EBA/GL/2017/17

12/01/2018

Ohjeet

maksupalvelujen operatiivisia riskejä ja turvallisuusriskejä koskevista turvatoimenpiteistä direktiivin (EU) 2015/2366 (PSD2) mukaisesti

1. Noudattamista ja ilmoittamista koskevat velvoitteet

Näiden ohjeiden asema

1. Tämä asiakirja sisältää ohjeita, jotka on annettu asetuksen (EU) N:o 1093/2010[1] 16 artiklan nojalla. Asetuksen (EU) N:o 1093/2010 16 artiklan 3 kohdan mukaan toimivaltaisten viranomaisten ja finanssilaitosten on kaikin tavoin pyrittävä noudattamaan ohjeita.

2. Ohjeissa esitetään Euroopan pankkiviranomaisen näkemys Euroopan finanssivalvojien järjestelmässä toteutettavista asianmukaisista valvontakäytännöistä tai siitä, miten unionin lainsäädäntöä on sovellettava tietyllä alalla. Asetuksen (EU) N:o 1093/2010 4 artiklan 2 kohdassa määriteltyjen toimivaltaisten viranomaisten, joihin näitä ohjeita sovelletaan, on noudatettava ohjeita sisällyttämällä ne tarpeen mukaan valvontakäytäntöihinsä (esim. muuttamalla lainsäädäntöään tai valvontamenettelyjään). Tämä koskee myös ohjeita, jotka on suunnattu ensisijaisesti laitoksille.

Raportointivaatimukset

3. Asetuksen (EU) N:o 1093/2010 16 artiklan 3 kohdan nojalla toimivaltaisten viranomaisten on ilmoitettava Euroopan pankkiviranomaiselle viimeistään 12.03.2018, noudattavatko ne tai aikovatko ne noudattaa näitä ohjeita, sekä syyt niiden noudattamatta jättämiseen. Jos ilmoitusta ei toimiteta tähän määräaikaan mennessä, Euroopan pankkiviranomainen katsoo, etteivät toimivaltaiset viranomaiset noudata ohjeita. Ilmoitukset lähetetään Euroopan pankkiviranomaisen verkkosivustolla olevalla lomakkeella sähköpostitse osoitteeseen compliance@eba.europa.eu. Viitteeksi merkitään ”EBA/GL/2017/17”. Ilmoituksen voi lähettää ainoastaan henkilö, jolla on asianmukaiset valtuudet ilmoittaa ohjeiden tai suositusten noudattamisesta toimivaltaisen viranomaisen puolesta. Myös ohjeiden noudattamisen osalta tehtävistä muutoksista on ilmoitettava Euroopan pankkiviranomaiselle.

4. Ilmoitukset julkaistaan Euroopan pankkiviranomaisen verkkosivustolla 16 artiklan 3 kohdan mukaisesti.

[1] Euroopan parlamentin ja neuvoston asetus (EU) N:o 1093/2010, annettu 24 päivänä marraskuuta 2010, Euroopan valvontaviranomaisen (Euroopan pankkiviranomainen) perustamisesta sekä päätöksen N:o 716/2009/EY muuttamisesta ja komission päätöksen 2009/78/EY kumoamisesta (EUVL L 331, 15.12.2010, s. 12).

2. Sisältö, soveltamisala ja määritelmät

Sisältö ja soveltamisala

5. Nämä ohjeet perustuvat Euroopan pankkiviranomaiselle direktiivin (EU) 2015/2366 [2] (PSD2) 95 artiklan 3 alakohdassa annettuun tehtävään.

6. Näissä ohjeissa täsmennetään vaatimukset niiden turvatoimenpiteiden laatimisesta, toteutuksesta ja valvonnasta, jotka maksupalveluntarjoajien on toteutettava direktiivin (EU) 2015/2366 95 artiklan 1 kohdan mukaisesti hallitakseen tarjoamiinsa maksupalveluihin liittyviä operatiivisia riskejä ja turvallisuusriskejä.

Keitä ohjeet koskevat

7. Nämä ohjeet koskevat direktiivin (EU) 2015/2366 4 artiklan 11 kohdassa määriteltyjä maksupalveluntarjoajia ja asetuksen (EU) N:o 1093/2010 4 artiklan 1 kohdan määritelmän mukaisia finanssilaitoksia ja kyseisen asetuksen 4 artiklan 2 kohdan i) alakohdassa määriteltyjä toimivaltaisia viranomaisia viitaten kumottuun direktiiviin 2007/64/EY[3] (nykyisin direktiivi (EU) 2015/2366[4]).

Määritelmät

8. Ellei toisin ilmoiteta, näihin ohjeisiin sisältyvillä termeillä tarkoitetaan samaa kuin direktiivissä (EU) 2015/2366 käytetyillä ja määritellyillä termeillä. Lisäksi näissä ohjeissa käytetään seuraavia määritelmiä:

Ylin hallintoelin	– Niiden maksupalveluntarjoajien osalta, jotka ovat luottolaitoksia, tällä termillä tarkoitetaan samaa kuin direktiivin 2013/36/EU 3 artiklan 1 kohdan 7 alakohdan määritelmällä[5]. – Niiden maksupalveluntarjoajien osalta, jotka ovat maksulaitoksia tai sähköisen rahan

[2] Euroopan parlamentin ja neuvoston direktiivi (EU) 2015/2366, annettu 25 päivänä marraskuuta 2015, maksupalveluista sisämarkkinoilla, direktiivien 2002/65/EY, 2009/110/EY ja 2013/36/EU ja asetuksen (EU) N:o 1093/2010 muuttamisesta sekä direktiivin 2007/64/EY kumoamisesta (EUVL L 337, 23.12.2015, s. 35).

[3] Euroopan parlamentin ja neuvoston direktiivi 2007/64/EY, annettu 13 päivänä marraskuuta 2007, maksupalveluista sisämarkkinoilla, direktiivien 97/7/EY, 2002/65/EY, 2005/60/EY ja 2006/48/EY muuttamisesta ja direktiivin 97/5/EY kumoamisesta (EUVL L 319, 5.12.2007, s. 1).

[4] Direktiivin (EU) 2015/2366 114 artiklan toisen alakohdan mukaisesti viittauksia kumottuun direktiiviin 2007/64/EY pidetään viittauksina direktiiviin (EU) 2015/2366 direktiivin (EU) 2015/2366 liitteessä II olevan vastaavuustaulukon mukaisesti.

[5] Euroopan parlamentin ja neuvoston direktiivi 2013/36/EU oikeudesta harjoittaa luottolaitostoimintaa ja luottolaitosten ja sijoituspalveluyritysten vakavaraisuusvalvonnasta, direktiivin 2002/87/EY muuttamisesta sekä direktiivien 2006/48/EY ja 2006/49/EY kumoamisesta (EUVL L 176, 27.6.2013, s. 338).

	liikkeeseenlaskijalaitoksia, tällä termillä tarkoitetaan johtajia tai maksupalveluntarjoajan johtotehtävistä vastuussa olevia henkilöitä jasoveltuvin osin maksupalveluntarjoajan maksupalvelutoiminnan johtamisesta vastuussa olevia henkilöitä. – Direktiivin (EU) 2015/2366 1 artiklan 1 kohdan c), e) ja f) alakohdissa tarkoitettujen maksupalveluntarjoajien osalta tällä termillä tarkoitetaan samaa kuin sovellettavassa EU:n tai kansallisessa lainsäädännössä annetulla määritelmällä.
Operatiivinen tai turvallisuushäiriö	Yksittäinen tapahtuma tai toisiinsa liittyvien tapahtumien sarja, jota maksupalveluntarjoaja ei ole suunnitellut ja joka vaikuttaa tai todennäköisesti vaikuttaa haitallisesti maksuihin liittyvien palvelujen luotettavuuteen, saatavuuteen, luottamuksellisuuteen, aitouteen ja/tai jatkuvuuteen.
Ylin johto	(a) Niiden maksupalveluntarjoajien osalta, jotka ovat luottolaitoksia, tällä termillä tarkoitetaan samaa kuin direktiivin 2013/36/EU 3 artiklan 1 kohdan 9 alakohdan määritelmällä. (b) Niiden maksupalveluntarjoajien osalta, jotka ovat maksulaitoksia ja sähköisen rahan liikkeeseenlaskijalaitoksia, tällä termillä tarkoitetaan luonnollisia henkilöitä, jotka vastaavat maksupalveluntarjoajan päivittäisestä johtamisesta ja ovat siitä vastuussa ja tilivelvollisia ylimmälle hallintoelimelle. (c) Direktiivin (EU) 2015/2366 1 artiklan 1 kohdan c), e) ja f) alakohdissa tarkoitettujen maksupalveluntarjoajien osalta tällä termillä tarkoitetaan samaa kuin sovellettavassa EU:n tai kansallisessa lainsäädännössä annetulla määritelmällä.
Turvallisuusriski	Riski, joka johtuu riittämättömistä tai epäonnistuneista sisäisistä prosesseista tai ulkoisista tapahtumista, jotka vaikuttavat tai voivat vaikuttaa haitallisesti tieto- ja viestintätekniikan (ICT) järjestelmien ja/tai maksupalvelujen tarjoamiseen käytettävien tietojen saatavuuteen, eheyteen tai luottamuksellisuuteen. Tämä sisältää myös kyberhyökkäyksistä tai riittämättömästä fyysisestä turvallisuudesta johtuvan riskin.
Riskinottohalu	Niiden riskien yhteenlaskettu taso ja tyyppi, jotka laitos on valmis ottamaan riskinkantokykynsä rajoissa ja liiketoimintamallinsa mukaisesti saavuttaakseen strategiset tavoitteensa.

3. Täytäntöönpano

Voimaantulopäivä

9. Näitä ohjeita sovelletaan 13. tammikuuta 2018 alkaen.

4. Ohjeet

Ohje 1: Yleisperiaate

1.1 Kaikkien maksupalveluntarjoajien tulisi noudattaa kaikkia näissä ohjeissa esitettyjä säännöksiä. Yksityiskohtaisuuden taso tulisi suhteuttaa maksupalveluntarjoajan kokoon ja toiminnan luonteeseen, laajuuteen ja monimutkaisuuteen ja niiden palvelujen riskialttiuteen, joita maksupalveluntarjoaja tarjoaa tai aikoo tarjota.

Ohje 2: Hallinto

Operatiivisten riskien ja turvallisuusriskien hallintakehikko

2.1 Maksupalveluntarjoajien tulisi laatia tehokas operatiivisten riskien ja turvallisuusriskien hallintakehikko (jäljempänä ”riskienhallintakehikko”), joka ylimmän hallintoelimen ja, mikäli asianmukaista, ylimmän johdon, tulisi hyväksyä ja arvioida vähintään kerran vuodessa. Riskienhallintakehikossa tulisi keskittyä turvatoimenpiteisiin operatiivisten riskien ja turvallisuusriskien vähentämiseksi, ja se tulisi integroida kokonaan maksupalveluntarjoajan riskienhallinnan kokonaisprosesseihin.

2.2 Riskienhallintakehikon

a) tulisi sisältää direktiivin (EU) 2015/2366 5 artiklan 1 kohdan j) alakohdassa tarkoitettu kattava turvallisuuspolitiikka-asiakirja;

b) tulisi olla yhdenmukainen maksupalveluntarjoajan riskinottohalukkuuden kanssa;

c) tulisi sisältää tärkeimpien tehtävien ja vastuualueiden määrittely ja nimeäminen sekä asianmukaiset raportointikanavat, joita tarvitaan turvatoimenpiteiden toteutusta sekä turvallisuus- ja operatiivisten riskien hallintaa varten;

d) tulisi sisältää tarpeelliset menetelmät ja järjestelmät, joilla voidaan tunnistaa, mitata, valvoa ja hallita riskejä, jotka ovat peräisin maksupalveluntarjoajan maksupalvelutoiminnasta ja joille maksupalveluntarjoaja altistuu, mukaan lukien liiketoiminnan jatkuvuus järjestelyt.

2.3 Maksupalveluntarjoajien tulisi varmistaa, että riskienhallintakehikko on dokumentoitu asianmukaisesti ja sitä päivitetään ”opitun mukaisilla asioilla” sen toteutuksen ja valvonnan aikana..

2.4 Maksupalveluntarjoajien tulisi varmistaa, että ennen merkittävää infrastruktuuriin, prosesseihin tai menettelyihin kohdistuvaa muutosta ja kunkin merkittävän maksupalveluihin vaikuttavan operatiivisen häiriön tai turvallisuushäiriön jälkeen ne arvioivat ilman aiheetonta viivytystä, tarvitaanko riskienhallintakehikkoon muutoksia tai parannuksia .

Riskinhallinta ja -valvontamallit

2.5 Maksupalveluntarjoajien tulisi luoda kolmen puolustuslinjan malli tai vastaava sisäinen riskinhallinta- ja valvontamalli, jolla voidaan tunnistaa ja hallita operatiivisia riskejä ja turvallisuusriskejä. Maksupalveluntarjoajien tulisi varmistaa, että edellä mainittuun sisäiseen valvontamalliin sisältyvät riittävät valtuudet, riippumattomuus, resurssit ja suorat raportointikanavat ylimpään hallintoelimeen ja asian niin vaatiessa ylimpään johtoon.

2.6 Näissä ohjeissa esitettyjen turvatoimenpiteiden tarkastus tulisi antaa sellaisten tarkastajien tehtäväksi, joilla on IT-tietoturvaan ja maksupalveluihin liittyvä asiantuntemus ja jotka toimivat itsenäisesti maksupalveluntarjoajan yhteydessä tai joiden toiminta on maksupalveluntarjoajasta riippumatonta. Tarkastusten tiheydessä ja painopisteessä tulisi ottaa huomioon vastaavat turvallisuusriskit.

Ulkoistaminen

2.7 Maksupalveluntarjoajien tulisi varmistaa näiden ohjeiden mukaisten turvatoimenpiteiden tehokkuus, kun maksupalvelujen operatiivisia toimintoja, mukaan lukien IT-järjestelmät, ulkoistetaan.

2.8 Maksupalveluntarjoajien tulisi varmistaa, että asianmukaiset ja oikein suhteutetut turvallisuustavoitteet, turvatoimenpiteet ja palvelutasotavoitteet sisällytetään niiden palveluntarjoajien kanssa solmittaviin sopimuksiin ja palvelutasosopimuksiin, joille kyseiset toiminnot on ulkoistettu. Maksupalveluntarjoajien tulisi valvoa sitä, millä tasolla nämä palveluntarjoajat noudattavat turvallisuustavoitteita, turvatoimenpiteitä ja palvelutasotavoitteita, ja pyrkiä saamaan varmistus siitä.

Ohje 3: Riskiarviointi

Toimintojen, prosessien ja varojen yksilöinti

3.1 Maksupalveluntarjoajien tulisi yksilöidä liiketoimintonsa, tärkeimmät tehtävänsä ja tukitoimintonsa ja laadittava luettelo niistä sekä päivitettävä luetteloa säännöllisesti kartoittaakseen kunkin toiminnon, tehtävän ja tukiprosessin tärkeyden sekä niiden operatiivisiin riskeihin ja turvallisuusriskeihin liittyvät keskinäiset riippuvuudet.

3.2 Maksupalveluntarjoajien tulisi yksilöidä tietoresurssinsa kuten ICT-järjestelmänsä, niiden kokoonpanot, muut infrastruktuurit ja myös muiden sisäisten ja ulkoisten järjestelmien väliset riippuvuudet ja laadittava luettelo niistä sekä päivitettävä luetteloa säännöllisesti, jotta ne kykenisivät hallinnoimaan kriittisiä liiketoimintoja ja prosesseja tukevia resursseja.

Toimintojen, prosessien ja varojen luokitteleminen

3.3 Maksupalveluntarjoajien tulisi luokitella yksilöidyt liiketoiminnot, tukiprosessit ja tietoresurssit niiden kriittisyyden perusteella.

Toimintojen, prosessien ja varojen riskiarviot

3.4 Maksupalveluntarjoajien tulisi varmistaa, että ne valvovat jatkuvasti uhkia ja haavoittuvuuksia sekä arvioivat säännöllisesti niiden liiketoimintoihin, kriittisiin prosesseihin ja tietoresursseihin vaikuttavat riskiskenaariot. Osana velvollisuuttaan tehdä tarjoamiensa maksupalveluiden n operatiivisten riskien ja turvallisuusriskien sekä riskienhallinta- ja valvontamekanismien ja päivitetty, kattava riskiarvioi sekä toimittaa se toimivaltaisille viranomaisille, kuten on määrätty direktiivin (EU) 2015/2366 95 artiklan 2 kohdassa, maksupalveluntarjoajien tulisi toteuttaa ja dokumentoida riskiarvioita vähintään vuosittain tai useammin toimivaltaisten viranomaisten määrittämällä tavalla yksilöimistään ja luokittelemistaan toiminnoista, prosesseista ja tietoresursseista tunnistaakseen ja arvioidakseen tärkeät operatiiviset ja turvallisuusriskit.. Kyseiset riskiarviot tulisi tehdä myös ennen kuin tapahtuu merkittävä infrastruktuuriin, prosessiin tai menettelyihin kohdistuva muutos, joka vaikuttaa maksupalvelujen turvallisuuteen.

3.5 Maksupalveluntarjoajien olisi riskiarvioiden perusteella määritettävä, ovatko nykyisten turvatoimenpiteiden, käytettyjen tekniikoiden ja tarjottujen menettelyjen tai maksupalvelujen muutokset tarpeen ja missä laajuudessa.. Maksupalveluntarjoajien olisi otettava huomioon aika, joka tarvitaan muutosten ja asianmukaisten tilapäisten turvatoimenpiteiden toteuttamiseen, jotta voitaisiin minimoida operatiiviset poikkeamat tai turvallisuuspoikkeamat, petokset ja mahdolliset maksupalvelujen tarjoamiseen kohdistuvat haitat.

Ohje 4: Suojautuminen

4.1 Maksupalveluntarjoajien tulisi laatia ja toteuttaa ehkäiseviä turvatoimenpiteitä tunnistettujen operatiivisten riskien ja turvallisuusriskien torjumiseksi. Näiden toimenpiteiden olisi varmistettava tunnistettujen riskien mukainen riittävä turvallisuustaso .

4.2 Maksupalveluntarjoajien tulisi laatia ja toteuttaa ”kattavan puolustuksen” lähestymistapa ottamalla käyttöön kerroksittaisia valvontatoimia, jotka kattavat työntekijät, prosessit ja tekniikan ja joissa kukin kerros toimii edeltävien kerrosten turvaverkkona. Kattava puolustus tulisi ymmärtää siten, että useampi kuin yksi valvontatoimi on määritetty kattamaan sama riski. Esimerkkeinä voidaan mainita neljän silmän periaate, kahden tekijän tunnistus, verkon segmentointi ja usean palomuurin käyttö.

4.3 Maksupalveluntarjoajien tulisi varmistaa kriittisten loogisten ja fyysisten varojensa ja resurssiensa sekä maksupalvelunkäyttäjiensä arkaluonteisten maksutietojen luottamuksellisuus, eheys ja käytettävyys niin tietojen säilytyksessä, siirrossa kuin käytössäkin. Jos tietoihin kuuluu henkilötietoja, kyseiset toimenpiteet tulisi toteuttaa asetuksen (EU) 2016/679[6] tai tarvittaessa asetuksen (EY) N:o 45/2001 mukaisesti.[7]

[6] Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus) (EYVL 119, 4.5.2016, s. 1).

[7] Euroopan parlamentin ja neuvoston asetus (EY) N:o 45/2001, annettu 18 päivänä joulukuuta 2000, yksilöiden suojelusta yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta (EYVL 8, 12.1.2001, s. 1).

4.4 Maksupalveluntarjoajien tulisi jatkuvasti määrittää, vaikuttavatko toimintaympäristön muutokset nykyisiin turvatoimenpiteisiin tai vaativatko ne muiden toimenpiteiden käyttöönottoa niiden sisältämän riskin vähentämiseksi. Näiden muutosten tulisi olla osa maksupalveluntarjoajan muodollista muutoksenhallintaprosessia, jossa tulee varmistaa, että muutokset suunnitellaan, testataan, dokumentoidaan ja valtuutetaan asianmukaisesti. Testaaminen tulisi havaittujen turvallisuusuhkien ja tehtyjen muutosten perusteella tehdä niin, että siihen sisältyvät asiaan liittyvien ja tunnettujen mahdollisten hyökkäysten skenaariot.

4.5 Maksupalveluntarjoajien tulisi maksupalveluja suunniteltaessa, kehitettäessä ja tarjottaessa varmistaa, että tehtävien eriyttämisen ja pienimpien mahdollisten oikeuksien periaatteita sovelletaan. Maksupalveluntarjoajien tulisi kiinnittää erityishuomiota IT-ympäristöjen eriyttämiseen, erityisesti kehitys-, testaus- ja tuotantoympäristöjen osalta.

Tietojen ja järjestelmien luotettavuus ja luottamuksellisuus

4.6 Maksupalveluntarjoajien tulisi maksupalveluja suunniteltaessa, kehitettäessä ja tarjottaessa varmistaa, että maksupalvelunkäyttäjän arkaluonteisten maksutietojen kerääminen, reitittäminen, käsitteleminen, säilyttäminen ja/tai arkistoiminen ja visualisoiminen on riittävää ja asiaankuuluvaa ja rajoittuu vain siihen, mikä on tarpeen maksupalvelujen tarjoamiseksi.

4.7 Maksupalveluntarjoajien tulisi tarkistaa säännöllisesti, että maksupalvelujen tarjoamiseen käytettävät ohjelmistot, mukaan lukien käyttäjien maksuohjelmistot, ovat ajan tasalla ja että kriittiset turvallisuuskorjaukset otetaan käyttöön. Maksupalveluntarjoajien tulisi varmistaa, että käytössä on luotettavuuden tarkistusmekanismit niin, että ohjelmistojen, laiteohjelmistojen ja niiden maksupalveluja koskevien tietojen luotettavuus voidaan varmistaa.

Fyysinen turvallisuus

4.8 Maksupalveluntarjoajilla tulisi olla käytössä asianmukaiset fyysiset turvatoimenpiteet erityisesti maksupalvelunkäyttäjien arkaluonteisten maksutietojen sekä maksupalvelujen tarjoamiseen käytettyjen ICT-järjestelmien suojaamiseksi.

Pääsyn valvonta

4.9 Fyysinen ja looginen pääsy ICT-järjestelmiin tulisi sallia vain valtuutetuille henkilöille. Valtuudet tulisi antaa vain henkilöstön tehtävien ja vastuiden mukaisesti ja vain asianmukaisesti koulutetuille ja valvotuille henkilöille. Maksupalveluntarjoajien tulisi ottaa käyttöön valvontatoimia, jotka rajaavat tällaisen pääsyn ICT-järjestelmiin luotettavasti niille, joilla on perusteltu liiketoimintaan liittyvä vastuu. Elektroninen pääsy tietoihin ja järjestelmiin sovellusten avulla tulisi rajoittaa minimiin, joka on tarpeen asiaankuuluvan palvelun tarjoamiseksi.

4.10 Maksupalveluntarjoajien tulisi ottaa käyttöön järjestelmänvalvojan tai -ylläpitäjän oikeuksia koskevia vahvoja valvontatoimia rajoittamalla tiukasti ja valvomalla tarkasti henkilöstöä, jolla on suuremmat järjestelmän pääsyoikeudet. Tulisi toteuttaa valvontatoimia, kuten tehtäviin perustuvaa pääsyä, järjestelmänvalvojan tai -ylläpitäjän järjestelmiin kohdistuvan toiminnan lokiin

kirjaamista ja arviointia, vahvaa tunnistusta sekä poikkeamien valvontaa. Maksupalveluntarjoajien tulisi hallita tietoresurssien ja niiden tukijärjestelmien käyttöoikeuksia tarvepohjaisesti. Käyttöoikeudet tulisi arvioida säännöllisesti.

4.11 Käyttölokit tulisi säilyttää asiaankuuluvan ajan yksilöityjen liiketoimintojen, tukiprosessien ja tietoresurssien kriittisyyden perusteella, ohjeen 3.1 ja ohjeen 3.2 mukaisesti, rajoittamatta kuitenkaan EU:n ja kansallisessa lainsäädännössä asetettuja säilytysvaatimuksia. Maksupalveluntarjoajien tulisi käyttää näitä tietoja helpottaakseen sellaisten poikkeavien toimien tunnistamista ja tutkintaa, jotka on havaittu maksupalveluja tarjottaessa.

4.12 Turvallisen viestinnän varmistamiseksi ja riskin pienentämiseksi hallintaoikeudellinen etäpääsy kriittisiin ICT-komponentteihin tulisi myöntää vain tarvepohjaisesti ja vahvojen tunnistusratkaisujen ollessa käytössä.

4.13 Pääsynvalvontaprosesseihin liittyvien tuotteiden, työkalujen ja menettelyjen käytön tulisi suojata pääsynvalvontaprosessit niin, etteivät ne vaarannu tai ettei niitä päästä kiertämään. Tähän sisältyy kyseisten tuotteiden, työkalujen ja menettelyjen käyttöönotto, toimittaminen, kumoaminen ja peruminen.

Ohje 5: Havainnointi

Jatkuva valvonta ja havainnointi

5.1 Maksupalveluntarjoajien tulisi laatia ja ottaa käyttöön prosesseja ja kyvykkyyksiä, joilla voidaan valvoa jatkuvasti liiketoimintoja, tukiprosesseja ja tietoresursseja, jotta havaittaisiin poikkeamat maksupalvelujen tarjoamisessa. Maksupalveluntarjoajilla tulisi olla osana tätä jatkuvaa valvontaa käytössään asianmukaiset ja tehokkaat valmiudet, joilla voidaan havaita fyysinen tai looginen tunkeutuminen sekä maksupalveluiden tarjoamisessa käytettyihin tietoresursseihin kohdistuneet luottamuksellisuuden, eheyden ja käytettävyyden rikkomukset.

5.2 Jatkuvien valvonta- ja havainnointiprosessien tulisi kattaa seuraavat:

a) asiaan liittyvät sisäiset ja ulkoiset tekijät, mukaan lukien liiketoiminta ja hallinnolliset ICT-toiminnot;

b) maksutapahtumat, jotta havaittaisiin maksupalveluntarjoajien tai muiden yritysten pääsyyn liittyvät väärinkäytökset; ja

c) mahdolliset sisäiset ja ulkoiset uhat.

5.3 Maksupalveluntarjoajien tulisi toteuttaa havainnointitoimenpiteitä, jotta voitaisiin tunnistaa mahdolliset tietovuodot, haittakoodit ja muut turvallisuusuhat sekä yleisesti tunnetut ohjelmisto- ja laitteistohaavoittuvuudet, ja niiden tulisi tarkistaa vastaavat uudet turvallisuuspäivitykset.

Operatiivisten ja turvallisuushäiriöiden valvonta ja raportointi

5.4 Maksupalveluntarjoajien tulisi määritellä asianmukaiset kriteerit ja kynnysarvot sille, että tapahtuma luokitellaan operatiiviseksi tai turvallisuushäiriöksi, näiden ohjeiden Määritelmät-osion mukaisesti, sekä varhaiset varoitusmerkit, jotka antavat maksupalveluntarjoajalle hälytyksen, jotta tämä ottaisi operatiivisten tai turvallisuushäiriöidenvarhaisen havainnoinnin käyttöön.

5.5 Maksupalveluntarjoajien tulisi luoda asianmukaiset prosessit ja organisaatiorakenteet, joilla varmistetaan operatiivisten häiriöiden tai turvallisuushäiriöiden yhdenmukainen ja integroitu valvonta, käsittely ja seuranta.

5.6 Maksupalveluntarjoajien olisi luotava menettely operatiivisista häiriöistä tai turvallisuushäiriöistä sekä turvallisuuteen liittyvien asiakasvalitusten raportoimiseksi niiden ylimmälle johdolle.

Ohje 6: Liiketoiminnan jatkuvuus

6.1 Maksupalveluntarjoajien tulisi laatia luotettava liiketoiminnan jatkuvuussuunnitelma, joka maksimoi niiden kyvyn tarjota maksupalveluja jatkuvasti ja rajoittaa tappioita liiketoiminnan vakavien häiriöiden varalta.

6.2 Luotettavan liiketoiminnan jatkuvuussuunnitelman laatimiseksi maksupalveluntarjoajien tulisi analysoida huolellisesti alttiutensa vakaville liiketoiminnan häiriöille ja arvioitava (määrällisesti ja laadullisesti) häiriöiden mahdolliset vaikutukset käyttämällä sisäisiä ja/tai ulkoisia tietoja ja skenaarioanalyysia. Yksilöityjen ja luokiteltujen kriittisten toimintojen, prosessien, järjestelmien, maksutapahtumien ja riippuvuuksien perusteella ohjeen 3.1 – ohjeen 3.3 mukaisesti maksupalveluntarjoajien tulisi asettaa liiketoiminnan jatkuvuuden toiminnot tärkeysjärjestykseen käyttäen riskiperusteista lähestymistapaa , joka voi perustua ohjeen 3 mukaisesti toteutettuihin riskiarvioihin. Maksupalveluntarjoajan liiketoimintamallin mukaan tämä voi esimerkiksi helpottaa kriittisten maksutapahtumien jatkokäsittelyä korjaavan työn jatkuessa .

6.3 Ohjeiden kohdan 6.2 mukaan toteutetun analyysin perusteella maksupalveluntarjoajan tulisi ottaa käyttöön seuraavat:

a) liiketoiminnan jatkuvuussuunnitelmat, jotta se voisi reagoida asianmukaisesti hätätilanteisiin ja pystyisi pitämään kriittistä liiketoimintaansa yllä; ja

b) riskinvähentämiskeinot, jotka voidaan ottaa käyttöön, jos sen maksupalvelut ja nykyiset sopimukset päätetään, jotta maksujärjestelmiin ja maksupalvelunkäyttäjiin ei kohdistuisi haitallisia vaikutuksia ja jotta voitaisiin varmistaa vireillä olevien maksutapahtumien toteuttaminen.

Skenaariopohjainen liiketoiminnan jatkuvuussuunnittelu

6.4 Maksupalveluntarjoajan tulisi pohtia erilaisia skenaarioita, joille se voi altistua, mukaan lukien äärimmäiset mutta uskottavilta tuntuvat skenaariot, sekä arvioida kyseisten skenaarioiden mahdollinen vaikutus.

6.5 Ohjeiden kohdan 6.2 mukaan toteutetun analyysin ja ohjeiden kohdan 6.4 mukaisten uskottavien skenaarioiden perusteella maksupalveluntarjoajien tulisi laatia toipumis- ja elvytyssuunnitelmat,

a) joiden painopisteenä tulisi olla kriittisten toimintojen, prosessien, järjestelmien, maksutapahtumien ja keskinäisten riippuvuuksien toimintaan kohdistuva vaikutus;

b) jotka tulisi dokumentoida ja toimittaa liiketoiminta- ja tukiyksiköiden saataville ja joiden on oltava heti käytettävissä hätätilanteessa; ja

c) joita tulisi päivittää sen mukaisesti, mitä on opittu testeistä, uusista tunnistetuista riskeistä ja uhista sekä muuttuneista elvytystavoitteista ja prioriteeteista.

Liiketoiminnan jatkuvuussuunnitelmien testaaminen

6.6 Maksupalveluntarjoajien tulisi testata liiketoiminnan jatkuvuussuunnitelmansa ja varmistettava, että kriittisten toimintojen, prosessien, järjestelmien, maksutapahtumien ja keskinäisten riippuvuuksien toiminta testataan vähintään vuosittain. Suunnitelmien tulisi tukea tavoitteita siten, että ne suojaavat toimintojen luotettavuuden ja käytettävyyden sekä tietoresurssien luottamuksellisuuden ja tarvittaessa palauttavat ne.

6.7 Suunnitelmat tulisi päivittää vähintään vuosittain testitulosten, ajankohtaisten uhkatietojen, tietojen jakamisen ja aiemmista tapahtumista opittujen asioiden perusteella, muuttamalla jatkuvuustavoitteita sekä operatiivisesti ja teknisesti uskottavien, vielä toteutumattomien skenaarioiden analyysia, sekä tarvittaessa järjestelmien ja prosessien muutosten jälkeen. Maksupalveluntarjoajien tulisi kuulla asiaankuuluvia sisäisiä ja ulkoisia sidosryhmiä sekä koordinoida toimensa näiden kanssa liiketoiminnan jatkuvuussuunnitelmien laadinnan aikana.

6.8 Maksupalveluntarjoajien liiketoiminnan jatkuvuussuunnitelmien testauksen

a) tulisi sisältää riittävä määrä skenaarioita ohjeiden kohdassa 6.4 tarkoitetun mukaisesti;

b) tulisi olla suunniteltu haastamaan olettamukset, joihin liiketoiminnan jatkuvuus suunnitelmat nojaavat, mukaan lukien hallintajärjestelyt ja kriisiviestintäsuunnitelmat; ja

c) tulisi sisältää menettelyt, joilla voidaan varmistaa niiden henkilöstön ja prosessien valmiudet vastata riittävästi edellä esitettyihin skenaarioihin.

6.9 Maksupalveluntarjoajien tulisi valvoa säännöllisesti liiketoiminnan jatkuvuussuunnitelmien tehokkuutta sekä dokumentoida ja analysoida testauksissa ilmenneet haasteet tai virheet.

Kriisiviestintä

6.10 Häiriö- tai hätätilanteessa ja liiketoiminnan jatkuvuussuunnitelmien toteutuksen aikana maksupalveluntarjoajien tulisi varmistaa, että niillä on käytössään tehokkaat kriisiviestintämenettelyt, jotta kaikille asiaankuuluville sisäisille ja ulkoisille sidosryhmille, mukaan lukien ulkoiset palveluntarjoajat, tiedotetaan hyvissä ajoin ja asianmukaisella tavalla.

Ohje 7: Turvatoimenpiteiden testaaminen

7.1 Maksupalveluntarjoajien tulisi laatia ja toteuttaa testaussuunnitelma, jolla voidaan validoida turvatoimenpiteiden perusteellisuus ja tehokkuus, ja varmistaa, että testaussuunnitelma on mukautettu ottamaan huomioon uudet uhat ja haavoittuvuudet, jotka on tunnistettu riskinvalvontatoimilla.

7.2 Maksupalveluntarjoajien olisi varmistettava, että testit suoritetaan, jos infrastruktuuriin, prosesseihin tai menettelyihin kohdistuu muutoksia ja jos muutokset tehdään merkittävän operatiivisen tai turvallisuushäiriön seurauksena.

7.3 Testaussuunnitelman tulisi sisältää myös turvatoimenpiteet, joilla on merkitystä i) niiden maksupäätteiden ja laitteiden kannalta, joita käytetään maksupalvelujen tarjoamiseen, ii) niiden maksupäätteiden ja laitteiden kannalta, joita käytetään maksupalvelunkäyttäjän tunnistamiseen, ja iii) niiden laitteiden ja ohjelmistojen kannalta, jotka maksupalveluntarjoaja tarjoaa maksupalvelunkäyttäjälle todennuskoodin luomiseksi/vastaanottamiseksi.

7.4 Testaussuunnitelman tulisi varmistaa, että testit

a) suoritetaan osana maksupalveluntarjoajan muodollista muutoksenhallintaprosessia niiden perusteellisuuden ja tehokkuuden varmistamiseksi;

b) ovat sellaisten riippumattomien testaajien toteuttamia, joilla on riittävät tiedot, taidot ja asiantuntemus maksupalvelujen turvatoimenpiteiden testaamisesta ja jotka eivät osallistu turvatoimenpiteiden kehittämiseen vastaaville maksupalveluille tai järjestelmille kuin testattavana on, ainakin viimeisten testien osalta ennen turvatoimenpiteiden käyttöönottoa; ja

c) sisältävät haavoittuvuustarkistukset ja penetraatiotestittestit, jotka ovat riittävät maksupalvelujen tunnistetun riskitason mukaan.

7.5 Maksupalveluntarjoajien tulisi suorittaa jatkuvia ja toistuvia turvatoimenpiteiden testejä maksupalveluilleen. Niiden järjestelmien osalta, jotka ovat kriittisiä maksupalvelujen tarjoamisen kannalta (kuten on kuvattu ohjeessa 3.2), testit tulisi suorittaa vähintään vuosittain. Ei-kriittiset järjestelmät tulisi testata riskiperusteisesti säännöllisin väliajoin, mutta vähintään kolmen vuoden välein.

7.6 Maksupalveluntarjoajien tulisi valvoa ja arvioida suoritettujen testien tuloksia ja päivittää turvatoimenpiteensä vastaavasti ja ilman tarpeetonta viivytystä kriittisten järjestelmien osalta.

Ohje 8: Tilannetietoisuus ja jatkuva oppiminen

Uhkakuvat ja tilannetietoisuus

8.1 Maksupalveluntarjoajien tulisi perustaa ja ottaa käyttöön prosesseja ja organisaatiorakenteita voidakseen tunnistaa ja valvoa jatkuvasti turvallisuus- ja operatiivisia uhkia, jotka voisivat vaikuttaa merkittävästi niiden kykyyn tarjota maksupalveluja.

8.2 Maksupalveluntarjoajien tulisi analysoida operatiivisia operatiivisia häiriöitä ja turvallisuushäiriöitä, jotka on tunnistettu tai joita on tapahtunut organisaation sisällä ja/tai ulkopuolella. Maksupalveluntarjoajien tulisi ottaa huomioon tärkeimpiä näistä analyyseista opittuja asioita ja päivittää turvatoimenpiteitä vastaavasti.

8.3 Maksupalveluntarjoajien tulisi seurata aktiivisesti tekniikan kehitystä varmistaakseen tietoisuutensa turvallisuusriskeistä.

Koulutus- ja turvallisuustietoisuusohjelmat

8.4 Maksupalveluntarjoajien tulisi laatia koulutusohjelma koko henkilöstölle varmistaakseen, että henkilöstö on koulutettu suorittamaan tehtävänsä ja vastuunsa asiaankuuluvien turvallisuuskäytäntöjen ja -menettelyjen mukaisesti, jolloin pienennetään inhimillisen virheen, varkauden, petoksen, väärinkäytön tai tappion vaaraa. Maksupalveluntarjoajien tulisi varmistaa, että koulutusohjelmassa tarjotaan koulutusta henkilöstön jäsenille vähintään vuosittain ja tarvittaessa useammin.

8.5 Maksupalveluntarjoajien olisi varmistettava, että tärkeimmissä tehtävissä toimivat, ohjeiden kohdan 3.1 mukaiset henkilöstön jäsenet saavat kohdennettua turvallisuuskoulutusta vuosittain tai tarvittaessa useammin.

8.6 Maksupalveluntarjoajien tulisi laatia ja ottaa käyttöön määräaikaisia turvallisuustietoisuusohjelmia henkilöstönsä kouluttamiseksi ja tietoturvaan liittyvien riskien käsittelemiseksi. Näiden ohjelmien tulisi edellyttää, että maksupalveluntarjoajan henkilöstö raportoi epätavanomaisista tapahtumista ja poikkeamista.

Ohje 9: Maksupalvelunkäyttäjään liittyvien suhteiden hallinta

Maksupalvelunkäyttäjän tietoisuus turvallisuusriskeistä ja riskinhallintatoimista

9.1 Maksupalveluntarjoajien tulisi laatia ja ottaa käyttöön prosessit, joilla parannetaan maksupalvelunkäyttäjien tietoisuutta maksupalveluihin liittyvistä turvallisuusriskeistä, tarjoamalla maksupalvelunkäyttäjille apua ja neuvontaa.

9.2 Maksupalvelunkäyttäjille tarjottu apu ja neuvonta tulisi päivittää uusien uhkien ja haavoittuvuuksien mukaan, ja muutoksista tulisi kertoa maksupalvelunkäyttäjälle.

9.3 Jos tuotteen ominaisuudet sallivat, maksupalveluntarjoajien tulisi mahdollistaa se, että maksupalvelunkäyttäjät voivat poistaa käytöstä tietyt maksupalveluntarjoajan maksupalvelunkäyttäjälle tarjoamiin maksupalveluihin liittyvät maksutoiminnot.

9.4 Jos maksupalveluntarjoaja on direktiivin (EU) 2015/2366 artiklan 68 kohdan 1 mukaisesti sopinut maksajan kanssa käyttörajoista tietyillä maksuvälineillätoteutettujen maksutapahtumien osalta, maksupalveluntarjoajan tulisi tarjota maksajalle mahdollisuus muokata näitä rajoja suurimpaan sovittuun rajaan asti.

9.5 Maksupalveluntarjoajien tulisi tarjota maksupalvelunkäyttäjille mahdollisuus saada hälytyksiä käynnistetyistä maksutapahtumista ja/tai maksutapahtumien epäonnistuneista käynnistysyrityksistä, jotta käyttäjät voisivat tunnistaa tiliensä petollisen tai haitallisen käytön.

9.6 Maksupalveluntarjoajien tulisi pitää maksupalvelunkäyttäjät ajan tasalla sellaisten turvatoimenpiteiden päivityksistä, jotka vaikuttavat maksupalvelunkäyttäjiin maksupalvelujen osalta.

9.7 Maksupalveluntarjoajien tulisi tarjota maksupalvelunkäyttäjille apua kaikissa kysymyksissä, tukipyynnöissä ja poikkeamailmoituksissa tai ongelmissa, jotka koskevat maksupalveluihin liittyviä turvallisuusasioita. Maksupalvelunkäyttäjille tulisi tiedottaa asianmukaisesti siitä, miten kyseistä apua saa.