Liikenne- ja viestintävaliokunta

Asia: **ELISA OYJ LAUSUNTO EHDOTUKSESTA EU VERKKO- JA TIETOTURVADIREKTIIVIN KANSALLISESTA TOIMEENPANOSTA HE 57/2024 vp**

Liikenne- ja viestintävaliokunta on pyytänyt Elisa Oyj:ltä lausuntoa hallituksen esityksestä kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanoa koskevaksi lainsäädännöksi. Elisa Oyj kiittää mahdollisuudesta tulla kuulluksi ja esittää asiaan liittyen seuraavaa.

Yleistä esitetystä sääntelystä ja sen tavoitteista

Verkko- ja tietoturvadirektiivissä ja sen perusteella tehdyssä hallituksen esityksessä pyritään kokonaisvaltaisesti kehittämään kriittisten verkko- ja tietoteknisten palveluiden resilienssiä ja turvallisuutta. Kokonaisuutena asia on kannatettava.

Esityksessä on kyberuhka, -riski, ja -tapahtuma on määritelry direktiivin mukaisesti nykyaikaiseen kokonaisvaltaiseen ”All hazards” -ajatteluun perustuen.

Esityksessä valittu riskien tunnistamiseen ja hallitsemiseen perustuva lähestyminen vastaa näkemystämme tarkoituksenmukaisesta kyberturvallisuuden hallinnasta.

Valittu lähestyminen, jossa EU sääntely sovitetaan suomalaiseen toimintaympäristöön direktiiviä vastaavana, ilman lisättyä sääntelyä, on kannatettava.

Yhdymme toimialajärjestömme Ficom ry:n lausuntoon esityksestä.

Haluamme erityisesti nostaa esiin seuraavia näkökulmia

Riskienhallinta

Kyberturvallisuuslain 9§ käsitellään toimenpiteitä kyberturvallisuutta koskevien riskien hallinnassa. Pykälän 1. momentissa esitetään: *Toimijoiden on toteutettava kyberturvallisuutta koskevan riskienhallinnan toimintamallin mukaiset oikeasuhtaiset tekniset, operatiiviset tai organisatoriset hallintatoimenpiteet viestintäverkkojen ja tietojärjestelmien turvallisuuteen kohdistuvien riskien hallitsemiseksi ja haitallisten vaikutusten estämiseksi tai minimoimiseksi.* Pykälän 2. momentissa on 12 kohtainen lista toimenpiteistä, jotka ainakin on toteutettava. Lista on kattava ja sisältää nykyisen laajan riskienhallintakäsityksen mukaiset asiat.

Yrityksillä tulee olla mahdollisuus toteuttaa esitetyt vaatimukset omasta riskienhallinnasta lähtien. Pykälä antaa tähän mahdollisuuden. Käytännössä yritykset tuntevat

oman toimintansa ja siihen liittyvät riskit parhaiten. Riskinä on, että tulkintaa sitovasti ohjaavilla viranomaismääräyksillä rajoitetaan yritysten toimintavapautta tämän suhteen. Asia tulisi ilmaista vahvemmin esityksen perusteluissa.

Valvonta

Esityksen 26 § määritellään valvovat viranomaiset ja niille velvoite yhteistoiminnasta ja edelleen 9 § määritetään valvovalle viranomaiselle toimivaltuus antaa riskienhallintavelvotteita täsmentäviä teknisiä määräyksiä. Pykälän perustelujen mukaan *Viranomaisen määräyksenantovaltuus koskisi riskienhallintavelvoitteen tarkentamista ja täsmentämistä momentissa tarkoitettujen seikkojen osalta. Määräykset voisivat kuitenkin koskea vain teknisiä seikkoja, eli niillä ei saisi laajentaa 9 §:ssä säädettyjä velvoitteita.*

Perusteluun kirjattu rajaus on erittäin tärkeä, samoin viranomaisten välinen yhteistoimintavelvoite.

Valvonnan toteuttaminen edellyttää osaamista ja resursseja. Oletettavasti osa tulevaista valvovista viranomaisista joutuu hankkimaan tarvittavat resurssit ja osaamisen. Valtionhallinnon tehostamisen ja resurssoinnin rinnalla tulee varmistaa valvonnan kannalta asianmukainen ja vaikuttava toiminta.

Ilman em. rajauksia vaarana on, että sääntelyn vaatimusten hajautuminen toimialoilla, tai sääntelyn faktinen laajeneminen lakiin kirjatusta.

Asia on erityisen merkityksellinen, toimijalle, johon kohdistuu valvontaa useiden viranomaisten taholta, tai useilla toimialoilla toimiville toimijoille palveluita tarjoaville yrityksille.

Eri viranomaisten antamien määräysten yhteismitallisuutta tulisi tarkastella säännöllisesti ja asia tulisi kirjata perusteluihin.

Haluamme korostaa Ficom ry:n lausunnossa esittämää CSIRT-yksikön ja yksityisten sidosryhmien välisen yhteistyövelvoitteen kirjaamista pykälätasolle

Liikenne- ja viestintäviraston resurssien turvaaminen.

Haluamme erityisesti korostaa Ficom ry:n lausunnossaan esittämää Liikenne- ja viestintäviraston resurssien turvaamista sekä Kyberturvallisuuskeskuksen 24/7päivystyksen varmistamista.

Merkittävän kyberhäiriön tehokas hallinta, tilannekuvan muodostaminen ja jakaminen tulee edellyttää jatkuvaa toiminta- ja reagointikykyä.

CER-direktiivin kansallinen toimeenpano

EU:n Verkko- ja tietoturvadirektiivin kansallisen toimeenpanon rinnalla EU Kriittisen infrastruktuurin direktiivin (CER) kansalliseen toimeenpanoon liittyvää hallituksen esitystä ei ole vielä annettu. Direktiivit muodostavat kokonaisuuden, jolloin myös niihin liittyvästä lainsäädännöstä olisi hyvä pystyä käsittelemään soveltuvin osin

kokonaisuutena, jolloin pystytään tunnistamaan mahdolliset valmistelussa syntyneet epäyhtenäisyydet.

Yritysten kannalta mahdollisesti yhteistä tarkastelua edellyttävät kokonaisuudet liittyvät mm. valvontaan ja poikkeamista ilmoittamiseen.

Tässäkin tulisi päästä yhden luukun periaatteeseen, jossa vältetään päällekkäinen valvonta ja useat ilmoituksia vastaanottavat toimijat.

Kunnioittaen

Jaakko Wallenius
Turvallisuusjohtaja

Antti-Pekka Manninen
Head of Privacy