Länsi-Uudenmaan hyvinvointialue

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

Kiitämme mahdollisuudesta lausua luonnoksesta hallituksen esitykseksi kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanemiseksi. Direktiivin ja sitä täytäntöönpanevan lainsäädännön tavoite on lähtökohtaisesti kannatettava. Hyvinvointialueita koskettava tietoturva- ja tietosuojasääntely on kuitenkin sangen runsas ja yksityiskohtainen, ja lausuntopyynnön kohteena olevalla lainsäädännöllä luodaan tosiasiallisesti uusia velvoitteita osin vanhojen päälle. Kokonaisuudesta tulee helposti erittäin monimutkainen.

On myös syytä huomata, että kyvykkyydet ja osaaminen eivät vahvistu sääntelyllä, vaan sen toimeenpanon vaatimilla koulutuksilla, projekteilla ja myös lisäresursseilla. Samoin uusilla velvoitteilla on vaikutuksia merkittävään osaan hyvinvointialueen ict-sopimuksia.

Tältä osin on todettava, että hallituksen esityksen taloudelliset vaikutukset säädöksen määräyksiä toteuttaville toimijoille on arvioitu ylioptimistisesti. Tosiasiallinen kustannusvaikutus on merkittävä eikä velvoitteita kyetä täyttämään ilman mm henkilöstövaikutuksia.

Soveltamisalaa koskevat huomiot

Soveltamisalan osalta keskeisin kysymys liittyy hyvinvointialueen monialaiseen rooliin sekä terveydenhuollon, sosiaalihuollon, pelastustoimen järjestäjänä että yleishallinnollisena toimijana. Onko hyvinvointialue yksi toimija, jolla yhtenäinen sääntely vai eri toimialojensa osalta erikseen säädelty? Toimialasääntelyä on toki muutenkin, mutta tietoturvan kaltaiset tukitoiminnot on organisoitu keskitetysti.

Riskienhallintavelvoitetta koskevat huomiot

Ehdotetussa lainsäädännössä kuvattu kyberturvallisuuden riskienhallinnan toimintamalli on sellaisenaan uusi käsite, joka vastaa muussa lainsäädännössä ja toimalakohtaisissamääräyksissä

edellytettyjä tietoturvasuunnitelmia ja -toimintamalleja, mutta eri termein ja laajuuksin kuin muualla. Yksityiskohtien tarkempi ohjaus ratkaisee kuinka merkittävä ero tosiasiallisesti on, ja yksityiskohdilla on myös merkittäviä vaikutuksia kustannuksiin.

Organisaation johdon osaamisvaatimuksen konkreettinen sisältö vaatii tarkennusta. Tämä on erityisen tärkeää johtuen soveltamisalaan ja valvoviin viranomaisiin liittyvistä kysymyksistä. Pahimmillaan moniportaiset vaatimukset johdon osaamiselle voivat olla kokonaisuutena epärealistisen laajoja.

Raportointivelvoitetta koskevat huomiot

Raportointivelvoitteen kohdalla mainittu 24h ensi-ilmoituksen aikaraja (ja siitä seuraava 72h jatkoilmoitusvaatimus) ovat tiukkoja. Epäselväksi jää, millainen tapahtuma laukaisee ilmoitusvelvoitteen. Toisaalta ensi-ilmoituksen vaatimus tarkoittaa tosiasiallisesti laajamittaista, koko toimittaja- ja alihankintaketjun läpimenevää valmiutta, joka tarkoittaisi muutoksia merkittävään osaan ict-sopimuksista sekä myös lisäresurssointia omaan toimintaan. Tämä on toteutettavissa, mutta rahalliset vaikutukset on esityksessä aliarvioitu.

Myös IP-osoitteiden ilmoitusvelvoite on raskas jatkuvan ylläpidon vaatimuksineen. Velvoite on paljon suurempi kuin mitä vaikutuksenarviointi antaa ymmärtää, eikä ole realistista ainakaan ilman teknistä rajapintaa. Epäselväksi jää mitä sillä tosiasiallisesti tavoitellaan ja toisaalta mitä tarkoittaa IP-osoitealue tässä kontekstissa. Toisaalta erilaisten pilvipalveluiden (SaaS, IaaS ja PaaS) kasvavan merkityksen takia vaatimus on vanhentunut jo lähtöhetkellä, käytössä oleva ip-avaruus on toissijainen ja muuttuva tekninen yksityiskohta.

Valvontaa koskevat huomiot

Hallituksen esityksessä valvontavastuu jakautuu useille eri viranomaisille, toimialasääntelyn mukaisen valvonnan lisäksi. Kokonaisuuden kannalta olisi keskeistä selventää miten kyseisten viranomaisten valvontavastuut rajataan siten, ettei synny päällekkäistä valvontaa tai vastaavasti jää valvonnan ulkopuolisia osa-alueita. Varsinkin, kun sekä organisaation johto, että moni keskitetty tekninen ratkaisu vaikuttavat kaikkiin organisaation toimialoihin, on epäselvää, minkä valvovan viranomaisen vastuulle kuuluu näiden yhteisten osa-alueiden hallintatoimien osalta valvontavastuu. Käytännössä päällekkäiset valvontarakenteet aiheuttavat lisäkustannuksia ja epäselvyyttä sekä valvoville että valvottaville toimijoille.

Seuraamusmaksua koskevat huomiot

Ei lausuttavaa.

CSIRT-yksikön tehtäviä koskevat huomiot

Ei lausuttavaa.

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

Tiedonhallintalakiin esitettävät muutokset ovat 4. luvun osalta samansisältöisiä kuin uuden kyberturvallisuuden riskienhallintalain säädökset ja toiston välttämiseksi tiedonhallintalaissa voisi

viitata kyberturvallisuuden riskienhallintalakiin. Tämä on erityisen tärkeää tulevaisuudessa kun lainsääntöä päivitetään, jolloin vaarana on että ko. lait erkanevat toisistaan tahattomasti synnyttäen ristiriitaista sääntelyä.

Verkkotunnusvälittäjiä koskevat huomiot

Ei lausuttavaa.

Kumottavaksi ehdotettuja säännöksiä koskevat huomiot

Ei lausuttavaa.

Vaikutustenarviointia koskevat huomiot

Ehdotetun lainsäädännön vaikutuksiin on kiinnitetty huomiota muulla tässä lausunnossa, mutta selvyyden vuoksi toistettakoon että kiristyvät, ja osin hyvin yksityiskohtaisetkin vaatimukset tulevan tosiasiallisesti lisäämään kustannuksia merkittävästi, varsinkin kun velvoitteita siirretään hankintasopimuksiin. Vaikutuksia ei voida tässä vaiheessa edes realistisesti arvioida, koska sekä komission toimeenpanosäännöksilla kuin niitä tulkitsevilla kansallisilla ohjeilla ja määräyksillä on olennainen vaikutus siihen millaisiksi vaadittavat muutokset muodostuvat.

Muut huomiot ja avoin palaute esityksestä

21 artiklan 1 kohta korostaa teknisten, operatiivisten ja organisatoristen toimenpiteiden tärkeyttä riskienhallinnassa, se jättää avoimeksi, että kuinka näitä toimenpiteitä tarkasti arvioidaan ja päivitetään ajan myötä ja tähän kansallisessa toimeenpanossa tulisi kiinnittää huomiota. Jatkuvasti muuttuva kybermaailma edellyttää tarkennuksia siitä, miten toimijoiden tulee riskienhallintastrategioitaan säännöllisesti arvioida ja päivittää vastaamaan uusia uhkia ja haavoittuvuuksia.

21 artiklan 2 kohdassa mainitaan useita tärkeitä hallintatoimenpiteitä, kuten riskianalyysit ja poikkeamien käsittely ja kansallisessa toimeenpanossa tulisi huomioida, kuinka näitä toimenpiteitä tulisi soveltaa käytännössä. Esimerkiksi toimitusketjun turvallisuuden osalta tulisi määritellä tarkemmin, millaisia toimenpiteitä jäsenvaltioiden tulisi ottaa käyttöön varmistaakseen toimitusketjunsa turvallisuuden kaikissa vaiheissa.

Kolmanneksi, 5 kohdan mukaan komissio aikoo hyväksyä täytäntöönpanosäädöksiä, jotka määrittelevät teknisiä ja menetelmällisiä vaatimuksia. Tämä on toki tärkeä askel, mutta olennaista on, että nämä säädökset ovat riittävän joustavia, jotta ne voivat mukautua nopeasti kehittyvään teknologiaan ja kyberuhkiin. Lisäksi olisi hyvä, että kansalliset täytäntöönpanosäädökset ottaisivat huomioon eri toimialojen ja toimijoiden erityistarpeet, jotta ne voivat olla mahdollisimman tehokkaita ja soveltuvia laajasti erilaisiin organisaatioihin.

NIS2-direktiivin kyberturvallisuusriskien hallintatoimenpiteet ovat kattavia, mutta niiden toteutuksessa ja kansallisessa täytäntöönpanossa sekä soveltamisessa tarvitaan lisätarkennuksia, erityisesti jatkuvan arvioinnin, käytännön soveltamisen ja joustavuuden näkökulmista.

Kuukka Tommi
Länsi-Uudenmaan hyvinvointialue

Uski Lauri
Länsi-Uudenmaan hyvinvointialue - Digipalvelut