HSL Helsingin seudun liikenne

Lausunto

24.11.2023

Asia: VN/18157/2023

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

Lausunnonantajan lausunto

Yleiset huomiot NIS2-direktiivin tavoitteista ja tarkoituksesta

HSL kiittää saamastaan mahdollisuudesta antaa lausuntonsa luonnoksesta hallituksen esitykseksi NIS2 direktiivin täytäntöönpanemiseksi.

Yleisellä tasolla kyberturvallisuuden tason kehittämistä niin EU-tasolla kuin kansallisella tasolla NIS2-direktiivin täytäntöönpanon muodossa on pidettävä yksinomaan myönteisenä ja tervetulleena asiana. Näemme direktiivin ensisijaisesti kuvaavan kansallisella tasolla soveltamisalaan kuuluvien organisaatioiden kyberturvallisuuden riskienhallinnan minimivaatimustason sekä siihen liittyvän raportoinnin ja julkisen valvonnan.

Soveltamisalaa koskevat huomiot

NIS2 direktiivin ja nyt käsillä olevan luonnoksen hallituksen esitykseksi kohdalla soveltamisalan määrittely on kokonaisuutena osoittautunut huomattavan tulkinnanvaraiseksi mahdollistaen myös virheelliset tulkinnat. Soveltamisalaan kuulumisen kriteerit on hajautettu useampaan osaan, mikä ainakin rajatapauksissa osaltaan vaikeuttaa tulkintaa. Esimerkiksi oman organisaatiomme kohdalla voinee päätyä tulkinnallisesti perusteltavissa olevin argumentein soveltamisalaan kuulumisen osalta molempiin vaihtoehtoihin. Valtaosassa tapauksia tulkinta lienee kuitenkin yksiselitteinen.

Riskienhallintavelvoitetta koskevat huomiot

Kyberturvallisuuden riskienhallinnan osalta hallituksen esityksen luonnoksessa kuvattujen vaatimusten laajuuden voi tulkita edustavan yleisesti käytössä olevien kyberturvallisuuden viitekehysten näkökulmasta valtavirtaa. Vaatimusten käytännön toteutukset ovat organisaatiokohtaisia. Kokonaisuutena vaatimusten laajuuden määrittelyä voi pitää tarkoituksenmukaisena.

Kyberturvallisuuden riskienhallinnassa ISO/IEC 27001 -standardi mahdollistaa sertifioitumisen. Luonnos ei ota tähän globaalilla tasolla vakiintuneeseen mahdollisuuteen kantaa osoituskyvyn

näkökulmasta. ISO/IEC 27001 on samalla yleisesti kyberturvallisuuden riskienhallinnassa käytettävä viitekehys. Tätä on pidettävä merkittävänä, koska NIS2 asettama kyberturvallisuuden riskienhallinnan vaatimustaso on oletettavasti kokonaisuutena varsin samankaltainen.

Hallituksen esityksen luonnoksen ja ISO/IEC 27001 standardin käsitteistöt ovat varsin samankaltaisia. Haasteena voi pitää sitä, syntyykö käsitteiden välille yhtenäisestä ilmiasusta huolimatta tulkinnasta johtuvia sisällöllisiä eroja. Tällaisen eräänlaisen kaksoisstandardin synty olisi erinomaisen haitallista.

Raportointivelvoitetta koskevat huomiot

Ei lausuttavaa.

Valvontaa koskevat huomiot

Ei lausuttavaa.

Seuraamusmaksua koskevat huomiot

Ei lausuttavaa.

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

Ei lausuttavaa.

Muut huomiot ja avoin palaute esityksestä

Ei lausuttavaa.

Kukko Petri
HSL Helsingin seudun liikenne