EURO&TALOUS

SUOMEN PANKIN AJANKOHTAISIA ARTIKKELEITA TALOUDESTA

Sisältö

Voisiko kyberhyökkäys johtaa finanssikriisiin?

8.5.2015 09:00 • EURO & TALOUS 2/2015 • RAHOITUSVAKAUS • OTSO MANNINEN

Jos vuoden 2008 kriisiä kärjisti pankkien epäluottamus toistensa taseisiin, voi seuraavan kriisin taustalla olla pankkien epäluottamus toistensa järjestelmiin, varoittavat asiantuntijat. Luottamus on modernin rahoitusjärjestelmän elinehto, ja kun tilisaldot sijaitsevat bittiavaruudessa, on ehdottoman tärkeää pystyä luottamaan näyttöruudulla näkyviin lukuihin. Käytännön kannalta ei ole merkitystä, johtuuko epäluottamus kyberriskien vai rahoitusmarkkinariskien toteutumisesta.

Digitaalisuus on mullistanut koko rahoitusjärjestelmän

Rahoitussektori on edelläkävijä digitalisoitumisessa: arvopaperikauppa ja suurin osa maksamisesta hoidetaan sähköisesti. Digitaalisuus on jo mullistanut koko perinteisen pankkitoiminnan, eikä kehitys ole pysähtymässä. Pääosin muutos on ollut positiivinen ja tuonut pankkipalveluita helpommin saataville sekä lisännyt palveluntuottajien välistä kilpailua. Digitalisoituminen on kuitenkin tuonut mukanaan aivan uudenlaisen uhan, kyberrikollisuuden.

Moni havaitsi vuodenvaihteessa, että verkkopankkiin ei pääse, korteilla ei voi maksaa eikä rahan nostaminen automaateista onnistu. Vaikka käyttökatkoja ilmeni vain muutamana päivänä, heikensi se luottamusta koko järjestelmää kohtaan: käyttäjän kannalta on ongelmallista, jos ei voi luottaa siihen, että maksut onnistuvat ajallaan. Yksittäiseen pankkiin kohdistuva lyhytaikainen palvelunestohyökkäys ei vielä kuitenkaan vaikuta koko rahoitusjärjestelmän vakauteen.

Vakavammat rahoitusalan toimijoihin tai erityisesti rahoitusinfrastruktuuriin kohdistuvat kyberhyökkäykset voivat vaikuttaa jo suoraan reaalitalouteen ja luottamukseen markkinatoimijoita kohtaan. Siinä missä aiemmin kalasteluviestillä jonkun käyttäjän tunnukset huijanneen kyberrikollisen omissa intresseissä on ollut

järjestelmien toiminnan jatkuminen, moderni kyberrikollinen saattaakin tavoitella mahdollisimman vakavaa ja pitkäkestoista häiriötä. Tämä synnyttää linkin kyberturvallisuuden ja rahoitusjärjestelmän vakauden välille.

Kyberturvallisuus ylläpitää rahoitusjärjestelmän vakautta

Kyberturvallisuus on osa rahoitusjärjestelmän vakautta, mutta kyberhyökkäystä ei aikaisemmin ole otettu huomioon finanssikriisin mahdollisena alkupisteenä. Todennäköisyys, että ongelmat leviäisivät kyberhyökkäyksestä koko rahoitusjärjestelmää koettelevaksi kriisiksi, on moniin muihin riskeihin verrattuna vielä kohtuullisen pieni. Kyberturvallisuus ei toistaiseksi olekaan ensimmäisenä tärkeysjärjestyksessä, kun arvioidaan makrovakausriskejä. Merkittävä ero moniin muihin järjestelmäriskeihin tulee kuitenkin siitä, että joillain tahoilla voi olla selkeä kannustin ja työkalut yrittää aiheuttaa kriisin puhkeaminen.

Edellisen finanssikriisin jälkeen viranomaiset ja lainsäätäjät ovat tuottaneet entistä tarkempaa ja täsmällisempää sääntelyä pankeille ja muille finanssialan toimijoille. Uuden sääntelyn tarkoituksena on ollut pienentää finanssisektorin kriisien todennäköisyyksiä, vähentää kriisien kustannuksia yhteiskunnalle ja yleisemminkin vahvistaa luottamusta rahoitussektoria kohtaan. Oikein toimiessaan tämä uusi sääntely pienentää finanssikriisien todennäköisyyttä ja kriisien kustannuksia. Finanssikriisit kuitenkin monesti lähtevät liikkeelle sieltä, mistä niiden ei odoteta alkavan.

Vaikka kyberhyökkäys ei sinänsä aiheuttaisi järjestelmäriskiä, se saattaa aiheuttaa ongelmia epäsuorasti. Tuoreen arvion mukaan globaali vakuutussektori voisi kärsiä jopa 20 mrd. punnan tappiot kybervakuutusten korvauksien maksamisesta.[1] Mikäli kybervakuutusten lukumäärä lisääntyy, voi suurimman mahdollisen tappion summa kasvaa jo suuremmaksi kuin ison luonnonkatastrofin tapauksessa. Tietojärjestelmillä toisiinsa tiivisti linkittyneiden rahoitusalan toimijoiden välillä kyberhyökkäys voi levitä järjestelmästä toiseen ja kasvattaa suurten vakuutuskorvausten todennäköisyyttä ja siten aiheuttaa riskin vakuutussektorin tappionkantokyvylle.

Viranomaiset heränneet kyberturvallisuuden merkitykseen

Viimeisen parin vuoden aikana keskuspankit ja rahoitusmarkkinavalvojat sekä lainsäätäjät ovat korostaneet erityisesti kyberturvallisuuden merkitystä. Rahoitusmarkkinatoimijat ovat joutuneet ottamaan kyberturvallisuuden huomioon jo aikaisemminkin, mutta tietoisuuden lisääminen ja todellisten kyberriskien huomioiminen ovat edelleen tärkeitä kehittämisalueita.

Suomen Pankin yleisvalvonnassa ja Finanssivalvonnan valvontatyössä rahoitusmarkkinatoimijoiden kyberturvallisuuden merkitys korostuu jatkossa.

---

1. HM Government -viraston ja March-vakuutusyhtiön raportti ”UK cyber security: the role of insurance in managing and mitigating the risk.” Ks. https://www.gov.uk/government/news/cyber-security-insurance-new-steps-to-make-uk-world-centre.

Kyberturvallisuus käsittää paljon muitakin osa-alueita kuin vain tekniset tietojärjestelmät. Kyberturvallisuus on kokonaisvaltainen käsite, joka sisältää niin toimintatavat, henkilöstön koulutuksen kuin selkeät viestintä- ja toimintasuunnitelmat kyberhyökkäyksen varalle. Tätä kokonaisvaltaista kyberturvallisuutta valvojat pyrkivät arvioimaan ja ohjaamaan kohti parhaita käytäntöjä.

Kyberturvallisuuden parhaita käytäntöjä kehitetään kansainvälisellä tasolla. Kansainvälinen järjestelypankki (BIS) julkaisi vuoden 2014 lopussa ensimmäisen raportin kyberturvallisuudesta ja siitä, miten rahoitusmarkkinatoimijoiden tulisi ottaa kyberturvallisuus huomioon omassa toiminnassaan.[2] Jokainen toimija ja maa on erilainen, ja kansainvälisillä suosituksilla voidaan puuttua vain yhteismitalliseen osaan. Siksi jokaisen rahoitusmarkkinatoimijan on itse oltava aktiivinen oman kyberturvallisuutensa kehittämisessä.

Kyberturvallisuus vaikuttaa ihmisten luottamukseen rahoitusjärjestelmää kohtaan. Tästä on kuitenkin vielä pitkä askel rahoitusjärjestelmän vakauden horjumiseen. Tähän asti sääntelijät ja valvojat ovat pyrkineet tekemään rahoituslaitoksista kestäviä finanssikriiseihin nähden. Entistä tiukemmat vakavaraisuusvaatimukset, suuremmat vakuudet, paremmat riskimallit ja monet muut muutokset ovat olleet osa tätä prosessia. Seuraavaksi on pidettävä huolta, että tietojärjestelmät eivät jää haavoittuviksi. Kokonaisvaltainen kyberturvallisuus on otettava vakavasti, jotta seuraava kriisi ei lähde liikkeelle sieltä, mistä asiantuntijat sen varoittivat lähtevän.

Avainsanat

- kyberturvallisuus
- rahoitusmarkkinainfrastruktuuri
- digitalisoituminen
- rahoitusvakaus

Kirjoittajat

Otso Manninen
Ekonomisti
etunimi.sukunimi(at)bof.fi

2. Raportti ”Cyber resilience in financial market infrastructures”, ks. http://www.bis.org/cpmi/publ/d122.htm.