Huoltovarmuuskeskus

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

Direktiivin tavoitteet ovat hyvät, tervetulleet ja tukevat kansallista huoltovarmuutta parantamalla toimialojen kyberturvallisuutta ja jatkuvuudenhallintaa organisaatiokohtaisesti sekä organisaationa osana laajempaa verkostoa. Riskiperusteisuus, toimitusketjujen huomiointi ja verkostomainen toimintamalli tukevat digitaalisen toimintaympäristön jatkuvuudenhallintaa. Direktiivin asettamat vaatimukset ovat joiltain osin tulkinnanvaraisia. Vaatimuksia olisi näiltä osin hyvä tarkentaa, jotta yritykset voivat helpommin tunnistaa heihin kohdistetut vaatimukset.

Soveltamisalaa koskevat huomiot

Soveltamisala ei koske rakennetun ympäristön alaa tai yksityistä turva-alaa. Näiden alojen kybervarautuminen olisi hyvä ottaa lainsäädännössä huomioon, sillä ko. toimialojen mahdolliset häiriöt voivat vaikuttaa voimakkaasti yhteiskunnan kriittisiin toimintoihin.

Riskienhallintavelvoitetta koskevat huomiot

Riskienhallintavelvoite vaikuttaa kattavalta kokonaisuudelta, jossa on huomioitu riskienhallinta suurelta osin. Riskienhallintavelvoitteessa ei mainita jäännösriskejä eikä niiden hyväksyntäprosessia. Tämä on oleellinen osa riskienhallintaa ja siitä olisi hyvä mainita velvoitteessa. Velvoitteen mukaan riskienhallinnalla tulee estää tai minimoida poikkeamien vaikutus toimintaan, toiminnan jatkuvuuteen, palvelujen vastaanottajiin ja muihin palveluihin. Tässä rajataan pois riskin siirtäminen ja pitäminen, jotka ovat osa riskienhallinnan käytänteitä. Ehdotetaan, että velvoitteessa huomioitaisiin jäännösriskit sekä riskin siirtäminen ja pitäminen.

Raportointivelvoitetta koskevat huomiot

Raportointivelvoite huomioita kattavasti poikkeaman kohteena olevan toimijan velvollisuudet. Poikkeamatilanteessa toimija on hyvin työllistetty ja erilaiset raportoinnit nähdään helposti lisätyönä. Valvovan viranomaisen tulisi järjestää raportointi mahdollisimman suoraviivaiseksi ja automatisoiduksi, jotta siitä ei koituisi toimijalle kohtuutonta työmäärää poikkeamatilanteessa. Luonnoksen mukaan poikkeamailmoitus tulee tehdä vakavasta toimintahäiriöstä. Vakavan

toimintahäiriön määritelmää olisi hyvä avata laissa. Nyt sen määrittely jätetään toimijan vastuulle. Luonnoksen 14 §:n mukaan toimijan on ilmoitettava viipymättä merkittävästä kyberuhkasta sekä kyberuhkan hallitsemiseksi käytettävissä olevista toimenpiteistä niille palvelujensa vastaanottajille, joihin merkittävä kyberuhka saattaa vaikuttaa. Merkittävä kyberuhka on lisätty terminä lakiin julkisen hallinnon tiedonhallinnasta annetun lain muuttamisesta, mutta ei kyberturvallisuuden riskienhallinnasta annettavaan lakiin.

Valvontaa koskevat huomiot

Valvonnan hajauttaminen toimivaltaisille viranomaisille on hyvä malli. Hajautettu valvonta tukee kyberturvallisuuden vastuunjakoa Suomessa, jossa kyberturvallisuuteen liittyviä viranomaisvastuita ei ole keskitetty yhdelle toimijalle vaan se on osa kaikkien toimialojen tekemistä. Eri sektoreiden valvonnan yhteismitallisuus voidaan varmistaa koordinaatiotoimin.

Seuraamusmaksua koskevat huomiot

Ei huomioita.

CSIRT-yksikön tehtäviä koskevat huomiot

Ei huomioita.

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

Ei huomioita.

Verkkotunnusvälittäjiä koskevat huomiot

Ei huomioita.

Kumottavaksi ehdotettuja säännöksiä koskevat huomiot

Ei huomioita.

Vaikutustenarviointia koskevat huomiot

Kyberturvallisuudella on yhteiskunnan digitalisaation myötä kasvava merkitys kansalliselle huoltovarmuudelle. Vakavilla kyberturvallisuuden poikkeamilla on seurannaisvaikutuksia yhteiskunnan kannalta kriittisen palveluiden tarjoamiseen esimerkiksi energian, liikenteen tai elintarvikehuollon sektoreilla. Tämänhetkisessä versiossa NIS2 sääntelyn vaikutuksia huoltovarmuudelle ei ole huomioitu. Vaikutukset olisi perusteltua tuoda esiin luvun 4.5 yhteydessä, arvioidessa esityksen ihmisiin ja yhteiskuntaan kohdistuvia vaikutuksia. Uusi NIS2-sääntely tukee osaltaan Suomen huoltovarmuusjärjestelmää ja sen kasvattaa sen häiriönsietokykyä.

Muut huomiot ja avoin palaute esityksestä

NIS2 ja direktiivi kriittisten toimijoiden häiriönsietokyvystä (CER-direktiivi) ovat tavoitteiltaan toisiaan täydentäviä ja toimintaperiaatteeltaan samankaltaisia: kriittiset toimijat velvoitetaan ylläpitämään ja kehittämään omaa varautumistaan ja ilmoittamaan poikkeamista.

Sekä NIS2 että CER-direktiiveissä kehotetaan varmistamaan johdonmukainen lähestymistapa direktiivien välillä. Useat EU-jäsenmaat täytäntöönpanevat NIS2- ja CER-direktiivit yhteisellä lainsäädäntöhankkeella. Vaikka Suomessa direktiivien kansallinen toimeenpano tehdään kahtena

erillisenä kokonaisuutena, tulisi toimeenpanossa varmistaa, että saavutettavissa olevat synergiat hyödynnetään ja tehtävät ratkaisut olisivat mahdollisimman yhdenmukaisia. CER-valmistelussa tulisi esimerkiksi tarkastella NIS/NIS2 toimeenpanoa varten rakennetun poikkeamailmoitusprosessin hyödyntämistä.

Ilkka Juha
Huoltovarmuuskeskus