Finnish Information Security Cluster (FISC) – Kyberala ry

Lausunto

15.07.2022

Asia: VN/18738/2022

Luonnos valtioneuvoston asetukseksi tietoturvan kehittämisen tuesta

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

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. Haluamme tarkentaa seuraavia kohtia:

1. Ehdotuksen tavoitteet: Kannatamme vahvasti esityksen tavoitteita ja pidämme välttämättömänä, että erityisesti digitalisaation voimakkaasti kehittyessä ja turvallisuusympäristön nyt nopeasti muuttuessa panostetaan riittävästi koko yhteiskunnan digitaaliseen turvallisuuteen.

Lisäbudjetissa ehdotettu 6 M€ on merkittävästi liian pieni summa laajan yhteiskunnallisen digitaalisen turvallisuuden kehittämishaasteen ratkaisemiseksi. Summan tulisi olla vähintään jo aiemmin ehdottamamme 15 M€ suuruinen. Paljoksumme myös arvioituja yli 10% hallintokuluja. Hallintokulujen tulisi olla enintään 5%.

2. Yritysten tietoturvallisuuden vahvistaminen: tietoturvasetelin käyttöala tulisi rajata ainoastaan PK-sektorin työnantajayrityksille sekä järjestöille siten, että tukisumma voi olla suurempi, mikäli yritys toimii myös yhteiskunnan toiminnan kannalta kriittisellä alalla.

Muistion mukaan ”Muuttuneen turvallisuusympäristön kehityksen myötä on entistä keskeisempää kiinnittää huomioita laaja-alaisesti yhteiskunnan kyberturvallisuuteen ja varmistaa kyberturvallisuuden korkea taso yhteiskunnan kaikilla sektoreilla siten, että eri sektoreilla toimivat organisaatiot ovat varautuneet kyberturvallisuusuhkiin ja -loukkauksiin. Etenkin pienten ja keskisuurten yritysten sekä yhdistysten osalta on havaittu tarve parantaa niiden varautumista

kyberturvallisuusuhkiin ja -loukkauksiin ja kehittää niiden toimintaa, tietojärjestelmiä, sähköisiä palveluja kuin myös kyberturvallisuusosaamista.”

Näin ollen yllä mainittuun liittyen yhteiskuntamme digitaalisen resilienssin tulisi perustua siihen, että mikään organisaatiosegmentti ei jää jälkeen digitaalisten riskien torjunnassa ja toiminnan jatkuvuuden hallinnassa.

On tiedossa, että huoltovarmuuskriittiset yritykset ovat usein myös kooltaan suurempia, jolloin toisin kuin PK-sektorilla, niillä on sekä omaa vahvaa tietoturvallisuusosaamista, että muun sääntelyn kautta jo olemassa olevia säädös- tai sopimusperustaisia velvoitteita digitaalisten riskien hallintaan. Lisäksi Suomen Yrittäjien tuoreen gallupin mukaan on tiedossa, että nimenomaan PK-sektorilla lähes puolet yrityksistä ei tiedä miten toimia tietoturvaloukkaustapauksissa ja n. 60% prosenttia pk-yrityksistä kokee esteitä tietoturvan toteutumisessa. Näistä merkittävimpiä ovat osaamisen puute ja tietoturvan kustannukset.

Tulosten perusteella voidaan todeta, että vaikka digitaalinen turvallisuus on yhä olennaisempi osa yritysten liiketoiminnan riskienhallintaa, nimenomaan monen pk-yrityksen tietoturva alimitoitettua. Digitaalista turvallisuutta olisi parannettava niin yritysten käytössä olevien järjestelmien tietoturvan kuin henkilöstön tietoturvaosaamisen osalta. Yksi keskeinen kehittämisen kohde on pk-yritysten kyky arvioida ja seurata oman tietoturvansa tasoa sekä tehdä tietoturvaa lisääviä järjestelmä- ja palveluhankintoja. Tämän kaltaisen palvelun (tietoturvan arviointi ja hankinta) tulisikin kuulua tuettujen palveluiden piiriin.

Koska ehdotuksessa tukeen osoitettu 6 M€ rahamäärä on varsin rajallinen, vaatimus siitä, että tuen saadakseen yrityksen (tai muun toimijan) tulee toimia kriittisellä toimialalla tarkoittaa, että valtaosa Suomen pk-yrityksistä jää kokonaan tuen ulkopuolelle. Valtioneuvoston määritelmän mukaisessa huoltovarmuustoiminnassa on mukana vain 1000–2000 yritystä, kun taas Suomessa on kuitenkin 85 045 työnantajayritystä (2019) ja yhteensä 292 377 (ei-työnantajayritykset ml.) yritystä.

Lisäksi kiinnitämme huomiota siihen, että Huoltovarmuuskeskuksen hankeportfoliossa on jo 130 M€ varattuna huoltovarmuuskriittisiä yrityksiä hyödyttävään yhteiskunnan digitaalista turvallisuutta parantavaan työhön vuosina 2021–2026 (Digitaalinen turvallisuus 2030). Näin huoltovarmuuskriittiset yritykset, joilla on jo muutenkin keskimääräistä paremmat resurssit turvallisuustyöhön, voivat myös huoltovarmuustoiminnan kautta saada monenlaista merkittävää tukea omaan digitaaliseen varautumistyöhönsä ja erilaiseen hanketoimintaan. Tämän instrumentin käytön mahdollisuudet tulisikin hyödyntää täysimääräisesti ja tarvittaessa kehittää aiempaa vaikuttavammaksi.

Tuen kohdentaminen yhdessä edellä kerrotun kanssa johtaa siihen, että tietoturvallisuuden kypsyyden erot kriittisten ja muiden yritysten välillä kasvavat entisestään. Valtioneuvoston ajankohtaisselonteossa turvallisuusympäristön muutoksesta (13.4.2022) mukaisesti tulee huomioida, että tietoturvaloukkauksista voi syntyä laajojakin heijastevaikutuksia, jotka vaikuttavat laajasti suureen joukkoon eri toimijoita. On vältettävä kehitystä, jossa erityisesti pk-yrityssektori

eriytyy yhä pahemmin varautumiseltaan vahvoihin kriittisten alojen yrityksiin ja heikkoihin muiden alojen yrityksiin. Kyberturvallisuuden tason nostaminen organisaatioissa parantaa tosiasiallisesti myös työtekijöitä ja asiakkaita koskevaa tietosuojaa.

3. Tuensaajan omavastuuosuus: Esitämme, että käyttöön otetaan kaksi eritasoista tukiluokkaa: 15 000 € ja 75 000 €. Näistä suuremmalla voisi kattaa 70 prosenttia tietoturvaprojektin kuluista, eli hakijan omavastuuosuus projektin rahoituksesta olisi 30 prosenttia. Pienemmässä tukiluokassa tuensaajalla tulisi olla 20% omavastuuosuus.

Tietoturvallisuuden kehittäminen on pitkäjänteistä toimintaa, jolla ei ole varsinaista päätepistettä. On tärkeää, että nyt esitetyllä tuella kehittämistoimet saadaan liikkeelle ja merkittävimpiä riskejä pienennettyä. Siksi tukea saavan yrityksen (tai muun toimijan) sitoutuminen kehittämiseen on tärkeää. Omavastuuosuus mahdollistaisi myös sen, että useampi PK-yritys pääsisi hyödyntämään tukea.

4. Hyväksytyt palveluntarjoajat: sallittujen palveluntarjoajien tulee olla Suomeen rekisteröityneitä yhtiöitä.

Muistiossa todetaan ansiokkaasti, että ”Tietoturvan kehittämistuella myös vauhditettaisiin suomalaisen kyberturvallisuustoimialan ja -markkinan kehitystä sekä luodaan uutta liiketoimintaa toimialle ja kyberturvallisuusosaamista Suomeen parantaen muun muassa Suomen kyberturvallisuuden omavaraisuutta.” Ottaen huomioon ko. tavoitteet ja niiden tunnistaminen myös huoltovarmuuden näkökulmasta mm. Valtioneuvoston ajankohtaisselonteossa turvallisuusympäristön muutoksesta (13.4.2022), Valtioneuvoston päätöksessä huoltovarmuuden tavoitteista (1048/2018) sekä Kyberturvallisuuden kehittämisohjelmassa (LVM 2021:7) on perusteltua, että tuetaan nimenomaan Suomeen rekisteröityneiden palveluntarjoajien kehittymistä.

5. Tuettavien kustannusten ajallinen takaraja: Ehdotamme, että aikaraja siirrettäisiin esim. vuoden 2024 loppuun.

Asetusluonnoksen 2 §:n 3 momentin mukaan tukea voidaan myöntää vain kustannuksiin, jotka syntyvät tukihakemuksen jättämisen jälkeen ja viimeistään 30.6.2024. Huomioiden asiaan liittyvät tarpeet, esitetty takaraja 30.6.2024 arvioidaan liian tiukaksi.

Kiinnitämme huomiota siihen, että yritysten kannalta on erittäin tärkeää, että tuen hakuprosessi, tarvittavat selvitykset ja myöntökriteerit avataan riittävän ajoissa niin, että niiden tukemana on helppo arvioida oman yrityksen soveltuvuus tuen saajaksi samoin kuin se, miten tukea haetaan ja mitä selvityksiä tarvitaan. On myös välttämätöntä, että epäselvyyksien varalta on olemassa

neuvontapiste, johon voi olla tarvittaessa yhteydessä. Liikenne- ja viestintäviraston Kyberturvallisuuskeskus ei myöskään liene laajalti tunnettu kaikissa tukeen oikeutetuissa yrityksissä ja siksi onkin mielestämme tärkeää, että viranomainen tukeutuu tuen toimeenpanon valmistelussa, neuvonnassa ja viestinnässä kohderyhmän yrityksiä edustaviin sidosryhmiin samoin kuin pk-yrityksille avustuspalveluja tarjoaviin muihin julkistoimijoihin. Kyberala ry. voi ottaa neuvontatehtävän vastaan julkistoimijalta erikseen siitä ja kustannusten korvaamisesta sovittaessa.

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