Suomen Yrittäjät

Lausunto

03.03.2021

Asia: VN/3501/2021

Valtioneuvoston periaatepäätös tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla; lausuntopyyntö (Huom! Lausuntoaika päättyy 3.3.2021)

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

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

Tietoturvahaasteiden ennaltaehkäisemiseksi on tarkasteltava kattavasti eri vaihtoehtoja niin tietoturvan parantamisen kuin toimenpiteiden kohteena oleville toimijoille aiheutuvien vaikutusten osalta. Liian tiukkojen vaatimusten asettaminen voi johtaa yllättäviin seurauksiin. Suomen Yrittäjät on huolissaan siitä, että yksittäisen, vaikkakin sinänsä vakavan tapauksen seurauksena valmistelussa on kiirehditty tavalla, joka voi johtaa toimenpidekokonaisuuden kannalta epätyydyttävään lopputulokseen. Nopean valmistelun vuoksi jää riski siitä, että ehdotettavaa kokonaisuutta ei ole riittävällä tavalla tarkasteltu tai arvioitu. Suomen Yrittäjät suhtautuu periaatepäätöksen luonnokseen varauksellisesti erityisesti sen vuoksi, ettei siinä ole riittävällä tavalla arvioitu eri toimenpiteiden yritysvaikutuksia. Yritysvaikutusten huomioon ottamista helpottaisi myös tehokkaiden ja tarkoituksenmukaisten toimenpiteiden kartoitustyötä.

Lisävelvoitteita sekä lisäkustannuksia aiheuttavaa sääntelyä tulee harkita tarkoin ja tietoturvan parantamiseen olisi pyrittävä sellaisin keinoin, jotka eivät lisää toimijoiden hallinnollista taakkaa, erityisesti jos tavoitteet olisivat saavutettava muiden keinojen avulla. Kriittisten toimialojen lakisääteiset tietoturvavaatimukset tulee olla selkeitä ja oikeasuhtaisia ja esitettävien

toimenpiteiden osalta olisi pyrittävä kustannustehokkuuteen. Lainsäädäntömuutosten osalta tulee torjua sellaisen monipolvisen alempiasteista sääntelynkokonaisuuden syntyminen, joka ei välttämättä olisi mitenkään yhteismitallista tai yhteensovitettavaa. Tällainen sääntely olisi omiaan heikentämään suomalaisen elinkeinoelämän kykyä reagoida muuttuvaan toimintaympäristöön ja siten heikentäisi koko yhteiskunnan resilienssin turvaamista.

On tärkeää, että toimijoiden on mahdollista helposti selvittää minkälaisia tietoturvavaatimuksia lainsäädäntö niille asettaa. Kannatamme toimintamalleja, joissa hyödynnettäisiin toimijoille suunnattavaa konkreettista tiedottamista tietoturvavaatimuksista ja niiden saavuttamiseksi tehtävistä toimista. Korostamme, että tietoturvan ja tietosuojan parantaminen kriittisillä toimialoilla vaatii ennen kaikkea sitä, että toimijoilla on riittävä tietämys ja osaaminen velvoitteiden noudattamisessa sekä vahva ymmärrys siitä, että jokainen toimija kantaa itse vastuun oman toimintansa tietoturvasta ja tietosuojasta.

Asetettavien tietoturvavaatimuksien olisi käytännössä oltava myös pk-yritysten toteutettavissa. Sääntelyn taikka viranomaisen tarkastusmahdollisuuksien 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.

Toimijoiden riittävä tietoturvaan ja tietosuojaan liittyvä osaaminen olisi varmistettava. Ohjauksen ja neuvonnan mahdollistamiseksi on tärkeää, että viranomaisilla on riittävä osaaminen ja resurssit tietoturvaa ja tietosuojaa 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.

Yhtenä toimenpiteenä esitetään kriittisille toimialoille säädettävää auditointivelvoitetta. 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. Näiden seikkojen vuoksi on tärkeää, että auditointimallissa huomioitaisiin taloudelliset vaikutukset ja toimenpiteiden oikeasuhtaisuus eri kokoisten toimijoiden osalta.

On selvää, että ISO 27001 -sertifioinnin hankkimisesta aiheutuvat kokonaiskustannukset ovat liian suuria pk-yritysten kannettavaksi. ISO 27001 -sertifiointipakko vuoden 2025 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

Katila Karoliina
Suomen Yrittäjät