Verkko- ja tietoturvadirektiivi

Seuraavassa Aktia Pankki Oyj:n kommentit Liikenne- ja viestintämisteriön toimittamaan arviomuistioluonnokseen verkko- ja tietoturvadirektiivin kansallisesta voimaansaattamisesta.

Helsingissä

14.12.2016

Aktia Pankki Oyj

Petri Vuontela

johtaja, IT-riskienvalvonta ja tietoturva

----

Aktia Pankki toteaa, että finanssialan toimilupakäytäntöjen avulla pystytään määrittelemään pitävästi tässä direktiivissä tarkoitetut keskeiset palveluntarjoajat finanssialalla.

Aktia Pankki toteaa, että direktiivissä esitetyt vaatimukset riskienhallinnasta ja riskitapahtumien ilmoittamisesta koskevat sitä jo nykyisellään. Velvoitteet laajenevat jo hyväksytyn uuden tietosuoja-asetuksen myötä, minkä lisäksi EBA suunnittelee raportointivelvoitteiden tarkentamista vuoden 2018 alusta osana PSD2-direktiiviä (GUIDELINES ON MAJOR INCIDENTS REPORTING UNDER THE PSD2).

Näillä perusteilla direktiiviä varten ei ole tarvetta säätää kokonaan uutta lakia. Aktia Pankki toteaa, että missään olosuhteissa direktiivi ei saa johtaa uusiin valvontamaksuihin.

Finanssivalvonnalla on jo tarvittavat valtuudet sekä keinot arvioida Aktia Pankin riskienhallintaa, riskitapahtumia sekä tietojärjestelmäturvallisuuden tasoa. Aktian tietoturvallisuuden tason arvioinnille ei tule asettaa mitään lisävaatimuksia saati tarkastusvelvoitteita.

Aktia Pankki ei kannata kuin direktiivin vähimmäisvelvoitteiden säätämistä verkko- ja tietojärjestelmien turvallisuudelle. Lisäksi on huomioitava, että juuri tästä syystä Valtiota ja yksityisiä yrityksiä ei saa rinnastaa toisiinsa.

Direktiivin vaatimus kaikkien poikkeamien raportoinnista ei ole linjassa direktiivissä esitettyyn tavoitteeseen varmistaa riskiin suhteutettu verkko- ja tietojärjestelmien turvallisuuden taso uusin tekniikka huomioon ottaen. Esimerkiksi ohjelmistohaavoittuvuuksissa

* löydetyn haavoittuvuuden korjaamiseksi ei ole välittömästi saatavilla korjaavaa päivitystä
* korjauksen asentamista on päätetty lykätä, koska ensimmäinen korjauksen asentamiseen soveltuva ajankohta on myöhemmin tai haavoittuvuuden ei ole arvioitu olevan kriittinen
* on ylipäätänsä riskinanalyysin perusteella päätetty ottaa ko. riski

Aktia Pankki näkee että, käsitteenä tulee erotella toisistaan poikkeama ja insidentti. Direktiivissä ei tulisi asettaa poikkeamille mitään minimirajoja, koska ne ovat vain ja ainoastaan yrityksen itsensä määriteltävissä. Näkemyksemme on, että kenenkään ulkopuolisen ei ole mahdollista arvioida poikkeaman rajat ylittävää vaikutusta ilman syvällistä tietoa ko. yrityksen koko toiminnasta.

Finanssialalla toimivaltaiset viranomaiset ovat luontevasti Finanssivalvonta sekä Viestintäviraston CERT-FI/Kyberturvallisuuskeskus.

* insidentit raportoidaan Finanssivalvonnalle (ei siis kaikkia poikkeamia)
* ulkoisista tietoturvallisuusinsidenteistä (verkkopankkien haittaohjelmat, verkkopankkitunnusten ja korttinumeroiden kalastelu ja palvelunestohyökkäykset) ilmoitetaan Viestintäviraston CERT-FI:lle ja heidän tuellaan torjutaan insidenteistä aiheutuvia haittoja.

Aktia Pankki näkee, että nykyisten viranomaisten toimintaedellytyksiä tulee parantaa sekä veloittaa ne tekemään yhteistyötä tehokkaasti. Aktia Pankki lukee myös Huoltovarmuuskeskuksen viranomaiseksi. Aktian näkee Huoltovarmuuskeskuksen finanssipoolissa mahdollisuuden sektorien rajat ylittävään yhteistyöhön, mutta Aktia Pankin näkökulmasta finanssipoolin toiminta on ollut pysähdyksissä syksyllä 2015 pidetyn FATO-harjoituksen jälkeen. Myöskään Aktia Pankin pyyntöön päästä virallisesti mukaan finanssipoolin toimintaan olen vastattu.

Viranomaisilla tulee olla yhteistyövelvoite, jolloin heille tulee säätää valtuudet luovuttaa tietoja toisille viranomaisille. Tietojen luovutuksen laajuus ja tietosisältö on määriteltävä erikseen.

Viranomaisille tulle säätää myös velvollisuus koostaa ja jakaa eri toimialoille tuotettuja tilannekuvia sekä raportoiduista insidenteistä koostettua tietoa, jotta yleinen tietoisuus tietoturvallisuuden kokonaistilanteesta olisi mahdollisimman monen toimijan käytettävissä.

Direktiivi itsessään ei tule kohottamaan Suomen yleisen tietoturvallisuudentasoa. Se edellyttää sen sijaan tarjottava tietoa, koulutusta sekä solmittavissa kaupallisissa sopimuksissa ehtoja, jotka edistävät yleisesti käytössä olevien hyvien tietoturvakäytäntöjen omaksumista sekä tietoturvastandardien käyttöönottoa.