FIN-FSA
FINANSSIVALVONTA

Digitalisaatio ja analyysi

Muistio

31.5.2024
SP/FIVA-EI RAJOITETTU
Julkinen

Teema-arvio: Varautumisen tilanne

1 Teema-arvion tausta ja johtopäätökset

Digitalisoituvan finanssisektorin valvonta on yksi Finanssivalvonnan strategian painopistealueista. Finanssivalvonnalla on ollut tilannekuvaa merkittävien finanssisektorin toimijoiden varautumisen tilanteesta jatkuvan valvonnan sekä aiemmin tehtyjen tarkastusten ja teema-arvioiden perusteella. Yhtenäinen kokonaiskuva finanssisektorin tilanteesta kuitenkin on puuttunut.

Finanssivalvonta laati teema-arvion huhti-toukokuussa 2024 Suomessa toimivien merkittävien finanssissektorin toimijoiden varautumisen tilanteesta, eli siitä kuinka merkittävät finanssialan toimijat ovat varmistaneet häiriönsietokykynsä normaali- ja poikkeusoloissa.

Teema-arvio perustuu merkittäville finanssialan toimijoille tehtyyn teemakyselyyn. Kyselyssä selvitettiin yhtiöiden toiminnan häiriöihin varautumisen organisointia ja tilannetta. Kysely koostui 40 kysymyksestä, jotka on laadittu Finanssivalvonnan Määräykset ja ohjeet 8/2014 ”Operatiivisen riskin hallinta rahoitussektorin valvottavissa” perusteella. Kysely lähetettiin 22 yhtiölle ja vastaus saatiin kaikilta.

Teema-arvion johtopäätökset perustuvat yhtiöiden antamiin vastauksiin, eikä niitä ole verifioitu Finanssivalvonnassa. Finanssivalvonta on tehnyt viime vuosina useille vastaajista IT- ja tietoturvariskien hallinnan tarkastuksia, jotka ovat sisältäneet myös jatkuvuus- ja valmiussuunnittelu. Tarkastusten havainnot ovat linjassa teemakyselyssä saatujen vastausten kanssa.

Merkittävät finanssisektorin valvottavat ovat järjestäneet toimintansa jatkuvuus- ja valmiussuunnittelun vaatimusten mukaisesti siten, että toiminnan häiriönsietokyky normaali- ja poikkeusoloissa on varmistettu. Valvottavasektorien välillä ei havaittu merkittäviä eroja varautumisessa. Valvottavat ovat havainneet omassa toiminnassaan yksittäisiä puutteita, joita riskienhallintaprosessin mukaisesti havaittaessa korjataan.

Yhtiöiden kyselyyn antamien vastausten perusteella tehtiin seuraavia havaintoja:

- Osalla toimijoista oli puutteita jatkuvuussuunnitelmien säännöllisessä testaamisessa.
- Osalla toimijoista ei ollut ajantasaisia toipumissuunnitelmia tai toipumissuunnitelmia ei ole testattu säännöllisesti.
- Varautuminen tason ja siihen liittyvän palautumisen tavoiteajat voivat olla ja ovat eritasoisia ajantasaisissa transaktiopohjaisissa maksujärjestelmissä, esimerkiksi korttimaksamisen yhteydessä, verrattuna lakisääteisten eläkkeiden maksatukseen (TyEL, liikennevakuutus, lakisääteinen tapaturmavakuutus) tai riskihenkivakuuttamisen ja vakuutussijoittamisen yhteydessä.

- ICT-infrastruktuuriin liittyvää maantieteellisen hajauttamisen riskiä esimerkiksi kriittisten konesalitoiminnallisuuksien sekä varmuuskopioiden hallinnoinnin yhteydessä on syytä arvioida valvonnan yhteydessä aiempaa tarkemmin

Kyselyn tulokset auttavat kohdentamaan jatkuvaa valvontaa sekä yleisesti että yhtiökohtaisesti. Tuloksia hyödynnetään IT- ja tietoturvariskien hallinnan tarkastusten suunnittelussa.

Yleisesti jatkuvassa valvonnassa ja mahdollisissa erillisissä tarkastuksissa tulee kiinnittää erityistä huomiota jatkuvuus- ja toipumissuunnitelmien säännölliseen päivittämiseen, testaamiseen ja harjoitteluun sekä fyysisen IT-infrastruktuurin varautumiskykyyn maantieteellisen hajauttamisen osalta.

Vastausten perusteella ei tullut ilmi sellaisia puutteita yksittäisten valvottavien toiminnassa, että Finanssivalvonta kehottaisi niiden perusteella valvottavaa välittömiin toimiin puutteen korjaamiseksi. Puutteiden korjaus on jo käynnissä tai ne eivät olleet vakavia. Puutteiden korjauksen tilannetta tullaan kuitenkin seuraamaan jatkuvan valvonnan ja tarkastusten yhteydessä.

Finanssialan digitaalista häiriönsietokykyä koskeva asetus (DORA[1]) yhtenäistää EU-alueella vaatimuksia ja tuo myös uusia vaatimuksia. DORAa sovelletaan 17.1.2025 lähtien. Kansallista varautumista koskevat vaatimukset ja ohjeet säilyvät ennallaan. Teema-arvion perusteella merkittävät finanssisektorin valvottavat pystyvät noudattamaan DORAn häiriönsietokyvylle asettamia vaatimuksia.

2 Jatkuvuussuunnittelu

Jatkuvuussuunnittelulla tarkoitetaan varautumista liiketoiminnan keskeytyksiin siten, että valvottava pystyy jatkamaan toimintaansa ja rajoittamaan tappioita erilaisissa liiketoimintaa kohtaavissa häiriötilanteissa. Häiriötilanteita ovat muun muassa valvottavan henkilöstöä, toimitiloja, tietojärjestelmiä tai tietoliikennettä kohdanneet vahingot tai tahalliset teot, vesivahingot, tulipalot sekä katkot esimerkiksi sähkön, lämmön tai veden saannissa. Jatkuvuussuunnittelussa laaditaan tärkeimmille liiketoiminta-alueille jatkuvuussuunnitelmat, joiden pohjalta toimintaa jatketaan mahdollisessa häiriötilanteessa.

Pääsääntöisesti valvottavat täyttävät jatkuvuussuunnittelulle asetetut vaatimukset. Valvottavan keskeisillä liiketoiminnoilla on ajantasaiset ja riittävät jatkuvuussuunnitelmat. Valvottavalla on selkeä toimintamalli jatkuvuussuunnitelmien laatimiseen, ylläpitoon ja testaamiseen sekä jatkuvuussuunnittelun tilanteen seuraamiseen. Tietojärjestelmille laaditaan toipumissuunnitelmat, joissa kuvataan, kuinka eri tietojärjestelmät saa-

[1] Digital Operational Resiliency Act, linkki https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32022R2554&qid=1682057478749

daan toimintakuntoon vakavassa häiriötilanteessa tai katastrofissa. Jatkuvuussuunnitelmat päivitetään säännöllisesti. Jatkuvuussuunnitelmia testataan, ja niiden mukaista toimintaa harjoitellaan säännöllisesti.

Puutteita on kuitenkin tunnistettu jatkuvuussuunnitelmien säännöllisessä testaamisessa ja toipumissuunnitelmien säännöllisessä päivittämisessä tai testaamisessa.

3 Varautuminen poikkeusoloihin

Valmiussuunnittelu, eli poikkeusoloihin varautuminen pohjautuu normaaliolojen jatkuvuusjärjestelyihin. Poikkeusoloilla tarkoitetaan valmiuslain 3 §:ssä määriteltyjä tilanteita.

Poikkeusolojen häiriötilanne kestää tyypillisesti pidempään kuin tilanteet, joihin normaaliolojen jatkuvuussuunnitelmassa on varauduttu. Lisäksi poikkeusolojen uhat ovat yleensä vakavampia kuin uhat, joiden varalta jatkuvuussuunnitelmia laaditaan.

Poikkeusolojen varautumista voidaan soveltaa myös muihin vakaviin häiriöihin ja kriiseihin kuin valmiuslaissa määriteltyihin poikkeusoloihin. Vakavia häiriöitä ja kriisejä voivat olla esimerkiksi valvottavan henkilöstön toimintakykyä vakavasti vaarantava uhka tai valvottavan toimitilojen tai tietojenkäsittely-ympäristön tuhoutuminen.

Joistakin vastauksista käy ilmi, ettei IT-infrastruktuuria ole maantieteellisesti täysin hajautettu. Säädökset eivät tällä hetkellä anna tarkkaa määrettä sille, millä tavoin infrastruktuuri tulisi hajauttaa. Pääpiirteissään vastaajien tulisi huomioida, että yksittäisten alueiden pidemmät sähkö- tai tietoliikennekatkokset tulisi huomioida. Luonnonkatastrofien johdosta Suomessa tapahtuvien sähkö- tai tietoliikennekatkosten mahdollisuus on kohtalaisen pieni, mutta onnettomuudet tai tahalliset vaikuttamisyritykset nostavat riskitasoa esimerkiksi sellaisissa tilanteissa, joissa IT-infrastruktuuri on sijoitettu yksittäiseen konesaliin tai kahdennettu maantieteellisesti toisiaan lähellä oleviin sijainteihin. Hajauttamattomuus voi tehdä IT-infrastruktuurin toiminnan haavoittuvaksi esimerkiksi ympäröivään infrastruktuuriin liittyvän vaikuttamisen tai onnettomuuden takia, esimerkiksi tilanteessa, jossa sähkönjakelu keskeytyy vakava häiriön tai kyberhyökkäyksen takia. Mahdollinen on myös skenaario, jossa hajauttamatonta IT-infrastruktuuria palveleva kriittinen tietoliikenneyhteys ei ole syystä tai toisesta käytettävissä tai ei pysty toimimaan täydellä kapasiteetilla.

4 Valmiussuunnittelu

Valmiussuunnitelmalla tarkoitetaan etukäteen laadittavaa kuvausta toimenpiteistä, joiden avulla varautumisvelvollinen varmistaa toimintansa jatkamisen vakavissa normaaliolojen häiriötilanteissa ja poikkeusoloissa. Valmiussuunnitelma voi olla osana jatkuvuussuunnitelmaa, sillä edellytyksellä, että siinä on otettu riittävästi huomioon poikkeusolojen varautumisen tarpeet. Valmiussuunnitelma on useimmilla yhtiöillä osana jatkuvuussuunnitelmaa.

Osa vastaajista on tunnistanut puutteita valmiussuunnitelmien testaamisessa esimerkiksi häiriöistä toipumisen osalta. Toipumissuunnitelmia oli luotuina, mutta niiden toimimista ei ollut harjoiteltu tai testattu useaan vuoteen esimerkiksi palomuurien tai eläkkeiden maksatuksen osalta.

Tapauksissa, joissa valmius- ja toipumissuunnitelmien toimivuuden puuttuva harjoittelu, testaaminen tai haasteet asetettuun tavoitetasoon pääsemisessä nostavat jatkuvuuden turvaamisen riskitasoa normaalioloissa, on huomionarvoista, että myös poikkeusoloihin varautumisen riskitaso nousee merkittävästi. On oletettavaa, että kyky toipua poikkeusoloissa tapahtuvista vakavammista ja kompleksisemmista skenaarioista on alhaisempi kuin normaaliolosuhteissa tapahtuvien skenaarioiden.

Kansallinen huoltovarmuus pitää varmistaa myös tilanteissa, joissa vastaajat hoitavat lakisääteisiä velvoitteita maksuliikenteen ja rahoituspalveluiden lisäksi esimerkiksi eläkkeiden maksamiseen liittyen (TyEL-toimijat, vahinkovakuutustoimijat).