ANALYYSI

Rahoitussektorin varautumisella tuetaan yhteiskunnan toiminnan jatkuvuutta kaikissa oloissa

Rahoitusvakaus | 27.04.2023 | Päivi Tissari, Terhi Wathén

KIRJOITTAJAT

Päivi Tissari
Vanhempi neuvonantaja

Terhi Wathén
Toimistopäällikkö

Geopoliittisen epävarmuuden takia rahoitusjärjestelmän infrastruktuuriin kohdistuvat uhat ja operatiiviset riskit ovat kasvaneet, mikä on lisännyt tarvetta varautua infrastruktuurin vakaviin toimintahäiriöihin. Suomessa viranomaiset valmistelivat vuoden 2022 aikana päivittäismaksamisen varajärjestelyn. EU:ssa puolestaan luotiin rahoituspalveluiden häiriönsietokyvyn parantamiseen tähtäävää sääntelyä, ja Euroopan järjestelmäriskikomitea (ESRB) on tehnyt rahoitusjärjestelmään kohdistuvien kyberriskien arviointiin liittyvää työtä.

Venäjän hyökkäyssota Ukrainassa ja Suomen Nato-jäsenyysprosessi ovat osaltaan kasvattaneet

Suomen kriittiseen rahoitusinfrastruktuuriin kohdistuvia uhkia. Lisäksi rahoitussektorin digitalisaatio ja lisääntynyt ostopalveluiden käyttö kasvattavat rahoitusalan toimijoiden teknisiin järjestelmiin kohdistuvia riskejä. Esimerkiksi kyberhyökkäysten uhkaan tulee varautua entistäkin vahvemmin. Jos pankki ei pysty vakavan kyberhyökkäyksen takia toimimaan, ongelmat välittyvät myös muihin pankkeihin, ja tallettajien ja sijoittajien epäluottamus pankkisektoria kohtaan voi kasvaa.

Suomessa yksittäiset toimijat, kuten pankit, ovat pitkään kehittäneet varautumista erilaisiin häiriötilanteisiin. Myös Suomen Pankki on varautunut rahoitusmarkkinainfrastruktuurin häiriötilanteisiin ja tukemaan rahoitustoimialan varautumistyötä mm. huoltovarmuusorganisaation ja TIBER-FI[1]-testaamisen kautta.

Lisäksi viranomaiset valmistelivat vuonna 2022 varajärjestelyn päivittäismaksamisen turvaamiseksi siltä varalta, että yhteiskunnan vakavissa häiriötilanteissa tai poikkeusoloissa ei voitaisi käyttää normaaleja eurooppalaisia maksujärjestelmiä tai joidenkin pankkien järjestelmiä[2]. Jos suomalainen pankki tai Suomessa toimiva ulkomaisen pankin merkittävä sivuliike kärsisi vakavasta ja pitkäaikaisesta toimintahäiriöstä, sen asiakkaiden tili- ja korttipalvelut voitaisiin tarvittaessa tuottaa Rahoitusvakausviraston ylläpitämässä huoltovarmuustilijärjestelmässä. Suomen Pankin tehtävänä on puolestaan turvata kotimainen maksuliikenne pankkien välillä.

Suomessa on käytössä varautumisen yhteistoimintamalli, jossa yhteiskunnan elintärkeistä toiminnoista huolehditaan viranomaisten, elinkeinoelämän, järjestöjen ja kansalaisten yhteistyönä. Valtioneuvosto antoi eduskunnalle historian ensimmäisen huoltovarmuusselonteon[3] syyskuussa 2022. Selonteon mukaan Suomen rahoitusmarkkinoiden varautumisen taso ei tällä hetkellä täysin vastaa yhteiskunnan turvallisuusstrategiassa asetettuja linjauksia ja valtioneuvoston asettamia varautumisen tavoitteita, sillä rahoitusyritysten varautumisvelvollisuutta koskeva sääntely on yleisluonteista. Tähän tullaan kiinnittämään huomioita selonteon mukaisessa kehitystyössä.

Myös EU:ssa on annettu sääntelyä, joka vaikuttaa suomalaiseen huoltovarmuus- ja varautumistyöhön jatkossa. Keskeisimpiä uusia direktiivejä ovat yhteiskunnan kriittisten toimijoiden häiriönsietokykyä koskeva CER-direktiivi (Resilience of Critical Entities) ja NIS2-direktiivi (ns. kyberturvallisuusdirektiivi), jotka astuivat voimaan 16.1.2023.

CER-direktiivin tarkoituksena on mm. parantaa Euroopan unionin kannalta välttämättömien palvelujen häiriönsietokykyä. NIS2-direktiivin tavoitteena on vahvistaa sekä EU:n yhteistä että jäsenvaltioiden kansallista kyberturvallisuuden tasoa kriittisiksi katsottujen sektoreiden ja toimijoiden osalta. Näiden direktiivien täytäntöönpano Suomen lainsäädäntöön on käynnissä.

Finanssialan digitaalista häiriönsietokykyä koskevan asetuksen (DORA, Digital Operational Resilience Act) tavoitteena taas on tehostaa rahoitusmarkkinatoimijoiden ICT-riskien hallintaa ja järjestelmien testausta sekä valvojien tietoisuutta valvottavien kohtaamista kyberriskeistä. DORA astuu voimaan tammikuussa 2025.

Kyberuhkiin ja muihin operatiivisiin riskeihin varautuminen vaatii keskuspankilta jatkuvaa panostusta mm. stressitesteihin ja koulutukseen. Euroopan järjestelmäriskikomitea ESRB suosittelee lisäksi viranomaisia kehittämään tapoja arvioida, mitä vaikutuksia rahoitusjärjestelmän vakautta uhkaavilla kyberhyökkäyksillä on erilaisissa skenaarioissa, ja arvioimaan, millaisilla operatiivisilla toimenpiteillä näihin pystytään parhaiten vastaamaan[4]. Uhkiin varautumisella tuetaan rahoitusvakautta ja yhteiskunnan toiminnan jatkuvuutta niin normaaliaikoina kuin äärimmäisissä tilanteissa.

Viitteet

1. Ks. https://www.suomenpankki.fi/fi/raha-ja-maksaminen/tiber-fi-soveltamisohje/. ↑
2. Laki eräistä huoltovarmuuden turvaamisen järjestelyistä rahoitusalalla (666/2022). ↑
3. Ks. Valtioneuvoston huoltovarmuusselonteko. ↑
4. Ks. Advancing macroprudential tools for cyber resilience, ESRB, 2023. ↑

Asiasanat

geopolitiikka, huoltovarmuus, kyberriski, varautuminen