FIN-FSA
FINANSSIVALVONTA

Ajankohtaista kyberturvallisuudesta

Eduskunnan talousvaliokunta 9.3.2022

Markku Koponen

Maksu- ja tietojärjestelmiin sekä tietoturvallisuuteen liittyvä Finanssivalvonnan sääntely



Lainsäädäntöä

- Luottolaitoslaki 5 luku, 16§
  - Luottolaitoksen tulee varmistaa tehtäviensä mahdollisimman häiriötön hoitaminen myös poikkeusoloissa osallistumalla rahoitusmarkkinoiden valmiussuunnitteluun ja valmistelemalla etukäteen poikkeusoloissa tapahtuvaa toimintaa sekä muilla toimilla.

- Luottolaitoslaki 9 luku, 16§
  - Luottolaitoksella on oltava riittävät, turvalliset ja toimintavarmat maksu-, arvopaperi- ja muut tietojärjestelmät.
  - Luottolaitoksella on oltava varautumis- ja jatkuvuussuunnitelmat liiketoiminnan vakaviin häiriöihin varautumiseen, toiminnan jatkuvuuden turvaamiseen sekä häiriötilanteissa aiheutuvien vahinkojen rajoittamiseen.

- Vastaavat varautumisvelvoitteet myös mm. sijoitusrahastolaissa ja vakuutusyhtiölaissa.

Finanssivalvonnan määräys/ohje operatiivisen riskin hallinta rahoitussektorin valvottavissa

- Maksu- ja tietojärjestelmiin, tietoturvallisuuteen, jatkuvuussuunnitteluun liittyviä määräyksiä ja ohjeita.
- Lisäksi velvollisuus raportoida Finanssivalvonnalle asiakkaille tarjotuissa palveluissa sekä maksu- ja tietojärjestelmissä esiintyneistä merkittävistä häiriöistä ja virheistä viipymättä niiden ilmaannuttua.
- Maksujenvälityksessä ja korttimaksamisessa merkittäviksi häiriöiksi katsotaan esimerkiksi suurta määrää asiakkaita koskeva häiriö tai viivästys. Merkittävä häiriö on myös verkko- ja tietoturvallisuuteen liittyvä häiriö tai poikkeama sekä häiriö, jossa asiakastietoja on joutunut ulkopuoliselle taholle.

Finanssivalvonnan maksu- ja tietojärjestelmien sekä tietoturvallisuuden valvonta



Finanssivalvonnan maksu- ja tietojärjestelmien sekä tietoturvallisuuden valvonta

- Tehdään tarkastuksia ja teema-arvioita (kyselyt ja vastausten analyysi).
- Laaditaan valvottavakohtaiset riskiarviot, joissa arvioidaan valvottavien tilaa riskialueittain.
- Jatkuva valvonta: mm. häiriöilmoitusten seuranta ja tarvittaessa asioihin puuttuminen ottamalla yhteyttä valvottavaan ja käymällä asiaa tarkemmin läpi.
- Yhteistyö ja tietojen vaihto muiden viranomaisten kanssa: mm. Suomen Pankki, Valtiovarainministeriö, Kyberturvallisuuskeskus, Huoltovarmuuskeskus.
- Finanssivalvonta on mukana Huoltovarmuusorganisaation poolityössä yhdessä toimialan edustajien ja muiden viranomaisten kanssa.
- Finanssivalvonta harjoittelee yhteistyössä toimialan ja muiden viranomaisten kanssa finanssisektorin eri uhkaskenaarioita: FATO- ja TIETO-harjoitukset.
  - Myös joidenkin harjoitusten valmisteluun ja tulosten analysointiin osallistuminen.

Kyberuhkista ja niihin varautumisesta



Mahdollisia uhkia

- Mahdollisia finanssialan kriittisen infrastruktuurin uhkia
  - Tietoliikenneverkon ja sähköverkon häiriöt
    - Esim. kansainvälisen tietoliikenteen toimivuuden kannalta kriittisten merikaapelien vahingoittaminen.
  - Kyberhyökkäykset merkittäviä yksittäisiä toimijoita vastaan.
  - Kyberhyökkäykset finanssimarkkinoiden toimivuuden kannalta keskeisiä palveluntuottajia ja järjestelmiä kohtaan.
- Finanssimarkkinoiden toimivuuden kannalta keskeisiä järjestelmiä ovat maksuliikenteeseen, korttimaksamiseen ja arvopaperikaupankäyntiin sekä selvitykseen liittyvät järjestelmät, jotka pääosin sijaitsevat Suomen rajojen ulkopuolella.
- Myös merkittävät IT-palveluntuottajat ja finanssialan toimijoiden omat järjestelmät ovat potentiaalisia hyökkäyskohteita.
- Hyökkäyksiä voidaan tehdä esim. palvelunestohyökkäyksillä ja erilaisten haitta- ja vakoilijaohjelmien kautta. Mahdollista on myös pyrkiä tietojen kryptaamiseen tai tuhoamiseen erilaisten haittaohjelmien avulla.

Kyberuhat – varautumisen tilanne

- Finanssiala on yleisesti ottaen varautunut hyvin erityisesti lyhyisiin häiriöihin ja varautuminen kyberuhkiin ja hyökkäyksiin on kohtuullisen hyvällä tasolla.
- Tilanne voi kuitenkin heiketä nopeastikin, jos valtiollinen toimija hyökkää kriittistä infrastruktuuria ja yksittäisiä toimijoita vastaan.
- Varautumisen taso vaihtelee: suurten toimijoiden kyberkypsyys on tyypillisesti korkeammalla tasolla kuin pienten toimijoiden.
- Varautumista mahdollisiin kyber- ja maksamiseen liittyviin häiriöihin harjoiteltiin FATO2021-harjoituksessa (rahoitusalan toimijoiden ja viranomaisten yhteinen toimintaharjoitus viime vuonna). Yhtenä johtopäätöksenä on, että toimiala ei ole varautunut riittävästi pitkäkestoisiin häiriöihin ja kyllin vakaviin häiriöihin.

Maksujärjestelmien uhkat ja varautuminen

- Suomessa käytetyt maksujärjestelmät sijaitsevat pääosin ulkomailla.
- Jos ulkomaisiin järjestelmiin ei Suomesta saada yhteyttä, maksaminen käytännössä pysähtyy.
- Maksujärjestelmien, korttimaksamisen ja arvopaperi-infrastruktuurin osalta ei ole kansallista varautumista – kaikki keskitetyt ja keskeiset järjestelmät sijaitsevat Suomen rajojen ulkopuolella (poikkeuksena Euroclear Finlandin järjestelmät).
- Myöskään valmiuksia palauttaa järjestelmät Suomeen ei ole.
- Valtiovarainministeriön nimeämä työryhmä on ehdottanut jo vuonna 2018 luottolaitoslain, maksulaitoslain, sijoituspalvelulain ja sijoitusrahastolain varautumisvelvollisuutta koskevia säännöksiä täsmennettäväksi siten, että näiden säännösten mukaiset valmistelut ja toimenpiteet tarkoittavat keskeytymättömän toiminnan kannalta välttämättömien tietojärjestelmien ja tietovarastojen ylläpitämistä Suomessa.
- Finanssivalvonnan näkemyksen mukaan varautumisvelvollisuutta koskevien säännösten täsmentäminen tulisi käynnistää pikaisesti.

Viimeaikaisia kyberhäiriöitä ja Finanssivalvonnan tiedote

- OP Ryhmän verkkosivuihin kohdistui 9.1.2022 useamman tunnin palvelunestohyökkäys – mobiilipankki kuitenkin toimi tänä aikana.
- Ajanjaksolla 28.2.2022 – 1.3.2022 kolmeen suomalaiseen pankkiin kohdistui palvelunestohyökkäyksiä.
- Hyökkäysten tekijöistä ei ole tietoa, mikä on tavanomaista tällaisissa tapauksissa.
- Kestoltaan pisin ja vakavin näistä kolmesta palvelunestohyökkäyksestä kohdistui Nordeaan. Tämä kesti lähes vuorokauden.
- Valvottavatiedote 4.3.2022 – 14/2022: Finanssivalvonta kehottaa tehostettuun kyberturvallisuuden seurantaan. Kansainvälisen turvallisuustilanteen kiristyminen lisää kyberhyökkäysten mahdollisuutta myös finanssialan toimijoita ja palveluntuottajia vastaan. Finanssivalvonta kehottaa valvottaviaan tehostettuun kyberturvallisuuden seurantaan.

Kiitos!