Fortum Oyj

Lausunto

05.01.2021

Asia: VN/24348/2020

Selvitys tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla; työryhmän väliraportti

Lausunnonantajan lausunto

Ehdotukset poliittisiksi linjauksiksi, kommentit:

Fortum Oyj kiittää mahdollisuudesta antaa lausunto väliraporttiin koskien tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla (Diaari VN/24348/2020). Lausunto on tehty Corporate Security-yksikön toimesta.

Pidämme tervetulleena tietoturvallisuuden esille nostamista, vaikkakin esityksessäkin mainittu taustalla oleva tapaus on hirvittävä. Pidämme myös tervetulleena asian tarkastelua laajemmin ja kokonaisvaltaisemmin kuin vain yksittäisten toimijoiden näkökulmasta.

Väliraportin muut osat, kommentit:

Kommentit raportissa esitettyihin ehdotuksiin

Ehdotus 1

Viranomaisten välinen yhteistyö on tärkeää tietoturvaloukkausten ehkäisyssä ja selvittämisessä. On kuitenkin syytä huomata, että viranomaiset eivät ole oma muista erillinen tai riippumaton toimintaympäristö. Viranomainen voi olla ensisijainen tai välillinen kohde aivan samoin kuin muutkin yhteisöt. Syynä, lähteenä tai kohteena loukkaukselle voi olla yritys tai muu organisaatio, joka ei ole viranomainen. Tämän vuoksi tarkastelua ei tulisi rajata liian suppeaksi.

Ehdotus 2

On kannatettava ehdotus. Hieman epäselväksi jää tarkoitetaanko ehdotuksessa jokaiselle kriittiselle toimijalle vai jokaiselle kriittiselle toimialalle perustettavaksi asiantuntijapalvelu. Tässä tulisi huomata edellisessä kohdassa kommentoitu rajaus. Myös yrityksillä on tarvetta tällaiselle palvelulle,

erityisesti kyberturvallisuuskeskuksen kansainväliset yhteydet tulisi saattaa muidenkin kuin vain viranomaisten käyttöön.

Ehdotus 3

Kannatettava ehdotus.

Ehdotus 4

Kannatettava ehdotus.

Ehdotus 5

Kannatettava ehdotus.

Ehdotus 6.

Kannatettava ehdotus.

Ehdotus 7.

Vastuu tietoturvallisuudesta huolehtimisesta ja sen vastuuttaminen olisi hyvä määritellä lainsäädäntötasolla mutta varsinaiset tietoturvallisuusvaatimuksien määrittelyt tulisi tehdä harkitusti ja toimialakohtaisesti huomioiden palveluiden toimintaympäristö ja edellytykset. Tietoturvallisuudella ei välttämättä ole itseisarvoa, tästä syystä sen mitoitus (vaatimukset ja tavoitteet) tulisi olla linjassa liiketoiminnan ja sitä ohjaavan muun lainsäädännön kanssa.

Harkinnan arvoinen lähestymistapa voisi olla; jossa viranomainen tuottaisi uhkaskenaarioita toimialakohtaisiksi suunnitteluperusteiksi. Tällöin toimialalla toimivat yritykset voisivat hyödyntää tietoturvallisuuden suunnittelussa, mitoituksessa ja testaamisessa samankaltaisia riski- ja uhkakuvia. Tämän seurauksena toimialat varautuisivat kokonaisvaltaisesti samankaltaisiin uhkiin. Lisäksi tämä mahdollistaisi kumppaneille asetettavien vaatimusten yhdenkaltaisuuden.

Ehdotus 8.

Tämä ehdotus on kirjoitettu epäselvästi. Viittaako toimiala vain viranomaisiin vai sisältyykö siihen myös yritysmaailma?

Ehdotus 9.

Kannatettava ehdotus. Epäselväksi jää onko vaatimukset sitovia ja jos ovat niin sitovatko vain viranomaisia vai myös muita yhteisöjä.

Ehdotus 10.

Kannatettava ehdotus. Tämä on perusedellytys tehokkaan tietoturvallisuustyön toteuttamiselle. Linjauksessa voisi harkita lisättäväksi kartoituksen piiriin myös velvoite tunnistaa kriittiset riippuvuudet ulkopuolisista toimijoista tai palveluista.

Ehdotus 11.

Periaatteessa kannatettava ehdotus. Haasteena voi olla lainsäädäntötasolla määritellä eri yhteisöille yksilöivästi mikä tieto tai järjestelmä on kriittinen milläkin hetkellä. Myös riskitilanteet muuttuvat Auditointi itsessään ei välttämättä paranna tilannetta, vaan parannus edellyttää korjaavia toimenpiteitä.

Ehdotus 12.

Tietoturvallisuuden hallintajärjestelmän sertifioinnin lisäarvo jäänee pieneksi mikäli Ehdotus 11 toteutetaan esitetyllä tavalla.

Sertifiointivelvoitteen määritteleminen yrityksen koon mukaan ei ole linjassa kansallisen turvallisuustason parantamisen kanssa, koska merkittävä osuus kriittisillä aloilla olevista yrityksistä ovat pieniä tai keskisuuria henkilöstömäärän perusteella (ks. väliraportin taulukko 3). Toisin sanoen, huomattava osa kriittisistä toimijoista jäisi sertifiointivelvoitteen ulkopuolelle eikä näin ollen kansallisen turvallisuuden kannalta toivottava vaikutus toteutuisi.

Mikäli sertifiointivelvoite annetaan, tulisi sertifiointi pystyä rajaamaan kriittisiin toimintoihin yrityksen koosta riippumatta siten että kaikille asetetaan samat velvoitteet.

Tietoturvallisuus on mahdollista toteuttaa ilman että hallintamallia sertifioidaan. Sertifioinnin toteutus (projekti) ja ylläpito aiheuttaa lisäkustannuksia toimijoille, joten mikäli sertifiointivaatimus asetetaan on siitä tuleva hyöty oltava tarkasti määritelty sekä mitattavissa.

Tietoturvallisuuden hallinta on oltava linjassa yrityksen muun johtamisjärjestelmän kanssa. Mikäli ei ole selkeitä syitä edellyttää tiettyä viitekehystä (esim. ISO 27001) olisi suotavaa jättää viitekehyksen valinta yrityksen vastuulle. Näin yritys voisi itse varmistaa että valittu viitekehys sopii tukemaan liiketoimintaa.

Sertifiointiehdotuksen toteutus edellyttää että linjaus 13 viedään nopeutetulla aikataululla käytäntöön.

Ehdotus 13.

Kannatettava ehdotus. Tulee kuitenkin huomioida, ettei arviointimenettely vääristä kilpailua toimialalla.

Huhta Jarmo
Fortum Oyj