HYVIL

Hyvilin näkemykset kyberturvallisuusdirektiivin (NIS 2 -direktiivi) täytäntöönpanoa koskevaksi lainsäädännöksi

Hallintovaliokunta, 5.9.2024

Erityisasiantuntija Hanna Menna

Yleistä

- Tietosuoja, tietoturva ja kyberturvallisuus ovat **kriittisiä menestystekijöitä** hyvinvointialueiden toiminnassa. Luottamus julkiseen sosiaali- ja terveydenhuoltoon sekä pelastustoimintaan on kytköksissä näihin.
- Kyberturvallisuusdirektiivin toimeenpanolla on **pitkällä tähtäimellä nähtävissä positiivisia vaikutuksia** niin toimijoiden osaamistason nousuun kuin varautumiseen kyberturvallisuuden osalta.
- **Pidämme hyvänä, että kansallista liikkumavaraa on käytetty** siten, että direktiivin soveltamista ei ole laajennettu vähimmäistasosta ja mahdollisuuksien mukaisesti on huomioitu julkisen hallinnon organisaatioiden ominaispiirteet myös seuraamuksia määrittäessä.

HYVIL

Hyvinvointialueiden lähtökohdat NIS2 direktiiviin

- Organisaatioina hyvinvointialueet ovat nuoria ja NIS2 soveltajina uusia toimijoita, vaikka terveydenhuolto on ollut osa NIS1 soveltamisalaa
- **Hyvinvointialueiden toiminta on moninaista ja vaikka ne tarjoavat sosiaali- ja terveydenhuollon sekä pelastustoimen palveluja kansalaisille, on niillä näiden lisäksi laajasti mm. henkilöstöhallintoon, päätöksentekoon, laskutukseen jne. liittyviä tukitoimintoja.**
- Selvää on, että hyvinvointialue kokonaisuutena on NIS2 soveltamisen piirissä, mutta epäselvää on, miten eri soveltamisalojen osalta tulee yhden hyvinvointialueen sisällä toimia ja miten valvonta tähän suhteutuu kun toimialoja on monta
- **Hyvinvointialueet ovat keskenään erilaisia suhteessa NIS2 direktiiviin**
- Hyvinvointialueet omistavat myös toimijoita (mm. inhouse-yhtiöt) joista osa tulee soveltamisen piiriin

HYVIL

Soveltaminen hyvinvointialueiden toiminnassa

- **Hyvinvointialueiden käytännön toiminnassa ja palveluita järjestettäessä eri toimialoja on haastavaa erottaa toisistaan (esim. sosiaali- ja terveydenhuolto + pelastustoimi, palvelujen integrointi)**
- Esim.
  - 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?

HYVIL

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
- Apteekkitoimiala (uusi toimiala), keskeinen toimija, valvova viranomainen Fimea
- Epäselviä toimialoja ovat pelastustoimi (julkishallinto/CER-direktiivi), jonka valvova viranomainen olisi molemmissa tapauksissa liikenne- ja viestintävirasto sekä tutkimustoiminta, jonka valvova viranomainen olisi liikenne- ja viestintävirasto.

- **Direktiivissä kyseiset toimialat ovat erilaisia suhteessa toisiinsa erityisesti valvonnan näkökulmasta.**
- **HE on selkiytynyt siten, että seuraamusmaksuja tai johdon toiminnan rajoittamistoimenpiteitä ei voitaisi määrätä hyvinvointialueille, joka on mielestämme hyvä ja selkiyttävä asia.**

HYVIL

Hyvinvointialueiden valvonta 1/2

- **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.
- **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, kuten kyberturvallisuuslain 26§ velvoittaa.
- Hallituksen esityksestä käy ilmi, että **viranomaisten yhteistyölle ei olla osoittamassa lisäresursseja**, vaan se nähdään asiaksi, joka voidaan hoitaa nykyisillä resursseilla siitä huolimatta, että NIS2 **valvontaan on tulossa täysin uusia viranomaistahoja,** joilla ei ole kokemusta NIS1 soveltamisesta.

HYVIL

Hyvinvointialueiden valvonta 2/2

Voitaisiinko ilmoittaminen ja rekisteritiedot kuitenkin toteuttaa keskitetysti ja asiakaslähtöisesti sen sijaan, että valvoville viranomaisille toimitetaan erilliset ilmoitukset ja ne sitten ilmoittavat keskitetylle yhteispisteelle sen tarvitsemat tiedot? Tämä edistäisi myös sitä, että koordinaatiota tosiasiallisesti tapahtuu valvovien viranomaisten välillä.

- Valvovien viranomaisten yhteystyön ja koordinaation toimimattomuudella on suoria vaikutuksia hyvinvointialueisiin kohdistuviin valvontatoimiin ja niiden yhteismitallisuuteen. Erityisesti soveltamisen alkuvaiheessa tulee kiinnittää huomiota siihen, että hyvinvointialueiden kaltaisten useammasta näkökulmasta valvottavien toimijoiden valvonnan järjestämiseen, rajoihin ja yhteisiin ohjeisiin kiinnitetään riittävää huomiota.
- Ehdotamme, että Liikenne- ja viestintäviraston koordinaatiovastuuseen kiinnitetään riittävästi resursseja, jotta yhteistyölle saadaan toimivat kehykset, ohjeet ja yhtenäiset toimintamallit
- Hyvinvointialueiden näkökulmasta on kestämätöntä, jos eri valvovat viranomaiset kohdistavat valvontatoimenpiteitä eri tavoilla, tasoilla ja eriaikaisesti organisaatioon ja sen toimintaan.
- Osa valvontaviranomaisista on uusia toimijoita, joilla ei ole NIS1 valvontavelvollisuutta. Osaamisen kehittämiseksi tukea tarvitaan Liikenne- ja viestintävirastolta.

HYVIL

Muita huomioita 1/2

- **Hyvinvointialueiden tulee kattaa NIS2 direktiivin toimeenpanosta syntyvät kustannukset yleiskatteellisesta rahoituksestaan. Iso osa toimijoista joutuu sitomaan suuren osan tietoturvaan ja tietosuojaan varatusta rahoitusosuudesta NIS2 toimeenpanoon ja kyberturvallisuuden tason nostamiseen. Rahoituksen käyttäminen tarkoituksenmukaisiin toimenpiteisiin ja todellisen kyberturvallisuuden tason nostoon vaatii yhtenäisiä ja yhdenmukaisia ohjeita valvovilta viranomaisilta sekä koulutusta & tukea näiden ohjeiden ja mahdollisten kriteerien noudattamiseen.**
- Hyvinvointialueiden omistamien ns. inhouse-yhtiöiden kuuluminen osin NIS2 soveltamisalaan. Näiden toimijoiden osalta tulisi vielä harkita seuraamustoimenpiteiden oikeellisuutta tilanteessa, jossa toimijat käytännössä toimivat julkisella rahalla tarjoten palveluita omistajilleen. Esimerkiksi seuraamusmaksut tulisivat käytännössä omistajien maksettaviksi. Hyvinvointialueet omistavat valtion kanssa erillistoimialayhtiö DigiFinland Oy:n joka tullee osaksi soveltamisalaa ja jonka osalta seuraamustoimenpiteitä tulisi myös harkita.

HYVIL

Muita huomioita 2/2

- Uhkatietojen ja tietoturvallisuusloukkausten kerääminen on annettu CSIRT-yksikölle. Olisi tärkeää, että tätä tietoa jaettaisiin myös toimijoille kyberturvallisuuden parantamiseksi.
- **Substanssilakien tarkempia säädöksiä noudatetaan jatkossakin siltä osin mikäli ne ovat tiukempia, kuin kyberturvallisuuslain menettelyt. Hyvinvointialueiden osalta tarkoittaa esim. sitä, että useat valvovat viranomaiset voivat antaa tarkentavia teknisiä määräyksiä liittyen riskienhallintavelvoitteisiin ja oikeasuhtaisiin toimenpiteisiin.**
- Tiedonhallintalain 18a eroaa määräaikojen suhteen Kyberturvallisuuslain 41§:stä (3 momentti IP-osoitealueet muutosmääräaika 3kk, TihL 18a kaikki muutokset 2vkoa)

HYVIL