Yrityslainsäädäntö
Markku Rajamäki

Eduskunnan liikenne- ja viestintävaliokunnalle
LiV@eduskunta.fi

Muistio 1 (3)

22.5.2025

Viite: Liikenne- ja viestintävaliokunta perjantai 23.05.2025 klo 11.30 / HE 27/2025 / Asiantuntijapyyntö 14.5.2025

Elinkeinoelämän keskusliitto EK:n asiantuntijalausunto luonnoksesta hallituksen esitykseksi kyberturvallisuuslain muuttamisesta

Kiitämme mahdollisuudesta tulla kuulluksi. Keskitymme asiantuntijalausunnossamme kyberturvallisuuslakiin ehdotettuihin muutoksiin.

Katsomme, että esitetyt muutokset ovat sinällään tarpeellisia, jotta NIS2-direktiivin toimeenpaneva kyberturvallisuuslaki ja CER-direktiivin toimeenpaneva laki yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta toimisivat yhdessä siten kuin on tarkoitettu.

Esitettyjen muutosten vaikutusten arviointi on kuitenkin haastavaa erityisesti siksi, ettei annetuilla tiedoilla ole mahdollisuutta kattavasti arvioida esitettyjen muutosten perusteella NIS2-soveltamisalaan tulevien uusien yritysten määrää tai sitä, kuinka paljon pienempiä, keskisuuren yrityksen kokokriteerit alittavia yrityksiä soveltamisalaan tulisi kuulumaan. Näin ei ole myöskään mahdollista arvioida esitettyjen muutosten kustannus- ja muita vaikutuksia sen enempää yksittäiseen yritykseen kuin vaikutuksia yksittäisellä toimialalla tai koko suomalaisessa yrityskentässä.

Kuten esityksessäkin on todettu, sekä taloudelliset että toiminnalliset vaikutukset voivat olla merkittäviä yksittäiseen keskisuurta pienempään yritykseen, jolle CER-kriittiseksi määrittäminen ja sen myötä nyt esitetty NIS2-keskeiseksi toimijaksi määrittäminen tulee yllätyksenä.

Nämä haasteet pohjautuvat osin myös siihen, ettei myöskään HE 205/2024 vp:ssä laiksi yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta ole tarkkoja arvioita suoraan siinä esitettyjen lainmuutosten kautta soveltamisalaan kuuluvien yritysten määristä.

Edellä kerrottu huomioiden esitämme, että esitettyjä kuukauden siirtymämääräaikoja tulisi pidentää. Esityksen mukaan kyberturvallisuuslain 10–18 ja 41 §:ää sovelletaan kriittiseen toimijaan kuukauden kuluttua siitä, kun tämä on saanut tiedon päätöksestä, jolla tämä on määritetty kriittiseksi toimijaksi. Viitatut säännökset koskevat johdon vastuuta, poikkeamailmoituksia viranomaiselle, poikkeamaa koskevaa väliraporttia ja loppuraporttia, poikkeamasta ja kyberuhkasta ilmoittamista muulle kuin viranomaiselle, vapaaehtoista ilmoittamista, poikkeamailmoituksen vastaanottoa ja käsittelyä sekä keskitettyä yhteyspistettä.

Kuukauden määräaika on erittäin lyhyt tilanteessa, jossa toimija ei ole välttämättä voinut juuri mitenkään varautua sitä koskeviin uusiin velvoitteisiin. Yksinään jo poikkeamien havaitsemiseen, arviointiin ja ilmoittamiseen liittyvän prosessin kehittäminen voi olla aikaa vievää. Pidämme kuukauden määräaikaa näiltä osin kohtuuttomana.

Sen sijaan esitettyä yhdeksän kuukauden siirtymämääräaikaa kyberturvallisuuslain 7-9 §:ien soveltamisesta voitaneen pitää riittävänä, joskin sekin voi olla yrityksen kyberturvallisuusriskien hallinnan status huomioiden erittäin vaativa. Viitatut säännökset koskevat riskienhallinnan järjestämistä, kyberturvallisuutta koskevaa riskienhallinnan toimintamallia sekä toimenpiteitä kyberturvallisuutta koskevien riskien hallinnassa.

Olemme myös erittäin huolissamme viranomaisten valvontaresursseista liittyen sekä kyberturvallisuuslain että yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsieto-kyvyn parantamisesta annettavan lain osalta. Yritykset, ja erityisesti nyt käsiteltävänä olevien muutosten kohteena olevat yritykset tulevat tarvitsemaan tukea. Kuitenkaan valvoville viranomaisille ei ole myönnetty lisämäärärahoja uusien lakisääteisten tehtävien hoitamiseksi, ja monet ovat indikoineet, etteivät ne kykene hoitamaan näitä tehtäviä muillakaan järjestelyillä, esim. tehtäviä priorisoimalla.

Lisäksi kiinnitämme huomiota seuraavaan:

Kyberturvallisuuslain ehdotettu muutos laajentaa kyberturvallisuusvelvoitteita keskisuurta pienempiin yrityksiin, jotka tultaisiin määrittelemään kriittisiksi toimijoiksi. Terveyssektorilla MD- ja IVD-asetukset määrittävät jo tällä hetkellä lääkinnällisille laitteille ja niiden valmistajille tiukat kyberturvallisuusvaatimukset ihmisille kohdistuvien riskien ehkäisemiseksi. MD- ja IVD-asetukset eivät sisällä suoranaisesti kyberturvallisuutta koskevaa erillistä lukua tai määritelmää, mutta ne

asettavat vaatimuksia, jotka efektiivisesti liittyvät kyberturvallisuuteen erityisesti lääkinnällisten laitteiden turvallisuuden ja suorituskyvyn näkökulmasta. Kyberturvallisuuslain soveltaminen voi johtaa tilanteeseen, jossa terveysteknologiayritykset joutuvat noudattamaan sekä MD- ja IVD-asetusten että uuden kyberturvallisuuslain ilmoitusvelvoitteita erikseen, mikä lisää hallinnollista taakkaa ja kustannuksia. Ehdotamme, että terveysteknologian osalta lainsäädännössä tunnistetaan MD- ja IVD-asetusten fokusalue sekä vaatimukset ja varmistetaan, että sääntely on yhdenmukaista ja kohdistettu oikein. Tämä pätee todennäköisesti joidenkin muidenkin alojen tuoteturvallisuuslainsäädännön ja kyberturvallisuuslain keskinäiseen suhteeseen.