Tieto- ja viestintätekniikan ammattilaiset TIVIA ry **LAUSUNTO**

Satu Koskinen

Lausuntopyyntö 28.6.2022 VN/18738/2022

Tieto- ja viestintätekniikan ammattilaiset TIVIA ry kiittää mahdollisuudesta lausua näkemyksensä tähän tärkeään asiaan. Kyseessä on määräaikainen tuki, jonka avulla organisaatiot voisivat hankkia tarkastuksen ja arvion uhkamallinnuksesta järjestelmiensä tietoturvatasosta markkinaehtoisilta toimijoilta, sekä ryhtyä tulosten perusteella parantamaan järjestelmiensä tietoturvaa ja tietoturvaosaamistaan määrätietoisesti.

JOHDANTO

Tietoturvan, tietosuojan ja kyberturvan merkitys on kasvanut nopeasti yhteiskunnassamme. Koulutusjärjestelmämme eri muodoissaan ei pysty tuottamaan tällä hetkellä osaajia riittävästi ja muuttunee geopoliittisen tilanteen vuoksi yrityksillä on entistä suurempi tarve saada osaavaa henkilökuntaa sekä konsultointia. Liikenne- ja viestintäministeriön muistiossa viitataan helmikuussa 2022 toteutettuun Yrittäjägallup- tietoturvatutkimukseen, jonka perusteella ”on epätodennäköistä, että pk-yrityksillä olisi mahdollisuuksia ylläpitää omaa, yrityksen sisäistä tietoturvaosaamista. Saman tutkimuksen mukaan, tietoturvan kustannusten arvioidaan olevan toiseksi merkittävän este tarvittavien toimenpiteiden toteuttamiselle”.

Selvitykseen viitaten, olisi hyvä korostaa, että tietoturvaosaamista voi jokainen yritys parantaa myös hyvin pienin toimenpitein. Erilaisiin ilmaisiin koulutuksiin osallistuminen, hyödyntäminen kyberturvallisuuskeskuksen ohjeita ja materiaaleja, pääsee jo alkuun. Monesti tietoturvaosaaminen nähdään vain syvänä asiantuntijatyönä, vaikka osaamista pitäisi olla jokaisella tasolla aina asiantuntijasta hallituksen jäseniin.

KANNATAMME ESITYSTÄ TIETYIN HUOMIOIN

Me TIVIA:ssa näemme, että esitys on kannatettava, mutta vaatii joitakin asioita vielä tarkennettavaksi.

Yllä mainitussa Yrittäjägallup tietoturvatutkimuksessa nostetaan esille hankintaosaaminen. Näemme riskiä puutteellisessa hankintaosaamisessa. Yrityksellä on rekisterinpitäjänä laaja vastuu, jossa osto-osaaminen korostuu. Ehdotamme, että jokainen tukea hakeva yritys osallistuisi Liikenne- ja viestintäministeriön infoon/koulutukseen tietoturvan perusteista, sekä hankkisi näkemyksiä osto-osaamisen tueksi. EU:n tietosuoja-asetuksen noudattamiseen tarvittavaa tietoa voi kartuttaa esim. sivuilla https://www.tietosuojaapkyrityksille.fi/ . Siellä on EU:n rahoituksella Tieken ja Tietosuovaltuutetun toimisten laatima työkalu mikro- ja pk-yrityksille. Sen avulla voi täydentää omaa osaamistaan ja arvioida oman organisaation tietosuojan tasoa.
Esityksessä palveluja voi hankkia markkinaehtoiselta toimijalta. Miten varmistetaan, että markkinaehtoinen toimija on riittävän asiantunteva ja turvallinen kumppani erilaisiin selvityksiin?

Lisäksi selvityksessä puhutaan uhkamallinnuksesta, mutta toisaalta nostetaan esille koulutusyhteistyö, tietosuojan- ja tietoturvan toimet, sekä kyberturvallisuus. Painottaisimme tässä kohtaa kyberturvallisuuden toimenpiteitä, vallitsevan geopoliittisen tilanteen vuoksi. Kyberturvallisuuden toimenpiteistä voisi olla alustava esitys, perustasosta kehittyneempään tasoon, joka antaisi pk-yritykselle mahdollisuuden arvioida omaa tasoaan jo etukäteen ennen hakemuksen jättämistä. Esityksessä kerrotaan, että ”tukea koskevassa hakemuksessa on ilmoitettava yksilöity suunnitelma tai kuvaus tietoturvan kehittämisen toimenpiteistä, sekä ilmoitettava tämän asetuksen mukaan haettavan tuen määrä”.

Tämä voi olla haasteellista, mikäli oma lähtötaso ei ole tiedossa. Tähän auttaisi edellä kuvattu pakollinen perustason perehdytys hakevan yrityksen nimetyille henkilöille. Mitä enemmän ymmärrät, sitä paremmin hahmotat omaa tilannettasi ja osaat ostaa palveluja.

Näemme erittäin positiivisena, että avustuksen saajan on toimitettava Liikenne- ja viestintävirastolle selvitys avustuksen käytöstä ja vaikutuksista toimijan tietoturvaan viimeistään kuusi kuukautta tuella katettavien kustannusten syntymisen jälkeen. Analysointi jälkikäteen, on mitä parhain keino lisätä osaamista ja varmistaa jatkotoimenpiteiden läpimeno

On myös huomioitava, että kyberturvan palveluja tarjoavat yritykset ovat jo nyt melkoisen työllistettyjä. Olisi ehdottoman hyödyllistä pohtia eri kyberturvakoulutusta tarjoavien oppilaitosten kanssa tehtävää yhteistyötä, jotta aikataulu ja kysynnän ja tarjonnan kohtaaminen varmistettaisiin.

KYBERTURVALLISUUS ALIHANKINTAKETJUISSA

Usein palvelut ovat ketjutettuja, alihankkijoiden rooli, joista sopimusosapuoli toki sopimuksen mukaan vastaa kuin omistaan, ovat usein haasteellisia. Kuuluuko tuen piiriin pieni pk-yritys joka tekee osatoimitusta yhteiskunnan kannalta kriittisellä toimialalla toimivalle yritykselle? Entä yritys, joka on juuri tarjoutunut tekemään projektin ko. sektorille?

LOPUKSI

Konkreettiset keskeisimmät ehdotuksemme ovat :

1) Määritellä tarkemmin markkinaehtoisien toimijoiden osaamisen kriteerit, jotta vääriltä ja turhilta hankinnoilta säästyttäisiin. Edellytetäänkö yritykseltä, joka tarjoaa setelillä ostettavaa palvelua, esimerkiksi tiettyjä kyberturvan sertifikaatteja?
2) Auttaa pk-yrityksiä osto-osaamisen kasvattamisella koskien kyberturvaa (esim. pakollinen osallistuminen infoon/koulutukseen, koulutuksen pystyy varmasti järjestämään Suomessa toimivat kyberturvallisuutta edistävät tahot, kuten vaikkapa kyberturvallisuuskeskus. Myös TIVIA ry auttaa tarvittaessa osto-osaamisen liittyvissä asioissa yhdistettynä kyberturvan osaamiseen.
3) Fokusoida tuki kyberturvaan geopoliittisen tilanteen vuoksi