FINANSSIALA

16.8.2019

Linna Mika

Finanssivalvonnalle

Finanssiala ry:n lausunto Finanssivalvonnan määräys- ja ohjekokoelman luonnokseen Operatiivisen riskin hallinta rahoitussektorin valvottavissa (FIVA 13/01.00/2019)

Finanssiala ry (FA) pitää tärkeänä, että verkko- ja tietoturvaloukkaukset ja maksupalveluihin liittyvät petostiedot raportoidaan Finanssivalvonnalle voimassa olevien säädösvelvoitteiden mukaisesti ja ilman aiheetonta viivytystä.

Rahoitussektorin yritysten raportointivelvoitteet ovat laajentuneet ja kiristyneet merkittävästi viime vuosien aikana, mikä on merkittävästi lisännyt näihin käytettävän työajan ja henkilöresurssien tarvetta. Erityisesti tietoturvaloukkausten osalta raportointiin usein osallistuvat henkilöt, joiden työpanos on välttämätön loukkauksen selvittämiseksi ja siitä toipumiseksi.

FA pitääkin tärkeänä, että poikkeama- ja petosraportointien sisältöjä ja menetelmiä kehitetään yhteistyössä toimialan kanssa, jottei raportoinnin aiheuttama työmäärä kasva kohtuuttomaksi. Samassa yhteydessä tulisi kiinnittää raportoinnin perusteella annettavan viranomaispalautteen laatuun ja nopeuteen sekä yksittäisen toimijan että koko toimialan tasolla. Valvovan viranomaisen ajantasainen ja hyvin perusteltu palaute on tarpeellista paitsi yrityksen oman toiminnan ja riskienhallinnan kehittämiselle, myös toimialan tilannekuvan ylläpitämiselle.

Luonnoksen kohdan 9.1 alakohta 4 edellyttää, että haittaohjelman levittäminen tietojärjestelmään tulisi raportoida Finanssivalvonnalle. FA pitää ilmaisua tulkinnanvaraisena, koska se voisi kattaa esim. tilanteet, joissa saastuneen liitetiedoston sisältävä viesti on päässyt sisään yrityksen sähköpostijärjestelmään, vaikka viesti olisikin sittemmin poistettu organisaation tietoturvaohjeiden mukaisesti. FA ehdottaakin, että raportointi rajoitettaisiin tilanteisiin, jossa haittaohjelma on päässyt leviämään rahoitusalan yrityksen tietojärjestelmään.

Saman alakohdan mukaisesti toimijan tulisi myös raportoida kaikki palvelunestohyökkäykset. FA pitää velvoitetta tarpeettoman laajana ja esittää, että se rajataan vain hyökkäyksiin, jotka ovat ilmenneet yrityksen toimintojen tai asiakkaille tarjottavien palvelujen näkyvänä häiriönä. Rahoitusalan yritysten ohella käytännössä kaikkiin yksityisen ja julkisen sektoriin toimijoihin kohdistuu jatkuvia palvelunestohyökkäyksiä, joista valtaosa torjutaan menestyksellisesti ja vain murto-osa aiheuttaa näkyviä vaikutuksia yrityksen sisäisiin toimintoihin tai asiakkaille näkyviin palveluihin.

Luonnoksen kohdan 9.1 alakohdan 9 mukaisesti Finanssivalvonnalle tehtävä ilmoitus ei poistaisi valvottavan velvollisuutta raportoida tietojen paljastumisesta asiattomille myös tietosuoja-asetuksen raportointivelvoitteiden mukaisesti. Tietosuoja-asetuksen asettamat raportointivelvoitteet ovat laajoja ja FA pitää tärkeänä, ettei niitä pyritä edelleen laajentamaan rahoitustoimialan osalta. Rahoitusalan toimijat ovat panostaneet merkittävästi tietosuoja-asetuksen toimeenpanoon ja FA katsoo, että tältä osin asetuksen vaatimusten ja sen edellyttämien toimintatapojen noudattamisen tulisi riittää. Tällöin Finanssivalvonnalle raportoitavat tietosuojatapahtumat rajattaisiin niihin, jotka ilmoitetaan tietosuojavaltuutetulle.

Mika Linna
Finanssiala ry