

Asia: VN/18738/2022

Luonnos valtioneuvoston asetukseksi tietoturvan kehittämisen tuesta

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

Suomen Yrittäjät kiittää liikenne- ja viestintäministeriötä mahdollisuudesta lausua näkemyksemme valtioneuvoston asetusluonnoksesta koskien tietoturvan kehittämisen tukea.

Ehdotus perustuu vuoden 2022 toiseen lisätalousarvioon, jossa myönnettiin LVM:n alalle tietoturvallisuuden kehittämiseen suomalaisissa yrityksissä kuuden miljoonan euron määrärahaa. Sen avulla voitaisiin myöntää määräaikaista tietoturvaseteleitä yhteiskunnan toiminnan kannalta kriittisten alojen yrityksille ja järjestöille sekä näiden keskeisille palveluntarjoajille.

Pk-yritysten tietoturvan ja kybervarautumisen tilannekuva

Asetusluonnoksen muistio viittaa helmikuussa 2022 toteuttamaamme Yrittäjägallupiin. Gallupin mukaan pk-yrityksistä 34 prosenttia arvioi tietomurrot suureksi tai melko suureksi riskiksi liiketoiminnalle, ja 58 prosenttia pitää tietoturvasta huolehtimista erittäin tärkeänä. Yrityksistä 56 prosenttia arvioi tietoturvansa tason hyväksi, 15 prosenttia erinomaiseksi. Tätä heikommaksi tason arvioi 27 prosenttia yrityksistä.

Samana kyselyn mukaan peräti 61 prosenttia pk-yrityksistä kokee esteitä tietoturvan toteutumisessa. Näistä merkittävimpiä ovat osaamisen puute ja tieto-turvan kustannukset. Reilu puolet yrityksistä tietää, miten toimia tietomurron tapahduttua. Epävarmoja tai tietämättömiä on 41 prosenttia.

Toukokuussa 2022 toteuttamamme Yrittäjägallup taas osoittaa, että 23 prosenttia pk-yrityksistä on varautunut Suomen Nato-jäsenyysprosessiin liittyvään mahdolliseen häirintään. Näistä yrityksistä 59

prosenttia on varautunut kyberuhkiin ja -iskuihin. Toisin sanoen joka seitsemäs yritys on arvioinut kybervaikuttamisen riskien kohonneen niin paljon, että ne edellyttävät yrityksessä erityisiä toimia.

Kevään kyselytutkimustemme tuloksista voidaan päätellä, että vaikka digitaalinen turvallisuus on yhä olennaisempi osa pk-yritysten liiketoiminnan riskien-hallintaa, on monen yrityksen tietoturva muuttuneen tilanteen valossa alimitoitettua. Varautumista olisi parannettava niin käytettyjen järjestelmien tieto-turvan kuin henkilöstön tietoturvaosaamisen osalta. Yksi keskeinen kehittämisen paikka on pk-yritysten kyky arvioida ja seurata oman tietoturvasa tasoa sekä tehdä tietoturvaa lisääviä järjestelmä- ja palveluhankintoja.

Yleisnäkemykset ehdotuksesta

Pidämme asetusehdotusta yleisiltä tavoitteiltaan kannatettavana. On yhteiskunnan edun mukaista kohdistaa politiikkatoimia yritysten tieto- ja kyberturvallisuuden vahvistamiseen.

Digitalisaation myötä yhteiskunnan elintärkeät toiminnot, joista osa on yritysten tuottamia, ovat yhä riippuvaisempia tietojärjestelmistä ja -verkoista. Suomen turvallisuusympäristö, mukaan lukien sen kyberulottuvuus, on muuttunut kuluneen vuoden aikana, ja on oletettavaa, että muutos ei ole lyhyt- tai väliaikaista. Näiden tekijöiden yhteisvaikutuksesta kyberrikollisuuden ja hybrdivaikuttamisen taloudelliset ja sosiaaliset riskit kasvavat.

Esitetty tietoturvan kehittämisen tuki eli niin sanottu ”tietoturvaseteli” kannustaisi yrityksiä kyberturvainvestointeihin. Lisäksi se kasvattaisi yrityskentän yleistä tietoisuutta kybervarautumisen tärkeydestä sekä ohjaisi kyberturvallisuusalan palveluntarjoajia kehittämään tuotteita ja palveluita pk-yrityssegmentin tarpeisiin.

Tietoturvasetelin kohderyhmä ja sovellusala

Tietoturvan kehittämisen tuki olisi kohdistettu vain kriittisten alojen yrityksille ja järjestöille. Muuttuneen turvallisuustilanteen ja ripeän teknologiakehityksen takia yhteiskunnan ja erityisesti pk-yrityssektorin kyberresilienssiä on kuitenkin pyrittävä vahvistamaan laajasti kaikilla toimialoilla. On vältettävä kehitys, jossa pk-yrityskenttä eriytyy kybersuojaltaan vahvoihin kriittisten alojen yrityksiin ja kybervarautumiseltaan heikkoihin muiden alojen yrityksiin. Tämä ei ole toivottava suunta voimakkaasti keskinäisverkottuneessa taloudessa.

Esitämme, että tuen piiriin otettaisiin myös muiden kuin kriittisten alojen pk-yritykset. Tukisumma voisi olla suurempi, mikäli yritys toimii yhteiskunnan toiminnan kannalta kriittisellä

alalla. Mikäli tuki päädytään kuitenkin tässä vaiheessa rajaamaan vain kriittisten alojen toimijoihin, on tuen jatkoa harkittaessa selvítettävä mahdollisuutta laajentaa tuki koskemaan myös ei-kriittisten alojen organisaatioita.

Sikäli kun kriittisten toimialojen rajausta on tuen sovellusalan ja myöntöperusteiden kannalta keskeinen, ehdotamme, että viittaus kriittisten toimialojen määrittelyyn (valtioneuvoston päätös huoltovarmuuden tavoitteista 1048/2018) sisällytetään perustelumuiiston lisäksi itse asetuksen tekstiin.

Pk-sektorin yrityksille ja järjestöille ehdotettu, enintään 15 000 euron suuruinen tietoturvaseteli madaltaisi näiden kynnystä ryhtyä toimiin, jotka kehittäisivät nopeavaikutteisesti kyberturvallisuutta Suomessa. Setelin määrä ja käyttöala vastaavat mielestämme tuelle asetettuja tarkoituksia. On perusteltua, että tuen saava pk-yritys voisi vapaasti valita suomalaisen tai ulkomaisen toimijan, jolta hankkia tukea hyödyntäen tietoturvatarpeisiinsa vastaavan palvelun. On myös kohtuullista, että yhdelle toimijalle voitaisiin myöntää vain yksi tietoturvan kehittämisen tuki.

Laajempi, enintään 100 000 euron suuruinen seteli olisi tarkoitettu hyökkäyksenestotestausta, tärkeimpien sähköisten palveluiden varautumistason testausta tai näistä nousevaa välitöntä tietoturvallisuutta parantavaa toimea varten. Tämän tuen osalta hakijan omavastuu olisi 30 prosenttia tukikelpoisista kustannuksista.

Ehdotuksen mukaan laajempaa tukea voisivat hakea myös muut kuin pk-yritykset. Koska tietoturvan kehittämistarpeet ovat suurimmat nimenomaan pk-sektorissa ja koska tukeen varattu määräraha on suhteellisen pieni, katsomme tarkoituksenmukaiseksi kohdentaa myös suurempi tietoturvaseteli ainoastaan pk-kokoluokan yrityksille ja järjestöille.

Hyväksyttävien kustannusten takaraja

Pidämme perusteltuna sitä, että tukea voitaisiin myöntää vain kustannuksiin, jotka toteutuvat tukihakemuksen jättämisen jälkeen. Hyväksyttävien kustannusten olisi toteuduttava viimeistään 30.6.2024. Mikäli tuen hakemis- ja myöntämisprosessi viivästyy tuen hakijoista ja saajista riippumattomista syistä, voi tämä takaraja osoittautua liian tiukaksi. Kannattamme aikarajan siirtämistä vähintään vuoden 2024 loppuun. Tämä jättäisi viranomaiselle sekä tuettaville liikkumatilaa yllättävien tilanteiden varalle.

Tuen toimeenpano

Tuen myöntäjänä toimisi Liikenne- ja viestintäviraston Kyberturvallisuuskeskus. Tuen myöntäminen ei olisi harkinnanvaraista, vaan Liikenne- ja viestintävirasto myöntäisi tuen, jos edellä mainitut edellytykset täyttyisivät ja tukeen varattua määrärahaa olisi edelleen jäljellä niin, että tuki voitaisiin myöntää. Pidämme tätä menettelyä kannatettavana, sillä se jouduttaisi tuen myöntämistä ja näin nopeuttaisi tuetuista toimenpiteistä seuraavien tietoturvaikutusten syntymistä.

On kuitenkin syytä olettaa, että tuen myöntävä viranomais ei ole laajasti tunnettu tukeen oikeutetuissa pk-yrityksissä ja että vastaavasti viranomaisen yhteydet näihin yrityksiin ovat rajallisempia kuin muilla pk-yrityksiä tyypillisesti avustavilla julkishallinnon organisaatioilla, kuten Business Finlandilla ja ELY-keskuksella. Siksi onkin tärkeätä, että viranomais tukeutuu tuen toimeenpanon valmistelussa pk-yrityksiä edustaviin sidosryhmiin sekä pk-yrityksille avustuspalveluja tarjoaviin muihin julkistoimijoihin.

Eriyksen tärkeätä on varmistaa, etteivät hakemukseen tarvittava yksilöity suunnitelma tai kuvaus tietoturvan kehittämisen hankkeesta sekä muut selvitykset muodosta hakijalle kohtuutonta hallinnollista taakkaa. Haku- ja selvitysmenettelyiden on oltava sellaisia, että ne eivät muodosta estettä myöskään pienemmän kokoluokan pk-yrityksillä hakea ja käyttää tukea.

Lisäksi on huolehdittava siitä, että tarjolla on riittävästi informaatiota ja neuvontaa tukemaan tukihakemuksen jättämistä sekä tuen käyttämistä. Yrityksillä on oltava oikea käsitys soveltuvuudestaan tuen hakijaksi sekä riittävä ymmärrys tuella korvattavista hyväksyttävistä kustannuksista.

Tukikokonaisuuden viestinnässä pk-yritykset ovat keskeinen kohderyhmä. Näiden tavoittaminen edellyttää oikeiden viestintäkanavien tunnistamista ja hyödyntämistä. Erityisesti yritys- ja yrittäjäjärjestöt onkin syytä ottaa mukaan tuesta viestimiseen.

Muut toimet pk-yritysten tietoturvan vahvistamiseen

Esitetyn tietoturvasetelin lisäksi tarvitaan myös muita toimia pk-yritysten tieto- ja kyberturvan vahvistamiseksi. Toimet voisivat käsittää yleisen tietoturvatietoisuuden kasvattamiseen tähtäävän viestinnän lisäksi esimerkiksi käytännönläheisiä koulutuksia, oppaita sekä yhteiskunnan eri sektorien yhteisiä kyberturvaharjoituksia. On tärkeätä, että toimet valmistellaan tarkoituksenmukaisilta osin viranomaisten ja yrityskentän ja kyberalan sidosryhmien yhteistyönä.

Huoltovarmuuskeskuksen toiminta käsittää hyödyllisiä työskentelymalleja ja työkaluja kybervarautumiseen. Olisi toivottavaa, että näitä avattaisiin mahdollisimman laajasti myös muiden

kuin kriittisten organisaatioiden varautumistyön käyttöön huoltovarmuustoiminnan fokusta haittaamatta.

Mikkilä Joonas
Suomen Yrittäjät ry