Sailab – MedTech Finland ry

Lausunto

23.11.2023

Asia: VN/18157/2023

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

Lausunnonantajan lausunto

Yleiset huomiot NIS2-direktiivin tavoitteista ja tarkoituksesta

Sailab – MedTech Finland ry kiittää liikenne- ja viestintäministeriötä mahdollisuudesta kommentoida luonnosta hallituksen esitykseksi NIS2-direktiivin täytäntöönpanemiseksi ja esittää yleisinä huomioina seuraavaa:

Terveysteknologia (lääkinnälliset laitteet; Eu-asetus 2017/745 ja IVD-laitteet EU-asetus 2017/746) on uusi soveltamisalaan kuuluva sektori. Esityksessä on hyvin tunnistettu MD- ja IVD-asetukset sekä näiden kautta lääkinnällisten laitteiden erityisasema. Tähän liittyen esitetään muutamat erityishuomiot:

o Osa korkean riskin lääkinnällisistä laitteista voivat olla myös konfiguroitavia laitteita, ohjelmistoja tai etäluettavia laitteita. Tästä syystä esityksessä tulee myös huolehtia siitä, että kyberturvallisuussäädökset eivät vaikuta potilasturvallisuuteen näiden laitteiden osalta.

o Liitteessä 1 kohdassa tulee varmistua, että luettelo keskeisistä toimijoista löytyy helposti ja siinä on huomioitu myös muut kuin esimerkiksi hengitystieinfektioihin liittyvät terveysuhat.

Yleisenä huomiona todetaan myös, että kyberturvallisuusdirektiivi astuu voimaan nopealla aikataululla (18.10.2024), ja yrityksille tulisi varata riittävästi aikaa esimerkiksi ilmoituksen tekemiseksi valvolvalle viranomaiselle. Milloin ilmoitusten tekeminen on Suomessa mahdollista?

Soveltamisalaa koskevat huomiot

NIS2-direktiivin soveltamisalaan liittyen lainsäädännössä tulisi myös ohjeistaa tarkemmin se, miten kansainvälisten yritysten osalta lasketaan yrityksen koko esimerkiksi Suomeen sijoittuvan tytäryhtiön osalta.

Riskienhallintavelvoitetta koskevat huomiot

Ei lausuttavaa.

Raportointivelvoitetta koskevat huomiot

Direktiivin soveltamisalaan kuuluvat toimijat raportoivat tietoturvapoikkeamat kolmiportaisesti: ensi-ilmoitus 24 h kuluessa, jatkoilmoitus 72 h kuluessa ja loppuraportti 1 kk kuluessa poikkeamasta. Tämä voi osoittautua haastavaksi terveysteknologian keskisuurissa yrityksissä, mikäli heillä ei ole aikaisemmin ollut tietoturvan tai kyberturvallisuuden hallintamallia toiminnassaan ja/tai ympärivuorokautista toimintaa.

Esityksen mukaan viranomaisille tulisi raportoida myös kyberturvallisuusuhista ja läheltä piti -tilanteista. Nämä kohdat ovat vaikeasti määritettävissä ja raportointia varten tarvittaneen tarkemmat kriteerit.

Valvontaa koskevat huomiot

-

Seuraamusmaksua koskevat huomiot

Seuraamusmaksu voidaan määrätä toimijalle, joka tahallaan tai törkeästä huolimattomuudesta laiminlyö 43 §:ssä tarkoitetut tiedot valvovalle viranomaiselle. Soveltamisalassa määriteltyjen toimijoiden joukko on kuitenkin jonkin verran epäselvästi määritelty ja tuntuisi kohtuuttomalta rankaista toimijaa, joka ei edes tiedä kuuluvansa lain soveltamisalaan. Tämä on erityisen totta terveysteknologian toimialalla, joka on lisätty uutena sektorina. Lain valmisteluvaiheessa tulisi olla helppo tapa tarkistaa, onko yritys lain piirissä vai ei sekä varmistaa informaation kulku toimialan yritysten suuntaan.

CSIRT-yksikön tehtäviä koskevat huomiot

Ei lausuttavaa.

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

Ei lausuttavaa.

Verkkotunnusvälittäjiä koskevat huomiot

Ei lausuttavaa.

Kumottavaksi ehdotettuja säännöksiä koskevat huomiot

Ei lausuttavaa.

Vaikutustenarviointia koskevat huomiot

Vaikutustenarvioinnin näkökulmasta velvoitteiden toteuttamisella on taloudellisia vaikutuksia, jotka tuntunevat erityisen raskailta keskisuurissa yrityksissä. Siksi olisi tärkeää luoda keskitetysti yhtenäisiä toimintamalleja, dokumenttipohjia, koulutuksia, työkaluja ja ohjeistuksia sekä riskienhallintaan että vaadittavien hallintatoimien osalta. Näiden tulisi olla käytössä hyvissä ajoin ennen lain voimaantuloa, jotta yritysten on mahdollista rakentaa toimivat riskienhallintamallit ja hallintakeinot. Yhtenäiset menettelytavat vähentäisivät myös päällekkäistä työtä ja vähentäisi todennäköisesti kustannuksia.

Muut huomiot ja avoin palaute esityksestä

-

Talman Kirsi
Sailab – MedTech Finland ry