Kymenlaakson hyvinvointialue
Kymmenedalens välfärdsområde

Tämä dokumentti on Kymenlaakson hyvinvointialueen lausunto Lausuntopyyntöön: Luonnos hallituksen esitykseksi kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanemiseksi
Lausuntopyynnön diaarinumero: VN/18157/2023

LAUSUNTO:

Yleiset huomiot NIS2-direktiivin tavoitteista ja tarkoituksesta

-

Soveltamisalaa koskevat huomiot

Terveys-toimiala oli mukana jo NIS1-direktiivissä. Hyvinvointialueen kannalta noudatettavaa lainsäädäntöä on jo mm. Asiakastietolaissa. Uusi laki kyberturvallisuuden riskienhallinnasta lisää velvoittavan lainsäädännön määrää, mutta toisaalta yksinkertaistaa kyber- ja tietoturvallisuuden toteuttamista, jos eri lakien säädökset ovat yhtenäisiä ja pätemisjärjestys selvästi esitetty.

Riskienhallintavelvoitetta koskevat huomiot

"Kaikki vaaratekijät" on absoluuttinen muotoilu ja aiheutti ongelmia myös Asiakastietolaissa ("Kaikki potilastiedot"). Sanamuoto tulee suoraan direktiivistä, joten sitä ei muutettane. Mutta huomioitavaa on se, HVA Tärkeänä toimijana ei ole ennakkovalvonnan alainen. Riskienhallinnan kattavuutta (kaikki vaaratekijät) arvioitaneen mahdollisissa jälkikäteisvalvonnoissa. Lain kyberturvallisuuden riskienhallinnasta ehdotetun 8 § perusteluissa (HE s. 119) on laajempi kuvaus kaikki vaaratekijät huomioivan lähestymistavan sisällöstä kuin ehdotetussa Tiedonhallintalain 18 b § perusteluissa (HE s. 161). Molempien perustelutekstien tulisi olla samansisältöiset, jotta HVA:lla ei ole erilaisia tulkintoja Terveys- ja Julkishallinto -toimialojen välillä.

Hyvinvointialueen on järjestettävä riskienhallintansa sekä Tiedonhallintalain (Julkishallinto) että uuden lain kyberturvallisuuden riskienhallinnasta (Terveys) mukaisesti. Käytännön kannalta olisi tärkeää, että pykälien ja momenttien järjestys ja sanamuoto olisivat mahdollisimman yhteneväiset Tiedonhallintalaissa ja laissa kyberturvallisuuden riskienhallinnasta. Nyt mm. TiHL 18b § on molemmat "Kyberturvallisuuden riskienhallintavelvoite ja riskienhallinnan toimintamalli", kun taas ehdotetussa riskienhallintalaissa on erikseen 7 § "Kyberturvallisuuden riskienhallintavelvoite" ja 8 § "Kyberturvallisuuden riskienhallinnan toimintamalli"

Lisäksi on huomioitava, että Pelastustoimen palvelutasopäätös perustuu toimintaympäristön riskien arviointiin. Kaikki vaaratekijät huomioiva, kokonaisvaltainen, fyysisen maailman, tietoturvallisuuden ja tietosuojankin huomioiva riskienarviointi on edullisempaa toteuttaa hyvinvointialueen organisaatiossa, mikäli riskienhallintaan kohdistuvat vaatimukset ovat mahdollisimman yhteensopivat kaikilta osin. Yhteensopivat vaatimukset myös kannustavat organisaatioita järjestämään riskienhallintansa siten, että se on yhtenäinen johtamiskokonaisuus ja huomioi NIS2-direktiivin tavoitteet yhteiskunnan toimivuuden varmistamisessa.

Raportointivelvoitetta koskevat huomiot

Yhtenäisen raportointikanavan toteuttamisen kannalta olisi hyvä, että pykälien ja momenttien järjestys ja sanamuoto olisivat mahdollisimman yhteneväiset Tiedonhallintalaissa ja laissa kyberturvallisuuden riskienhallinnasta. Nyt mm. TiHL 18b § on molemmat "Kyberturvallisuuden riskienhallintavelvoite ja riskienhallinnan toimintamalli", kun taas ehdotetussa riskienhallintalaissa on erikseen 7 § "Kyberturvallisuuden riskienhallintavelvoite" ja 8 § "Kyberturvallisuuden riskienhallinnan toimintamalli"

Valvontaa koskevat huomiot
Hyvinvointialueen toimintaan kohdistuu valvontaa usealta eri taholta:
- Terveys-toimiala: Valvira sekä Asiakastietolain että uuden lain kyberturvallisuuden riskienhallinnasta mukaisesti
- Julkishallinnon toimiala: Liikenne- ja viestintävirasto Tiedonhallintalain mukaisesti
- Valmistus/Lääkinnälliset laitteet – toimiala siltä osin, kun HVA toimii valmistajana: Fimea, uuden lain kyberturvallisuuden riskienhallinnasta mukaisesti.

Hyvinvointialueen riskienhallinnassa ja tietojärjestelmien elinkaarivaatimusten hallinnassa on tärkeää, että valvovien viranomaisten vaatimukset ja toiminta ovat keskenään koordinoituja ja yhdenmukaisia, myös sanamuodoiltaan, jotta mahdollisissa jälkivalvontatapauksissa ei synny ristiriitoja sovellettavien vaatimusten välille.

Seuraamusmaksua koskevat huomiot
-

CSIRT-yksikön tehtäviä koskevat huomiot
-

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot
TiHL 4a luvun ja lain kyberturvallisuuden riskienhallinnasta kanssa 2 luvun rakenteen ja sisällön yhtenäistäminen helpottaisi HVA:n yhteistyötä yksityisten Terveystoimialan, sekä kansainvälisten toimijoiden kanssa, kun ei tarvitsisi varmistaa sanamuotoja sekä Tiedonhallintalain että lain kyberturvallisuuden riskienhallinnasta (ja NIS2 direktiivin) kanssa.

Lakiesitykseen kyberturvallisuuden riskienhallinnasta ei sisälly mahdollista asetuksenantovaltuutusta standardien käytöstä. Tiedonhallintalain kohdalla tällainen mahdollisuus on mainittu (HE s. 232). Voiko tästä aiheutua, että HVA:lle kohdistuisi standardien käyttövaatimus Tiedohallintalain kautta, mutta se ei kohdistuisi Terveystoimialaan?

Sinänsä viittaukset standardien käyttöön olisivat tervetulleita, koska moni organisaatio on omaehtoisesti lähtenyt soveltamaan ISO/IEC hallintajärjestelmästandardeja (9001, 27001, jne.). Tiedonhallintalain ja asiakastietolain perusteella annetuissa ohjeissa ja suosituksissa käsitellään yleensä samoja tietoturvan hallintakeinoja kuin standardeissa, mutta osin eri sanoin. Tästä aiheutuu turhaa yhteensovittamistyötä organisaatioissa, joiden on täytettävä sekä lakiperusteiset vaatimukset että vapaaehtoiseen sertifiointiin tarvittavat standardivaatimukset.

Verkkotunnusvälittäjiä koskevat huomiot
-
Kumottavaksi ehdotettuja säännöksiä koskevat huomiot
-
Vaikutustenarviointia koskevat huomiot
-
Muut huomiot ja avoin palaute esityksestä
Riskienhallintatoimenpiteisiin sisältyy kohta d) toimitusketjun turvallisuus. Hyvinvointialueen toimitusketjuihin sisältyy useita NIS2-toimialoihin kuuluvia organisaatioita. Toimitusketjujen toimijoihin kohdistuu samoja vaatimuksia ja yksi toimija voi olla toimittaja useammalle ”alavirran”

toimijalle. NIS2-direktiivin toimeenpanon ohjauksessa olisi hyvä löytää yhteistyömalleja, joissa mm. toimitusketjujen sopimuksiin sisältyviä vastuukuvauksia yms. laadittaisiin yhteisesti, ei toimijakohtaisissa ”siiloissa”, kukin erikseen omin resurssein.

Lausunnon toimitti:
Matti Ahola, tietohallintojohtaja
matti.ahola@kymenhva.fi, p. 020633 2006