Elisa 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

Elisa Oyj kiittää mahdollisuudesta lausua luonnoksesta.

Verkko- ja tietoturvadirektiivi ja sen kansallinen toimeenpano laiilla kyberturvallisuuden riskienhallinnasta sekä muilla siihen liittyvillää leilla yhtenäistävät kyberriskien hallintaa kohteena olevilla toimialoilla ja niihin liittyvien yritysten alihankinytaketjussa. Tavoite vahvistaa laissa määriteltyjen toimijoiden kyberriskien hallintaa on kannatettava.

Elisa Oyj yhtyy Tietoliikenteen ja tietotekniikan keskusliitto FICOM ry:n lausuntoon kaikilta osin. Tässä lausunnossa esittelemme joitain keskeisiä teemoja.

Elisa Oyj keskeiset viestit:

- Direktiivin kansallinen täytäntöönpano sen alkuperäisessä laajuudessa ilman sen yli meneviä vaatimuksia on hyvä lähtökohta
- Yrityksille asetettavien raportointivelvoitteiden täsmentäminen ja raportointi yh-delle viranomaiselle tulisi varmistaa. Muiden raportointi- ja tiedottamisvelvoittei-den osalta tulisi noudattaa Direktiivissä määriteltyä tasoa sellaisenaan.
- Teleyritysten tuottamien viestintäpalvelujen yhteydessä tapahtuneiden henkilö-tietojen tietoturvaloukkausten ilmoittaminen ainoastaan Liikenne- ja viestintävi-rastolle tulee selkeyden vuoksi tuoda myös pykälätekstiin.
- Liikenne- ja viestintäviraston resurssit on turvattava, jotta uudet valvontatehtävät ja jo olemassa olevat viraston tehtävät voidaan toteuttaa.

- Kyberturvallisuuskeskuksen 24/7-päivystyksen jatkuminen tulee varmistaa

Soveltamisalaa koskevat huomiot

Nyt lausuttavan oleva lainsäädäntökokonaisuus liittyy keskeisesti samalla aikataululla tehtävään CER-direktiivin kansalliseen toimeenpanoon. Valitettavasta CER dierktiivin toimeenpanoon liittyvä hallituksen esitys ei ole samanaikaisesti käytettävissä tästä kokonaisuudesta lausuttaessa. Epätahtisuus synnyttää riskin yrityksiin ja muihin toimijoihin kohdistuvista ristiriitaisista vaatimuksista ja päällekkäisestä sääntelystä.

Ehdotuksessa on useassa kohdassa lakitekstiä myöten todettu kytkentä CER-direktiivin toimeenpanoon. Ristiriitojen tunnistamiseksi ja niistä lausumisen mahdollistamiseksi olisi hyvä, että esimerkiksi CER-direktivin toimeenpanoon liittyvissä lausunnoissa olisi mahdollista tarvittessa lausua vielä tähän kokonaisuuteen liittyvistä asioista siten että ne huomioitaisiin myös tämän Hallituksen esityksen jatkokäsittelyssä.

Riskienhallintavelvoitetta koskevat huomiot

Esitysluonnoksessa todetaan, että lähtökohdaksi on valikoitunut riskienhallinta- ja raportointivelvoitteiden vähimmäistaso direktiivin asettamalla tasolla. Direktiivin toimeenpano kasvattaa kyberturvallisuuteen liittyviä uusia resurssitarpeita myös aloilla, joihin kohdis-tuu jo ennestään kattavia kyberturvallisuusvaatimuksia.

Lähestyminen on erittäin kannatettava.

Johdon vastuisiin liittyen viittaamme Kyberala ry:n lausuntoon, jossa esitetään johdon henkilökohtaisiin vastuisiin liittyvien määritysten ja perusteluiden täsmentämistä.

Raportointivelvoitetta koskevat huomiot

Raportointivelvoitteet ehdotuksessa ovat paikoin epäselviä ja tulkinnanvaraisia. Esimerkkinä ehdotettavan lain 14 §:ssä säädettävä poikkeamasta ja kyberuhkasta ilmoit-tamisesta muulle kuin viranomaiselle. Toimijan on ilmoitettava viipymättä merkittävästä kyberuhkasta sekä kyberuhkan hallitsemiseksi käytettävissä olevista toimenpiteistä niille palvelujensa vastaanottajille, joihin merkittävä kyberuhka saattaa vaikuttaa. Kyberuhka on kuitenkin varsin laaja käsite, joten pykälän perusteella ei ole selvää, mistä pitäisi ilmoittaa ja mistä ei.

Nykytilanteessa, riippumatta tietosuojaneuvoston lausunnosta, tietosuojavaltuutetun toimisto edellyttää yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajilta Liikenne- ja viestintävirastolle tehdystä ilmoituksesta erillistä ilmoitusta henkilötietojen tietoturvaloukkauksesta tietosuojavaltuutetun toimistolle. Yleisen tietosuoja-asetuksen ankarista seuraamusriskeistä ja

tietosuojavaltuutetun toimiston linjanvedosta johtuen palveluntarjoajat joutuvat nykyään vastoin kansainvälistä tulkintaa tekemään kaksi eril-listä ilmoitusta samasta tietoturvaloukkauksesta. Näin ollen perusteluissa asianmukaisesti ehdotettu tavoitetila tulisi nostaa myös pykälätekstiin tai vähintäänkin se tulee esittää vielä selkeämmin perusteluissa.

Teleyrityksillä ja Liikenne- ja viestintäviraston välillä on jatkuvasti toimiva ja tilanteisiin mukautuva tiedonvaihtoyhteys. Myös jatkossa toiminnan tulisi perustua siihen, eikä teleyrityksille pitäisi säätää raportointivelvoitteita mulille viranomaiille asioissa, joissa on jo velvoite raportoida Liikenne- ja viestintävirastolle.

Valvontaa koskevat huomiot

-

Seuraamusmaksua koskevat huomiot

-

CSIRT-yksikön tehtäviä koskevat huomiot

Lausumme asiasta osana Liikenne- ja viestintäviraston resurssien turvaamista ja 24/7 päivystyksen varmistamiseen liittyvää kommenttiamme.

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

-

Verkkotunnusvälittäjiä koskevat huomiot

-

Kumottavaksi ehdotettuja säännöksiä koskevat huomiot

-

Vaikutustenarviointia koskevat huomiot

Vaikutustenarvioinnissa todetaan hyvin, että direktiivin toimeenpano vaatii kohteena olevilta yrityksiltä osin merkittäviäkin panoksia. Yrityksiin kohdistuvaa resurssirarvetta tulisi arvioida myös toimeenpanon jälkeen, jotta voidaan varmistua myös sääntelyyn perustuvien toimenpiteiden tehokkuudesta ja merkityksellisyydestä. Ilmoituksiin, raporointiin ja tietopyyntöihin vastaamiseen liittyvän kuormituksen määrään tulee kiinnittää erityistä huomiota ja toiminnnan kannalta toisarvoista tai päällekkäisiä raportointivelvoitteita välttää.

Muut huomiot ja avoin palaute esityksestä

Liikenne- ja viestintävirastolle esitetään uusien valvontatehtävien lisäksi myös muita viranomaistehtäviä, joista aiheutuu lisäresursointitarpeita. NIS2-direktiivin myötä Uudet tehtävät edellyttävät uudenlaisten toimintojen perustamista sekä olemassa olevien toi-mintojen sekä tietojärjestelmien kehittämistä.

Liikenne- ja viestintäviraston resurssit on turvattava, jotta sekä uudet valvontatehtävät että jo olemassa olevat viraston tehtävät voidaan toteuttaa. Lisäresurssien rahoitus tulee järjestää muuten kuin korottamalla viestintämarkkinamaksua. Kasvava valvonta kohdis-

tuu muihin tahoihin kuin teleyrityksiin, jolloin tämän rahoituksenkin tulee tulla muista läh-teistä.

Tällä hetkellä Liikenne- ja viestintäviraston Kyberturvallisuuskeskus ylläpitää valtionhal-linnolle ja huoltovarmuuskriittisille toimijoille tarkoitettua 24/7-päivystystä. Esityksen pe-rusteella Kyberturvallisuuskeskuksen ympärivuorokautiselle päivystykselle ei viran-omaisten tietoiseksi tulemista koskevaan säännöksen ehdotetun poikkeuksen mukaisesti välttämättä olisi tarvetta eikä virastolta toisaalta edellytettäisi valmiutta päivystää viikonloppuisin, öisin tai arkipyhinä poikkeamailmoituksiin vastaamista varten.

Ehdotetun sääntelyn mahdollistama valvovan viranomaisen ympärivuorokautisesta päivystyksestä luopuminen olisi huomattava heikennys nykytilanteeseen ja kykyyn ylläpitää jatkuvaa tilannekuvaa, vaikka yrityksillä on joka tapauksessa velvoite lähettää ennakkovaroitus merkittävästä poikkeamasta ilmoittamisesta 24 tunnin kuluessa sen havaitsemisesta. Kyberturvallisuuskeskuksen CERT-toiminnolla on keskeinen rooli informaation ja uhkatilanteen tiedottamisessa kansallisille kriittisen infran toimijoille sekä muille viran-omaisille. Näkemyksemme mukana Liikenne- ja viestintäviraston Kyberturvallisuuskes-kuksen 24/7-päivystys on säilytettävä.

Elisa Oyj yhtyy Tietoliikenteen ja tietotekniikan keskusliitto FICOM ry:n lausuntoon kaikilta osin.

Wallenius Jaakko
Elisa Oyj