Telia Finland Oyj

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

Telia Finland Oyj (”Telia”) kiittää mahdollisuudesta lausua luonnoksesta hallituksen esitykseksi eduskunnalle kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöön-panemiseksi.

Viittaamme tämän lausunnon lisäksi FiCom ry:n asiassa antamaan lausuntoon, jonka valmistelussa Telia on ollut mukana ja jota Telia puoltaa kokonaisuudessaan.

Telia haluaa erityisesti nostaa esiin jäljempänä tässä lausunnossa nostetut asiakokonaisuudet hallituksen esityksestä ja sitä koskevasta FiComin lausunnosta.

Telia pitää hyvänä asiana, että NIS2-direktiivin täytäntöönpano ehdotetaan tehtäväksi sen vähimmäistason mukaisesti ja kansallinen liikkumavara täysimääräisesti hyödyntäen. Liian yksityiskohtaiset vaatimukset riskienhallinnan toimenpiteille estävät käytännössä teknologianeutraalien ja riskiperusteisten kyberturvakontrollien käytön ja rajaavat mahdollisuuksia suojautua riskeiltä täysimääräisesti.

Vastaavasti Telia pitää erittäin hyvänä ratkaisuna sitä, että NIS2-direktiivi täytäntöönpannaan keskitetysti yhdellä lailla kyberturvallisuuden riskienhallinnasta, jolloin yhteiskunnan toiminnan kannalta kriittisten toimijoiden kyberturvallisuuden riskienhallinta- ja raportointivelvoitteet on koottu yhteen sääntelyyn. Telia toivoo, että tässä yhteydessä käydään vielä kriittisesti läpi sektorikohtainen sääntely erityisesti teletoimialalla, jotta vältetään päällekkäinen sääntely.

Soveltamisalaa koskevat huomiot

Soveltamisala rajauksineen on perusteltu ja hyväksyttävä.

Riskienhallintavelvoitetta koskevat huomiot

Riskienhallintatoimenpiteisiin on esitysluonnoksessa pääsääntöisesti jätetty toimijoille harkintavaltaa toimenpiteiden suhteuttamisessa riskeihin ja suojattavan kohteen, kuten viestintäverkon tai tietojärjestelmän merkitykseen nähden. Esityksen perusteluissa viitataan kuitenkin käytänteisiin ja viestintäkanaviin, jollaisia ei voi katsoa kuuluvan peruskyberhygienian piiriin. Esimerkiksi kohdassa 9§ kohta 9 s. 123 todetaan, että “Vakaviin ja muihin toimijoihin ulottuviin poikkeamiin tulisi olla olemassa menettelyt, vastuut ja kommunikointikanavat muiden toimijoiden varoittamiseksi”. Toimijoille pyritään siis antamaan uusia vastuita tunnistaa muut toimijat ja ilmoittaa jollakin tavalla näille merkittävistä poikkeamista. Vaikka yhteistyöfoorumeita on toki olemassa, ne ovat yleensä kansallisen CERT/CSIRT yksikön tai muun kolmannen osapuolen järjestämiä, eivät toimijoiden keskinäisiä viestintäryhmiä. Vastaavasti 9§ kohdassa 11 s. 124 viitattu luottamattomuuden periaate (Zero-trust) ei ole ihan perustason kyberhygieniakäytäntö, vaan sen käyttöönotto voi olla hyvinkin kallista ja haastavaa, jos toimijalla on käytössään paljon legacy-järjestelmiä.

Raportointivelvoitetta koskevat huomiot

Telia pitää huolestuttavana esitysluonnoksen kirjausta, jonka mukaan valvovan viranomaisen edellytetään vastaavan häiriöilmoitusraportteihin ainoastaan virka-aikojen puitteissa. Valvovan viranomaisen ei siis edellytetä päivystävän raportteja iltaisin ja viikonloppuisin. Traficomin CERT:llä on keskeinen rooli informaation ja uhkatilanteen tiedottamisessa kansallisille kriittisen infran toimijoille sekä muille viranomaisille. Jos häiriöilmoitusten vastaanotto ja siten myös Nat CERT tilannetiedotus ei toimi 24/7, asettaa se myös kyseenalaiseksi raportointivaatimuksen aikataulun. Kun merkittävän poikkeaman kriteerit täyttävä häiriö tapahtuu torstai-iltana, on velvollisuus toimittaa ensi ilmoitus perjantaina illalla. Jos tämä liittyy uhkaan, joka voi vaikuttaa myös muiden toimijoiden riski- tai uhkatilanteeseen, miten Traficom CERT pystyy informoimaan muita viranomaisia ja toimijoita viiveettä.

Yleisesti raportointivelvoitteissa on tärkeää kiinnittää huomiota siihen, ettei toimijoille synny päällekkäisiä tai sektorikohtaisesti poikkeavia raportointivelvoitteita. Esitysluonnoksen mukaan sähköisen viestinnän palvelulain 275§ häiriöilmoituksista sekä sen nojalla annettu Traficomin määräys 66 jäävät voimaan siltä osin kuin ne koskevat teleyrityksiä, mikä tarkoittanee käytännössä sektorikohtaista poikkeamaa kyberturvallisuuden riskienhallintalain vaatimuksista. Tämä samoin kuin teleoperaattorien nykyinen tuplaraportointivelvollisuus henkilötietojen tietoturvaloukkauksista tulee esityksessä selkeästi todeta täysin tarpeettomaksi.

On tärkeää, että poikkeamien raportointi kyetään hoitamaan mahdollisimman kevyin menettelyin ja kustannustehokkaasti. Automaation myötä monet poikkeamat hoidetaan ilman ihmisen tekemää manuaalista työtä. Esimerkiksi palvelunestohyökkäysten raportointi onnistuu tällä hetkellä saumattomasti Kyberturvallisuuskeskuksen ja toimijoiden yhteisten rajapintojen kautta. Ei ole tarkoituksenmukaista, että raportointi tulee kuormittamaan tällaista muuten automaation hoitamaa aluetta. Silloin, kun automaattinen raportointi ei ole mahdollista, on raportointikäytännöt ja yksityiskohtaisuuden taso pidettävä mahdollisimman kevyenä ja maltillisena, jotta raportointi ei vie liiaksi aikaa itse poikkeaman tutkimiselta, torjumiselta ja vaurioiden korjaamiselta. Erityisesti on

syytä kiinnittää huomiota myös siihen, että poikkeamien raportointi on mahdollista hoitaa yhden viranomaisen kautta niin kansallisesti kuin myös rajat ylittävien poikkeamien osalta.

Liian raskaiden raportointimenettelyiden lisäksi epäselvät ja laajasti tulkittavat raportointivelvoitteet johtavat tarpeettomaan työhön. Esimerkiksi kyberuhka ja läheltä piti tilanne vaativat tuekseen tarkempia määrittelyitä, jotta niiden soveltaminen tarkoituksenmukaisella tavalla on käytännössä mahdollista.

Valvontaa koskevat huomiot

Telia kannattaa kansallisen liikkumavaran käyttämistä siinä, että valvova viranomainen saa kohdentaa valvontaa riskiperusteisesti ja ensisijaisesti keskeisiin toimijoihin, kuten esityksessä on ehdotettu. Turvallisuusauditointien osalta voisi olla hyvä harkita myös mahdollisuuksia suorittaa auditointi yrityksen itsearviointina esimerkiksi Traficomin kybermittaria hyödyntäen.

Seuraamusmaksua koskevat huomiot

Esitysluonnoksessa tehty päätös siitä, että NIS2-direktiivin edellyttämien hallinnollisten sanktioiden enimmäismäärät ovat tasolla, joka on direktiivin alin sallima enimmäismäärä, on hyvin perusteltu ja kannatettava.

CSIRT-yksikön tehtäviä koskevat huomiot

On erittäin hyvä, että tietoturvaloukkauksiin reagoivana ja niitä tutkivana CSIRT-yksikkönä sekä keskitettynä yhteyspisteenä toimii jatkossakin Liikenne- ja viestintäviraston Kyberturvallisuuskeskus. Kyberturvallisuuskeskuksella on laaja kokemus kyberturvallisuushäiriöiden tiedottamisesta ja hoitamisesta tiiviissä yhteistyössä teleoperaattoreiden kanssa. Telia kiinnittää huomiota siihen, ettei esitysluonnoksen 19 §:n 2 momentin 9 kohdasta kuitenkaan ilmene esityksen perusteluissa ja NIS2-direktiivissä todettu ”yhteistyö yksityisen sektorin sidosryhmien kanssa”.

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

-

Verkkotunnusvälittäjiä koskevat huomiot

-

Kumottavaksi ehdotettuja säännöksiä koskevat huomiot

Telia toivoo, että esitysluonnoksessa varmistetaan vielä sektorikohtaisen, päällekkäisen erityissääntelyn kumoaminen.

Vaikutustenarviointia koskevat huomiot

Vaikutustenarviointi on muilta osin varsin perusteellinen, mutta telesektorin osalta toteamaa lisäkustannusten syntymättömyydestä ei voida pitää täysin oikeana. Uusi sääntely, varsinkin ottaen huomioon sen, että nykyiseen, sektorikohtaiseen sääntelyyn ei puututa, aiheuttaa

teleoperaattoreille- väistämättä kustannuksia. Näiden kustannusten osalta vaikutustenarviointi telesektorin osalta on syytä tehdä yhtä huolella kuin muidenkin sektoreiden kohdalla on tehty.

Muut huomiot ja avoin palaute esityksestä

NIS2-direktiivin toimeenpanon myötä Traficomin Kyberturvallisuuskeskus saa huomattavia uusia vastuualueita ja tehtäviä. Telia kantaa huolta Traficomin ja Kyberturvallisuuskeskuksen resurssien riittävyydestä työmäärän kasvaessa. Telia toivookin, että esitysluonnoksessa kiinnitetään erityistä huomiota riittävien resurssien turvaamiseen Traficomille myös tämän esityksen piirissä olevien tehtävien ulkopuolella. NIS2-direktiivin toimeenpano ei saa heikentää Traficomin ja Kyberturvallisuuskeskuksen muuta perustyötä ja erityisesti Kyberturvallisuuskeskuksen 24/7-päivystys on säilytettävä.

Telia kiinnittää huomiota myös esitysehdotuksessa avattuihin laajoihin tiedonluovutusoikeuksiin luottamuksellisen viestinnän piiriin kuuluvien tietojen kuten välitystietojen osalta. Tehtäessä poikkeuksia lakiin sähköisistä viestintäpalveluista, tulee erityisesti huolehtia säädöksen ja perusteluiden selkeydestä ja tarkkarajaisuudesta sekä tietosuojalainsäädännön mukaisen käsittelyperusteen olemassaolosta. Jos esimerkiksi vapaaehtoisiin jakamisjärjestelyihin osallistuva taho voi olla kuka tahansa yksityinen tai julkinen taho, on huomattava, että tällöin 22 §:n 4 momentissa laajennetaan huomattavasti sitä piiriä, jolle viranomainen voi sähköisen viestinnän palvelulain 319 § 3 momentin nojalla luovuttaa näitä tietoja. Tätä ei voida pitää tarkoituksenmukaisena, joten kohta vaatii selvennystä. Samalla on hyvä myös selventää, mikä on jakamisjärjestelyihin osallistuvan tahon käsittelyperuste sähköisen viestinnän palvelulain nojalla. Tietosuojan toteutumiseksi on lisäksi tärkeää varmistaa, että viranomaisten luovuttaessa tietoja toisilleen tai eteenpäin EU:n sisällä, niiden tulee ilmoittaa siitä yritykselle, jonka tietoja on luovutettu.

Telia toivoo uudelleentarkastelua ja täsmentämistä esitysehdotuksen luottamuksellisen viestintätiedon käsittelyä koskeviin poikkeuksiin. Erityisesti esitysehdotuksen 20§ ja 22§ perusteluineen sisältävät sekä sisäisiä ristiriitoja että epäselvyyttä siitä, mikä on kunkin tahon käsittelyperuste ja kattaako se myös välitiedon käsittelyn. Hallituksen esityksessä on äärimmäisen tärkeää käyttää selkeää kieltä siitä, puhutaanko telepäätelaitteiden yksilöintitiedoissa välitystiedosta ja milloin tarkalleen ottaen on oikeus käsitellä välitystietoja ja milloin ei. Suurin osa telepäätelaitteen yksilöivistä tiedoista on välitystietoa. Traficomin mukaan jopa päätelaitteen mallitieto (TAC-koodi) on välitystietoa, jos se on yhdistetty käyttäjään, joten selkeyttä erityisesti mainittujen tietojen välitystietoluonteeseen tarvitaan. Jollei esitysehdotusta tarkenneta, on vaarana, ettei kyseisiä pykäliä ole mahdollista soveltaa käytännössä niiden ristiriitaisuuden vuoksi. Uusien poikkeusten epäselvyyden lisäksi Telia kantaa huolta myös siitä, että esityksellä tahattomasti kavennetaan teleoperaattorin sähköisen viestinnän palvelulain 138 § ja 272 § mukaisia käsittelyperusteita. Telia suosittaakin, että tätä asiaa erikseen selvennetään hallituksen esityksessä.

Kitinprami Irina
Telia Finland Oyj