



Eduskunnan liikenne- ja viestintävaliokunnalle
LiV@eduskunta.fi

Muistio

1 (3)

13.9.2024

Liikenne- ja viestintävaliokunta tiistai 17.09.2024 klo 12.00 / HE 57/2024 vp / Asiantuntijapyyntö
2.8.2024

Elinkeinoelämän keskusliitto EK:n asiantuntijalausunto HE 57/2024 vp:stä kyberturvallisuusdirektiivin (NIS 2 -direktiivi) täytäntöönpanoa koskevaksi lainsäädännöksi

Kiitämme mahdollisuudesta tulla kuulluksi.

Keskitymme asiantuntijalausunnossamme erityisesti kahteen keskeiseen asiaan: A) hallituksen esityksen soveltamisalamääritelmän haasteisiin, sekä B) soveltamisalan organisaatioiden tarvitsemaan tukeen ja siihen osoitettaviin viranomaisresursseihin.

A) Soveltamisalamääritelmän haasteet

Nähdäksemme soveltamisalamääritelmään liittyy kolme haasteellista kohtaa.

1 luku 3 §:n 3 momentin tulkinta

Hallituksen esityksessä on lähdetty siitä, että liitteiden I ja II toimialoihin lukeutuvat ja henkilöstömäärä- tai liikevaihto- ja tasekriteerit ylittävät, 1 luku 3 §:ssä tarkoitetut toimijat ilmoittautuvat toimijaluetteloon itse 6 luku 41 §:n mukaisesti. Tämä on poikkeuksellista verrattuna valmistelussa olevaan CER-direktiivin kansalliseen toimeenpanoon, jossa lähdetään siitä, että viranomainen määrittelee kriittiset toimijat ja viranomaisella on velvollisuus ilmoittaa tekemästään päätöksestä sen kohteelle.

Osalle toimijoista ehdotetun kyberturvallisuuslain 1 luku 3 §:n soveltamisalamääritelmän tulkitseminen on selkeää, mutta kaikille ei. Sillä, kuuluuko ylipäättään soveltamisalaan ja onko keskeinen vai tärkeä toimia, on kuitenkin iso merkitys mm. valvonnan luonteen ja toimijan johdon henkilökohtaisen vastuun kannalta.

Erityisen ongelmallinen tässä suhteessa on ehdotettu 3 §:n 3 momentin kriteerien tulkinta tilanteessa, jossa 1) liitteiden I ja II toimialoilla toimiva joko alittaa keskisuuren toimijan kokokriteerin tai 2) liitteen II toimialoilla toimiva täyttää vähintään keskisuuren toimijan kokokriteerin. Ymmärryksemme mukaan molemmissa tapauksissa toimija voi

Lainsäädäntö ja hallinto/Yrityslainsäädäntö
Markku Rajamäki

13.9.2024

ilmeisesti nousta keskeiseksi toimijaksi ja siten ennakkovalvonnan ja mm. johdon ankaran henkilökohtaisen vastuun piiriin, mikäli 3 §:n 3 momentin kriteerien katsotaan täyttyvän.

Pidämme kohtuuttomana, että yritysten pitäisi 3 §:n 3 momentin kriteerejä tulkiten päätyä asiassa oikeaan lopputulokseen. Sen vuoksi kannattamme esityksen perusteluissakin (s. 153–154) omaksuttua näkemystä, että kriteerejä tulisi vielä tarkentaa antamalla asiasta valtioneuvoston asetus. Lisäksi ehdotamme, että valvoville viranomaisille asetettaisiin joka tapauksessa esim. 6 luku 41 §:ssä velvollisuus olla yhteydessä soveltamisalaan kuuluviin toimijoihin ja kertoa soveltamisalaan kuulumisesta, tai vähintäänkin niihin toimijoihin, joiden viranomainen harkitsee täyttävän 3 §:n 3 momentin kriteerit, mutta ei vähintään keski-suuren toimijan kokokriteeriä.

Henkilöstömäärää koskevan kriteerin tulkinta

Toimialamääritelmän lisäksi toinen keskeinen kriteeri on kokokriteeri, joka on rakennettu siten, että henkilöstömäärä toisaalta ja liikevaihtosekä tasekokonaisuus toisaalta ovat vaihtoehtoisia. Riittää, että toinen niistä täyttyy. Liikevaihto- ja tasekriteeri on nähdäksemme selkeä, mutta henkilöstömääräkriteeriä tulisi tarkentaa. Säännöstekstistä tai esityksen perusteluista ei nähdäksemme ilmene, minkä mukaan henkilöstömäärä tulee määritellä. 1 luku 3 momentin perusteluissa (s. 146) puhutaan toimijan palveluksessa olevien määrästä. Työelämä nykypäivänä on kuitenkin monimuotoista ja alat eroavat toisistaan esim. sen suhteen, kuinka suurta työntekijöiden määrän kausivaihtelu on tai kuinka suuren osan työntekijöistä osa-aikaiset työntekijät muodostavat. Sen vuoksi kriteeriä tulisi tarkentaa määrittelemällä, tarkoitetaanko tilikauden koko tai keskimääräistä työntekijämäärää, työntekijämäärää työtunnit täysiksi työvuosiksi muutettuna vai jotain muuta. Määritelmä perustuu komission suositukseen 2003/361/EY, jossa asiaa ei myöskään ole määritelty tämän tarkemmin. Oikeudenmukaisimmalta nähdäksemme vaikuttaisi käyttää työntekijämäärää työntekijöiden työtunnit täysiksi työvuosiksi muutettuna (ns. FTE/WTE, full-time equivalent / whole time equivalent), joka huomioisi alat, joissa työntekijöiden määrän kausivaihtelu on suurta tai osa-aikaisten työntekijöiden määrä on suuri.

Oikeussubjektikohtaisuus

Esityksen perusteluissa (s. 146–147) on hyvin avattu sitä, että toimijan määritelmää on tutkittava oikeussubjektikohtaisesti. Kuitenkin sivun 147 toisessa kappaleessa pohditaan sitä, millainen merkitys konsernirakenteessa voi olla erilaisilla omistusyhteyksillä ja sidoksilla. Näiden merkitys toimijan määritelmän kannalta jää kuitenkin täysin avoimeksi. Näkemyksemme on, että kohtaa tulisi tarkentaa, jotta ei synny sellaista tulkintaa, että välittömän viranomaisvalvonnan kohteeksi tuleva toimija määräytyisi jotenkin muuten kuin oikeussubjektikohtaisesti.

Lainsäädäntö ja hallinto/Yrityslainsäädäntö
Markku Rajamäki

13.9.2024

B) Soveltamisalan organisaatioiden tarvitsema tuki ja siihen osoitettavat viranomaisresurssit

Esitettävä lainsäädäntö tuo mukanaan merkittäviä ja osin hyvin yksityiskohtaisia ja teknisiäkin kyberturvallisuusvaatimuksia soveltamisalan toimijoille. Vaatimukset ovat lisäksi riskiperusteisia, mikä tarkoittaa, että samakin riski voi eri toimialoilla ja eri toimijoiden arjessa näyttäytyä eri tavoin ja eri suuruisena. Tällöin myös hallintatoimien kokonaisuus ja taso voi toimijoiden välillä vaihdella ja riskienhallinnan taso voi silti olla riittävä. Samaa ratkaisua riskiin ei siksi voi edellyttää kaikilta. Näistä syistä on tärkeää, että viranomaisilla on osoittaa toimijoiden tarvitsemaan tukeen riittävästi osaavaa valvontaresurssia, joka ymmärtää ammattilaistasoisesti sekä kyberturvallisuutta että kyseisen toimialan erityispiirteitä.

Mikäli käy niin, että toimialakohtaisten valvontaviranomaisten resurssit eivät ole riittävät, sitä tärkeämpää on pitää huolta Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen resursseista. Huomioiden sen, että valvovilla toimialaviranomaisilla ei ole päivitysvelvollisuutta virkaajan ulkopuolella, Kyberturvallisuuskeskus on ainoa viranomaistaho, jolta toimija voi odottaa tukea poikkeaman tapahtuessa pyhänä, yöllä tai viikonloppuna. Toivomme myös, että poikkeamien ilmoittaminen tehdään toimijoille mahdollisimman helpoksi esim. luomalla NIS2- ja GDPR-poikkeamien ilmoittamiselle yhteinen kanava. Mikäli poikkeama kohdistuu henkilötietoihin, täyttyy tyypillisesti ilmoitusvelvollisuus sekä tietosuojavaltuutetulle että myöhemmin kyberturvallisuusviranomaisille.

Muut huomiot

Esitetyn 20 §:n 1 momentin 9 kohdan tekstiin olisi hyvä sisällyttää NIS 2 -direktiivin 11 artiklan 4 kohdassa asetettu velvoite, jonka mukaan CSIRT-yksikön tulee luoda yhteistyösuhteet asiaankuuluviin yksityisen sektorin sidosryhmiin. Tämä velvoite löytyy nyt perustelutekstistä, mutta merkittävyytensä vuoksi se olisi hyvä nostaa säädöstekstiin.

Esityksen 6 luku 44 §:ssä säädetään kyberkriisinhallintaviranomaisesta, jollaisena toimii kukin laissa tarkoitettu valvova viranomainen sille säädettyjen tehtävien mukaisesti. Ehdotuksen mukaan: ”Liikenne- ja viestintäviraston Kyberturvallisuuskeskus toimii koordinaattorina laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien hallinnassa.” Katson, että laajojen moniviranomaistilanteiden hallitsemiseksi olisi syytä harkita tulisiko koordinaattorin tehtävä kuvata laissa tarkemmin. Koordinointi ei ole sama asia kuin johtaminen.