Solita Oy

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

Yleisesti ottaen voidaan todeta, että Solita katsoo NIS2-direktiivin olevan tervetullut parannus kriittisen infrastruktuurin toimijoiden tietoturvaan ja riskienhallintavelvoitteisiin. Direktiivin pääasiallinen täytäntöönpanoinstrumentti, eli ehdotettu laki kyberturvallisuuden riskienhallinnasta sisältää kuitenkin tiettyjä tulkintaepäselvyyksiä, jotka tulisi ottaa paremmin huomioon tai korjata hallituksen esityksessä ja/tai lain tasolla. Näitä havaitsemiamme tulkintaepäselvyyksiä pyrimme avaamaan tarkemmin jäljempänä.

Soveltamisalaa koskevat huomiot

NIS2-direktiivin mukaisesti sääntelyn alaan kuuluvia TVT-palvelutarjoajia olisivat yritysten väliset hallinta- ja tietoturvapalveluntarjoajat, jotka ovat keskisuuria tai suuria yrityksiä. Ehdotetun lain kyberturvallisuuden riskienhallinnasta mukaisesti hallintapalveluntarjoajalla tarkoitettaisiin toimijaa, joka tarjoaa TVT-tuotteiden, verkkojen, infrastruktuurin, sovellusten tai muiden viestintäverkkojen ja tietojärjestelmien asentamiseen, hallintaan, käyttöön tai ylläpitoon liittyviä palveluja joko asiakkaan tiloissa tai etäyhteyden välityksellä toteutettavan tuen tai aktiivisen ylläpidon muodossa. Tämän osalta huomio kiinnittyy siihen, että määritelmässä ei oteta yksiselitteisesti kantaa, kuuluuko tietojärjestelmien ohjelmointityö hallintapalveluntarjoajan määritelmän piiriin. Suotavaa olisi, että tähän kysymykseen saadaan tarkennuksia, jotta TVT-palveluntarjoajat pystyvät paremmin arvioimaan, missä määrin heidän toimintaansa sovelletaan ehdotettua sääntelyä.

TVT-palveluntarjoajat toimivat usein kansainvälisesti ja/tai useissa eri EU-jäsenvaltioissa. Tämän seurauksena ehdotetun lain yhteensovittaminen muiden jäsenvaltioiden kansallisten täytäntöönpanevien lakien kanssa voi olla haastavaa, jos NIS2-direktiivin täytäntöönpanossa esiintyy eroja eri jäsenvaltioiden välillä. Tätä haastetta ei poista se, että TVT-palveluntarjoajan katsotaan kuuluvan vain sen jäsenvaltion lainkäyttövaltaan, jossa sen päätoimipaikka sijaitsee, koska palveluntarjoajan toiminta toisessa jäsenvaltiossa sijaitsevan NIS2-direktiivin piiriin kuuluvan asiakkaan lukuun aiheuttaa vääjäämättä sen, että kyseisessä toisessa jäsenvaltiossa vallitsevat tulkinnat ja käytännöt ottavat etusijan. Tältä osin on myös huomioitava, että ehdotettu hallituksen esitys viittaa siihen, että sääntelyn piiriin kuuluvan toimijan voi olla tarpeellista tehdä muutoksia

alihankkijoiden kanssa tehtäviin sopimuksiin tietoturvaa koskien, jotta toimija pystyy varmistamaan kyberturvallisuusriskien hallintatoimenpiteitä koskevat velvoitteensa. Näin ollen on erittäin tärkeää, että jäsenvaltiot varmistavat mahdollisimman yhdenmukaiset tulkinnat ja ohjeistukset tällaisia sopimuksellisia muutoksia ja vaatimuksia koskien, jotta toimijoiden hallinnollinen ja sopimusten uudelleen neuvotteluun liittyvä taakka pysyy kohtuullisena. Euroopan laajuiset, sitomattomat, vakiosopimusehdot voisivat olla hyödyllisiä epävarmuuden ja hallinnollisen taakan vähentämiseksi.

Riskienhallintavelvoitetta koskevat huomiot

Ehdotetun lain kybertuvallisuuden riskienhallinnasta 9 §:ssä määritetty lista riskienhallinnan toimenpiteistä on epäselvä niiltä osin, mitkä nimenomaiset toimenpiteet katsotaan riittäviksi säännöksen vaatimusten täyttämiseksi. On toki ymmärrettävää, että lain tasolla on haastavaa määrittää tarkasti (kulloinkin) vaadittavia toimenpiteitä. Toisaalta säännösehdotuksessa ei tehdä viittauksia taustalla vaikuttaviin kansainvälisiin tietoturvakehyksiin, kuten ISO 27001, ISO 27002 tai CIS kontrolleihin. Tämä aiheuttaa epäselvyyttä siitä, mitä tarkalleen ottaen vaaditaan riskienhallinnan toimenpiteiden osalta. Näin ollen olisi suositeltavaa, että ehdotettuun lakiin tehtäisiin riskienhallintatoimenpiteiden kontekstissa nimenomaisempi viittaus kansainvälisesti tunnistettuihin tietoturvastandardeihin.

Lisäksi ehdotetun lain 9 §:n mukaiset riskienhallintaa koskevat velvoitteet sisältävät velvoitteen henkilöstöturvallisuuden varmistamiseksi. Edelleen ehdotetussa hallituksen esityksessä tarkennetaan, että tämä pitää sisällään velvoitteen toteuttaa asianmukaiset menettelyt henkilöstön taustatarkastusten suorittamiseksi. Koska ehdotettu laki asettaa toimijoille velvoitteen suorittaa henkilöstöä koskevia taustatarkastuksia, on taustatarkastusten suorittamista koskevaa sääntelyn nykytilaa Suomessa arvioitava uudelleen. Tämä johtuu siitä, että turvallisuusselvityslain mukaisia turvallisuusselvityksiä tekevät viranomaiset tulkitsevat turvallisuusselvityslakia tällä hetkellä erittäin tiukasti, minkä johdosta ainakin hallintapalveluntarjoajien on hyvin vaikeaa saada oikeutta teettää turvallisuusselvityksiä omaa henkilöstöään koskien. Näin ollen NIS2-direktiivin kansallisessa täytäntöönpanossa tulisi varmistaa, että ehdotetun lain velvoitteiden piiriin kuuluvat toimijat, mukaan lukien hallintapalveluntarjoajat, voivat kohtuudella suorittaa turvallisuusselvityksiä henkilöstöään koskien. Kansallisen täytäntöönpanon tulisikin varmistaa, että ehdotetun lain piiriin kuuluville toimijoille muodostuu oikeudellinen perusta suorittaa turvallisuusselvityksiä turvallisuusselvityslain alla.

Raportointivelvoitetta koskevat huomiot

Ehdotetun lain kybertuvallisuuden riskienhallinnasta mukainen “merkittävää poikkeamaa” koskeva määritelmä on ongelmallinen. Lain 11 §:n mukaan merkittävällä poikkeamalla tarkoitetaan poikkeamaa, joka on aiheuttanut tai voi aiheuttaa palvelujen vakavan toimintahäiriön tai asianomaiselle toimijalle taloudellisia tappioita taikka poikkeama on vaikuttanut tai voi vaikuttaa muihin luonnollisiin henkilöihin tai oikeushenkilöihin aiheuttamalla huomattavaa aineellista tai aineetonta vahinkoa. Vaikka määritelmä vaikuttaa ensisilmäyksellä yksityiskohtaiselta, on sen nykyinen sanamuoto sellainen, että merkittävän poikkeaman piiriin voitaisiin katsoa kuuluvan myös sellaisia poikkeamia, jotka eivät niiden tosiasiallisen luonteen ja vaikutuksen perusteella ole merkittäviä. Ehdotetun merkittävää poikkeamaa koskevan määritelmän tiukka sanatulkinta viittaa siihen, että mikä tahansa taloudellinen menetys, riippumatta sen vähäisyydestä, tulisi ilmoittaa viranomaiselle. Merkittävän poikkeaman tulkinta tulee lopulta tapahtumaan subjektiivisesti ja nykyisessä sanamuodossaan se jättää hyvin paljon harkintavaltaa päätöksentekijälle. Asiassa on

syytä huomioida, että jo yksittäinen kalasteluviestikin voi aiheuttaa jonkin asteista taloudellista menetystä yritykselle, mikä merkittävää poikkeamaa koskevan määritelmän perusteella johtaisi velvollisuuteen ilmoittaa poikkeamasta lain 11 §:n menettelyn mukaisesti. Suositeltavaa olisi, että merkittävää poikkeamaa ja toimijan ilmoitusvelvoitteen soveltamiskynnystä nostetaan, jotta ilmoitusvelvoitteen tarkoitus ja tavoitteet tullaan saavuttamaan paremmin. Säännöksen tarkoitusta ja tavoitetta palvelisi paremmin ilmoitusvelvoite, joka sidotaan pelkästään merkittäviin aineellisiin tai aineettomiin vahinkoihin (kuten säännöksessä todettu sen osalta, kun poikkeama ei aiheuta toimijalle taloudellisia vahinkoja, mutta vaikuttaa muihin luonnollisiin tai oikeushenkilöihin). Vaihtoehtoisesti määritelmää tulisi muuttaa siten, että toimijan taloudelliseen tappioon viittaavaa edellytystä nostetaan siten, että taloudellisella tappiolla tarkoitetaan jotain muuta kuin vain vähäisiä taloudellisia menetyksiä. Mikäli nykyistä merkittävän poikkeaman määritelmän sanamuotoa ei muuteta, on olemassa aito riski siitä, että toimijat tulevat tekemään ilmoituksia varmuuden vuoksi myös vähäisistä poikkeamista, mikä aiheuttaisi tarpeetonta hallinnollista taakkaa sekä toimijoille että valvovalle viranomaiselle.

Edelleen poikkeamailmoitusten määräajat ovat erittäin tiukkoja, mistä johtuen toimijoiden saatavilla tulisi olla vakioituja lomakkeita, joiden kautta viranomaisilmoitukset voisi suorittaa. Viranomaisilmoituksia koskevat lomakkeet tulisi lisäksi sovittaa yhteen yleisen tietosuoja-asetuksen mukaisten tietoturvaloukkauksia koskevien ilmoitusten ja näihin liittyvien lomakkeiden kanssa, sillä kyberturvallisuuspoikkeamat voivat useissa tapauksissa koskea myös henkilötietoja.

Valvontaa koskevat huomiot

Ei huomioita.

Seuraamusmaksua koskevat huomiot

Ei huomioita.

CSIRT-yksikön tehtäviä koskevat huomiot

Ei huomioita.

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

Ei huomioita.

Verkkotunnusvälittäjiä koskevat huomiot

Ei huomioita.

Kumottavaksi ehdotettuja säännöksiä koskevat huomiot

Ei huomioita.

Vaikutustenarviointia koskevat huomiot

Ei huomioita.

Muut huomiot ja avoin palaute esityksestä

Ei muita huomioita.

Nurminen Saana
Solita Oy