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

Kattava ja vaativa direktiivi kyberturvallisuuden parantamiseksi EU-tasolla. Hallituksen esityksessä on selkeät kuvaukset tavoitteista ja tarkoituksesta. Käytännön tasolla NIS2-direktiivin suhde jo voimassaoleviin ja sovellettaviin lakeihin, asetuksiin ja suosituksiin / vaatimuksiin (mm. Julkri, Pitukri, Katakri, ISO-standardit) jää avoimeksi ja saattaa aiheuttaa tulkintaristiriitoja käytännön tasolla. Tästä syystä pätemisketjut tulisi kuvata selkeästi jokaiseen lisää vaatimuksia tuovaan säädökseen.

Soveltamisalaa koskevat huomiot

Koska koko Tullin toiminta pääosin suojaa yhteiskuntaa, ympäristöä ja kansalaisia (ilman tulliselvitystä näin ei olisi), ulkomaankauppa- ja verotusosaston näkemyksen mukaan Tulli kokonaisuudessaan olisi jätettävä direktiivin soveltamisalan ulkopuolelle, ei pelkästään Tullin rikostorjunta.

Huomioitavaa on, että ICT-palveluketjut ovat nykyisin vahvasti riippuvia toisistaan. Voi olla käytännön tasolla vaikea vetää rajaa siihen, mihin kohtaa kybertapahtumat kohdistuvat tai rajoittuvat. Selkeintä olisi käsitellä Tullia yhtenä turvallisuusviranomaisena, joka käsittelee turvallisuusluokiteltua tietoa. Tällöin raportointivelvollisuuksien järjestäminen olisi selkeää ja ei aiheuttaisi päällekkäisyyksiä / ylimääräistä hallinnollista työtä.

Direktiivin soveltaminen käytännön tasolla tarkoittaa esimerkiksi päivystystehtävien vaatimustason nousua ja valmiudessa olevaa tietoturvan asiantuntijaa kellon ympäri. Tarvitaan viraston asiantuntijoiden näkemystä kybertapahtumasta ja sen vaikutuksista sekä ostopalveluna ostettavien erikoisasiantuntijoiden (usein käyttöpalvelutoimittajan ja sovellustoimittajien) yhteistyötä.

Direktiivin johdanto-osan kappaleen 8 mukaan ”julkishallinnon toimijoista olisi jätettävä direktiivin soveltamisalan ulkopuolelle ne, jotka harjoittavat toimintaa pääasiassa kansallisen turvallisuuden, yleisen turvallisuuden, puolustuksen tai lainvalvonnan alalla, mukaan lukien rikosten ennalta estäminen, tutkiminen, paljastaminen ja rikoksiin liittyvät syytetoimet. Niitä julkishallinnon toimijoita, joiden toiminta liittyy vain marginaalisesti mainittuihin aloihin, ei kuitenkaan olisi jätettävä tämän direktiivin soveltamisalan ulkopuolelle.” Tämän perusteella ehdotetun tiedonhallintalain 4 a luvun soveltamisalasta on rajattu pois Tullin rikostorjunta.

Riskienhallintavelvoitetta koskevat huomiot

Laki täsmentää käytäntöjä ja tekee hallintatoimet velvoittaviksi. Tähän asti käytännön toimia on tehty tietoturvan varmistamiseksi. Lakiin kirjoitettuna hallintatoimien dokumentointi lisääntyy ja tähän on Tullinkin varauduttava resurssein.

Raportointivelvoitetta koskevat huomiot

On kannatettavaa, että toimijoilla on liikkumavaraa raportointivelvoitteen kohdalla. Samalla esitetään huomio, että määritelmiä, kuten ”huomattava aineeton vahinko” tai ”taloudellisia tappioita” olisi ehkä syytä tarkentaa esimerkiksi mahdollisessa lainsoveltamiseen liittyvässä suosituksissa. Muussa tapauksessa saattaa käydä niin, että toimijat tulkitsevat ja soveltavat lakia eri tavalla. Kansallisella toimivaltaisella valvontaviranomaisella on merkittävä rooli siinä, että se ohjeistaa keskeisiä ja tärkeitä toimijoita toimimaan yhdenmukaisesti.

Poikkeamailmoituksen loppuraportin laatimisen määräaika on kuukauden kuluttua ilmoituksen toimittamisesta. Määräaika noudattaa muissakin viranomaisvelvoitteissa toistuvaa 30 päivän toimenpideaikaa. Ehdotus kuitenkin mahdollistaa kohtuullisen rajaamattoman aikarajan, jos poikkeaman käsittely on kesken. Yksi vaihtoehto olisi, että määräaika olisi kuukausi ja jos toimija tekee ilmoituksen määräajan pidennyksestä, perustellusta syystä, määräaikaa pidennettäisiin esimerkiksi kuukauden tai kaksi. Joka tapauksessa olisi ehkä tarpeen, että toimija hallinnollisesti ilmoittaisi, miksi määräaikaa tarvitaan lisää ja mikä on peruste sekä käynnissä olevat toimenpiteet.

Raportointivelvoite on rinnastettavissa tietosuojan ilmoitusvelvollisuuteen. Toimijoille tämä voi lisätä hallinnollista taakkaa. Käytännön soveltamisen kannalta on esitettävä kysymys, että voiko poikkeamasta rekisteröidylle aiheutuva riski olla samaan aikaan aiheuttamatta tälle huomattavaa aineellista tai aineetonta vahinkoa. Toisin sanoen, jos poikkeama tietosuojan soveltamisen näkökulmasta ylittää kynnyksen henkilötietojen tietoturvaloukkauksesta ilmoittamiseen, voiko kyberturvallisuuden raportointivelvoitteen kynnys jäädä toteutumatta. Näistä käytännön soveltamisista olisi tarpeen saada parhaita käytäntöjä ja suosituksia sekä valvontaviranomaisten tulkintaohjeistuksia.

Keskeisten ja tärkeiden toimijoiden raportointivelvollisuus Kyberturvallisuuskeskukselle 24 tunnin kuluessa havainnosta on tiukka velvoite. Jotta raportointi onnistuu ja täyttää raportointivelvoitteen tarkoituksen, organisaatiolla tulee olla tietoturvan pätevä 24/7/365 päivystys. Kybertapahtuma tulee

analysoida ja tunnistaa kriteerit, jotta raportointi tuottaa haluttua tulosta. Päivystystyyppistä työtä tekevien tietoturva-asiantuntijoiden tarve muodostaa resurssitarpeen organisaatiolle.

Valvontaa koskevat huomiot

-

Seuraamusmaksua koskevat huomiot

-

CSIRT-yksikön tehtäviä koskevat huomiot

-

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

Hallituksen esityksessä ehdotetaan NIS2-direktiivin soveltamislaiksi Tiedonhallintalakia. Lisäksi uusi Laki kyberturvallisuuden riskienhallinnasta. Kuitenkin on huomioitavaa, että julkishallinnon ICT-palveluita säädellään usealla eri lailla, asetuksella ja suosituksella. Lisäksi on muita tietoturvaan liittyviä vaatimuksia (Julkri, Katakri, Pitukri, ISO-standardit ja soveltamisohjeet) eri TVT-palvelutyypeille. Näiden suhde nyt lausunnolla olevaan Hallituksen esitykseen tulisi kuvata selkeämmin. Tällä varmistettaisiin direktiivin ohjausvoima ja tulkinnan mahdollisuudet vähenisivät.

Verkkotunnusvälittäjiä koskevat huomiot

-

Kumottavaksi ehdotettuja säännöksiä koskevat huomiot

-

Vaikutustenarviointia koskevat huomiot

NIS2-direktiivin soveltaminen aiheuttaa kustannustason nousua Tullille. Tarvitaan enemmän omaa tietoturvahenkilöstöä ja ostopalveluna hankittavaa osaamista. Kustannusvaikutukset tuli arvioida virastokohtaisesti ja huomioida määrärahoissa.

Muut huomiot ja avoin palaute esityksestä

Toimivaltaisten viranomaisten resurssitarpeet olisi huomioitava ennakoivasti. Jos ilmoitusmäärät kasvavat huomattavasti, toimijat tarvitsevat myös valvontaviranomaisten palautetta ja yhteistyötä – tämä edellyttää resursseja.

Raportointivelvollisuus näyttäytyy aikanaan resurssikysymyksenä ja se saattaa ilmetä mm. tehtävään nimettävänä yhteys-/ vastuuhenkilönä. Lisäksi lainsäädännön toimeenpanon seurauksena syntyy koulutustarpeita ja osaamishaasteita.

Toimivaltaisen viranomaisen osalta on tärkeä huomioida riittävät resurssit onnistuneelle täytäntöönpanolle. Täytäntöönpano tulee vaatimaan valmistelua, suunnittelua, prosessien mallintamista, mahdollisten tehtäväroolien kohdentamista sekä koulutusresursseja. Nämä resurssit olisi hyvä varmistaa lainvalmisteluvaiheessa, jotta prosessit saadaan aikanaan käyttöön, toimeenpanoa viivästymättä.

Tullin tietoturvallisuuden kokonaisuuden hallinnan kannalta tarkoituksenmukaisinta olisi käsitellä Tullia yhtenä kokonaisuutena, jossa tiedonhallintalakia sovelletaan samoilla yhtenäisillä periaatteilla koko Tulliin. Sovellustavan tulee olla yhtenevä muiden turvallisuusviranomaisten kanssa.

Biltekin Riina
Tulli.fi