Nordcloud Oy

Lausunto

24.11.2023 NC-NIS2D-2023

Asia: VN/18157/2023

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

Lausunnonantajan lausunto

Yleiset huomiot NIS2-direktiivin tavoitteista ja tarkoituksesta

Yleisellä tasolla pidämme lakiesitysluonnoksen tavoitteita kannetettavina. Keskisimpänän tulkintahaasteena pidämme sitä, että esityksessä soveltamisalaan kuuluva toimija ja palvelu on lähes poikkeuksetta kytketty yhteen, eli oletusarvoisesti puhutaan aina toimijasta ja kyseisen toimijan palvelusta (ymmärtääksemme tällä viitataan palvelun omistajuuteen). Kuitenkin ottaen huomioon esim. TVT-hallintapalvelun tuottajan roolin esim. tuki- ja ylläpitopalveluiden tuottajana, tulisi huomioida se, ettei ko. palveluntuottaja useinkaan ole lakiehdotuksessa tarkoitetulla tavalla sellainen toimija, joka samanaikaisesti olisi esim. tuottamiensa palveluiden kohteena olevan tietojärjestelmän tai palvelun omistaja.

Tavoitteiden kannalta olennaista on pystyä tukemaan erityisesti monikansallisten yritysten toimintaa missä paikalliset viranomaiset viestivät paikallisilla kielillä mutta uhat saattavat koskettaa konsernien eri osia mutta organisaatiolla ei mahdollisesti ole kykyä olla yhteydeydessä jokaisen maan viranomaiseen. EU-tason englanninkielistä uhka-viestintää tulisi kasvattaa ja konsolidoida maakohtaisia hälytyksiä jotta myös yrityksillä olisi parempi tilannekuva EU:n alueella tapahtuvista uhista.

Soveltamisalaa koskevat huomiot

Soveltamisalan merkittävä laajentuminen verrattuna NIS1-direktiiviin voi arviomme mukaan vaikuttaa ehdotetun lainsäädännön mukaisiin TVT-hallintapalveluiden tarjoajiin sekä suoraan että välillisesti. Sen lisäksi, että ko. palveluntarjoajat kuuluvat mahdollisesti kokoluokkansa perusteella suoraan lainsäädännön soveltamisalaan, tulevat tämän ohella huomioitavaksi mainittujen palveluntuottajien asiakkaiden vaatimukset, joiden arvioimme lisääntyvän ja heijastuvan sopimusvelvoitteisiin asiakkaita kohtaan etenkin tilanteessa, jossa asiakkaat lähtökohtaisesti kuuluvat esim. toimialansa perusteella NIS2-direktiivin soveltamisalaan.

Riskienhallintavelvoitetta koskevat huomiot

-

Raportointivelvoitetta koskevat huomiot

Koska lähes mikä tahansa kyberhäiriö voi aiheuttaa taloudellista tappiota, merkittävyyden kynnys on hieman epätarkka. Taloudellisen tappion osalta raja-arvo pitäisi sitoa esim. Riskienhallinnan kautta määritettävään yrityksen liiketoiminnan kokoon suhteutettuun “merkittävän tappion” kriteeristöön jotta yritys voi itse paremmin määrittää milloin mahdollinen tappio on yrityksen kannalta merkittävä ja näin ollen, milloin merkittävän poikkeaman raportointikynnys ylittyy.

Kohdassa 2.6 kirjoitusvirhe: “Ilmoitukseen tulee tapauksen mukaan sisällyttää tieto siitä, epäilläänkö poikkeaman johtuvan lainvastaisista” (pitäisi olla lainvastaisista).

Ensi-ilmoituksen osalta etenkin rajat ylittävän poikkeaman ilmoitusvastuissa on tehtävä selväksi minne ilmoitus tulee tehdä ja miltä osin viranomaiset ilmoittavat poikkeamasta eteenpäin. HE muoto “Kun poikkeamalla on rajat ylittäviä vaikutuksia, siitä on tiedotettava niille muille jäsenvaltioille, joihin poikkeama vaikuttaa sekä ENISA:lle.” voi johtaa monikansalliselle toimijalle vaatimukseen ilmoittaa samasta asiasta kymmenien maiden viranomaisille eri tavoin.

Kansainvälinen standardointi ilmoituskanavien tai edelleenilmoitusten automatisointiin on ehdoton edellytys ja kohta 2.6 osin on ristiriidassa §6 kanssa missä

“Pykälän 3 momentissa säädettäisiin poikkeuksesta 1 momentin pääsääntöön eräiden toimijoiden osalta NIS2-direktiivin 26 artiklan 1 kohdan b alakohtaa ja 26 artiklan 2-5 kohtia vastaavasti. Momentissa tarkoitetut toimijat kuuluisivat NIS2-direktiivissä tarkoitettujen velvoitteiden osalta sen jäsenvaltion lainkäyttövaltaan, jossa sijaitsee toimijan NIS2-direktiivin 26 artiklan 2 kohdassa tarkoitettu päätoimipaikka”

Eli kokonaisuus monikansallisten toimijoiden velvoitteiden osalta on hieman epäselvä koskien sitä miltä osin velvoitteita tulee toteuttaa myös rajat ylittävissä tilanteissa.

Poistaako Lain 17§ toteamus viranomaisen tekemästä ilmoituksesta tietosuojavaltuutetulle rekisterinpitäjän vastuun ilmoittaa asiasta tietosuojavaltuutetulle myös, vai tuleeko samasta tapauksesta ilmoittaa yhä riippumattomasti sekä CSIRT-yksikölle että tietosuojavaltuutetulle, CSIRT-yksikön ilmoittaen uudestaan samasta asiasta tietosuojavaltuutettua.

Valvontaa koskevat huomiot

Lain 43§ mukaisten toimijan IP-alueiden ilmoittamisessa tulisi määritellä miten toimia jos toimijalla ei ole yleistä pakotettua yritysverkkoa, onko velvoite ilmoittaa selvästi tiedossa olevien IP-alueiden tiedot vai kaikkien toimijan palveluiden & päätelaitteiden IP-alueet. Miten toimia esim. SaaS-palveluiden käytön osalta jossa toimijan kriittiset alustat ovat täysin SaaS-pohjaisia ja näin ollen IP-alueet jaettuna muidenkin samaa SaaS-palvelua käyttävien toimijoiden kanssa, ainoina toimijaa yksilöivinä tietoina ollen päätelaitteiden IP:t, jotka taas voivat olla myös kotiosoitteita.

Seuraamusmaksua koskevat huomiot

-

CSIRT-yksikön tehtäviä koskevat huomiot

-

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

-

Verkkotunnusvälittäjiä koskevat huomiot

-

Kumottavaksi ehdotettuja säännöksiä koskevat huomiot

-

Vaikutustenarviointia koskevat huomiot

Lakiesityksen kustannusvaikutusten arvioinnissa on keskitytty pääsääntöisesti toimijoille aiheutuvien välittömien kustannusten arviointiin. Emme sinällään halua ottaa kantaa kustannusvaikutusten arvioituun kokoluokkaan, mutta toteamme, että lisääntyvät raportointivaatimukset sekä mahdolliset merkittäviin poikkeamiin reagoinnin valmius ja kyvykkyydet ovat tekijöitä, joiden arvioimme mahdollisesti vaikuttavan tuotettavien palveluiden hintoihin.

Muut huomiot ja avoin palaute esityksestä

-

Sane Petri
Nordcloud Oy