin kannustavia ja niitä mahdollistavia rakenteita, yhteistyömalleja sekä kaikki toimijat huomioivia tukitoimia ja kannustimia. Näistä esimerkkinä mm. kyberalan aiemmin esittämä tietoturvasetelin käyttöönotto sekä muut vastaavat menettelyt ja uudet rakenteet.

4) Raportissa tulee huomioida vireillä olevat EU:n lainsäädäntöhankkeet sekä linjausten suhde EU-sääntelyn kokonaisuuteen. Vireillä olevia ajankohtaisia hankkeita ovat esimerkiksi verkko- ja tietoturvadirektiivin (NIS) päivittäminen sekä rahoitusmarkkinoiden digitaalista häiriönsietokykyä koskeva asetus (DORA). Lisäksi sertifiointitoiminnassa tulee ottaa tarkasti huomioon kansainvälinen kehitys ja menettelytavat sekä nojautua siinä kansainvälisiin tunnustettuihin standardeihin markkinaongelmien välttämiseksi.

5) Väliraportissa on joukko kannatetavia linjauksia, mutta niistä olisi tarpeen priorisoida vaikuttavimmat sekä samalla tunnistaa toimenpiteet, jotka voidaan toteuttaa jo nykyisen sääntelyn puitteissa olemassa olevia toimivaltuuksia hyödyntämällä.

Muut yleiset huomiot

Laadukkaalla sääntelyllä, valvonnalla, oikein suunnatuilla investoinneilla ja hyvällä osaamiselle voidaan luoda olosuhteet kriittisten toimintojen kannalta riittävän tietoturvallisuuden ja tietosuojan tason saavuttamiselle sekä ylläpitää tärkeää luottamusta yhteiskunnan kaikkiin kriittisiin digitaalisiin toimintoihin. Sääntely on kuitenkin hidas ja monin paikoin myös haastava keino hallita ja edistää tietoturvallisuuden kehittymistä erittäin nopeasti muuttuvassa ympäristössä.

Väliraportin johdanto-osassa käsitellään kattavasti tietoturvallisuuden ja tietosuojan eri ulottuvuuksia mukaan luettuna niiden yhteiskunnallinen ja taloustieteellinen merkitys. Sääntelyn merkitys tietoturvan ja tietosuojan kehittämisessä on väistämättä monitahoinen. Sääntelyllä voidaan ohjata toimintaa haluttuun suuntaan, mutta samalla yksityiskohtaisesti määritellyt velvoitteet voivat suunnata organisaatioiden toimintaa liikaa vain lain edellyttämän ja ulkoa tuodun minitason saavuttamiseen. Tällöin organisaation varsinaiset riskienhallintaprosessin kautta nousevat kaikkein olennaisimmat toimenpiteet voivat jäädä sivuosaan. Tietoturvan ja tietosuojaan panostaminen tulisi aina kokea tarpeellisena ja hyödyllisenä investointina, ei niinkään ulkopuolisen regulaattorin edellyttämänä pakollisena kulueränä.

Tietoturvallisuutta ei ole mahdollista kehittää hyppäyksenomaisesti, vaan se edellyttää pitkäjänteistä ja suunnitelmallista kehittämistä. Kaikkiaan yhteiskunnan kyberturvallisuuden laaja-alainen kehittäminen voidaan toteuttaa ainoastaan julkisen ja yksityisen sektorin hyvällä yhteistyöllä, jossa molemmilla on oma tärkeä roolinsa. Viranomaisen tulee edistää palveluntarjoajien toimintaa sekä mahdollistaa onnistunut tiedonvaihto kaikkien toimijoiden välillä. Toisin sanoen luoda olosuhteet, jotka tukevat keskeisten kyvykkyyksien kehittymistä, tietoturvallisuustuotteiden ja -palveluiden laajaa hyödyntämistä sekä yhteiskunnan sietokykyisyyden vahvistumista digitaalisessa maailmassa.

Susi Mika
Finnish Information Security Cluster – Kyberala ry