Badrap Oy

Lausunto

15.07.2022

Asia: VN/18738/2022

Luonnos valtioneuvoston asetukseksi tietoturvan kehittämisen tuesta

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

Kiitämme mahdollisuudesta lausua mielipiteemme tietoturvan kehittämisen tuen asetusluonnoksesta.

Tietoturvan kehittämisen tuki sopii erinomaisesti kyberturvallisuuden demokratisointiin

Monen suomalaisen suuryrityksen kyberturvallisuus on hyvällä tasolla. Toisaalta Suomi on täynnä pieniä ja keskisuuria sekä kriittisiä yrityksiä, joiden panostukset kyberturvallisuuteen ovat olleet tähän mennessä minimaalisia. Uusi tukimuoto ("tietoturvaseteli") on erinomainen tapa käynnistää kyberturvallisuustyö tällaisissa yrityksissä. Ja työ on todella tarpeen: Liikenne- ja Viestintävirasto Traficomin Kyberturvallisuuskeskuksen Tonttu-kokeilut ovat osoittaneet, että Suomen kyberturvallisuustilannetta voidaan kohentaa merkittävästi auttamalla mahdollisimman monia yrityksiä laittamaan perusteet kuntoon tehokkailla ja täsmällisillä menetelmillä.

Miten demokratisointi onnistuu?

Jotta tietoturvaseteli löytäisi sitä eniten tarvitsevat yritykset ja uuden tukimuodon vaikuttavuus suomalaisten yritysten ja sitä kautta koko yhteiskunnan tietoturvaan olisi mahdollisimman suuri, tuella tulee olla seuraavat ominaisuudet:

- Mahdollisimman monen yrityksen täytyy pystyä hakemaan tukea.

- Tuella tulee pystyä hankkimaan käytännöllisiä toimenpiteitä, joilla saadaan aikaan pysyviä parannuksia kohdeyritysten tietoturvaan. Kun keskitytään kyberturvallisuudeltaan perustason yrityksiin, tarvekartoitukseen menee korkeintaan 60 minuuttia, jonka jälkeen voidaan siirtyä käytännön toimenpiteisiin. Monimutkaisemmat esiselvitykset kuuluvat yrityksiin, jotka ovat jo pitkään tehneet kyberturvallisuustyötä. Näissä yrityksissä parannuskohteiden etsiminen on jo työtä itsessään.

- Tuella hankittavien toimenpiteiden täytyy olla mahdollisimman helppoja toteuttaa kohdeyrityksissä.

Pidämme erittäin hyvänä asetusluonnoksessa esitettyä 15000€ ylärajaa pienemmälle tukimuodolle. Myös pienemmän tukimuodon käyttökohteiden määrittely laajasti (henkilökunnan kouluttaminen, osaamisen kehittäminen ja tietoturvan parantamiseen tähtäävät hankinnat) kannustaa yrityksiä käytännöllisiin, tehokkaisiin ja pysyviin toimenpiteisiin. Pienemmän tukimuodon rajaaminen pk-yrityksille on hyvä lähtökohta, joskin tietyin seuraavassa esitellyin varauksin.

Demokratisoinnin tehokkuuteen vaikuttavat riskit

Suuri tukimuoto kohdentuu tehottomasti

Asetusluonnoksen mukainen suurempi, enintään 100000€ tukimuoto heikentää tuen tehoa parannuksiin käytettyä euroa kohti. Suuremman tukimuodon tarjoaminen kaikenkokoisille yrityksille tulee johtamaan valtaosan tuen 6M€ määrärahasta valumiseen nopeasti suuryrityksille, joilla on valmiiksi kokemusta yritystukien hakemisesta, riittävä tekninen kyvykkyys monimutkaisempien testausprojektien järjestämiseen, sekä valmiiksi neuvoteltu kumppani suorittamassa testausta ja vastaanottamassa tukirahoja. Kuten korona-ajan yritystukimuodoissa nähtiin, tukia tullaan hakemaan maksimimäärä mahdollisimman pian kuin ne ovat haettavissa, ja monimutkaisia 100000€ testausprojekteja tarjoavat toimijat tulevat saamaan valtaosan tuelle varatuista määrärahoista, ilman että kohdeyritysten tietoturva kohenee merkittävästi, laajasti ja pysyvästi testien tuloksena.

Suuri tukimuoto on rajattu asetusluonnoksessa vaikuttavuudeltaan epävarmempiin menetelmiin "hyökkäyksenestotestaukseen" ja "tärkeimpien sähköisten palveluiden varautumistason testaukseen". Kritisoimme yksittäisten testausprojektien rajaamista tuen piiriin – kertaluonteinen testaus tai yksittäisten palveluiden tietoturva-auditointi ei paranna minkään yrityksen tietoturvaa pysyvästi ja mahdollisimman laajasti. Kritisoimme tietoturva-alalla varsin harvoin käytetyn termin "hyökkäyksenestotestaus" käyttöä asetuksessa ilman asianmukaista teknistä määritelmää.

Tukea tarvitsevat myös yritysten toimittajat

Toimitusketjujen kautta tapahtuvat kyberhyökkäykset kasvattavat suosiotaan. Olemme tarkastelleet ja korjanneet asiakkaidemme kanssa heidän palvelutoimittajiensa tietoturvaa. 343 palveluntarjoajan otoksen perusteella 17% palveluntarjoajilta löytyy yksinkertaisia haavoittuvuuksia. Kolmasosa palveluntarjoajista pystyy korjaamaan ongelmat tehokkaasti. 2/3 palveluntarjoajista ei onnistu korjaamaan ongelmia kunnolla tai lainkaan kyberturvallisuuskulttuurin puutteiden vuoksi.

Tukimuodon rajaaminen vain kriittisten alojen yrityksille ja järjestöille on siis toinen tuen vaikuttavuutta heikentävä tekijä. Monet (etenkin suuremmat) kriittisten alojen yritykset ovat jo tehneet toimenpiteitä oman tietoturvansa kehittämiseksi. Nykyisin yhä enemmän yritysten tietoturvaongelmat eivät johdu omien järjestelmien haavoittuvuuksista tai henkilöstön puutteellisesta tietoturvaosaamisesta, vaan yrityksen palveluntarjoajien ja yhteistyökumppanien tietoturvaongelmista. Jotta kriittisten alojen yritysten tietoturvaa voidaan parantaa aidosti, tukimuodon tulee olla myös käytettävissä näiden yritysten toimitusketjujen tietoturvan parantamiseen.

Ylläolevista perusteluista johtuen esitämme asetusluonnokseen seuraavia muutoksia:

1. Tuen rajaus kriittisten alojen yrityksille ja järjestöille poistetaan asetuksesta, eli tuki laajennetaan myös kaikkien suomalaisten pk-yritysten haettavaksi.

1a. Mikäli rajaus kriittisten alojen yrityksille ja järjestöille säilytetään asetuksessa, yritysten ja järjestöjen tulisi voida kohdentaa tuki myös omien palveluntarjoajiensa tai yhteistyökumppaneidensa tietoturvan kehittämiseksi.

2. Laajempi enintään 100000€ tukimuoto poistetaan asetuksesta.

2a. Mikäli 100000€ tukimuoto säilytetään asetuksessa, sille varataan erillinen, suhteessa huomattavasti pienempi kiintiö (esim. 1M€) koko määrärahasta. Tämän tukimuodon käyttökohteiksi sallitaan myös muuta kuin "hyökkäyksenestotestaus" ja "tärkeimpien sähköisten palveluiden varautumistason testaus". Suurempaa tukimuotoa olisi hyvä voida käyttää erityisesti yritysten toimitusketjujen tietoturvan parantamiseen.

Esittämiemme muutosten jälkeen asetus:

- Vaikuttaa mahdollisimman laajasti, pysyvästi ja tehokkaasti suomalaisten pk-yritysten sekä koko yhteiskunnan tietoturvaan ja varautumistasoon.

- Tekee tuen hakemisesta mahdollisimman selkeää, ja sillä saadaan aikaan käytännöllisiä, ripeästi toteutettavia pitkän tähtäimen kehitystoimenpiteitä.

Kunnioittaen,

Badrap Oy

Heikki Kortti

Kortti Heikki
Badrap Oy