Mika Linna
29.11.2023

Liikenne- ja viestintäministeriö
Kirjaamo

kirjaamo.lvm@gov.fi

Diaarinro VN/18157/2023

Finanssiala ry:n lausunto luonnoksesta hallituksen esitykseksi NIS2-direktiivin täytäntöönpanemiseksi

Liikenne- ja viestintäministeriö on pyytänyt Finanssiala ry:n (FA) lausuntoa luonnoksesta hallituksen esitykseksi NIS2-direktiivin täytäntöönpanemiseksi (HE-luonnos).

1 HE-luonnoksessa finanssialan toimijoita ei ehdoteta sisällytettävän kyberturvallisuuden riskienhallinnasta annetun lain soveltamisalaan, sillä kyseisiin toimijoihin sovellettaisiin DORA-asetusta ja sitä täytäntöönpanevaa sääntelyä. FA pitää ratkaisua johdonmukaisena, koska DORA-asetus on NIS2-direktiiviin nähden erityislaki (*lex specialis*), minkä lisäksi se asettaa finanssialan toimijoille NIS2-direktiivin velvoitteita pidemmälle meneviä velvoitteita kyberuhkiin varautumiseksi.

2 FA pitää välttämättömänä, että NIS2- ja CER-direktiivejä implementoitaessa ja niihin liittyviä tarkempia teknisiä määräyksiä laadittaessa varmistetaan, että annettava sääntely on yhteensopivaa ja oikeasuhtaista finanssialan toimijoihin ja niiden tarjoamiin palveluihin sovellettavan EU-oikeuden ja siihen nojautuvan kansallisen lainsäädännön kanssa.

3 Konsernirakenteiden osalta tulisi säätää selkeästi vaatimuksista ja menettelytavoista esim. tilanteessa, jossa konsernin yhtiöistä vain osa kuluu NIS2-direktiivin soveltamisalaan. Jos tällainen konserni kuitenkin toimii yhteisen ICT-infrastruktuurin varassa, epäyhtenäiset kyberturvallisuusvaatimukset mahdollistavat mm. konsernin heikommin suojattujen yksiköiden hyödyntämisen hyökkäyskanavana konsernin vahvemmin suojattuja yksiköitä vastaan (ns. toimitusketjuhyökkäys).

4 Johdon vastuuta koskevan 2 luvun 10 §:n osalta FA katsoo, että vastuu tulee rajata voimassa olevan lainsäädäntömme mukaisesti osakeyhtiön toimielimiin – hallitukseen, mahdolliseen hallintoneuvostoon ja toimitusjohtajaan. Vastuun ulottaminen toimitusjohtajan välittömässä alaisuudessa kuuluviin tehtäviin on yhtiöoikeudellemme vieras ja se tulisi poistaa lakiehdotuksesta.

5 NIS2-direktiivin soveltamisalaan kuuluva tietoturvaloukkaus voi synnyttää useita päällekkäisiä raportointivelvoitteita sekä kansallisesti että muiden jäsenvaltioiden viranomaisille. Tarpeettomien taloudellisten ja hallinnollisten kustannusten välttämiseksi ja tietoturvaloukkausten tehokkaan selvittämisen ja hoitamisen varmistamiseksi FA pitää välttämättömänä, että raportointia varten luotaisiin keskitetty kanava. Käytännön syistä tulisi myös sallia se, että raportointi olisi aina mahdollista tehdä englanniksi.

FINANSSIALA RY

Taina Ahvenjärvi