BLOGI

TIBER-FI – lipunryöstöä finanssialan kyberturvallisuuden kehittämiseksi

Raha ja maksaminen | 29.04.2020 | Jussi Terho

KIRJOITTAJA

Jussi Terho

Kyberriskit voivat realisoituessaan olla finanssialalla systeemisesti merkittäviä. Hyökkäys yksittäiseen pankkiin tai esimerkiksi maksujärjestelmään tai kaupankäyntipaikkaan voisi aiheuttaa epäluottamusta ja vaikuttaa jopa koko rahoitusjärjestelmän vakauteen. Tästä syystä Suomen Pankki julkaisi 29.4.2020 Suomen finanssitoimijoille TIBER-FI-soveltamisohjeen, jonka tarkoituksena on tukea finanssisektorin kyberresilienssiä eli kestävyyttä kyberriskejä vastaan.

Finanssiala hyödyntää digitalisaation luomia mahdollisuuksia monella tavalla. Tänä päivänä suurin osa esimerkiksi pankkien asiakkaista saa lähes kaikki palvelunsa digitaalisten kanavien kautta. Palveluiden taustalla on valtava määrä erilaisia järjestelmiä, jotka keskustelevat keskenään tietoverkkojen kautta.

Pankit ja rahoitusjärjestelmän käyttämä infrastruktuuri, kuten maksu- ja selvitysjärjestelmät, kytkeytyvät toisiinsa hyvin kiinteästi. Yksi Suomen Pankin tehtävistä on huolehtia osaltaan maksu- ja muun rahoitusjärjestelmän luotettavuudesta ja tehokkuudesta. Tätä tehtävää Suomen Pankissa hoitaa yleisvalvonta, joka valvoo rahoitusmarkkinoiden kannalta tärkeän infrastruktuurin ja järjestelmien toimintaa kokonaisuutena.

Digitalisaatio edellyttää suojautumista kyberriskeiltä

Digitalisaatio lisää tehokkuutta ja tarjoaa uusia toimintamahdollisuuksia. Samanaikaisesti se myös tuo uusia riskejä, joille digitalisaation hyödyntäjä, esimerkiksi pankki, altistuu. Yleisellä tasolla operatiiviset riskit usein vähenevät automaation myötä. Kuitenkin rahan, arvopaperien tai muun omaisuuden käsittelyyn käytettävät järjestelmät houkuttelevat myös rikollisia yrittämään järjestelmien murtamista taloudellisen edun saavuttamiseksi. Tämä altistaa järjestelmiä käyttävät

organisaatiot riskille niihin kohdistuvista hyökkäyksistä. Tällaisista riskeistä käytetään yleisesti termiä kyberriski.

Kyberriskit voivat olla systeemisesti merkittäviä. Rahoitusmarkkinatoimijat ovat tänä päivänä tiiviissä kytköksissä toisiinsa, mikä voi johtaa siihen, että yhteen toimijaan kohdistuneen kyberhyökkäyksen vaikutukset heijastuvat nopeasti myös muihin toimijoihin. Muun muassa tästä syystä eri maiden viranomaisten ja finanssialan yritysten yhteistyö ja koordinaatio on korostunut viime vuosina.

Keskuspankit ovat ottaneet käyttöön uusia työkaluja, jotka tukevat finanssisektorin kyberresilienssiä eli kestävyyttä kyberriskejä vastaan. Euroopan keskuspankki julkaisi keväällä 2018 TIBER-EU-kehikon, joka antaa ohjeet todelliseen uhkatietoon perustuvien eettisten tunkeutumistestausten tekemiselle. Lyhenne TIBER tulee englanninkielisistä sanoista Threat Intelligence-based Ethical Red Teaming. Kehikon käyttäminen tapahtuu kansallisen soveltamisohjeen avulla ja se on käytössä jo mm. Hollannissa, Belgiassa, Tanskassa ja Saksassa. Suomen Pankki julkaisi TIBER-FI-soveltamisohjeen Suomen finanssialalle 29.4.2020.

Yhtenäisen mallin avulla voidaan saada kokonaiskuva kyberturvallisuuden tasosta

Tunkeutumistestauksessa yrityksen tuotantojärjestelmiin pyritään tunkeutumaan todellisen hyökkääjän keinoin. Tunkeutumistestaus on perinteistä tietoturvatestausta laajempaa ja sen avulla etsitään haavoittuvuuksia niin yrityksen käyttämistä teknologioista, prosesseista kuin ihmisistä. Samalla testataan yrityksen kykyä havaita hyökkäykset, vastata niihin ja toipua niistä. Tunkeutumistestaukset ovat perinteisesti olleet yritysten ja testauspalveluita tarjoavien tahojen keskinäistä toimintaa, eikä kokonaiskuvaa kyberturvallisuuden tasosta ja mahdollisista heikkouksista esimerkiksi finanssialalla ole välttämättä ollut.

TIBER-kehikon mukaisessa kansallisessa ohjeistuksessa käydään läpi testauksen suunnittelun ja toteutuksen eri vaiheet, ja mitä tuotoksia prosessin eri vaiheissa tulee saada aikaan. Koska tunkeutumistestauksessa jäljitellään todellisen hyökkääjän toimintatapoja, myös testauksen rajoista ja lopettamisesta ennen vahinkojen syntymistä on oltava selkeät sopimukset.

TIBER-kehikon mukainen testaushanke lähtee käyntiin ajantasaisesta uhkatietoraportista, joka antaa kuvan juuri sen hetkisistä kyberuhista. Yhdenmukaisia toimintatapoja ja prosessin vaiheita noudattamalla voidaan varmistaa, että testauksen tulokset ovat luotettavia ja niitä voidaan hyödyntää hyökkäysten torjunnan kehittämisessä. Kehikossa määritellään myös viranomaisyhteistyö kansainvälisten yritysten tunkeutumistestauksessa. Kehikon mukainen raportointi auttaa lisäksi viranomaisia kohdistamaan huomionsa kyberturvallisuuden osalta

todellisiin riskeihin.

Eurooppalainen kehikko käyttöön TIBER-FI-soveltamisohjeella

Suomen Pankin julkaisema TIBER-FI-soveltamisohje täydentää TIBER-EU-kehikkoa. Vaikka kehikko on yleiseurooppalainen, määritellään soveltamisohjeessa käytännössä kansallisesti merkittävät testauksen osa-alueet. Näitä ovat testauksen suunnittelussa käytettävä uhkatieto, huomioon otettavat juridiset seikat sekä testauksille tarjottava tuki ja koordinointi.

Suomen soveltamisohjeen valmistelussa on kuunneltu toimialan yrityksiä ja soveltamisohjetta kehitetään edelleen käytössä saatujen kokemusten perusteella. TIBER-FI:n soveltaminen on yrityksille vapaaehtoista. TIBER-FI:tä sovellettaessa Suomen Pankki toimii kontaktipisteenä ja tarjoaa apua testausten suunnitteluun ja koordinointiin. Malli on herättänyt kiinnostusta myös muiden toimialojen keskuudessa jo sen valmisteluvaiheessa.

Finanssialan kyberresilienssin kehittämiseksi tarvitaan yhteistyötä ja tiedonvaihtoa niin uhista kuin parhaista käytännöistäkin. Finanssisektorin systeemiset ulottuvuudet korostavat sitä tosiseikkaa, ettei turvallisuus ole yksittäisen toimijan kilpailutekijä, vaan koko toimialan yhteinen etu.

Asiasanat

kyberturvallisuus, maksujärjestelmät, rahoitusjärjestelmän vakaus, selvitysjärjestelmät, TIBER-EU, TIBER-FI