ANALYYSI

# Uudenlaiset uhkakuvat kohdistuvat myös rahoitusalaan

Rahoitusvakaus | 04.05.2022 | Pasi Miettinen

KIRJOITTAJA

Pasi Miettinen
Vanhempi ekonomisti

Maksujärjestelmät kuuluvat Suomen huoltovarmuuden tärkeään infrastruktuuriin. Rahoitustoimiala on osa huoltovarmuusketjua, joka ei saa katketa edes poikkeusoloissa. Tämän vuoksi tarvitaan maksamisen kansallista varautumistyötä, jolla pyritään luomaan toimivia varautumisjärjestelyjä erilaisiin poikkeustilanteisiin. Riittävä varautuminen auttaa siinä, että luottamus rahoitusjärjestelmään säilyy myös häiriötilanteissa.

## Ennakointi ja harjoittelu varautumisen ytimessä

Pankit ja muut maksupalveluntarjoajat siirtyivät käyttämään yhteiseurooppalaisia

maksuinfrastruktuureja 2000-luvun alkuvuosina. Niiden tehokkuuteen perustuvat hyödyt ovat kiistattomat, ja niiden käyttö on globaalissa kanssakäymisessä jopa välttämätöntä. Myös yksittäisten pankkien omia prosesseja on siirretty niiden ulkomailla sijaitseviin toimintayksikköihin tai ulkomaisille alihankkijoille. Pitkäkestoiset häiriöt näissä toiminnoissa vaikuttaisivat merkittävästi maksu- ja arvopaperiliikenteen toimintakykyyn Suomessa.

Rahoitusala ja muut kriittiset toimialat harjoittelevat[1] säännöllisesti varautumista erilaisiin häiriöihin. Harjoitusten kautta osallistujat saavat tarpeellista tietoa toimialan ja organisaatiotason heikkouksista ja vahvuuksista. Harjoitusten tulokset antavat näkymän, miten kyseisen hetken uhkien toteutuminen vaikuttaa toimialaan, ja mahdollisuuden kehittää toimialan häiriönsietokykyä. Pelkkä harjoittelu ei tosin riitä, vaan johtopäätökset on sovitettava käytäntöön niin yksittäisen toimijan kuin toimialan tasolla.

Rahoitusalaa koskevissa harjoituksissa on jo vuosien ajan tunnistettu, että suomalaisessa maksuliikenneinfrastruktuurissa on haavoittuvuuksia. Vaikka suomalaiset toimijat ovat panostaneet omaan häiriönhallintaansa ja esimerkiksi kyberuhkien parempaan ehkäisyyn, on koko toimialaa koskeva varautuminen puutteellista.

## Uhkakuvien kirjo kasvaa

Perinteisesti suurimpana uhkakuvana rahoitusalalle on pidetty Suomen muualle Eurooppaan yhdistävien tietoliikennekaapeleiden vaurioitumista ja sitä kautta yhteyksien katkeamista järjestelmiin ja palveluihin, jotka sijaitsevat Suomen rajojen ulkopuolella.

Yksittäiset kyberhyökkäykset ovat arkipäivää. Lyhytkestoiset palvelunestohyökkäykset, tietojen kalastelut sekä tietomurrot ovat olleet esillä laajasti mediassa. Toistaiseksi ne eivät ole vaikuttaneet merkittävästi yhteiskunnan kriittisiin toimintoihin. Kyberrikollisuus on laajentunut yksittäisistä ja epäammattimaisista toimijoista organisoituihin järjestöihin ja valtiollisiin toimijoihin. Tällaisilla toimijoilla on käytössään huippuluokan osaamista ja huomattavat resurssit. Toiminnan motiiveina ovat perinteisesti olleet taloudellinen hyöty, haitanteko ja jännityksen hakeminen. Hyökkäysten syyt voivat liittyä myös hybridivaikuttamiseen. Kyberhyökkäysten ja muiden jatkuvuushäiriöiden varalta on tärkeää miettiä, miten toimitaan suojausten pettäessä ja miten palaudutaan normaaliin tilanteen rauettua.

Vaikka yksittäisen toimijan kyky suojautua kyberriskeiltä olisi hyvä, toimialalla voi kokonaisuutena olla suuriakin puutteita. Monet yritykset ovat ulkoistaneet toimintojaan. Ulkoistamalla ne ovat voineet lisätä tehokkuuttaan ja jakaa uuteen teknologiaan liittyviä investointeja muiden kanssa. Esimerkiksi pilvipalveluiden käyttö on yleistynyt viime vuosien aikana kaikilla toimialoilla. Ulkoistaminen voi kuitenkin olla vaikeasti hallittavissa, jos ulkoistusketjut ovat pitkiä ja näkymä

kokonaisuudesta heikko.

## Kriittisten toimialojen keskinäisriippuvuuksien riskit teknologian muutoksessa

Eri toimialat ovat keskenään verkostoituneita, ja yhden toimialan haavoittuvuus voi johtaa koko ketjun haavoittuvuuteen ja pahimmillaan laajempiin ongelmiin. Esimerkiksi sähköntuotannon tai tietoliikenteen ongelmat heijastuisivat laajasti yhteiskuntaan, myös rahoitusalaan. Rahoitusalan ongelmat voisivat heijastua edelleen esim. vähittäismaksamiseen. Keskinäisriippuvuuksien tunnistaminen ja jokaisen ketjun oma varautuminen on erityisen tärkeää, koska kokonaisuus on yhtä vahva kuin sen heikoin lenkki.

Olemme tulleet yhä enemmän riippuvaisiksi tietoverkkojen toimintavarmuudesta. Myös pääsy tietovarastoihin on muuttunut kriittiseksi. Tietoliikenteen häiriöt vaikuttavat muihin toimialoihin. Pelkkä operatiivisten järjestelmien kahdentaminen varautumistarkoitukseen ei riitä, vaan on oltava selkeät suunnitelmat siitä, miten tietoverkot ja tietovarastot ovat käytettävissä myös häiriötilanteissa.

Globaalisti verkostoitunut maailma hyödyntää yhä enemmän teknologiaa. Tämän tulisi tapahtua tehokkaasti ja turvallisesti. Kehitys on pääasiassa positiivista, ja sen avulla olemme osa maailmanlaajuista kokonaisuutta, mutta samalla se kaventaa kansallisia vaikutusmahdollisuuksiamme.

## Millä maksamme poikkeusoloissa

Maksaminen on yksi yhteiskunnan välttämättömistä toiminnoista. Palkat, eläkkeet ja etuudet on voitava maksaa ja kansalaisten on pystyttävä ostamaan elämisen kannalta välttämättömiä hyödykkeitä, kuten elintarvikkeita, lääkkeitä ja energiaa. Maksamiseen käytettävien järjestelmien tulee olla turvallisia, luotettavia ja tehokkaita. Mikäli järjestelmien käyttö jostain syystä estyy, on yhteiskunnan toiminnan kannalta välttämätön maksaminen hoidettava jollain toisella tavalla.

Varautumiselle on asetettava sopiva ja riittävä tavoitetaso. Kaikkia normaaliolojen palveluita ei tarvita pitkittyneissä häiriötilanteissa tai poikkeusoloissa, vaan varautuminen on kustannustehokkuudenkin näkökulmasta kohdistettava välttämättömiin tarpeisiin.

Rahoitusmarkkinoiden toiminta perustuu luottamukseen. Maksamiseen tai maksujen välitykseen kohdistuva häiriö voisi erityisesti pidempään jatkuessaan aiheuttaa luottamuspulaa pankkijärjestelmää kohtaan. Riittävä varautuminen auttaa siinä, että luottamus säilyy myös häiriötilanteissa.

## Viitteet

1. Esimerkiksi FATO21- ja TIETO22-harjoitukset. ↑

## Asiasanat

maksujärjestelmät, rahoitusala, selvitysjärjestelmät, uhkakuva, varautuminen