Elinkeinoelämän keskusliitto EK

Lausunto

14.07.2022

Asia: VN/18738/2022

Luonnos valtioneuvoston asetukseksi tietoturvan kehittämisen tuesta

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

Kiitämme lausuntomahdollisuudesta ja toteamme seuraavaa:

Pidämme esityksen tavoitteita erittäin kannatettavina. On tärkeää, että muulloinkin, mutta erityisesti turvallisuusympäristön nyt nopeasti muuttuessa ja digitalisaatiokehityskin huomioiden panostetaan riittävästi tieto- ja kyberturvallisuuteen koko yhteiskunnassa. Digitalisaatiotakaan ei voida kestävästi kehittää ja hyödyntää ilman, että tietoturvallisuus on kehittämisessä kaiken aikaa mukana. Se on toisaalta digitalisaation mahdollistaja, toisaalta sen elinehto. Turvallisuustilanteen muuttumiseen liittyvät uhat tuovat tarpeeseen oman lisänsä.

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

Viittaamme jäsenyhdistystemme Teknologiateollisuus ry:n ja Kyberala – FISC ry:n yhteiseen lausuntoon ja ehdotamme tuen kohdentamisen, omavastuuosuuden ja tuen käyttämisen määräajan osalta muutoksia seuraavasti:

1. Tuen kohdentaminen

Muistiossakin todetaan mielestämme (s. 1) aivan oikein, että ”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.”

Tämä on nähdäksemme aivan oikein todettu ja kannatettavaa. Koska po. määräaikaiseen tukeen osoitettu 6 M€ rahamäärä on kuitenkin melko rajallinen, vaatimus siitä, että tuen saadakseen yrityksen (tai muun toimijan) tulee toimia kriittisellä toimialalla tarkoittaisi, että valtaosa Suomen pk-yrityksistä jää kokonaan tuen myöntökriteerien ulkopuolelle: Huoltovarmuustoiminnassa on mukana vain 1000–2000 yritystä ja Suomessa on (vuosi 2019) kuitenkin laskentatavasta riippuen yhteensä 85 045 (vain työnantajayritykset) – 292 377 (ei-työnantajayritykset ml.) yritystä.

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 näkee esteitä oman tietoturvallisuutensa toteutumisessa. Näistä merkittävimpiä ovat osaamisen puute ja tietoturvan kustannukset.

Kiinnitämme huomiota myös 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, joskaan ei suoraa rahallista tukea niin asiantuntijatuen, yhteisen harjoittelun ja muun toiminnan kautta merkittävästi tukea omaan varautumistyöhönsä.

Tuen kohdentaminen luonnoksessa esitetyllä tavalla yhdessä edellä kerrotun kanssa johtaisi siihen, että tietoturvallisuuden kypsyyden erot kriittisten ja muiden yritysten välillä tulisivat kasvamaan entisestään. Tämä olisi erittäin huono kehityssuunta voimakkaasti keskinäisverkottuneessa yhteiskunnassa.

Kuten esityksessäkin todetaan, muuttuneen turvallisuustilanteen ja nopean digitalisaatiokehityksen takia yhteiskunnan tietoturvallisuutta on pyrittävä vahvistamaan laajasti, suunnitelmallisesti ja monipuolisesti. On vältettävä kehitys, jossa erityisesti pk-yrityssektori eriytyy yhä pahemmin varautumiseltaan vahvoihin kriittisten alojen yrityksiin ja heikkoihin muiden alojen yrityksiin. Kyberturvallisuuden tason nostaminen organisaatioissa parantaa tosiasiallisesti myös työntekijöitä ja asiakkaita koskevaa tietosuojaa.

Tämän vuoksi esitämme, että esitetty tuki tulisi rajata ainoastaan pk-sektorin työnantajayrityksille sekä järjestöille siten, että tukisumma voisi olla suurempi, mikäli yritys toimii lisäksi yhteiskunnan toiminnan kannalta kriittisellä alalla.

Vaikka tuen kohdentamista ei muutettaisi esittämällämme tavalla, on joka tapauksessa tärkeää, että viranomaiset yhdessä yrityskentän ja kyberalan sidosryhmien kanssa valmistelevat toimia myös muiden kuin kriittisten alojen yritysten kyberturvallisuuden kohentamiseen. Toimet voisivat käsittää yleisen tietoturvatietoisuuden kasvattamiseen tähtäävän viestinnän lisäksi esimerkiksi käytännönläheisiä koulutuksia, oppaita sekä yhteiskunnan eri sektorien yhteisiä kyberturvaharjoituksia.

Huoltovarmuuskeskuksen toiminnassa kehitetään paljon työskentelymalleja ja työkaluja varautumiseen. Olisi hyvä, että näitä voitaisiin mahdollisimman paljon avata yleiseen käyttöön huoltovarmuustoiminnan fokuksen siitä kärsimättä. Samoja työskentelymalleja ja työkaluja voivat yleensä käyttää muutkin kuin kriittiset organisaatiot omassa varautumistyössään.

Mikäli tuen kohdentamista ei muutettaisi esityksestä, esitämme, että jos nyt esitettävän määräaikaisen tuen kokemukset ovat hyviä, tukea tulisi myöhemmin jatkaa ja viimeistään tässä yhteydessä harkita myöntökriteerien muuttamista nyt esittämällämme tavalla.

2. Tuen suuntaaminen kriittisille toimialoille

Tuki on suunnattu kriittisille toimialoille, mutta asetuksessa ei määritellä täsmällisesti, mitkä toimialat katsotaan kriittisiksi. Perustelumuistiossa kuitenkin todetaan: ”Yhteiskunnan toiminnan kannalta kriittisten alojen toimijoilla tarkoitetaan tässä niitä perusrakenteita, palveluja ja niihin liittyviä toimintoja, jotka ovat välttämättömiä yhteiskunnan elintärkeiden toimintojen ylläpitämiseksi, niin kuin ne on valtioneuvoston päätöksessä huoltovarmuuden tavoitteista (1048/2018) määritelty.”

Mikäli tuen kohdentamista ei nyt muutettaisikaan 1-kohdassa esittämällämme tavalla, esitämme, että yllä kerrottu määritelmä mainittaisiin viittauksena perustelumuistion asemesta jo asetuksen tekstissä, koska se on esitettyjen myöntöperusteiden kannalta aivan keskeinen.

3. Omavastuuosuudet

Esitykseen sisältyy kaksi eritasoista ja eri käyttötarkoituksiin tarkoitettua tukiluokkaa: 15 000 € ja 100 000 €. Näistä suuremmalla voisi kattaa 70 prosenttia tietoturvaprojektin kuluista, eli hakijan omavastuuosuus projektin rahoituksesta olisi 30 prosenttia. Sen sijaan pienemmässä tukiluokassa ei tuensaajalla olisi esityksen mukaan omavastuuosuutta.

Koska jaettavan tuen kokonaismäärä on varsin rajallinen, esitämme, että korkeamman tukiluokan enimmäistuki olisi 75 000 € ja omavastuuosuus edelleen esityksen mukainen 30 %. Tällä

tukisummalla olisi jo mahdollista hankkia merkittävästi 3 §:n 1 momentin 2) -kohdassa tarkoitettuja palveluita.

Tietoturvallisuuden kehittäminen on pitkäjänteistä, jatkuvaa toimintaa, joka ei tule koskaan valmiiksi. On tärkeää, että nyt esitetyllä tuella pitkäjänteinen kehitystoiminta saataisiin alulle ja vauhtiin, mutta on myös tärkeää, ettei kehittäminen jää vain julkisin varoin tuetuksi kertaprojektiksi. Siksi tukea saavan yrityksen (tai muun toimijan) sitoutuminen pitkäjänteiseen, jatkuvaan kehittämiseen on tärkeää. Ehdotamme sen vuoksi, että myös pienempään tukiluokkaan liitettäisiin edellytyksenä tuensaajan omavastuuosuus, joka voisi tässä tukiluokassa olla esimerkiksi 20 %.

Pienemmän tukiluokan omavastuuosuus ja suuremman tukiluokan enimmäistuen määrän pienentäminen yhdessä mahdollistaisivat luonnollisesti myös sen, että useampi tuensaaja pääsisi hyödyntämään tukea.

4. Tuettavien kustannusten ajallinen takaraja

Asetusluonnoksen 2 §:n 3 momentin mukaan tukea voidaan myöntää vain kustannuksiin, jotka syntyvät tukihakemuksen jättämisen jälkeen ja viimeistään 30.6.2024.

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 ja viestinnässä kohderyhmän yrityksiä edustaviin sidosryhmiin samoin kuin pk-yrityksille avustuspalveluja tarjoaviin muihin julkistoimijoihin. Viittaamme tältä osin Teknologiateollisuus ry:n ja Kyberala – FISC ry:n yhteisen lausunnon ehdotukseen, jonka mukaan Kyberala ry. voi ottaa neuvontatehtävän vastaan julkistoimijalta erikseen siitä ja kustannusten korvaamisesta sovittaessa.

Huomioiden asiaan liittyvät viestinnälliset tarpeet, esitetty takaraja 30.6.2024 voi nähdäksemme osoittautua liian tiukaksi. Ehdotamme, että aikaraja siirrettäisiin esim. vuoden 2024 loppuun.

Kunnioittavasti

Elinkeinoelämän keskusliitto EK

Lainsäädäntö ja hallinto

Tommi Toivola

Johtaja

Rajamäki Markku
Elinkeinoelämän keskusliitto EK - Lainsäädäntö ja hallinto