# Digitalisaatio haastaa maksujärjestelmien turvallisuuden

8.5.2018 – Euro & talous 2/2018 – Rahoitusvakaus

Tatu Laine
Vanhempi ekonomisti

**Luotettavat maksu- ja selvitysjärjestelmät ovat perusedellytys rahoitusvakaudelle ja taloudelliselle kasvulle. Mikäli ihmisten ja yritysten luottamus esimerkiksi maksujenvälityksen toimivuuteen ja tilitietojen oikeellisuuteen horjuu, yhteiskunnan sujuva toiminta häiriintyy nopeasti.**

Hyvin toimivat maksujärjestelmät sekä arvopapereiden selvitys- ja toimitusjärjestelmät (nk. infrastruktuuri) ovat vakaan rahoitusjärjestelmän perusta. Osana rahoitusjärjestelmän kokonaisriskejä mainitaan usein kyberriskit, joiden hallitseminen on keskeistä rahoitusvakauden säilymisen kannalta.[1] Kyberriskillä tarkoitetaan yleensä organisaation tietojärjestelmiin kohdistuvaa haitallisen tapahtuman uhkaa.[2] Käytännössä tämä voi tarkoittaa esimerkiksi sitä, että pankkitilin tietoihin ei voisi enää luottaa eikä niihin kytkeytyviä palveluja voisi enää käyttää. Digitalisoituvaan ympäristöön liittyvät haasteet kasvavat muun muassa finanssitoimijoiden hallussa olevan tiedon ylläpidon, säilyttämisen ja ongelmatilanteista palautumisen suhteen.

---

1. Euro & talous 2/2015: Voisiko kyberhyökkäys johtaa finanssikriisiin? (https://www.eurojatalous.fi/fi/2015/2/voisiko-kyberhyokkays-johtaa-finanssikriisiin/).
2. Aleksi Grymin blogi: Kyberriskit huomioitava, jotta rahoitusvakaus säilyy (https://www.eurojatalous.fi/fi/blogit/2017/kyberriskit-huomioitava-jotta-rahoitusvakaus-sailyy/).

Näihin voidaan varautua parantamalla suojautumista kyberuhkia vastaan.

Kansainvälisen järjestelypankin (BIS) maksu- ja markkinainfrastruktuurikomitea[3] ja kansainvälisen arvopaperimarkkinavalvojien järjestö[4] ovat julkaisseet ohjeistusta, jolla pyritään parantamaan finanssi-infrastruktuurien kyberturvallisuutta.[5] Ohjeistus kattaa riskienhallinnan johtamisen, riskien tunnistamisen, riskeiltä suojautumisen, hyökkäyksen havaitsemisen ja hyökkäyksestä palautumisen. Erityisen tärkeäksi nähdään johdon sitoutuminen kyberturvallisuuden parantamiseen sekä yhteistyö eri järjestelmien kesken. Kyberriskit pitää hallita eri tasoilla yksittäisestä kuluttajasta aina järjestelmien muodostamaan kokonaisuuteen asti.

Kyberturvallisuutta voidaan lähestyä finanssitoimialalla eri näkökulmista. Yksittäisen toimijan tehtävänä on huolehtia päivittäisestä kyberturvallisuudesta esimerkiksi torjumalla palvelunestohyökkäyksiä, huolehtimalla virusturvasta ja ottamalla varmuuskopioita päivittäisistä tilisaldoista. Jos finanssipalvelun tiedot jostain syystä turmeltuvat, vääristyvät tai joutuvat vääriin käsiin, oikeat tiedot on pystyttävä palauttamaan varmuuskopioista mahdollisimman nopeasti. Jos myös varmuuskopiot ovat korruptoituneet, virheettömän tilanteen palauttaminen on haasteellista.

Yksittäiset rahoitusalan toimijat muodostavat yhdessä laajemman kokonaisuuden eli systeemisen tason. Yksittäisellä toimijalla voi olla toimintoja useassa maassa, ja se voi osallistua moniin maksu- ja selvitysjärjestelmiin. Mikäli tällaisella laajasti verkostoituneella toimijalla olisi vakavia ongelmia, se voisi aiheuttaa häiriöitä monissa maissa ja järjestelmissä. Systeemitason näkökulmasta tuleekin huolehtia siitä, että kaikilla finanssitoimijoilla on riittävät kyberturvallisuusvalmiudet ja parhaat käytännöt instituution koosta tai sijaintimaasta riippumatta.  Näin voidaan yhdessä ennalta ehkäistä laaja kyberhäiriötilanteen syntyminen. Verkoston heikompia lenkkejä tulisi vahvistaa yhteisin voimin.

Kyberturvallisuuden edistämiseksi tehdään Euroopassa töitä usealla taholla. Hollannissa on laadittu malli, joka simuloi edistyneitä kyberhyökkäyksiä ja testaa palautumiskykyä niitä vastaan (TIBER, Threat Intelligence Based Ethical Red – teaming)[6]. Hiljattain on perustettu myös uusi eurooppalainen komitea, Euro Cyber Resilience Board (ECRB)[7], joka edistää erityisesti rahoitusjärjestelmän infrastruktuurin kyberturvallisuutta. Euroalueella on tehty yli 70:tä järjestelmää koskeva kysely kyberturvallisuudesta. Kyselyn perusteella kehitettäviä alueita ovat etenkin kyberriskien hallinto, koulutus ja tietoisuus näistä riskeistä sekä kyberhyökkäyksestä palautuminen. Lisäksi työn alla on yhteinen TIBER-EU-kehikko, jolla voidaan parantaa kyberturvallisuutta maarajojen yli.[8]

---

3. CPMI, Committee on Payments and Market Infrastructures (https://www.bis.org/cpmi/).
4. IOSCO, International Organization of Securities Commissions (https://www.iosco.org/).
5. Raportti “Guidance on cyber resilience for financial market infrastructure” (https://www.iosco.org/library/pubdocs/pdf/IOSCOPD535.pdf).
6. Hollannin keskuspankin vakausraportti vuodelta 2017 (https://www.dnb.nl/en/binaries/OFS_Autumn%202017_tcm47-363954.pdf).
7. EKP:n johtokunnan jäsenen, Benoît Cœuré, puhe 9.3.2018 (http://www.ecb.europa.eu/press/key/date/2018/html/ecb.sp180309_1.en.html).
8. EKP:n lehdistötiedote, 2.5.2018 (http://www.ecb.europa.eu/press/pr/date/2018/html/ecb.pr180502.en.html)

## Maksupalveluiden turvallisuus olennaista käyttäjälle

Kyberturvallisuutta voidaan tarkastella myös yksilön näkökulmasta. Päätelaitteisiin, kuten henkilökohtaisiin tietokoneisiin ja kännyköihin, asennettavien uusien rahoituspalveluita käyttävien sovellusten määrä todennäköisesti kasvaa lähitulevaisuudessa. Päivitetyn maksupalveludirektiivin[9] myötä ns. kolmannet palveluntarjoajat (maksutoimeksiantopalvelun tarjoajat ja tilitietopalvelun tarjoajat) voivat asiakkaan suostumuksella käynnistää asiakkaan puolesta maksun tai tehdä analyysia asiakkaan pankkitilin tapahtumista. Näin rakennetaan uusia rajapintoja perinteisten pankkien ja muiden palveluntarjoajien välille. Luottamusketju pankin ja loppuasiakkaan välillä jakautuu useamman toimijan ylläpidettäväksi. Käyttäjän näkökulmasta kustannukset saattavat laskea ja palveluiden käytettävyys parantua, mutta samalla uudessa toimintaympäristössä on tärkeää varmistaa, että käyttäjät voivat luottaa uusien toimijoiden palveluihin ja niiden kyberturvallisuuteen. Käyttäjiä pitää valistaa maksusovellusten yhteydessä hyväksyttävistä käyttöehdoista. Käyttäjien pitää myös tietää, mitä ehtojen hyväksyminen tarkoittaa ja mille toimijalle hän antaa oikeuden käyttää tilipalveluitaan.

## Viranomaisen tehtävä tarjota turvallinen toimintaympäristö

Kokonaiskyberturvallisuuteen liittyvät läheisesti myös hybridiuhat. Hybridiuhilla tarkoitetaan kaikkia niitä keinoja, joilla valtiolliset tai ei-valtiolliset toimijat pyrkivät aiheuttamaan haittaa kilpailijoidensa, vastustajiensa tai uhkiksi kokemiensa kohteiden toimintaan. Tämä voi finanssisektorilla ilmetä esimerkiksi vääränä markkina- tai muuna informaationa, jota valheellisesti levitetään jonkun luotettavan uutisten välittäjän kautta, tai markkinainformaation ennenaikaisena leviämisenä kyberrikollisten toimien kautta.

Viranomaisten tehtävänä on yhteistoiminnan ja sääntelyn avulla varmistaa, että kyberturvallisuuden kehittämisessä ovat mukana sekä yksittäiset toimijat että systeemitaso. Finanssialan toimijoiden tulee osoittaa riittävät resurssit finanssi-infrastruktuurien kyberturvallisuuden takaamiseksi. Kyberturvallisuuden alalla ei saa tuudittautua turvallisuuden tunteeseen, sillä kyberrikollisuus on olemassa oleva uhka ja kasvava toimiala.


### Avainsanat

kyberturvallisuus, rahoitusvakaus


9. Payment Services Directive, PSD2 (http://www.finanssivalvonta.fi/fi/Saantely/Saantelyhankkeet/PSD2/Pages/Default.aspx).