TietoEVRY 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

Tietoevry Oyj kiittää mahdollisuudesta esittää näkemyksensä hallituksen esityksestä kyberturvallisuusdirektiivin toimeenpanemiseksi. Tietoevryn näkökulmasta keskeistä on taata kansalaisten ja yhteiskunnan muiden toimijoiden luottamus digitaalisiin palveluihin. Digitalisaation avulla voimme parantaa tuottavuutta, joka on välttämätöntä yhteiskunnan kokonaisturvallisuuden ylläpitämiseksi ja parantamiseksi.

Tietoevry on seurannut kyberturvallisuusdirektiivin valmistelua, tutustunut direktiiviin ja hallituksen esitykseen sekä osallistunut EK:n ja Kyberala ryn kautta asian valmisteluun. Tietoevry yhtyy EK:n sekä Teknologiateollisuus ryn, Puolustus- ja Ilmailuteollisuus (PIA) ryn ja Kyberala (FISC) ryn lausunnossaan esittämiin näkemyksiin ja pykäläkohtaisiin huomioihin.

Haluamme vielä erikseen nostaa esiin tärkeimpiä huomioitamme.

Soveltamisalaa koskevat huomiot

Kuinka lain vaatimuksia sovelletaan globaalissa monialayrityksessä? Viitaten ehdotetun 3 §:n sanamuotoon, toivomme selkeän näkemyksen vaatimusten soveltuvuuden osalta erityisesti huomioiden useassa eri maassa oleva liiketoiminta, joka perustuu usean eri tytäryhtiön käyttämiseen palveluntarjoajan palveluiden toimittamisessa.

Riskienhallintavelvoitetta koskevat huomiot

Toimitusketjuvastuiden osalta NIS2 direktiivi viittaa "välittömiin" palveluntarjoajiin – hallituksen esityksessä ei ole tätä rajoitusta. Olisi hyvä myös tarkentaa, että vaatimus koskee vain kyberturvallisuuden riskienhallinnan kannalta oleellisia toimittajia.

Lain vaatimusten huomiointi toimitusketjuihin liittyvissä sopimuksissa tulee olemaan haasteellista. Sopimuksissa pelkkä viittaus lain vaatimuksiin ei ole riittävä, kun velvoitteet kohdistuvat suoraan vain asiakkaaseen, ei palveluntarjoajaan.

Raportointivelvoitetta koskevat huomiot

HE luonnoksen mukaan toimijan on ilmoitettava viipymättä merkittävästä poikkeamasta palvelujensa vastaanottajille, jos merkittävä poikkeama "todennäköisesti" haittaa toimijan palvelujen tarjoamista. Lisäksi toimijan on ilmoitettava "viipymättä" merkittävästä kyberuhkasta sekä kyberuhkan hallitsemiseksi käytettävissä olevista toimenpiteistä niille palvelujensa vastaanottajille, joihin merkittävä kyberuhka "saattaa vaikuttaa". Tässä on paljon tulkinnanvaraisia termejä, jotka toivotaan selvennettävän lopulliseen hallituksen esitykseen.

Merkittävä poikkeama saattaa velvoittaa raportoimaan useille viranomaisille. Yhden luukun raportointimalli olisi erittäin suotavaa toteuttaa.

Mikäli ICT-palveluntarjoajalla on merkittävä poikkeama, onko siitä raportoitava sekä asiakkaille että viranomaisille? Nykyinen yleinen käytäntö poikkeamatilanteissa on, että palveluntarjoaja raportoi poikkeamista herkästi asiakkailleen ja asiakas arvioi tarpeen viranomaisraportointiin.

Poikkeamaraportointivaatimuksista saa kuvan, että tieto liikkuu pääasiassa toimijoilta viranomaisille. Olisi hyvä, jos laissa edellytettäisiin viranomaisilta ja CSIRTiltä selkeämmin kyberturvallisuuden tilannekuvan jakamista takaisin toimijoille.

Valvontaa koskevat huomiot

Valvovan viranomaisen tietopyyntöön liittyvät tiedot on luovutettava "viipymättä, viranomaisen pyytämässä muodossa ja maksutta". On huomattava, että tietomäärä voi olla merkittävä ja erityisesti yhteiskäyttöisissä palveluissa pyydetyn tiedon hakeminen koko tietomassasta työlästä, Tietojen konvertointi viranomaisen vaatimaan muotoon ei myöskään välttämättä ole helppo toimenpide. Tietopyynnön aiheuttamasta merkittävästä työmäärästä tulisi saada kohtuullinen korvaus.

Kuinka varmistetaan toimijoiden valvonnan ja auditointien sopiva taso ja tasalaatuisuus?

Vastuullisen johdon määritelmä on HE luonnoksessa laajempi kuin NIS2 direktiivissä.

Seuraamusmaksua koskevat huomiot

Seuraamusmaksun perusteet eivät ole selkeät esim. tilanteessa, jossa globaalin yrityksen tytäryhtiö tietyssä maassa tuottaa lain piiriin kuuluvaa palvelua. Täten seuraamusmaksun perusteet tulisi olla yksiselitteiset.

CSIRT-yksikön tehtäviä koskevat huomiot

Kuinka eri maiden CSIRT-yksiköiden tekemiä haavoittuvuuskartoituksia koordinoidaan? Globaaleilla yrityksillä ja palveluntarjoajilla on hallinnassaan laajoja IP-osoitealueita, joita käyttävät palvelut sijaitsevat eri maissa. Palveluntarjoajan IP-osoite saattaa olla myös täysin asiakkaan vastuulla olevan palvelun käytössä.

ENISAn tehtävänä on perustaa ja ylläpitää haavoittuvuustietokantaa. Onko tarkoitus, että tänne kerätään tietoa myös ei-julkisista haavoittuvuuksista, joille ei vielä ole korjausta? Tällöin haavoittuvuustietokanta itsessään olisi suuri EU-tasoinen riski.

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

-

Verkkotunnusvälittäjiä koskevat huomiot

-

Kumottavaksi ehdotettuja säännöksiä koskevat huomiot

-

Vaikutustenarviointia koskevat huomiot

-

Muut huomiot ja avoin palaute esityksestä

-

Pirhonen Jari
TietoEVRY Oyj