Päijät-Hämeen hyvinvointialue

Lausunto

21.11.2023

Asia: VN/18157/2023

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

## Lausunnonantajan lausunto

**Yleiset huomiot NIS2-direktiivin tavoitteista ja tarkoituksesta**

Luonnoksessa hallituksen esitykseksi ehdotetaan säädettäväksi laki kyberturvallisuuden riskienhallinnasta, jossa säädettäisiin yhteiskunnan toiminnan kannalta kriittisten toimijoiden kyberturvallisuuden riskienhallinta- ja raportointivelvoitteista. Julkishallinnon osalta velvoitteista säädettäisiin lisäksi julkisen hallinnon tiedonhallinnasta annetussa laissa.

Tavoite kehittää kyberturvallisuutta kansallisella ja EU-tasolla NIS2 direktiivin kautta on erinomainen.

**Soveltamisalaa koskevat huomiot**

Valvontaviranomaisia voi olla samalle organisaatiolle useita yhtaikaa (hyvinvointialueet mm. Valvira, Fimea, liikenne- ja viestintäministeriö). Esityksestä ei saa kovin tarkkaa käsitystä siitä, koskeeko soveltaminen aina koko organisaatiota, vai koskeeko se organisaatiossa sitä osaa, joka tekee jotain tiettyä toimintoa (terveys- ja sosiaalitoimi, pelastustoimi jne.). Julkishallinnolle ja erityisesti hyvinvointialueille asetettuja velvotteita olisi hyvä selventää ja tarkentaa.

**Riskienhallintavelvoitetta koskevat huomiot**

NIS2:n yleinen riskienhallintavelvoite tuo organisaation riskienhallinnan kokonaisprosessiin tiettyjä reunaehtoja ja on huomattava, että riskienhallintatoimet voivat aiheuttaa merkittäviä kustannuksia hyvinvointialueille.

**Raportointivelvoitetta koskevat huomiot**

Raportointivelvoitekohdassa mainitaan juurisyyn osalta jyyrisyyn tyyppi, mitä tällä tarkoitetaan? Onko tyyppilistaus julkaistu jossain? Kansallisessa toteutuksessa koskien merkittävien poikkeamien raportointia tulisi olla yhtenäinen koordinointi. Raportointivelvoitteen piirissä olevilla organisaatioilla tulisi olla yksi raportointikanava,

johon poikkeamasta ilmoitetaan ja josta tieto leviää tarvittaville viranomaisille.

**Valvontaa koskevat huomiot**

Esityksestä ei saa selkeää kuvaa kuinka valvonta toteutettaisiin käytännössä niin, ettei päällekkäistä valvontaa synny tai osa-alueita ei jää valvomatta varsinkin tilanteissa, joissa valvovia viranomaisia on useampia. 43§: IP-osoitealueet on epäselvästi ilmaistu. Perinteiset IP-osoitealueet on helppo ilmoittaa mutta IP-osoitteiden ilmoittaminen tuottaa hankaluuksia organisaatioille, jotka käyttävät pilvipalveluja palvelujensa tuottamiseen. Nämä osoitteet muuttuvat useasti ja niiden ilmoittamiseen tarvitaan automatisoitu rajapinta.

**Seuraamusmaksua koskevat huomiot**

Ei ole.

**CSIRT-yksikön tehtäviä koskevat huomiot**

Ei ole.

**Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot**

Tiedonhallintalain 4 luvusta suuri osa tekstistä on samaa kuin esitetyssä laissa kyberturvallisuuden riskienhallinnasta. Koska on organisaatioita, joita koskee molempien lakien säätely, olisi selkeämpää, että tiedonhallintalaissa viitattaisiin lain kyberturvallisuuden riskienhallinnasta määräyksiin ja eriteltäisiin vain ne asiat selkeästi, jotka ovat täydennyksiä lakiin kyberturvallisuuden riskienhallinnasta tai poikkeavat siitä.

**Verkkotunnusvälittäjiä koskevat huomiot**

Ei ole.

**Kumottavaksi ehdotettuja säännöksiä koskevat huomiot**

Ei ole.

**Vaikutustenarviointia koskevat huomiot**

Ei ole.

**Muut huomiot ja avoin palaute esityksestä**

Terminologiaan olisi hyvä kiinnittää huomiota.

Linnonmaa Tanja
Päijät-Hämeen hyvinvointialue