FINANSSIVALVONTA
FINANSINSPEKTIONEN
FINANCIAL SUPERVISORY AUTHORITY

11.10.2017 FIVA 23/01.01.00/2017

Julkinen

Operatiiviset riskit, Anne Nisén

Liikenne- ja viestintäministeriö
kirjaamo@lvm.fi

Viite: LVM/1616/03/2016

Lausunto hallituksen esityksestä laeiksi Euroopan unionin verkko- ja tietoturvadirektiivin täytäntöönpanoon liittyvien lakien muuttamisesta

Finanssivalvonta kiittää mahdollisuudesta lausunnon antamiseen liittyen LVM/1616/03/206 hallituksen esitykseen laeiksi Euroopan unionin verkko- ja tietoturvadirektiivin täytäntöönpanoon liittyvien lakien muuttamisesta. Pahoittelemme lausunnon lähettämistä erillisenä dokumenttina, mutta Finanssivalvonnassa ei ole vielä ehditty ohjeistaa lausuntopalvelun käyttöä.

Finanssivalvonnan lausunto on ryhmitelty lausuntopalvelussa olevan lausuntopyynnön otsikoiden mukaisesti.

Yhteiskunnan toiminnan kannalta keskeisten palveluiden määrittäminen

Hallituksen esitysluonnos ei sisällä ehdotusta lainsäädännön muuttamisesta pankkialan ja finanssialan infrastruktuurin keskeisten palvelujen määrittämisen osalta.

Yhteiskunnan toiminnan kannalta keskeisten palvelujen määrittämisessä tulisi palvelujen sijasta tarkastella keskeisiä palveluja tuottavia palveluntarjoajia.

NIS-direktiivin liitteessä II finanssialan osalta on määritelty kaksi osa-aluetta keskeisten palvelujen tarjoajien osalta:

1. Pankkiala: Luottolaitokset, sellaisina kuin ne määritellään Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 575/2013 [13] 4 artiklan 1 kohdassa
2. Finanssimarkkinoiden infrastruktuurit:
    a. Euroopan parlamentin ja neuvoston direktiivin 2014/65/EU [14] 4 artiklan 24 kohdassa määriteltyjen kauppapaikkojen ylläpitäjät
    b. Keskusvastapuolet, sellaisina kuin ne määritellään Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 648/2012 [15] 2 artiklan 1 kohdassa

Finanssialan osalta edellä mainittujen määritelmien mukaan direktiivin soveltamisalan piiriin keskeisten palvelujen tuottamisen osalta tulisivat ainakin seuraavat toimijat:

- suurimmat luottolaitokset
- (Suomessa ei ole tällä hetkellä keskusvastapuoliksi määriteltäviä toimijoita)
- Pörssi

Kysymys siitä, millä menettelyllä ja mihin toimivaltaan perustuen yhteiskunnan ja/tai talouden kannalta kriittiset palvelut ja toiminnot määriteltäisiin ja toisaalta miten yksittäiset

keskeisten palvelujen tuottajat nimettäisiin, tulisi ratkaista horisontaalisena kysymyksenä. Kriittisten palveluiden kriteerien määrittely soveltunee lakiteknisesti heikosti toteuttavaksi suoraan lainsäädännön tasolla, vaan tähän tarvittaisiin alempiasteista sääntelyä.

Finanssivalvonta on NIS-direktiivin valmistelumuistion yhteydessä nostanut esiin tarpeen kansallisen implementoinnin laajentamisesta sellaisiin finanssialan yrityksiin, joiden merkitys yhteiskunnan kriittisten toimintojen ylläpitämisessä on suuri. Tällaisia toimijoita ovat mm. arvopaperikeskus, maksulaitokset ja maksupäätepalveluja korttimaksamiseen tarjoavat toimijat. Näitä toimijoita ei nyt lausunnolla olevassa hallituksen esityksen luonnoksessa ole huomioitu.

Toiminnanharjoittajille ehdotettavat tietoturvallisuutta koskevat riskienhallintavelvoitteet

Hallituksen esitysluonnos ei sisällä pankkialan ja finanssialan infrastruktuurin osalta ehdotusta lakien muuttamisesta toiminnanharjoittajille ehdotettavien tietoturvallisuutta koskevien riskienhallintavelvoitteiden osalta.

Pankkialaa ja finanssialan infrastruktuuria koskevassa nykysääntelyssä on jo laajalti huomioitu NIS-direktiivistä tulevia velvoitteita riskien hallinnan, tietojärjestelmien ja tietoturvallisuuden järjestämiseksi ja poikkeamista raportoimiseksi.

Luottolaitoslain 5 luvun 10-11§§:ssä säädetään luottolaitoksen merkittävän toiminnan ulkoistamisesta ja ulkoistamisen edellytyksistä. Varautumisvelvollisuudesta on säädetty 16§:ssä. Yleiset luottolaitoksen riskienhallintajärjestelmälle asetettavat vaatimukset on annettu luottolaitoslain 9 luvun 2§:ssä ja operatiivisten riskien hallinnan osalta 16§:ssä. Sama artikla sisältää myös maininnan tietojärjestelmien luotettavuudesta ja varautumissuunnittelusta. Finanssivalvonnan määräystenantovaltuudesta on säädetty 24§:ssä.

Maksulaitoksien osalta maksulaitoslain 3 luvun 19§ sisältää velvoitteet toiminnan ja riskienhallinnan järjestämisestä sekä Finanssivalvonnan määräyksenantovaltuuden tarkempien määräysten antamisesta. Ulkoistamisesta annetut määräykset ovat 23§:ssä ja varautumisvelvollisuuteen liittyvät määräykset 41a§:ssä.

Finanssivalvonnan antamat tarkemmat operatiivisten riskien hallintaa ja ulkoistamista koskevat määräykset ja ohjeet:
Määräykset ja ohjeet 8/2014 Operatiivisen riskin hallinta rahoitussektorin valvottavissa
Määräykset ja ohjeet 1/2012 Ulkoistaminen

Soveltamisalaan lisättäväksi ehdotettujen arvopaperikeskuksien osalta Parlamentin ja neuvoston asetus 909/2014 (ns. I tason asetus) sisältää säännöksiä ulkoistamisesta ja operatiivisten riskien hallinnasta (artiklat 19 ja 30: ydinpalveluiden ulkoistaminen edellyttää toimilupaprosessia, muutoin ilmoitus toimivaltaiselle viranomaiselle riittää; artikla 45 operatiivisten riskien hallinta). Artikla 45 sisältää myös velvollisuuden raportoida operatiivisista riskeistä johtuvista toiminnan harjoittamiseen vaikuttavista tapahtumista (operational incidents) toimivaltaiselle viranomaiselle. II-tason asetus ((EU) 2017/392) sisältää tarkempaa sääntelyä mm. yleisesti riskienhallinnan järjestämisestä ja operatiivisista riskeistä sekä erityissäännöksiä mm. IT-järjestelmistä ja jatkuvuussuunnittelusta.

Operatiiviset riskit, Anne Nisén

Finanssivalvonnan määräyksiä ja ohjeita operatiivisten riskien hallinnasta ja ulkoistamisesta sovelletaan suosituksena arvopaperikeskukseen.

NIS-direktiivin soveltamisalaan kuuluvat kauppapaikkojen ylläpitäjät, joita ovat säännelty markkina, monenkeskinen kaupankäyntijärjestelmä (MTF) sekä organisoitu kaupankäyntijärjestelmä OTF). Myös pörssi katsotaan kuuluvaksi kauppapaikkojen ylläpitäjiin.

Kauppapaikkojen ylläpitäjät voivat olla sijoituspalveluyrityksiä, luottolaitoksia ja säännellyn markkinan ylläpitäjiä. Silloin kun kauppapaikan ylläpitäjä on luottolaitos tai sijoituspalveluyritys, noudatetaan näitä koskevia riskienhallinta- ja ulkoistamissäännöksiä.

Säännellyn markkinan ylläpitäjän yleistä riskienhallintaa koskevaa sääntelyä on mm. laissa kaupankäynnistä rahoitusvälineillä (RahkL, 2 luku 17§). Samassa laissa on säädetty myös ulkoistamisen edellytyksistä RahkL, 2 luku 19§). Finanssivalvonnalla on oikeus antaa tarkempia määräyksiä ja ohjeita(RahkL, 2 luku 44§) ja Finanssivalvonnan operatiivisten riskien hallintaa ja ulkoistamista koskevat määräykset ja ohjeet koskevat osittain myös pörssiä. Finanssivalvonnan operatiivisten riskien hallinnan määräyksissä ja ohjeissa annettavat velvoitteet poikkeamaraportoinnista koskevat pörssiä ainoastaan suosituksena tällä hetkellä. Tämä olisi syytä korjata NIS-direktiiviin pohjautuvassa sääntelyssä. Ulkoistamista koskevat Finanssivalvonnan antamat määräykset ja ohjeet velvoittavat myös pörssiä. Nasdaqin toiminta useissa Pohjoismaissa ja koordinoitu valvonta ovat syynä siihen, että raportointi tehdään kaikille valvojille yhteisesti sovittujen kriteerien mukaisesti.

MiFID2:n implementoinnin yhteydessä tammikuusta 2018 alkaen finanssisääntelyn piiriin tulee uusina toimijoina ns. raportointipalveluiden tarjoajat. Näiden toimijoiden tietoturvariskien hallintaa säännellään sekä MiFID2:ssa (art. 64(4), art. 65(4), art. 66(3)) että niiden nojalla annettavilla täytäntöönpanosäädöksillä. Säännellyn markkinan ylläpitäjää koskee yleinen riskienhallintavelvoite sekä tietojärjestelmien hallintaa ja jatkuvuutta koskeva velvoite sekä erityiset ns. systems resilience vaatimukset (artiklat 47-48). Tietoturvaa ei nosteta MiFID2:ssa erikseen esille, mikä olisi syytä huomioida NIS-direktiivin implementoinnin yhteydessä.

Valvontaviranomaisen tehokkaat ja riittävät toimivaltuudet (ml. seuraamukset ja sanktiot)

Laissa Finanssivalvonnasta 3 luvun 18§:ssä Finanssivalvonnalle annetaan oikeus saada valvonnassa tarvittavia tietoja valvottavilta ja samassa artiklassa Finanssivalvonnalle annetaan oikeus antaa määräyksiä näiden tietojen saamiseksi. Finanssivalvontaa koskevan lain 3 luvun 24§:ssä säädetään lisäksi tarkastusoikeudesta. Finanssivalvonnalla on oikeus myös toimeenpanokiellon asettamiseen ja oikaisukehotuksen antamiseen (2 luvun 33§). Siten valvontaviranomaisen tehokkaat ja riittävät toimivaltuudet on turvattu nykylainsäädännössä.

Muut yleiset huomiot

NIS-direktiivin mukainen viranomaisten välinen tiedonvaihto olisi hyvä ratkaista siten,

että poikkeamia voidaan käsitellä joustavasti useamman viranomaisen yhteistyönä. Tällöin toimijan ei tarvitsisi tehdä ilmoituksia useille viranomaisille.

Finanssialan osalta selkein vaihtoehto olisi toimia nykyisten raportointivelvoitteiden mukaisesti myös direktiivin mukaisten raportointivelvoitteiden täyttämiseksi. Finanssialan toimijoilla on jo nyt raportointivelvollisuus Finanssivalvonnalle eikä velvoite poistu NIS-direktiivin implementoinnin jälkeen. Joillakin finanssialan yrityksillä (tällä hetkellä ns. SI-pankit, Significant Institutions, jatkossa ehkä myös pienemmät pankit) on raportointivelvollisuus kyberturvallisuuteen liittyvien poikkeamatapausten osalta myös Euroopan keskuspankille.

Finanssivalvonta välittäisi tiedon muille kansallisille viranomaisille kuten Viestintäviraston CSIRTille. Finanssivalvonnalla on nykyisellään velvoitteita välittää tietoa nopeasti eteenpäin myös esim. Euroopan keskuspankille.

Laissa tulisi mahdollistaa laaja tiedonvaihto poikkeamista viranomaisten välillä. Finanssialan substanssilainsäädäntöön tulisi lisätä säännökset, joissa Finanssivalvonnalle varmistetaan oikeus luovuttaa salassapitosäännösten tai muiden tietojenluovuttamista koskevien rajoitusten estämättä laissa säädettyjen tehtäviensä hoitamisen yhteydessä saamansa, poikkeamia koskeva asiakirja tai raportti sekä ilmaista salassa pidettävä tieto muille viranomaisille kuten Viestintävirastolle, jos se näille verkko- ja tietoturvallisuuteen liittyvien tehtävien hoitamiseksi on välttämätöntä.

NIS-direktiivi edellyttää toisten jäsenvaltioiden kuulemista, jos jokin keskeiseksi palveluntarjoajaksi määriteltävä toimija tarjoaa palvelua kahdessa tai useammassa jäsenvaltiossa:

"Jos 1 kohtaa sovellettaessa toimija tarjoaa 2 kohdan a alakohdassa tarkoitetun kaltaista palvelua kahdessa tai useammassa jäsenvaltiossa, kyseisten jäsenvaltioiden on kuultava toisiaan. Tällainen kuuleminen on toteutettava, ennen kuin määrittämistä koskeva päätös tehdään."

Finanssialalla on useita tällaisia toimijoita: esim. Danske Bank, Nordea Bank, Handelsbanken, SEB, Swedbank, Nasdaq, jne.

Toisten jäsenvaltioiden kuulemisesta olisi välttämätöntä säätää kansallisessa sääntelyssä. Asiaa tulisi tarkastella horisontaalisena kysymyksenä, miten eri sektoriviranomaiset voisivat toimia, jotta menettely olisi yhdenmukainen.

FINANSSIVALVONTA

Markku Koponen
toimistopäällikkö

Anne Nisén
johtava riskiasiantuntija