Cyberismo Oy

Lausunto

09.11.2023

Asia: VN/18157/2023

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

Lausunnonantajan lausunto

Yleiset huomiot NIS2-direktiivin tavoitteista ja tarkoituksesta

Kyberturvallisuuden vahvistaminen on erittäin tärkeä ja ajankohtaisempaa kuin koskaan. Riskipohjaisuus tarjoaa hyvän lähtökohdan ja tuottanee tulosta riittävillä täytäntöönpanotoimenpiteillä.

Soveltamisalaa koskevat huomiot

Soveltamisalan määrittely on vaikeaselkoinen, erityisesti valmistussektorin osalta. Sen perustella on vaikea päätellä, kuuluuko esimerkiksi kokonaisen automaatiojärjestelmän toimittaja soveltamisalaan vai ei.

Myös muissa luokissa on vaikeaselkoisuutta, esimerkiksi tutkimusorganisaatioiden osalta. Esityksen sivulla 106 sanotaan, että "liikevaihtoa, tasetta ja henkilöstömäärää arvioidaan koko toimijan osalta eikä arviointia tule rajata vain liitteessä I tai II tarkoitetun toiminnan laajuuteen. Arviointi tehdään toimijakohtaisesti." Toisaalta Liitteessä II määritellään “Tutkimusorganisaatiot, joiden ensisijaisena tavoitteena on harjoittaa soveltavaa tutkimusta tai kokeellista kehitystyötä kyseisen tutkimuksen tulosten hyödyntämiseksi kaupallisiin tarkoituksiin, mutta joka ei ole korkeakoulu tai muu opetus- ja koulutus- alan laitos.” Seuraako näistä yhdessä, että mikä tahansa keskisuuren yrityksen määritelmän ylittävä yritys on automaattisesti soveltamisalan piirissä, jos yrityksessä on vaikkapa vain kahden henkilön tutkimustiimi?

Toinen soveltamisalaa koskeva huomio, että soveltamisalassa määritellyille yrityksille hyppäys 49 henkilön yrityksestä 50 henkilön yritykseksi tulee olemaan kustannusvaikutuksiltaan todella radikaali ja saattaa joissain tapauksissa muodostua kasvun esteeksi, ellei tuossa kohtaa ole yhteiskunnan vahvaa tukea tarjolla.

Riskienhallintavelvoitetta koskevat huomiot

Esityksen sivulla 106 sanotaan, että

"liikevaihtoa, tasetta ja henkilöstömäärää arvioidaan koko toimijan osalta eikä arviointia tule rajata vain liitteessä I tai II tarkoitetun toiminnan laajuuteen. Arviointi tehdään toimijakohtaisesti."

Pykälässä 7 säädetään riskienhallintavelvoitteesta seuraavasti:

"Toimijan on tunnistettava, arvioitava ja hallittava riskejä, joita kohdistuu sen toiminnoissa tai palveluntarjonnassa käytettävien viestintäverkkojen ja tietojärjestelmien turvallisuuteen. Kyberturvallisuuden riskienhallinnalla tulee estää tai minimoida poikkeamien vaikutus toimintaan, toiminnan jatkuvuuteen, palvelujen vastaanottajiin ja muihin palveluihin."

Tästä muotoilusta jää epäselväksi, kohdistuuko riskien hallintavelvoite tiukasti vain NIS2-direktiivissä määriteltyyn toimintaan vai missä määrin se laajenee koskemaan myös muuta tekemistä.

Erityisesti tämä kysymys nousee esille toimijoilla, joilla vain pieni osa toiminnasta (esimerkiksi yksittäinen tutkimusosasto tai pilvipalvelu) osuu NIS2-direktiivin varsinaiseen soveltamisalaan. Tuleeko tällöin arvioida viestintäverkkoja ja tietojärjestelmiä

1. Tiukasti vaikkapa vain pilvipalveluun tai tutkimukseen liittyen

2. Sekä pilvipalveluun että sen parissa työskentelevien henkilöiden osalta myös yrityksen verkkoihin ja järjestelmiin vai

3. Laajasti koko yrityksen tietoverkkoihin sekä sisäverkkojen (IT-yksiköt) että ulospäin tarjottavien palveluiden näkökulmasta (Business-yksiköt)?

Tällä tulkinnalla on merkittäviä vaikutuksia siihen, miten riskien hallinta kannattaisi toteuttaa, mutta toisaalta liian tiukat rajaukset saattavat viedä pohjan pois koko direktiiviltä, sillä tiukka eristäminen yrityksen sisällä voi olla haastavaa tai peräti mahdotonta.

Alkuperäisessä direktiivissä mainitaan erikseen toimittajakohtaiset haavoittuvuudet ja turvallisen tuotekehityksen menetelmät. Tätä on kuitenkin rajattu hallituksen NIS2-esityksessä, kun pykälän 9 kohdasta 4, joka kattanee alkuperäisen direktiivin Artiklan 21 kohdat 2 d) ja 3, on tiputettu pois nämä erillismaininnat. Mielestäni molemmat näkökohdat tulisi pitää eksplisiittisesti mukana myös suomalaisessa säädännössä, sillä ne ovat kokonaisturvallisuuden kannalta erittäin kriittisiä.

Valmistussektorin osalta pykälän 7 rajaukseen liittyy myös seuraava huomio. Pykälän 2 kohdan 28 b) mukaisesti viestintäverkolla ja tietojärjestelmällä tarkoitetaan myös laitetta taikka yhteen kytkettyjen tai toisiinsa yhteydessä olevien laitteiden ryhmää, joista yksi tai useampi suorittaa ohjelman avulla digitaalisten tietojen automaattista käsittelyä. Näin ollen riskien hallintavelvoite voisi koskea myös ainakin osaa toimitettavista tuotteista, mikä olisi vaikkapa liikkuvien koneiden näkökulmasta mielestäni erittäin tärkeää. Mutta pykälän rajaus "toiminnoissa tai palveluntarjonnassa" käytettäviin viestintäverkkoihin ja tietojärjestelmiin sulkee tämän pois. En tiedä, onko rajaus tehty mahdollisesti sen vuoksi, että nämä asiat tullaan kattamaan myöhemmässä kyberkestävyyssäädöksessä. Ymmärrän, että kaikkia pykälässä 9 listattuja hallintakeinoja ei voi soveltaa tuotemaailmaan. Olisi hyvä selventää rajanvetoa siitä, milloin tuotetoimittajan toiminta, mukaan lukien palvelut ja tuotteet, on NIS2:n alaista.

Raportointivelvoitetta koskevat huomiot

Ilmoituksen aikarajat ovat kohtuullisen tiukat ja saattavat käytännössä vaatia ulkopuolisen SOC-yksikön käyttöä. Pienemille yrityksille riittävän valvontatason saavuttaminen voi olla haastavaa ja olisi hyvä, jos valvontaan olisi näissä tapauksissa valmiita ratkaisuja ja/tai yhteiskunnan tukea. Onkin erinomaista, että valvonnassa avustaminen onkin määritelty CSIRT-yksikön yhdeksi tehtäväksi, ainakin mikäli palvelusta erikseen säädettävistä maksuista ei muodostu kynnyskysymystä.

Valvontaa koskevat huomiot

Tarkastusoikeuden rajaaminen (pykälä 29) muihin kuin pysyväisluonteiseen asumiseen tarkoitettuihin tiloihin saattaa olla näin etätyön aikakaudella haasteellinen ja mahdollisesti myös kannustaa ns. heikkojen lenkkien siirtämistä "kotiin turvaan". Entäpä jos haittaohjelma muhiikin siellä koventamattomassa kotiverkossa?

Seuraamusmaksua koskevat huomiot

Pykälän 37 mukaan hallinnollisen seuraamusmaksu voidaan määrätä toimijalle, joka tahallaan tai törkeästä huolimattomuudesta laiminlyö antaa 43 §:ssä tarkoitetut tiedot valvovalle viranomaiselle. Soveltamisalassa määriteltyjen toimijoiden joukko on kuitenkin kohtuullisen epäselvästi määritelty ja tuntuisi kohtuuttomalta rankaista toimijaa, joka ei edes tiedä kuuluvansa lain soveltamisalaan. Paikallisen lainsäädännön seuraamatta jättäminen kuitenkin lienee tulkittavissa tahalliseksi teoksi. Oman kokemuksen mukaan yritysten tietoisuus NIS2-direktiivistä ei välttämättä aina ole riittävällä tasolla ja erityisesti uusilla toimialoilla voi käydä niin, että ilmoituksia jää tekemättä, koska yritykset eivät tiedä asiasta. Vaihtoehtoisesti tämä voi johtaa myös siihen, että yritykset tekevät sakkojen pelossa ilmoituksia varmuuden vuoksi. Jo lain valmistelu vaiheessa yrityksille pitäisi olla käytössä helppo tapa tarkistaa, ovatko he lain piirissä vai eivät, koska valmistautuminen kuitenkin vaatii aikaa. Tai vaihtoehtoisesti aloitteen pitäisi tulla yhteiskunnan puolelta jonkinlaisella laajamittaisella selvityksellä, joka pakottaisi kaikki riittävän kokoiset yritykset tarkistamaan lain soveltamisalan omalta kohdaltaan.

CSIRT-yksikön tehtäviä koskevat huomiot

Onko CSIRT-yksiköllä riittävät resurssit tarvittaessa avustaa kaikkia NIS2-direktiivin soveltamisalaan kuuluvita toimijoita heidän viestintäverkkojen ja tietojärjestelmien tietoturvallisuuden reaaliaikaisessa tai lähes reaaliaikaisessa seurannassa?

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

Ei huomioita.

Verkkotunnusvälittäjiä koskevat huomiot

Ei huomioita.

Kumottavaksi ehdotettuja säännöksiä koskevat huomiot

Ei huomioita.

Vaikutustenarviointia koskevat huomiot

Velvoitteiden toteuttamisella on todella merkittäviä taloudellisia vaikutuksia, jotka tuntuvat varmasti erityisen raskailta keskisuurista yrityksistä. Tämän johdosta olisi erittäin tärkeää luoda keskitetysti yhtenäisiä toimintamalleja, dokumenttipohjia, koulutuksia, työkaluja, ohjeistuksia jne. sekä riskienhallintaan että vaadittavien hallintatoimien osalta. Mielellään jo hyvissä ajoin ennen lain voimaantuloa, koska toimivan riskienhallintamallin ja hallintakeinojen pystyttäminen ei käy yhdessä yössä. Näin vältettäisiin päällekkäistä työtä ja mahdollisesti saataisiin myös kustannusvaikutuksia alaspäin, mikä olisi yhteiskunnan kannalta merkittävä asia.

Muut huomiot ja avoin palaute esityksestä

Esityksessä on paljon hyvää ja se on monilta osin selkeämpi kuin alkuperäinen direktiivi. Pienillä soveltamisalan täsmennyksillä, tuotekehityksen turvallisuuden huomioinnilla (sekä tuotteiden että toimitusketjun osalta) ja yhtenäisten mallien rakentamisella päästään varmasti jo pitkälle.

Haverinen Henry
Cyberismo Oy

Kaartinen Suvi
Cyberismo Oy - Lead Security Advisor