Hyvinvointiala HALI

Lausunto

29.11.2023

Asia: VN/18157/2023

Lausuntopyyntö: luonnos hallituksen esitykseksi kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanemiseksi

Lausunnonantajan lausunto

Yleiset huomiot NIS2-direktiivin tavoitteista ja tarkoituksesta

Hyvinvointiala HALI ry kiittää mahdollisuudesta lausua luonnoksesta hallituksen esitykseksi kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanemiseksi. Hyvinvointiala HALI ry pitää lakiluonnoksen ja sen taustalla olevan NIS2-direktiivin tavoitteita kannatettavana.

Soveltamisalaa koskevat huomiot

Esityksessä käytetty rajaus/kuvaus ”terveyssektori" olisi mielekästä laajentaa sosiaali- ja terveyspalvelut selkeästi kattavaksi. On tärkeää huomata, että niin sosiaali- kuin terveyspalveluissa merkittäviä palveluntuottajia löytyy myös yksityiseltä sektorilta.

Erityisesti sosiaalipalveluissa käytännössä varsinaisen sosiaalipalvelun tuottajan lisäksi kyberturvallisuuden näkökulmasta merkittävä rooli on erilaisilla SaaS (Software as a Service) -palvelujen toimittajilla, jotka toimittavat palveluntuottajien käyttöön erilaisia ohjelmistoja esimerkiksi toiminnanohjauksen tai asiakastiedon hallintaan. Nämä yritykset saattavat kooltaan (henkilöstö tai liikevaihto) jäädä direktiivin soveltamisalan ulkopuolelle, mutta ne voivat kuitenkin käytännössä olla kriittisen tärkeitä esimerkiksi kymmenien tai satojen eri kokoisten sosiaalipalveluja tuottavien yritysten toiminnalle. Näin ollen mm. sosiaalipalvelujen palveluntuottajille merkittävimpiä ohjelmistoja toimittavat yritykset tulisi huomioida soveltamisalassa ja riskienhallintavelvoitteiden osalta.

Riskienhallintavelvoitetta koskevat huomiot

Ks. edellinen vastaus

Raportointivelvoitetta koskevat huomiot

Esityksen mukaan viranomaisille tulisi raportoida myös kyberturvallisuusuhista ja läheltä piti -tilanteista. Raportointivelvoitteessa on huomioitava, että eri toimijoiden poikkeamien havaintokyky vaihtelee. Esimerkiksi suurilla terveyspalveluntuottajilla on erinomainen kyky havaita eri suuruisia poikkeamia, ja näitä voikin pelkästään yksittäisen toimijan ”haaviin” jäädä päivittäin tuhansia. Jotta valvojan järjestelmät eivät kuormitu liikaa, tulee määritellä selkeästi, minkä tason poikkeamista on syytä ilmoittaa. Näiden ilmoittamiseen tulisi myös rakentaa oma rajapintansa.
Kyberturvallisuusuhkien ja läheltä piti -tilanteiden määrittely on tärkeää tehdä riittävän selkeästi, jotta raportointi ei kuormita liikaa niin raportointivelvollisia kuin viranomaistakaan. (Tämä ei ole toki lain tasolla tehtävää määrittelyä, vaan liittyy lain soveltamiseen.)

Loppuraportti poikkeamasta pitää tehdä kuukauden kuluttua poikkeaman havaitsemisesta. Tämä voi olla liian nopea takaraja joissain tilanteissa, joissa esimerkiksi hyökkäys voi kestää pitkään tai tilannekuva täydentyä vielä merkittävänkin ajan kuluttua. Tällaiset tilanteet on hyvä tunnistaa myös säädännön ja sen soveltamisen tasolla.

Valvontaa koskevat huomiot

On tärkeää erottaa selkeästi eri viranomaisten rooli erilaisissa valvontatilanteissa. Esimerkiksi THL:n osalta valvonta järjestelmien osalta keskittyy ennakolliseen valvontaan.

Seuraamusmaksua koskevat huomiot

Seuraamusmaksujen enimmäismäärät ovat verrattain korkeat ja voisivat toteutuessaan jopa vaarantaa organisaatioiden toiminnan.

Ehdotuksen mukaan seuraamusmaksut eivät koskisi julkista hallintoa. Ratkaisu olisi epäoikeudenmukainen ja johtaisi entistä vaikeampiin vastuullisuuskysymyksiin. Seuraamusmaksujen pitäisi koskea yhtäläisesti julkista ja yksityistä sektoria.

CSIRT-yksikön tehtäviä koskevat huomiot

On mahdollista, että Suomeen kohdistuisi laajempi, useisiin terveydenhuollon toimijoihin kohdistuva hyökkäys. Tällöin yhteisestä koordinaatiosta voisi olla hyötyä tilanteen torjumisessa. Olisi hyödyllistä, mikäli silloin tietoa ja tilannekuvaa voitaisiin jakaa paitsi CSIRT-yksikölle, myös ajantasaisesti sieltä toimijoiden suuntaan, mikäli jokin toimija olisi esimerkiksi löytänyt toimivan ratkaisun hyökkäyksen torjumiseen. Tällainen menettely edellyttäisi viranomaistahon riittävää resursointia ja valtuutusta operatiivisen toiminnan osalta. Olisi myös tärkeää, että CSIRT-yksikkö loisi toimintamalleja ja ohjeistuksia erilaisille toimijoille ja aloille kyberturvallisuuden vahvistamiseksi ja poikkeustilanteisiin vastaamiseksi.

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

Ei kommentteja

Verkkotunnusvälittäjiä koskevat huomiot

Ei kommentteja

Kumottavaksi ehdotettuja säännöksiä koskevat huomiot

Ei kommentteja

Vaikutustenarviointia koskevat huomiot

Ei kommentteja

Muut huomiot ja avoin palaute esityksestä

Ei muita huomioita

Kause Hanna-Maija
Hyvinvointiala HALI - Hanna-Maija Kause, johtaja (terveyspalvelut)