Hyvinvointialueyhtiö Hyvil Oy

Lausunto

20.11.2023 40/03.01.00/2023

Asia: VN/18157/2023

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

Lausunnonantajan lausunto

Yleiset huomiot NIS2-direktiivin tavoitteista ja tarkoituksesta

Hyvinvointialueyhtiö Hyvil Oy kiittää mahdollisuudesta lausua luonnoksesta hallituksen esitykseksi kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanemiseksi.

Direktiivin tarkoitus vahvistaa ja yhdenmukaistaa kyberturvallisuustasoa tietyillä yhteiskunnan sektoreilla koko EU-laajuisesti on hyvä asia. Yhtenäiset vähimmäistasoiset velvoitteet kyberturvallisuuden riskienhallinnasta ja merkittävien poikkeamien raportoinnista selkeyttävät ja edistävät kyberturvallisuustoimenpiteitä organisaatioissa.

Täytäntöönpanoehdotus sisältää kuitenkin soveltamiseen liittyviä haasteita hyvinvointialueiden näkökulmasta, joita avaamme seuraavissa kohdissa.

Hyvinvointialueiden lähtökohdat NIS2 direktiiviin

Hyvinvointialueille siirtyi 1.1.2023 vastuu järjestää sosiaalihuollon, terveydenhuollon ja pelastustoimen palvelut. Aiemmat terveydenhuollon toimijat (mm. sairaanhoitopiirit) ovat pääsääntöisesti olleet jo NIS1 direktiivin piirissä ja siten kyberturvallisuuden riskienhallinta on tästä näkökulmasta osalle toimijoista jo tuttua. Organisaatioina hyvinvointialueet ovat kuitenkin vielä nuoria ja soveltajina uusia toimijoita.

Hyvinvointialueet kuuluvat ymmärryksemme mukaan direktiivin toimialaan sekä jo aiemmin toimialaluettelossa olleen terveydenhuoltotoimialan kautta, mutta jatkossa myös julkishallinnon

toimialan sekä valmistustoimialan kautta (ainakin lääkinnällisten laitteiden tuottajana tämä koskee osaa hyvinvointialueista). Pääasiallisesti direktiivin toimeenpano tehdään säätämällä uusi kyberturvallisuuslaki, mutta julkishallinnon toimialan osalta säädökset viedään täydennyksenä tiedonhallintalakiin.

Soveltamisalaa koskevat huomiot

Soveltaminen hyvinvointialueiden toiminnassa

Hyvinvointialueiden käytännön toiminnassa ja palveluita järjestettäessä eri toimialoja on haastavaa erottaa toisistaan. Toiminnallisesti sosiaali- ja terveydenhuollon ja pelastustoimen integraatio haastaa toimialajaon. Tulisiko terveydenhuoltoa ja sosiaalihuoltoa käsitellä eri toimialojen kautta? Kuinka käsitellään tilanteita, joissa sosiaalihuollossa kirjataan terveydenhuollon rekisteriin? Mitä toimintoja hyvinvointialueelta toimialatulkinnan kautta kuuluu julkishallinnon toimialaan? Millaisia riskienhallinnan toimenpiteitä tulee hyvinvointialueen ulottaa kyberturvan näkökulmasta sen järjestämisvastuulla oleviin palveluketjuihin ja sen toimijoihin esim. sopimusjohtamisen kautta?

Miten pelastustoimen palvelut tulee tässä yhteydessä ymmärtää, kun pelastustoimi hyödyntää palvelutoiminnassa osittain TUVE-verkkoa, jonka toimijat eivät ole NIS2 direktiivin parissa? Osittain taas pelastustoimen tietojärjestelmät toimivat hyvinvointialueen verkoissa. Pelastustoimi käsityksemme mukaisesti kuulunee NIS2 direktiivin pariin ollen mahdollinen CER-direktiivin mukainen toimija, mutta ainakin yleisesti osana hyvinvointialuetta julkishallinnon toimialan kautta. Tuleeko pelastustoimi erottaa omaksi toimialakseen, jos se on CER-toimija vai riittääkö se, että sitä käsitellään julkishallinnon kokonaisuudessa?

Hyvinvointialue NIS2 toimijana

Ymmärryksemme mukaan hyvinvointialue näyttäytyy direktiivin soveltamisessa seuraavasti:

-Terveystoimiala (koskenut jo aiemmin), keskeinen toimija, valvova viranomainen Valvira

- Julkishallinnon toimiala (uusi toimiala), tärkeä toimija, valvova viranomainen liikenne- ja viestintävirasto

- Lääkinnällisten laitteiden osalta valmistustoimiala (uusi toimiala), keskeinen toimija, valvova viranomainen Fimea

Direktiivissä kyseiset toimialat ovat erilaisia suhteessa toisiinsa erityisesti valvonnan näkökulmasta. Eroja on mm. ennakkovalvonnan, seuraamusmaksujen, toiminnan rajoittamistoimenpiteiden sekä uhkasakkojen osalta. Direktiivi itsessään ei kerro, miten toimialarajat voidaan organisaatiossa

ymmärtää, jolloin kyse on soveltamisesta. Siksi on syytä tarkentaa viranomaisyhteistyötä ja toimialojen rajoja yhdessä hyvinvointialueiden kanssa.

Käytännön haasteita tulkinnan osalta voi tulla mm. siinä, millaiset koulutukset ovat organisaatioissa riittäviä. Tärkeää olisikin, että koulutusten tarkoitus ja tavoitteet olisivat selkeitä ja koulutusten suuntaaminen riittävän yksiselitteistä, jotta organisaatioiden on mahdollista toteuttaa direktiiviä oikean tasoisesti.

Riskienhallintavelvoitetta koskevat huomiot

-

Raportointivelvoitetta koskevat huomiot

Ilmoittautumismenettelyn osana tulee jatkossa ilmoittaa IP-osoitealueet valvovalle viranomaiselle sekä ylläpitää kyseistä tietoa. Pilvipalveluiden käyttö on lisääntynyt myös julkishallinnossa ja sotessa, sillä pilvipalveluiden käytön on todettu parantavan julkisen hallinnon tietoturvaa. Pilvipalveluiden IP-osoitealueiden muutoksista voi tulla jatkossa organisaatioille kohtuullisen aikaa vievää, mikäli palveluntarjoajat muuttavat niitä useasti. Tähän tulee kehittää lomakepohjasta poikkeava tiedonsiirtotapa (esim. rajapinta), mikäli tarve osoittautuu suureksi.

Valvontaa koskevat huomiot

Hyvinvointialueiden valvonta

Kolmen toimialan kautta direktiivin soveltamisalaan kuuluminen herättää kysymyksiä. Direktiivissä monitoimialaorganisaatioissa valvotaan organisaatioita toimialoittain, eli jokaista toimialaa valvoo kyseisen toimialan valvova viranomainen. Tiedonhallintalaki puolestaan viittaa tiedonhallintayksikköön, ja sitä kautta herääkin kysymys siitä, miten toimialat direktiivin puitteissa tulee rajata suhteessa toisiinsa? Mikä esimerkiksi on hyvinvointialueen julkishallinnon toimialaa?

Tuleeko hyvinvointialueita tulkita tässä yhteydessä siten, että terveystoimiala tulee erottaa omaksi toimialakseen, valmistustoimiala omakseen ja kaikki muut hyvinvointialueen toiminnot kuuluvat julkishallinnon toimialaan? Miten tämä käytännössä voidaan toteuttaa organisaatiossa, jossa palvelutoimintaa pyritään nimenomaisesti integroimaan? Erityisen tärkeää on, että hyvinvointialueilla ja valvovilla viranomaisilla on jatkossa yhteinen ymmärrys siitä, miten toimialakohtainen valvonta kohdistuu hyvinvointialueen toimintoihin ja mikä viranomainen valvoo mitäkin kohdealuetta ja antaa soveltamisesta ohjeita.

Pidämme tärkeänä, että soveltamista ja valvontaa selkeytetään tilanteessa, jossa organisaatio kuuluu NIS2 direktiivin piiriin useamman toimialan kautta. Kaikissa tilanteissa hyvinvointialueisiin kohdistuvan viranomaisten valvonnan tulee olla yhteismitallista ja velvoitteiden toteutumisesta tehtävien tulkintojen selkeitä ja yhtenäisiä silloinkin, kun valvovia viranomaisia on useita. Lisäksi

ohjeistuksen tulee olla yhtenäistä kaikille hyvinvointialueille, Helsingin kaupungille (kun se hoitaa sote-tehtäväänsä) ja hyvinvointiyhtymille.

Emme pidä järkevänä tilannetta, jossa hyvinvointialueet pyytävät ohjeita eri valvontaviranomaisilta tai keskustelevat erikseen valvontaviranomaisten kanssa tulkinnoista ennakkoon tai valvontatoimenpiteiden yhteydessä. Viranomaisvalvonnan yhtenäisyyteen, yhteismitallisuuteen ja valvovien viranomaisten yhteistyöhön tulee kiinnittää erityistä huomiota. Tämä tulee tehdä kansallisesti yhteistyössä.

Seuraamusmaksua koskevat huomiot

kts. soveltamisalaa koskevat huomiot

CSIRT-yksikön tehtäviä koskevat huomiot

-

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

kts. soveltamisalaa koskevat huomiot ja yleiset sekä valvontaa koskevat huomiot

Verkkotunnusvälittäjiä koskevat huomiot

-

Kumottavaksi ehdotettuja säännöksiä koskevat huomiot

Lisäksi on hyvä huomata, että Suomessa sosiaali- ja terveydenhuollon asiakastietolaissa on samankaltaista sääntelyä, jota osittain muokataan tämän direktiivin osalta, mutta myös THL:n määräyksistä löytyy sääntelyä tietoturvaan ja kyberturvaan liittyen jatkossakin mm. sosiaalihuollon osalta.

Vaikutustenarviointia koskevat huomiot

-

Muut huomiot ja avoin palaute esityksestä

Toivoisimme vielä, että hallituksen esityksessä käytetty termistö tarkistettaisiin siten, että se mahdollisimman hyvin vastaisi Suomessa jo tehtyä tietoturvan sanastotyötä (mm. TEPA termipankki ja Kyberturvallisuuden_sanasto.pdf (sanastokeskus.fi)). Tämä helpottaisi käytännön toteutuksia organisaatiossa ja edistäisi lainsäädännön yhteentoimivuutta.

Menna Hanna
Hyvinvointialueyhtiö Hyvil Oy