Suomen Yrittäjät

Lausunto

18.12.2020

Asia: VN/24348/2020

Selvitys tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla; työryhmän väliraportti

Lausunnonantajan lausunto

Ehdotukset poliittisiksi linjauksiksi, kommentit:

Digitaalisten palveluiden lisääntyessä ja erityisesti yhteiskunnan kriittisten toimintojen tietojärjestelmien luotettavuuden varmistamiseksi pidämme tietoturvan parantamista erittäin tärkeänä tavoitteena. Katsomme, että tietoturvan parantamiseksi on kiinnitettävä huomiota sellaisiin toimiin, jotka tosiasiassa tukevat toimijoiden kyvykkyyttä vastata havaittuihin tietoturvahaasteisiin. Tietoturvahaasteisiin vastaaminen edellyttää toimijoilta jatkuvaa tietoturvan kunnossapitoa, jonka onnistuminen on riippuvainen viranomaisen tarjoaman tuen, neuvonnan sekä ajankohtaisen tiedotuksen toteutumisesta.

Ilmenneiden tietoturvapuutteiden vuoksi katsomme laadittavan selvityksen tarkoituksenmukaiseksi. Tietoturvahaasteiden ennaltaehkäisemiseksi on tarkasteltava kattavasti eri vaihtoehtoja niin tietoturvan parantamisen kuin toimenpiteiden kohteena oleville toimijoille aiheutuvien vaikutusten osalta. Liian tiukkojen vaatimusten taikka säännösten säätäminen voi aiheuttaa yllättäviä markkinoiden toimintaan liittyviä vaikutuksia. Selvityksen väliraportissa ei ole riittävällä tavalla arvioitu eri toimenpiteiden yritysvaikutuksia. Yritysvaikutusten huomioon ottamista olisi parannettava selvityksen jatkotyössä, joka auttaa myös tehokkaiden ja tarkoituksenmukaisten toimenpiteiden kartoitustyötä.

Lisävelvoitteita sekä lisäkustannuksia aiheuttavaa sääntelyä olisi harkittava tarkoin ja kaikin keinoin olisi pyrittävä tietoturvan parantamiseen sellaisin keinoin, jotka eivät lisää toimijoiden hallinnollista taakkaa, erityisesti jos tavoitteet olisivat saavutettava muiden keinojen avulla. Kriittisten toimialojen lakisääteiset tietoturvavaatimukset olisivat, esitetyllä tavalla, oltava selkeitä ja oikeasuhtaisia. On tärkeää, että toimijoiden on mahdollista helposti selvittää minkälaisia tietoturvavaatimuksia lainsäädäntö niille asettaa. Kannatamme väliraportissa esitettyä toimintamallia, jossa hyödynnettäisiin toimijoille suunnattavaa konkreettista tiedottamista tietoturvavaatimuksista ja niiden saavuttamiseksi tehtävistä toimista.

Katsomme, että sellaisia toimenpiteitä, jotka kannustavat ja tukevat yksittäisiä toimijoita tietoturvan kunnossapitoon ovat tehokkaampia kuin pelotevaikutuksen luominen lainsäädäntöön asetettavilla seuraamuksilla. Mahdollisen tietoturvariskin aktualisoitumisesta aiheutuva mainehaitta on myös iso tekijä, jonka toimijat ottavat huomioon toiminnassaan ja jo itsessään luo toimijoille ison pelotevaikutuksen ilman, että sellaista tarvitsisi seuraamussääntelyn avulla luoda.

Asetettavien tietoturvavaatimuksien olisi käytännössä oltava myös pk-yritysten toteutettavissa. Viranomaisen tarkastusmahdollisuus taikka sanktioiden tehostaminen eivät ole toimivia keinoja tietoturvatason parantamiseksi, mikäli toimijalla ei ole tosiallisia mahdollisuuksia selviytyä sille asetetuista velvoitteista. Tarvittaessa olisi luotava erilaisia pk-yrityksille suunnattuja tukitoimintoja tietoturvavaatimusten saavuttamiseksi ja pk-yritysten toimintaedellytysten turvaamiseksi.

Katsomme, että linjaukset toimijoiden ohjauksen ja neuvonnan tehostamiseksi ovat kannatettavia. Toimijoiden riittävä osaaminen velvoitteiden noudattamiseksi olisi varmistettava. Ohjauksen ja neuvonnan mahdollistamiseksi on tärkeää, että viranomaisilla on riittävä osaaminen ja resurssit tietoturvaa koskevien kysymysten käsittelemiseksi. Kyberturvallisuuskeskuksen resurssien vahvistaminen, tietoturvasta vastaavien sektoriviranomaisten tukevan asiantuntijapalvelun perustaminen sekä koulutusvastuun antaminen Kyberturvallisuuskeskukselle ovat tärkeitä toimenpiteitä ja vahvistavat viranomaisten kykyä palvella tietoturvaa koskevissa kysymyksissä.

Väliraportissa on todettu, että kriittisten toimialojen tietoturvan ja tietosuojan tasoa voidaan parantaa prosessien, toimintojen ja tietojärjestelmien auditoinneilla sekä sertifioinneilla. Tietoturvapuutteiden tunnistamiseksi on tärkeää, että toimijoiden olisi mahdollista saada tietoturvan kartoituspalveluita ilman merkittäviä lisäkustannuksia. Merkittäviä kustannuksia aiheuttavien auditointiraporttien tuottaminen taikka pakollisten sertifikaattien hankkiminen vain viranomaisen valvontatyön helpottamiseksi ei ole perusteltua. Säännöllisesti toteutettavat auditoinnit voivat, toteuttamistavasta riippuen, edellyttää sellaisia resursseja, joita pk-yrityksillä ei ole. Myös toimijoiden sisäiset auditoinnit parantavat tietoturvan tasoa, jonka vuoksi ei ole tarkoituksenmukaista, että mahdollisen auditointivelvoitteen täyttämiseksi toimijan olisi pakottavasti hankittava se ulkopuoliselta taholta. On selvää, että ISO 27001 -sertifioinnin hankkimisesta aiheutuvat kokonaiskustannukset ovat liian suuria pk-yritysten kannettavaksi. ISO 27001 -sertifiointipakko vuoden 2024 loppuun mennessä merkitsisi, että monet sellaiset toimijat, jotka eivät pystyisi kantamaan sen hankkimisesta aiheutuvia kustannuksia olisivat pakotettuja poistumaan markkinoilta. Koska on selvää, että tällaisen velvoitteen asettaminen johtaisi kohtuuttomaan lopputulokseen, on syytä poistaa tämä velvoite poliittisia linjauksia koskevista ehdotuksista.

Kunnioittavasti

Suomen Yrittäjät

Janne Makkula — Karoliina Katila

työmarkkinajohtaja — asiantuntija

Väliraportin muut osat, kommentit:

-

Katila Karoliina
Suomen Yrittäjät