Sosiaali- ja terveysalan lupa- ja valvontavirasto Valvira

Lausunto

16.07.2024 V/27283/2024

Asia: VN/36693/2023

Lausuntopyyntö Suomen kyberturvallisuusstrategiasta

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

Sosiaali- ja terveysalan lupa- ja valvontavirasto (Valvira) kiittää mahdollisuudesta lausua kyberturvallisuusstrategiasta vuosille 2024-2035. On tärkeää, että valtioneuvosto laatii myös kyberturvallisuuden osalta strategioita, joissa pyritään vahvistamaan yhteiskunnan resilienssiä ja eri toimijoiden valmiuksia erilaisiin yhteiskunnallisiin uhkiin. Valvira kiinnittää huomiota siihen, että sosiaali- ja terveysalan (mukaan lukien esimerkiksi talousvesiasiat) turvaamisen tulisi näkyä asiakirjassa, sillä myös sosiaali- ja terveysala on enenevissä määrissä teknologiariippuvaista. Kyse ei ole pelkästään henkilöiden tiedoista vaan myös laitteiden toimimisesta. Valviran toiminta potilas- ja asiakasasiajärjestelmävalvonnassa on osa kyberturvallisuuden takaamista sosiaali- ja terveysalalla.

Kyberturvallisuusstrategiassa puhutaan paljon yksittäisten kansalaisten osaamisen vahvistamisesta ja heidän vastuunsa. On toki totta, että kansalaisten tulee tuntea kyberturvallisuusvastuunsa. Teknologioiden monimutkaistuessa on kuitenkin hyvä huomioida, että useat niin sanotut parhaat toimintamallit vaativat tekoja, joita kaikki eivät muista, osaa tai uskalla itse toteuttaa. Esimerkiksi monimenetelmäinen todentaminen ei ole oletuksena päällä useissakaan palveluissa ja jos sen haluaa päälle, tulee käyttäjän itse osata ja muistaa tehdä tämä. Sama käytäntö on esimerkiksi useissa internettiin kytketyissä laitteissa, joissa salasanaa ei pakoteta muuttamaan käyttöönoton yhteydessä. Myös mobiilivarmenteen käyttöönotto arveluttaa useita kansalaisia. Lisäksi palveluntarjoajien erilaiset maksut, joita he perivät tietoturvan lisäominaisuuksista, vähentävät kansalaisten halukkuutta ottaa niitä käyttöön. Tulisi arvioida sitä, pitäisikö palveluiden ja laitteistojen tarjoajilla itsellään olla velvollisuus tehdä tietoturvan lisäominaisuuksista palvelujen, ohjelmistojen ja laitteiden perusominaisuus. Tietoturvan elinkaarta tulisi myös pidentää niin, ettei kuluttaja ole pakotettu vaihtamaan laitteistoa/ohjelmistoa tietoturvan takia. Esimerkiksi Microsoft suunnittelee lopettavansa tietoturvapäivityksien tarjoamisen Windows10-käyttöjärjestelmälle vuonna 2024. Useat koneet eivät ole yhteensopivia Windows11-järjestelmän kanssa tai sen asentaminen yhteensopimattomaan laitteeseen edellyttää tietoteknisiä taitoja, joita tavankansalaisella ei ole. Käytännössä siis kuluttaja velvoitetaan ostamaan uusi laite, mikä ei ole aina mahdollista. Tämä heikentää tietoturvan tasoa, ja kertaantuessaan myös yhteiskunnan yleistä kyberturvallisuutta.

Lisäksi Valvira kiinnittää huomiota siihen, että strategiaa on tarkoitus päivittää viiden vuoden välein. Kun otetaan huomioon voimakkaasti muuttuva ja kehittyvät toimintaympäristö, onko viiden vuoden päivitysväli liian pitkä? Strategian toimeenpanoa on kyllä tarkoitus seurata vuosittain esimerkiksi säännöllisellä hallinnonalakohtaisella raportoinnilla. Se, mitä raportointi konkreettisesti tulee olemaan, ei ilmene kuitenkaan strategiasta. Myös vastuullisen ministeriön rooli strategian toimeenpanon seurannan toteutuksessa jää epäselväksi. Onko tarkoitus, että näitä asioita täsmennetään esimerkiksi toimeenpanosuunnitelmalla? Valviran näkemyksen mukaan kyberturvallisuus strategian toimeenpanoa tulisi täsmentää.

Kyberturvallisuusasiat ovat Euroopan unionin alueella yhteisiä ja niitä koskee merkittävästi monenlainen unionitasoinen säätely. Strategiassa tulisi ottaa tarkemmin kantaa unionitasoiseen yhteistyöhön valvontaviranomaisten toiminnasta alkaen. Miten unionitasoisella yhteistyöllä voimistetaan yhteiskunnan resilienssiä ja varautumista? Strategiasta ei myöskään ilmene, tuleeko EU:sta yhteiset ministandardit kyberturvallisuuden varmistamisessa jäsenmaiden välille.

Valviran näkemyksen mukaan on merkittävä puute, ettei NIS2-velvoitteita sovelleta asiakastietolain mukaisiin tietojärjestelmäpalvelun tuottajiin tai tietojärjestelmien valmistajiin. Kyseiset toimijat vastaavat terveydenhuollon palveluntuottajien ja -järjestäjien käyttämien potilastietojärjestelmien tietoturvasta ja sen vaatimusten noudattamisesta ja kehittämisestä järjestelmissä. Tämä soveltamisalan puute korostaa NIS2-velvoitteiden alaisten toimijoiden (esim. keskeisesti hyvinvointialueet potilastietojärjestelmien ja muun tietoliikenneverkoston käyttäjinä) varautumista ja omavalvontaa, johon kansallisesti tulee varata riittävästi resursseja. Paraskaan omavalvonta ei kuitenkaan riitä takamaan riittävää kyberturvallisuuden tasoa ja sitä, ettei epäkohtia ilmenisi toiminnan aikana. Toimijoiden omavalvonnan tukeminen, ennakoiva tarkastustoiminta mutta myös reaktiivinen valvonta yksittäistapausten kautta korostuu NIS2-valvontaviranomaisen tehtävissä, mikä tulee huomioida kansallista kyberturvallisuusstrategiaa valmisteltaessa ja toiminnan resurssoinnissa.

Lopuksi Valvira kiinnittää huomiota siihen, että strategia kaipaa vielä kielellistä tarkastusta ja hiomista. Esimerkiksi sivuilla 48 ja 49 kuvassa ja tekstissä, otsikon ”Valvovat viranomaiset” alle on kirjoitettu ”Sosiaali- ja terveydenalan lupa- ja valvontavirasto” kun pitäisi lukea ”Sosiaali- ja terveysalan lupa- ja valvontavirasto”.

Holmalahti Jussi
Sosiaali- ja terveysalan lupa- ja valvontavirasto Valvira

Lehtonen Niina
Sosiaali- ja terveysalan lupa- ja valvontavirasto Valvira