EURO&TALOUS

SUOMEN PANKIN AJANKOHTAISIA ARTIKKELEITA TALOUDESTA

Sisältö

Eurojärjestelmän kyberstrategia Suomeen

Tänään – Analyysi – Raha ja maksaminen

Jussi Terho
Toimistopäällikkö

Terhi Wathén
Neuvonantaja

Finanssisektorin kyberuhkien häiriönsietokykyä edistetään monella tasolla: infrastruktuurien, yksittäisten toimijoiden ja tiedonvaihdon valmiuksia parannetaan sekä kansainvälisesti että kansallisesti. Kyberhyökkäyksistä on tullut arkipäivää, ja häiriönsietokyvyn tulee muuntua muuttuvan uhkakuvan mukaan. Eurojärjestelmän kyberstrategia on yksi viitekehys, joka mahdollistaa suojautumisen kyberuhkia vastaan eri tasoilla ja tarkoituksenmukaisilla työkaluilla.

Kyberuhat maailmanlaajuinen ilmiö

Maailmanlaajuisesti yksi tunnetuimpia kyberhyökkäyksiä ja digitaalisia pankkiryöstöjä on Bangladeshin keskuspankin tapaus vuodelta 2016. Siinä hyökkääjät onnistuivat keskuspankin SWIFT[1]-infrastruktuurissa olleita haavoittuvuuksia hyödyntämällä siirtämään varoja keskuspankin tililtä Yhdysvaltain keskuspankista New Yorkissa.

1. Ks. https://www.finanssiala.fi/uutiset/mika-on-swift/.

Tilisiirtojen toteuttamisessa ja häivyttämisessä hyödynnettiin mm. eri aikavyöhykkeitä ja eri maiden pankkivapaita. Varoja siirrettiin mm. Filippiineille, jossa rahat pestiin ja lunastettiin kasinoilla jälkiä jättämättä. Suorat tappiot olivat lopulta noin 80 miljoonaa dollaria, mutta vieläkin suurempien siirtojen onnistuminen oli todella lähellä.

Suomessa kyberhyökkäykset tulivat kuluttajille tutuksi mm. vuodenvaihteessa 2015, jolloin suomalaisiin pankkeihin kohdistui merkittäviä palvelunestohyökkäyksiä. Hyökkäykset näkyivät mm. käteisnostoissa, verkkopankissa ja korttimaksuissa, mutta asiakkaiden varat tai henkilötiedot eivät kuitenkaan vaarantuneet. Samanaikaisesti palvelunestohyökkäyksiä tehtiin myös tiedotusvälineitä vastaan. Suomeen kohdistuu vuosittain arviolta noin 10 000 kyberhyökkäystä. Pääsääntöisesti ne onnistutaan torjumaan normaalein toimin.

Mahdollisten kyberhyökkäyksien kirjo on laaja. Ne voivat olla esimerkiksi palvelunestohyökkäyksiä, kiristyshaittaohjelmia, tuhoavia ohjelmia ja kriittiseen infrastruktuuriin kohdistuvia hyökkäyksiä. Motiivit hyökkäyksille voivat olla moninaisia. Kyseessä voi olla esimerkiksi sähköinen pankkiryöstö, tai hyökkääjä voi pyrkiä hyötymään hyökkäyksen vaikutuksista välillisesti. Kyse voi myös olla tiedustelusta, häirinnästä, sabotaasista tai tuhoamisesta. On hyvä tiedostaa, että pankeilla on merkittävä rooli tunnistuspalvelujen tarjoamisessa Suomessa ja mahdolliset hyökkäykset pankkeja kohtaan voivat myös heijastua tunnistautumiseen. Näin kävi esimerkiksi yhden pankin osalta vuonna 2022.

Vuonna 2022 sekä Venäjän hyökkäyssota Ukrainassa että Suomen Nato-jäsenyysprosessi nostivat Suomen kriittiseen infrastruktuuriin kohdistuvaa uhkaa sekä fyysisessä että kyberympäristössä. Toistaiseksi tapahtumat eivät kuitenkaan ole aiheuttaneet merkittäviä poikkeamia. Suomessa varautumistaso on ollut korkea jo ennen näitä tapahtumia.

Finanssisektorin rakenteen muutos ja vähittäismaksujen turvaaminen Suomessa

Suomessa pankkisektori oli 1990-luvun pankkikriisiin asti pitkälti kotimainen, ja pankit jakoivat samat varautumisen periaatteet. Kotimaisesta finanssisektorista on kuitenkin tullut kansainvälisempi, ja palvelun tarjonta on teknologisen kehityksen myötä hajaantunut. Suomessa tarjottavia palveluja tuotetaan nykyään laajasti ulkomailta ja ulkomailla sijaitsevilla tietojärjestelmillä. Muutoksen myötä finanssisektori ajautui osittain pois kotimaisesta varautumisyhteistyöstä. Tästä huolimatta Suomessa pankit ja muut yksittäiset toimijat ovat kuitenkin kehittäneet varautumistaan erilaisiin häiriötilanteisiin, mukaan lukien kyberuhkiin.

Yksittäisten toimijoiden varautumista täydentämään viranomaiset loivat vuonna 2022 varajärjestelyn päivittäismaksamisen turvaamiseksi siltä varalta, että yhteiskunnan vakavissa häiriötilanteissa tai poikkeusoloissa normaaleja eurooppalaisia maksujärjestelmiä tai joidenkin pankkien järjestelmiä ei voitaisi käyttää. Päivittäismaksamisen varajärjestelmien kehittäminen kuuluu viranomaisten normaaliin varautumistoimintaan, mutta Euroopan turvallisuuspoliittinen tilanne keväällä 2022 kiihdytti aikataulua huomattavasti. Varajärjestelmän toimeenpano vaati tarkennuksia

lainsäädäntöön, ja laki eräistä huoltovarmuuden turvaamisen järjestelyistä rahoitusalalla[2] (666/2022) astui voimaan 11.7.2022. Varajärjestelmällä parannetaan yhteiskunnan kriisinsietokykyä mm. kyberuhkia vastaan.

Eurojärjestelmän rooli kyberturvallisuuden häiriönsietokyvyn kehittämisessä

Euroopan keskuspankki (EKP) vastaa usean euroalueella toimivan systeemisesti merkittävän maksujärjestelmän (SIPS) yleisvalvonnasta. Sen lisäksi, että systeemisesti merkittävien toimijoiden häiriönsietokyvyn kyberuhkia vastaan tulee olla korkealla tasolla, tulee EKP:n myös varmistua, että koko finanssisektori on suojautunut kyberuhkia vastaan riittävästi. Yksittäisten merkittävien luottolaitosten kyberriskit ovat olleet yhteisen pankkivalvonnan (SSM) fokuksessa sen perustamisesta asti teema-arvioina, tarkastuksina ja häiriöraportointina[3]. Sekä EKP:n että SSM:n toimilla pyritään vähentämään systeemisiä kyberriskejä[4], joilla voisi olla vaikutusta rahoitusvakauteen. Vuosien saatossa kyberhyökkäykset ovat kehittyneet entistä monimutkaisemmiksi. Hyökkäysten lisäännyttyä kansainvälinen järjestelypankki julkaisi vuonna 2016 kyberturvallisuutta ja häiriönsietokykyä koskevan kansainvälisen ohjeistuksen rahoitusmarkkinoiden infrastruktuureille (CPMI-IOSCO: CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures (FMIs)[5]).

Ohjeistuksen pohjalta ja ohjeistuksen panemiseksi täytäntöön eurojärjestelmä muodosti vuonna 2017 oman strategiansa (Eurosystem cyber resilience strategy for FMIs[6]). Strategia koostuu kolmesta pilarista, ja sen tavoitteena on edistää sekä yksittäisten kriittisten toimijoiden että koko euroalueen finanssisektorin häiriönsietokykyä kyberuhkia vastaan. Lisäksi strategiassa korostetaan toimijoiden, kriittisten palveluntarjoajien ja viranomaisten välistä yhteistyötä.

Eurojärjestelmän kyberstrategia

Eurojärjestelmän kyberstrategian *ensimmäinen pilari* keskittyy yksittäisten rahoitusmarkkinoilla toimivien infrastruktuurien häiriösietokykyyn entistä kehittyneempiä kyberuhkia vastaan.

Yhtenä ensimmäisen pilarin elementtinä on Euroopan keskuspankin 2018 julkaisema TIBER-EU-toimintamalli[7] finanssialan kyberturvallisuuden kehittämiseksi. TIBER-EU on todellista kyberuhkatilannetta simuloiva malli Red Team -tunkeutumistestausten[8]

---

2. Ks. https://www.edilex.fi/lainsaadanto/20220666.
3. Ks. https://www.bankingsupervision.europa.eu/press/publications/newsletter/2019/html/ssm.nl190213_4.en.html.
4. Ks. https://www.esrb.europa.eu//pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf.
5. Ks. https://www.ecb.europa.eu/paym/pol/shared/pdf/CPMI_IOSCO_Guidance_on_cyber_resilience_for_FMIs.pdf.
6. Ks. https://www.ecb.europa.eu/paym/cyber-resilience/fmi/html/index.en.html.
7. Ks.https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html.
8. Ks. https://www.suomenpankki.fi/fi/raha-ja-maksaminen/tiber-fi-soveltamisohje/toimintamallin-kuvaus/testauksen-toteuttaminen/.

suorittamiseksi. Toimintamallin tavoitteena on tuottaa havaintoja finanssialan infrastruktuurin ja toimijoiden suojaamiseksi kohdennetuilta kyberhyökkäyksiltä.

TIBER-EU-malli on tähän mennessä otettu käyttöön neljässätoista maassa[9], mukaan lukien Suomi. Myös Euroopan keskuspankki soveltaa sitä itse silloin, kun systeemisesti merkittävät maksujärjestelmät, kuten T2[10], ovat testien kohteena. Tammikuuhun 2023 mennessä on valmistunut yli sata TIBER-EU-malliin tai sen kansallisiin toimintamalleihin perustuvaa testiä.

Yleisvalvojilla on käytössään myös muita työkaluja maksu- ja selvitysjärjestelmien kyberhäiriönsietokyvyn edistämiseksi. Infrastruktuurien kyberturvallisuuteen kohdistuvalla kartoituksella (cyber survey) arvioidaan säännöllisesti turvallisuuden tasoa ja suojaustoimintojen kypsyyttä. Lisäksi eurojärjestelmän kyberuhkien yleisvalvontaohjeistus (Cyber resilience oversight expectations, CROE[11]) tarjoaa tarkempaa ohjeistusta maksu- ja selvitysjärjestelmien operaattoreille.

Finanssisektorin häiriönsietokyky ei muodostu pelkästään yksittäisten toimijoiden valmiuksista, vaan keskeisenä tekijänä kokonaisuudessa ovat myös palveluntarjoajat ja eri toimijoiden väliset riippuvuussuhteet. *Toisen pilarin* tavoitteena on edistää Euroopan koko finanssisektorin häiriönsietokykyä kyberuhkia vastaan. Tähän kuuluu mm. eri viranomaisten välinen yhteistyö ja tiedonvaihto myös rajojen yli, sektorikokonaisuuden kartoitus, riippuvuussuhteiden arviointi ja koko markkinan kattavat liiketoiminnan jatkuvuusharjoitukset.

Kolmas pilari pyrkii varmistamaan, että Euroopan laajuiset keskustelut viranomaisten ja toimijoiden välillä käydään myös strategisella tasolla (ylin johto), jolloin luodaan luottamusta osapuolten välille, lisätään tietämystä ja edistetään yhteisiä hankkeita sektorin häiriönsietokyvyn parantamiseksi kyberuhkia vastaan. Euro Cyber Resilience Board for Pan-European Financial Infrastructures[12] on esimerkki tällaisesta Euroopan laajuisesta foorumista.

Kyberstrategian implementointi Suomessa

Eurojärjestelmän kyberstrategian kaikkia pilareita implementoidaan myös Suomessa suomalaiset rahoitusmarkkinoiden ominaispiirteet huomioiden. Suomen rahoitusmarkkinoiden käyttämän infrastruktuurin eli maksu- ja selvitysjärjestelmien ja keskusvastapuolten palvelut tuotetaan lähes kokonaan kotimaan ulkopuolella. Tältä osin suomalaisesta rahoitusmarkkinoiden infrastruktuurista huolehditaan yhteistyössä näiden toimijoiden, muiden maiden keskuspankkien ja muiden rahoitusmarkkina- ja kyberturvallisuusviranomaisten kanssa. Kotimaisissa olosuhteissa onkin keskeistä, että infrastruktuuri ymmärretään laajasti. Tämä noudattaa samaa periaatetta, jota BIS soveltaa maksujärjestelmiin, jolloin myös maksujärjestelmien osapuolet ovat osa

9. BE, DK, FI, DE, IS, IE, IT, LU, NL, NO, PT, RO, ES ja SE.
10. Ks. https://www.ecb.europa.eu/paym/target/t2/html/index.en.html.
11. Ks. https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf.
12. Ks. https://www.ecb.europa.eu/paym/groups/euro-cyber-board/html/index.fi.html.

järjestelmää[13]. Tämän vuoksi pilareiden sisältö on sovitettava toimintaympäristöömme.

Yksittäisten infrastruktuurien kyberhäiriönsietokyvyn edistäminen ulottuukin siis myös esimerkiksi pankkien edellytyksiin liittyä infrastruktuureihin. Esimerkiksi TIBER-FI-testauksia kohdennetaan varsinaisten infrastruktuuritoimijoiden lisäksi myös mm. pankkeihin ja vakuutusyhtiöihin. Varsinaisten infrastruktuuritoimijoiden osalta TIBERin lisäksi käytössä ovat myös niiden kyberkypsyyden selvittämiseen tarkoitetut, joka toinen vuosi toistettavat kyselyselvitykset ja myös erityisesti kyberuhkien yleisvalvontaohjeistus (CROE).

Toiseen pilariin liittyvää suojautumista kyberhäiriöiltä pyritään ulottamaan mahdollisimman kattavasti koko toimialalle. Työkaluina tässä ovat mm. sektoritoimijoiden kartoitus ja Huoltovarmuusrahaston tuki TIBER-FI-testeille niin, että testien laaja toteutuminen lisäisi koko toimialan suojautumista. Lisäksi monet huoltovarmuusorganisaation ohjauksessa tehtävät muut toimet, sektorikohtaiset yhteistoimintatestit ja selvitykset edistävät koko toimialan suojautumista ja ymmärrystä vallitsevasta tasosta.

Kolmantena pilarina ovat strategiset ylätason keskustelut vallitsevasta tilanteesta ja yhteisistä tavoitteista. Erilaisia keskustelu- ja tiedonvaihtofoorumeja tiedonvaihdolle on ollut olemassa jo pidempään, ja niitä on edelleen lisätty Venäjän hyökättyä Ukrainaan helmikuussa 2022. Huoltovarmuusorganisaation eri foorumeilla käytävien keskusteluiden ja tiedonvaihdon lisäksi häiriönhallinnan yhteistyöryhmä tulee olemaan relevantti foorumi Suomessa finanssialan yritysten ja viranomaisten väliseen strategisen tason tiedonvaihtoon. Yhteistyöryhmä perustettiin, kun Suomessa tuli heinäkuussa 2022 voimaan laki eräistä huoltovarmuuden turvaamisen järjestelyistä rahoitusalalla. Strategisen ja alemman tason tiedonvaihtofoorumeiden välisestä koordinaatiosta on kuitenkin pidettävä huolta. Viime kädessä vastuu fooruminen relevanssista, sopimisesta yhteen muiden foorumeiden kanssa ja foorumeiden välisestä tiedonvaihdosta on foorumin organisoijalla. Esimerkiksi Suomen Pankki vastaa huoltovarmuusorganisaatiossa finanssialan sektorin toiminnasta ja panostaa sen kautta tapahtuvaan tiedon kulkuun.

Häiriönsietokyvyn ja strategiatyön kehittämien

Suomen Pankki huolehtii osaltaan maksu- ja muun rahoitusjärjestelmän luotettavuudesta. Olennainen osa luotettavuutta on finanssisektorin häiriönsietokyky kyberuhkia vastaan.

Eurojärjestelmän kyberstrategia kokoaa työkaluja, joilla suojaudutaan kyberuhkia vastaan eri tasoilla ja muuttuvat uhkakuvat huomioiden. Suomessa strategian implementointi toteutuu yksittäisten toimijoiden ja toimijoiden välisen yhteistyön kautta. Kyberuhkien monimuotoisuuden takia yksikään osapuoli ei pysty yksinään varmistamaan häiriönsietokyvyn tai tiedonvaihdon riittävää tasoa. Lisäksi eri toimijoilla ja viranomaisilla on erityistä osaamista, jolla ne voivat tukea finanssisektorin häiriönsietokyvyn kehittymistä.

13. Ks. https://www.bis.org/cpmi/publ/d43.pdf.

Eurojärjestelmän kyberstrategian julkaisemisesta on jo kulunut useampi vuosi, ja strategian päivitys on käynnistynyt. Nykyisen strategian kolme pilaria on todettu toimiviksi työkaluiksi, ja vaikuttaa siltä, että myös eurojärjestelmä korostaa yksittäisten toimijoiden merkitystä jatkossa. Päivityksen yhteydessä mietitään lisäksi uuden sääntelyn, kuten finanssialan digitaalista häiriönsietokykyä koskevan asetuksen (DORA, Digital Operational Resilience Act), vaikutuksia.

Yksi tapa varmistaa eri työkalujen toimivuus on toteuttaa koko sektorin kattavia yhteistestejä. Finanssisektorilla näitä ovat olleet mm. FATO-harjoitukset. Seuraavan harjoituksen yhteydessä olisi hyödyllistä testata yksittäisten toimijoiden reagointikykyä sekä toimijoiden yhteistoimintaa yhdistettynä todellisiin strategisiin tämän päivän uhkakuviin. Samalla eurojärjestelmän kyberturvastrategian toimivuus Suomessa tulisi todennettua.

Avainsanat

kyberturvallisuus, häiriönsietokyky, kyberstrategia, eurojärjestelmä