Mika Linna
17.9.2024

Liikenne- ja viestintävaliokunnalle

HE 57/2024

FINANSSIALA RY:N LAUSUNTO HALLITUKSEN ESITYKSESTÄ KYBERTURVALLISUUSLAIKSI

Eduskunnan liikenne- ja viestintävaliokunta on 6.8.2024 pyytänyt Finanssiala ry:n (FA) lausuntoa hallituksen esityksestä kyberturvallisuuslaiksi.

1 Hallituksen esityksessä finanssialan toimijoita ei ehdoteta sisällytettävän kyberturvallisuuslain soveltamisalaan, sillä kyseisiin toimijoihin sovelletaan DORA-asetusta[1] ja sitä täytäntöönpanevaa sääntelyä. FA pitää ratkaisua johdonmukaisena: DORA-asetus on NIS2-direktiiviin[2] nähden erityislaki (*lex specialis*), minkä lisäksi se asettaa finanssialan toimijoille NIS2-direktiiviä pidemmälle meneviä velvoitteita kyberuhkiin varautumiseksi.

2 FA pitää välttämättömänä, että NIS2- ja CER-direktiivejä[3] implementoitaessa ja niihin liittyviä tarkempia teknisiä määräyksiä laadittaessa varmistetaan, että sääntely on yhteensopivaa ja oikeasuhtaista finanssialan toimijoihin ja niiden tarjoamiin palveluihin sovellettavan EU-oikeuden ja siihen nojautuvan kansallisen lainsäädännön kanssa.

3 Konsernirakenteiden osalta olisi tarpeen varmistaa yhtenäiset menettelytavat ja periaatteet tilanteisiin, joissa konserni toimii yhteisen tieto- ja viestintäteknisen infrastruktuurin varassa, mutta vain osa konsernin yhtiöistä kuluu NIS2-direktiivin soveltamisalaan. Näissä tilanteissa epäyhtenäiset vaatimukset voivat mahdollistaa konsernin heikommin suojattujen yksiköiden käytön hyökkäyskanavana muita yksiköitä vastaan (ns. toimitusketjuhyökkäys).

4 NIS2-direktiivin soveltamisalaan kuuluva tietoturvaloukkaus voi synnyttää useita päällekkäisiä ja tiukkoihin määräaikoihin sidottuja 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.

5 Yksityiskohtainenkaan sääntely ei itsessään saa aikaan tavoiteltua muutosta, vaan se edellyttää asianmukaista toimeenpanoa. FA pitääkin tarpeellisena, että vastuuviranomaisille varmistetaan riittävät taloudelliset ja henkilöresurssit niille osoitettujen tehtävien hoitamiseksi.

6 Lopuksi FA haluaa kiinnittää huomiota siihen, että yhteiskunnan toiminnan kannalta kriittisiin sektoreihin ja toimijoihin kohdistuvat kyberuhkat eivät ole vain ulkoisia. Tämän vuoksi lainsäädännön tulisikin tarjota kriittisille toimijoille nykyistä selvästi tehokkaampia keinoja varmistaa tietojärjestelmiensä, käyttöympäristöjensä ja tietoverkkojensa sekä niitä hyödyntävien prosessien ja palvelujen turvallisuus myös sisäisten virheiden, vahinkojen ja väärinkäytösten varalta.

FINANSSIALA RY

Taina Ahvenjärvi

[1] DORA = asetus (EU) 2022/2554 finanssialan digitaalisesta häiriönsietokyvystä ym.
[2] NIS2 = direktiivi (EU) 2022/2555 toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa ym.
[3] CER = direktiivi (EU) 2022/2557 kriittisten toimijoiden häiriönsietokyvystä ym.