EBA/GL/2017/17

12/01/2018

Suunised

direktiivi (EL) 2015/2366 (PSD2) alusel makseteenuste operatsiooni- ja turvariskide jaoks kasutatavate turvameetmete kohta

1. Järgimis- ja aruandluskohustus

Käesolevate suuniste staatus

1. Käesolev dokument sisaldab määruse (EL) nr 1093/2010[1] artikli 16 kohaselt väljastatud suuniseid. Määruse (EL) nr 1093/2010 artikli 16 lõike 3 kohaselt peavad pädevad asutused ja finantseerimisasutused võtma mis tahes meetmeid, et suuniseid järgida.

2. Suunistes esitatakse Euroopa Pangandusjärelevalve seisukoht nõuetekohase järelevalvetava kohta Euroopa Finantsjärelevalve Süsteemis, ehk kuidas tuleks liidu õigust konkreetses valdkonnas kohaldada. Suuniste adressaadiks olevad määruse (EL) nr 1093/2010 artikli 4 punktis 2 määratletud pädevad asutused peaksid suuniseid järgima, kaasates need sobival viisil oma järelevalvetavadesse (nt muutes oma õigusraamistikku või järelevalvemenetlusi) ka siis, kui suunised on mõeldud eelkõige finantseerimisasutustele.

Aruandluskohustus

3. Määruse (EL) nr 1093/2010 artikli 16 lõike 3 kohaselt peavad pädevad asutused teatama EBA-le 12.03.2018, kas nad järgivad või kavatsevad järgida kõnealuseid suuniseid, või vastasel juhul mittejärgimise põhjused. Kui selleks tähtajaks teadet ei saada, peab EBA pädevat asutust nõudeid mitte täitvaks. Teated tuleks saata EBA veebisaidil avaldatud vormil aadressil compliance@eba.europa.eu, märkides viite EBA/GL/2017/17. Teate peaksid saatma isikud, kes on asjakohaselt volitatud esitama oma pädeva asutuse nimel nõuete järgimise teateid. Nõuete järgimise staatuse mis tahes muutusest tuleb EBA-le teada anda.

4. Kooskõlas EBA määruse artikli 16 lõikega 3 avaldatakse teated Euroopa Pangandusjärelevalve veebilehel.

[1] Euroopa Parlamendi ja nõukogu määrus (EL) nr 1093/2010, 24. november 2010, millega asutatakse Euroopa Järelevalveasutus (Euroopa Pangandusjärelevalve), muudetakse otsust nr 716/2009/EÜ ning tunnistatakse kehtetuks komisjoni otsus 2009/78/EÜ (ELT L 331, 15.12.2010, lk 12).

2. Sisu, reguleerimisala ja mõisted

Sisu ja reguleerimisala

5. Käesolevad suunised lähtuvad EBA-le määruse (EL) nr 2015/2366[2] (PSD2) artikli 95 lõikes 3 antud volitustest.

6. Suunised sätestavad makseteenuse pakkujatele turvameetmete kehtestamise, rakendamise ja seire nõuded kooskõlas direktiivi (EL) 2015/2366 artikli 95 lõikega 1, et hallata operatsiooni- ja turvariske, mis on seotud nende pakutavate makseteenustega.

Adressaadid

7. Käesolevad suunised on adresseeritud makseteenuse pakkujatele, nagu on määratletud direktiivi (EL) 2015/2366 artikli 4 lõikes 11 ja nagu on viidatud finantseerimisasutuste määratluses määruse (EL) nr 1093/2010 artikli 4 lõikes 1, ning pädevatele asutustele, nagu on määratletud sama määruse artikli 4 lõike 2 punktis i viitega kehtetuks tunnistatud direktiivile 2007/64/EÜ[3] (praegu direktiiv (EL) 2015/2366[4]).

Mõisted

8. Kui ei ole sätestatud teisiti, on direktiivis (EL) 2015/2366 kasutatud ja määratletud mõistetel sama tähendus ka käesolevates suunistes. Peale selle kasutatakse käesolevates suunistes järgmisi mõisteid:

Juhtorgan	– Krediidiasutustest makseteenuse pakkujate jaoks on selle termini tähendus sama kui direktiivi 2013/36/EL[5] artikli 3 lõike 1 punkti 7 määratluses. – Makseasutustest või e-raha asutustest makseteenuse pakkujate jaoks tähendab see termin juhtkonda või teisi makseteenuse pakkuja juhtimise eest vastutavaid isikuid ja

[2] Euroopa Parlamendi ja nõukogu 25. novembri 2015. aasta direktiiv (EL) 2015/2366 makseteenuste kohta siseturul, direktiivide 2002/65/EÜ, 2009/110/EÜ ning 2013/36/EL ja määruse (EL) nr 1093/2010 muutmise ning direktiivi 2007/64/EÜ kehtetuks tunnistamise kohta (ELT L 337, 23.12.2015, lk 35).

[3] Euroopa Parlamendi ja nõukogu 13. novembri 2007. aasta direktiiv 2007/64/EÜ makseteenuste kohta siseturul ning direktiivide 97/7/EÜ, 2002/65/EÜ, 2005/60/EÜ ja 2006/48/EÜ muutmise ning direktiivi 97/5/EÜ kehtetuks tunnistamise kohta (ELT L 319, 5.12.2007, lk 1).

[4] Kooskõlas direktiivi (EL) 2015/2366 artikli 114 teise alalõiguga käsitatakse viiteid kehtetuks tunnistatud direktiivile 2007/64/EÜ viidetena direktiivile (EL) 2015/2366 ja loetakse vastavalt direktiivi (EL) 2015/2366 II lisas esitatud vastavustabelile.

[5] Euroopa Parlamendi ja nõukogu direktiiv 2013/36/EL, mis käsitleb krediidiasutuste tegevuse alustamise tingimusi ning krediidiasutuste ja investeerimisühingute usaldatavusnõuete täitmise järelevalvet, millega muudetakse direktiivi 2002/87/EÜ ning millega tunnistatakse kehtetuks direktiivid 2006/48/EÜ ja 2006/49/EÜ (ELT L 176, 27.6.2013, lk 338).

	(kui asjakohane) isikuid, kes vastutavad makseteenuse pakkuja juures makseteenustega seotud tegevuste eest. – Direktiivi (EL) 2015/2366 artikli 1 lõike 1 punktides c, e ja f nimetatud makseteenuse pakkujate jaoks on sellel terminil tähendus, mis omistatakse sellele kohalduva Euroopa Liidu või liikmesriigi õigusega.
Operatsiooniriski- või turvaintsident	Sündmus või mitu seotud sündmust, mida makseteenuse pakkuja ei ole kavandanud, mis kahjustavad või tõenäoliselt kahjustavad maksetega seotud teenuste terviklust, käideldavust, konfidentsiaalsust, autentsust ja/või talitluspidevust.
Kõrgem juhtkond	(a) Krediidiasutustest makseteenuse pakkujate jaoks on selle termini tähendus sama kui direktiivi 2013/36/EL artikli 3 lõike 1 punkti 9 määratluses. (b) Makseasutustest ja e-raha asutustest makseteenuse pakkujate jaoks tähendab see termin füüsilisi isikuid, kes täidavad asutuses juhtimiskohustusi ning kes vastutavad ja on aruandekohustuslikud juhtorgani ees makseteenuse pakkuja igapäevase juhtimise eest. (c) Direktiivi (EL) 2015/2366 artikli 1 lõike 1 punktides c, e ja f nimetatud makseteenuse pakkujate jaoks on sellel terminil tähendus, mis omistatakse sellele kohalduva Euroopa Liidu või liikmesriigi õigusega.
Turvarisk	Risk, mis tuleneb ebapiisavatest või mittetoimivatest siseprotsessidest või välissündmustest, millel on või võib olla kahjulik mõju info- ja sidetehnoloogia (IKT) süsteemide käideldavusele, terviklusele, konfidentsiaalsusele, autentsusele ja/või maksetega seotud teenuste talitluspidevusele. See hõlmab ka küberrünnakute ja ebapiisava füüsilise turbe riski.
Riskiisu	Nende riskide agregeeritud tase ja tüüp, mida asutus on kooskõlas oma ärimudeliga valmis riskitaluvusvõime piires võtma strateegiliste eesmärkide saavutamiseks.

3. Rakendamine

Kohaldamise alguskuupäev

9. Käesolevaid suuniseid kohaldatakse alates 13. jaanuarist 2018.

4. Suunised

Suunis 1: Üldpõhimõtted

1.1 Kõik makseteenuse pakkujad peaksid järgima kõiki nende suuniste sätteid. Täpsusaste peaks olema proportsionaalne makseteenuse pakkuja suuruse ja tema pakutavate või pakkuda kavatsetavate konkreetsete teenuste olemuse, ulatuse, keerukuse ja riskantsusega.

Suunis 2: Juhtimiskord

Operatsiooni- ja turvariskide juhtimisraamistik

2.1 Makseteenuse pakkujad peaksid kehtestama toimiva operatsiooni- ja turvariskide juhtimisraamistiku (edaspidi: riskijuhtimisraamistik), mille peaks kinnitama ja vähemalt kord aastas läbi vaatama juhtorgan ja (kui asjakohane) kõrgem juhtkond. Raamistik peaks keskenduma operatsiooni- ja turvariske maandavatele turvameetmetele ning see tuleks täielikult lõimida makseteenuse pakkuja üldistesse riskijuhtimisprotsessidesse.

2.2 Riskijuhtimisraamistik peaks:

a) sisaldama direktiivi (EL) 2015/2366 artikli 5 lõike 1 punktis j nimetatud üldist turvapoliitika dokumenti;

b) vastama makseteenuse pakkuja riskiisule;

c) määratlema ja omistama põhirollid ja vastutusalad ning asjakohased aruandlusahelad, mida on vaja turvameetmete jõustamiseks ning turva- ja operatsiooniriskide haldamiseks;

d) kehtestama vajalikud protseduurid ja süsteemid, et tuvastada, mõõta, seirata ja hallata riske, mis tulenevad makseteenuste pakkuja maksetega seotud tegevustest ning mis teda ohustavad, sealhulgas talitluspidevuse korraldus.

2.3 Makseteenuse pakkujad peaksid tagama, et riskijuhtimisraamistik dokumenteeritakse nõuetekohaselt ning seda ajakohastatakse raamistiku rakendamisel ja seirel dokumenteeritud kogemustega.

2.4 Makseteenuse pakkujad peaksid tagama, et enne taristu, protsesside ja protseduuride suuri muudatusi ning pärast iga olulist operatsiooniriski- või turvaintsidenti, mis kahjustab turvalisust või pakutavaid makseteenuseid, vaatavad nad üle, kas riskijuhtimisraamistikku on vaja kohe muuta või täiustada.

Riskijuhtimis- ja -kontrollimudelid

2.5 Makseteenuse pakkujad peaksid operatsiooni- ja turvariskide juhtimiseks kehtestama kolm tõhusat kaitseliini või samaväärse sisese riskijuhtimise- ja -kontrollimudeli. Makseteenuse pakkujad peaksid tagama, et nimetatud sisekontrollimudelil oleks piisav jõud, sõltumatus, vahendid ja otsesed aruandlusahelad juhtorganiga ja (kui asjakohane) kõrgema juhtkonnaga.

2.6 Käesolevates suunistes kehtestatud turvameetmeid peaksid auditeerima audiitorid, kel on pädevus IT-turbe ja maksete valdkondades ning kes on oma tegevuses makseteenuse pakkuja siseselt või sellest väljaspool sõltumatud. Selliste auditite sagedus ja fookus peaks arvestama vastavaid turvariske.

Tegevuse edasiandmine

2.7 Makseteenuse pakkujad peaksid tagama käesolevates suunistes kehtestatud turvameetmete rakendamise makseteenusega, sealhulgas IT-süsteemidega, seotud tegevuse edasiandmisel.

2.8 Makseteenuse pakkujad peaksid tagama, et lepingud ja teenustaseme kokkulepped, mis on sõlmitud neid ülesandeid täitvate allhankijatega, kirjeldaksid asjakohaseid ja proportsionaalseid turvaeesmärke, meetmeid ja tulemuseesmärke. Makseteenuse pakkujad peaksid jälgima ja veenduma, kuidas ja mis tasemel järgivad sellised teenusepakkujad neid turvaeesmärke, meetmeid ja tulemuseesmärke.

Suunis 3: Riski kaalutlemine

Toimingute, protsesside ja varade tuvastamine

3.1 Makseteenuse pakkujad peaksid tuvastama oma äritoimingud, põhirollid ja tugiprotsessid, koostama nende loetelu ja seda regulaarselt uuendama, et kaardistada iga toimingu, rolli ja tugiprotsessi olulisus ning operatsiooni- ja turvariskidega seotud vastastikused sõltuvused.

3.2 Makseteenuse pakkujad peaksid tuvastama oma infovarad, koostama nende loetelu ja seda regulaarselt uuendama, näiteks IKT-süsteemide, nende konfiguratsioonide, muu taristu ja nende vastastikuste seoste kohta muude sise- ja välissüsteemidega, et hallata varasid, mis toetavad nende kriitilise tähtsusega äritoiminguid- ja protsesse.

Toimingute, protsesside ja varade liigitamine

3.3 Makseteenuse pakkujad peaksid liigitama tuvastatud äritoimingud, tugiprotsessid ja infovarad nende kriitilisuse järgi.

Toimingute, protsesside ja varade riski kaalutlemine

3.4 Makseteenuse pakkujad peaksid tagama ohtude ja nõrkuste pideva seire ning regulaarselt läbi vaatama riskistsenaariumid, mis mõjutavad nende äritoiminguid, kriitilise tähtsusega protsesse ja infovarasid. Osana kohustusest teha ja pädevatele asutustele esitada ajakohastatud ja põhjalik hinnang nende osutatavate makseteenustega seotud operatsiooni- ja turvariskide ning neile

riskidele reageerimiseks nende poolt rakendatavate leevendusmeetmete ja kontrollimehhanismide piisavuse kohta, nagu on sätestatud direktiivi (EL) 2015/2366 artikli 95 lõikes 2, peaksid makseteenuse pakkujad vähemalt kord aastas või pädeva asutuse nõudmisel sagedamini kaalutlema ja dokumenteerima tuvastatud ja liigitatud toimingute, protsesside ja infovarade riskid, et tuvastada ja hinnata peamisi operatsiooni- ja turvariske. Selliseid riski kaalutlemisi tuleks teha ka enne kõiki makseteenuste turvalisust mõjutavaid taristu, protsesside või protseduuride suuri muudatusi.

3.5 Riski kaalutlemise alusel peaksid makseteenuse pakkujad määrama, kas ja mis ulatuses võib olla vaja muuta olemasolevaid turvameetmeid, kasutatavaid tehnoloogiaid ja protseduure ning pakutavaid makseteenuseid. Makseteenuse pakkujad peaksid arvestama ajaga, mis kulub muudatuste rakendamiseks, ning ajaga, mis kulub asjakohaste ajutiste turvameetmete rakendamiseks, et minimeerida operatsiooniriski- ja turvaintsidente, pettusi ja makseteenuste pakkumise võimalikke katkestusi.

Suunis 4: Kaitse

4.1 Makseteenuse pakkujad peaksid kehtestama ja rakendama tuvastatud operatsiooni- ja turvariskide vastu ennetavad turvameetmed. Meetmed peaksid vastavalt tuvastatud riskidele tagama piisava turbetaseme.

4.2 Makseteenuse pakkujatel peaks olema kehtestatud ja rakendatud mitmekihiline kaitse, kus inimesi, protsesse ja tehnoloogiaid kontrollitakse mitmel tasemel ning iga tase toimib eelmiste tasemete turvameetmena. Mitmekihiline kaitse tähendab, et sellel on sama riski jaoks mitu kontrollimeedet, näiteks nelja silma põhimõte, kaksikautentimine, võrgu segmentimine ja mitu tulemüüri.

4.3 Makseteenuse pakkujad peaksid tagama oma kriitilise tähtsusega loogiliste ja füüsiliste varade, vahendite ja makseteenuse kasutajate tundlike makseandmete konfidentsiaalsuse, tervikluse ja käideldavuse nii nende säilitamisel, edastamisel kui ka kasutamisel. Kui andmete hulgas on isikuandmeid, tuleks selliseid meetmeid rakendada kooskõlas määrusega (EL) 2016/679[6] või (kui asjakohane) määrusega (EÜ) 45/2001[7].

4.4 Makseteenuse pakkujad peaksid pidevalt jälgima, kas nende tegevuskeskkonna muutused mõjutavad olemasolevaid turvameetmeid või on kaasneva riski maandamiseks vaja täiendavaid meetmeid. Need muutused peaksid olema osa makseteenuse pakkuja ametlikust muudatuste halduse menetlusest, millega tagatakse, et kõiki muudatusi kavandatakse, testitakse, dokumenteeritakse ja volitatakse nõuetekohaselt. Leitud turvaohtude ja tehtud muudatuste põhjal tuleks teha testimine, milles kasutatakse ka asjakohaste ja teadaolevate potentsiaalsete rünnete stsenaariume.

[6] Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) (ELT L 119, 4.5.2016, lk 1).

[7] Euroopa Parlamendi ja nõukogu 18. detsembri 2000. aasta määrus (EÜ) nr 45/2001 üksikisikute kaitse kohta isikuandmete töötlemisel ühenduse institutsioonides ja asutustes ning selliste andmete vaba liikumise kohta (EÜT L 8, 12.1.2001, lk 1).

4.5 Makseteenuse pakkujad peaksid makseteenuste kavandamisel, arendamisel ja pakkumisel tagama ülesannete lahususe ja minimaalõiguste printsiibi rakendamise. Makseteenuse pakkujad peaksid erilist tähelepanu pöörama IT-keskkondade lahususele, eriti seoses arendus-, testi- ja tootmiskeskkondadega.

Andmete ja süsteemide terviklus ja konfidentsiaalsus

4.6 Makseteenuse pakkujad peaksid makseteenuste kavandamisel, arendamisel ja pakkumisel tagama, et makseteenuse kasutajate tundlike makseandmete kogumine, edastamine, töötlemine, säilitamine ja/või arhiveerimine ning visualiseerimine oleks piisav, asjakohane ja piiratud sellega, mida on vaja makseteenuste pakkumiseks.

4.7 Makseteenuse pakkujad peaksid regulaarselt kontrollima, et makseteenuste osutamise tarkvara, sealhulgas kasutajate maksetega seotud tarkvara, oleks ajakohane ning kriitilise tähtsusega turvaparandused oleksid tehtud. Makseteenuse pakkujad peaksid tagama terviklust kontrollivate mehhanismide rakendamise, millega tagatakse tarkvara ja püsivara ning makseteenuste teabe terviklus.

Füüsiline turvalisus

4.8 Makseteenuste pakkujad peaksid rakendama sobivaid füüsilise turvalisuse meetmeid, eelkõige selleks, et kaitsta makseteenuse kasutajate tundlikku makseteavet ning makseteenuse pakkumise IKT-süsteeme.

Pääsu reguleerimine

4.9 Füüsiline ja loogiline juurdepääs IKT-süsteemidele peaks olema lubatud ainult volitatud isikutele. Volitused peaksid olema määratud töötajate ülesannete ja kohustuste järgi ning piirnema isikutega, kellel on asjakohane väljaõpe ja kelle üle on tagatud seire. Makseteenuse pakkujad peaksid kehtestama meetmed, millega selline juurdepääs IKT-süsteemidele piirneks kindlalt isikutega, kellel on õigustatud ärivajadus. Rakenduste elektrooniline juurdepääs andmetele ja süsteemidele peaks olema piiratud miinimumini, mida on vaja asjakohase teenuse osutamiseks.

4.10 Makseteenuse pakkujad peaksid rangelt kontrollima administraatori õigustes juurdepääsu süsteemile, piirates rangelt ja jälgides hoolikalt töötajaid, kellel on süsteemile suuremad juurdepääsuõigused. Rakendada tuleks meetmeid, näiteks rollipõhist juurdepääsu, administraatorite süsteemitoimingute logimist ja ülevaatamist, tugevat autentimist ja anomaaliate seiret. Makseteenuse pakkujad peaksid haldama juurdepääsuõigusi infovarale ja nende tugisüsteemidele teadmisvajaduse põhiselt. Juurdepääsuõigused tuleks perioodiliselt üle vaadata.

4.11 Juurdepääsulogide säilitusaeg peaks olenema tuvastatud äritoimingute, tugiprotsesside ja infovarade kriitilisusest, kooskõlas suunistega GL 3.1 ja GL 3.2, ilma et see piiraks Euroopa Liidu ja riiklikus õiguses sätestatud säilitamisnõuete kohaldamist. Makseteenuse pakkujad peaksid selle

teabega toetama makseteenuse pakkumisel tuvastatud anomaalsete tegevuste tuvastamist ja uurimist.

4.12 Turvalise side tagamiseks ja riski vähendamiseks tuleks halduslik kaugjuurdepääs kriitilise tähtsusega IKT-komponentidele anda ainult teadmisvajaduse põhjal ja tugevate autentimislahenduste kasutamisel.

4.13 Pääsukontrolli protsessidega seotud toodete, vahendite ja protseduuride kasutamine peaks kaitsma pääsukontrolli protsesse rikkumise või eiramise eest. See hõlmab vastavate toodete, vahendite ja protseduuride identifitseerimist, väljastamist, tühistamist ja tagasivõtmist.

Suunis 5: Tuvastus

Pidev seire ja tuvastus

5.1 Makseteenuse pakkujad peaksid kehtestama ja rakendama äritoimingute, tugiprotsesside ja infovarade pideva seire protsessid ja võimekuse, et tuvastada anomaalsed tegevused makseteenuste pakkumisel. Pideva seire osana peaks makseteenuse pakkujatel olema asjakohane ja efektiivne võimekus tuvastada füüsilist või loogilist sissetungi ning makseteenuse pakkumise infovarade konfidentsiaalsuse, tervikluse ja käideldavuse rikkumisi.

5.2 Pideva seire ja tuvastuse protsessid peaksid katma:

a) asjakohaseid sise- ja välistegureid, sealhulgas äri- ja IKT-haldustoiminguid;

b) tehinguid, et tuvastada juurdepääsu kuritarvitamist teenuseosutajate või muude asutuste poolt; ja

c) võimalikke sise- ja välisohte.

5.3 Makseteenuse pakkujad peaksid rakendama tuvastusmeetmeid, et tuvastada võimalikud infolekked, ründekoodi ja muud turvaohud ning avalikult teadaolevad tarkvara ja riistvara nõrkused, ning kontrollima vastavate uute turvauuenduste olemasolu.

Operatsiooniriski- või turvaintsidentide seire ja teavitamine

5.4 Makseteenuse pakkujad peaksid määratlema asjakohased kriteeriumid ja läved, et liigitada sündmused operatsiooniriski- või turvaintsidendiks, nagu on sätestatud suuniste mõistete osas, samuti eelhoiatuse indikaatorid, mis peaksid toimima makseteenuse pakkuja jaoks hoiatusteatena, et operatsiooniriski- või turvaintsidente saaks aegsasti tuvastada.

5.5 Makseteenuse pakkujad peaksid kehtestama asjakohased protsessid ja organisatsioonilised struktuurid, et tagada operatsiooniriski- ja turvaintsidentide pidev ja lõimitud seire, käsitlemine ja järeltoimingud.

5.6 Makseteenuse pakkujad peaksid kehtestama operatsiooniriski- ja turvaintsidentide ning turvalisusega seotud kliendikaebuste kõrgemale juhtkonnale teatamise protseduuri.

Suunis 6: Talitluspidevus

6.1 Makseteenuse pakkujad peaksid kehtestama nõuetekohase talitluspidevuse halduse protsessi, et maksimeerida suutlikkust pakkuda makseteenuseid pidevalt ja piirata kahjusid tõsise tegevuse katkestuse korral.

6.2 Talitluspidevuse nõuetekohaseks juhtimiseks peaks makseteenuse pakkuja hoolikalt analüüsima tõsiste tegevuse katkestuste riske ning hindama (kvantitatiivselt ja kvalitatiivselt) nende võimalikku mõju, kasutades asutusesiseseid ja/või -väliseid andmeid ja stsenaariumide analüüsi. Tuvastatud ja liigitatud kriitilise tähtsusega toimingute, protsesside, süsteemide, tehingute ja vastastikuste sõltuvuste alusel peaksid makseteenuse pakkujad kooskõlas suunistega GL 3.1–GL 3.3 prioriseerima talitluspidevuse toimingud riskipõhiselt, mille aluseks võivad olla suunise osa GL 3 kohaselt tehtud riski kaalutlused. Olenevalt makseteenuse pakkuja ärimudelist võib see toetada näiteks kriitilise tähtsusega tehingute edasist töötlemist katkestuse kõrvaldamise ajal.

6.3 Suunise GL 6.2 alusel tehtud analüüsi põhjal peaks makseteenuse pakkuja kehtestama:

a) talitluspidevuse plaanid, et tagada asjakohane reaktsioon hädaolukordadele ja suutlikkus jätkata kriitilise tähtsusega äritegevust; ning

b) leevendavad meetmed, mis tuleks rakendada oma makseteenuste pakkumise lõpetamise ja olemasolevate lepingute lõpetamise korral, et vältida kahjulikku mõju maksesüsteemile ja makseteenuse kasutajatele ning tagada ootel maksetehingute täitmine.

Talitluspidevuse stsenaariumipõhine kavandamine

6.4 Makseteenuse pakkuja peaks arvestama paljude eri stsenaariumidega, sealhulgas äärmuslike, kuid usutavate stsenaariumidega, mis võivad tema puhul esineda, ning hindama nende võimalikku mõju.

6.5 Suunise GL 6.2 alusel tehtud analüüsi ja suunise GL 6.4 alusel tuvastatud usutavate stsenaariumide põhjal peaks makseteenuse pakkuja välja töötama reageerimis- ja taasteplaani, mis:

a) peaks keskenduma kriitilise tähtsusega toimingute, protsesside, süsteemide, tehingute ja vastastikuste sõltuvuste toimivuse mõjule;

b) tuleks dokumenteerida ning teha äri- ja tugiüksustele teatavaks ja kergesti kättesaadavaks hädaolukorras; ning

c) tuleks ajakohastada testide käigus saadud kogemuste, uute tuvastatud riskide ja ohtude ning muudetud taastamiseesmärkide ja prioriteetide järgi.

Talitluspidevuse plaanide testimine

6.6 Makseteenuse pakkujad peaksid testima oma talitluspidevuse plaane ning tagama, et nende kriitilise tähtsusega toimingute, protsesside, süsteemide, tehingute ja vastastikuste sõltuvuste

toimivust testitakse vähemalt kord aastas. Plaanid peaksid toetama eesmärke kaitsta ja vajaduse korral taastada operatsioonide terviklus ja käideldavus ning infovarade konfidentsiaalsus.

6.7 Plaane tuleks ajakohastada vähemalt kord aastas testitulemuste, ajakohase ohuluureteabe, jagatud teabe ja eelmistest juhtumitest saadud kogemuste alusel, samuti arvestades taastamiseesmärkide muutumist ning tegevuse seisukohast ja tehniliselt usutavate veel toimumata stsenaariumide analüüsi ning (kui asjakohane) pärast süsteemide ja protsesside muudatusi. Makseteenuse pakkujad peaksid talitluspidevuse plaanide väljatöötamisel konsulteerima ja koordineerima asjakohaste siseste ja väliste huvipooltega.

6.8 Talitluspidevuse plaanide testimine makseteenuse pakkujate poolt peaks:

a) sisaldama adekvaatset stsenaariumide kogumit, nagu on mainitud suunises GL 6.4;

b) olema ette nähtud kontrollima talitluspidevuse plaanide aluseeldusi, sealhulgas juhtimiskorraldust ja kriisikommunikatsiooni plaane; ning

c) sisaldama protseduure, millega kontrollitakse töötajate ja protsesside võimet nimetatud stsenaariumidele asjakohaselt reageerida.

6.9 Makseteenuse pakkujad peaksid regulaarselt jälgima oma talitluspidevuse plaanide tõhusust ning dokumenteerima ja analüüsima kõik testide käigus ilmnenud probleemid ja puudused.

Kriisikommunikatsioon

6.10 Tegevuste katkestuse korral või hädaolukorras ning talitluspidevuse plaanide rakendamisel peaksid makseteenuse pakkujad tagama, et neil oleksid olemas tõhusad kriisikommunikatsiooni meetmed, et kõik sisesed ja välised huvipooled, sealhulgas välised teenuseosutajad, saaksid teavet õigeaegselt ja asjakohasel viisil.

Suunis 7: Turvameetmete testimine

7.1 Makseteenuse pakkujad peaksid kehtestama ja rakendama testimisraamistiku, millega valideeritakse turvameetmete stabiilsus ja tõhusus, ning tagama, et testimisraamistik oleks kohandatud arvestama riskide seirel tuvastatud uusi ohte ja nõrkusi.

7.2 Makseteenuse pakkujad peaksid tagama, et testid tehtaks taristu, protsesside või protseduuride muutmisel ning siis, kui muudatused on tehtud tõsiste operatsiooniriski- või turvaintsidentide tõttu.

7.3 Testimisraamistik peaks hõlmama ka järgmiste vahendite turvameetmeid: i) makseteenuse pakkumise makseterminalid ja seadmed, ii) makseteenuse kasutaja autentimise makseterminalid ja seadmed ning iii) makseteenuse pakkuja poolt makseteenuse kasutajale autentimiskoodi genereerimiseks/saamiseks antavad seadmed ja tarkvara.

7.4 Testimisraamistik peaks tagama, et

a) testimine oleks makseteenuse pakkuja ametliku muudatuste halduse protsessi osa, et tagada katsete stabiilsus ja tõhusus;

b) teste teeksid sõltumatud testijad, kellel on piisavad teadmised, oskused ja asjatundlikkus makseteenuste turvameetmete testimise valdkonnas, ning kes ei ole seotud testitavate makseteenuste või -süsteemide turvameetmete arendamisega, vähemalt lõplike testide korral enne turvameetmete kasutusele võtmist; ning

c) sisaldavad nõrkuste uuringuid ja läbistustestimist, mis on makseteenuse tuvastatud ohutaseme jaoks piisavad ja asjakohased.

7.5 Makseteenuse pakkujad peaksid testima makseteenuse turvameetmeid pidevalt ja korduvalt. Makseteenuse pakkumiseks kriitilise tähtsusega süsteeme (nagu on kirjeldatud suunises GL 3.2) tuleks testida vähemalt kord aastas. Muid kui kriitilise tähtsusega süsteeme tuleks testida regulaarselt ja riskipõhiselt, kuid vähemalt kord kolme aasta jooksul.

7.6 Makseteenuse pakkujad peaksid jälgima ja hindama testide tulemusi ning ajakohastama nende järgi turvameetmeid, kriitilise tähtsusega süsteemide korral kohe.

Suunis 8: Olukorrateadlikkus ja pidev õppimine

Ohtude spekter ja olukorrateadlikkus

8.1 Makseteenuse pakkujad peaksid kehtestama ja rakendama protsesse ja organisatsioonilisi struktuure, et tuvastada ja pidevalt jälgida turva- ja operatsiooniohte, mis võivad oluliselt kahjustada nende võimet pakkuda makseteenuseid.

8.2 Makseteenuse pakkujad peaksid analüüsima operatsiooniriski- ja turvaintsidente, mis on tuvastatud või toimunud organisatsiooni sees ja/või mujal. Makseteenuse pakkujad peaksid arvestama nendest analüüsidest saadud olulisi kogemusi ja ajakohastama nende järgi turvameetmeid.

8.3 Makseteenuse pakkujad peaksid aktiivselt jälgima tehnika arengut ja tagama, et nad teadvustavad turvariske.

Koolitus ja turvateadlikkuse programmid

8.4 Makseteenuse pakkujad peaksid kehtestama koolitusprogrammi kõigile töötajaile, tagamaks, et nad kõik on saanud väljaõppe oma ülesannete ja kohustuste täitmiseks vastavalt asjakohastele turvaeeskirjadele ja -protseduuridele, et vähendada inimlikke eksimusi, vargusi, pettusi, väärkasutamist või kahju. Makseteenuse pakkujad peaksid tagama, et koolitusprogramm pakub töötajatele väljaõpet vähemalt kord aastas ning vajaduse korral sagedamini.

8.5 Makseteenuse pakkujad peaksid tagama, et töötajad, kellel on suunises GL 3.1 määratletud võtmerollid, saavad sihipärast infoturbe koolitust kord aastas või vajaduse korral sagedamini.

8.6 Makseteenuse pakkujad peaksid kehtestama ja rakendama regulaarsed turvateadlikkuse programmid, et koolitada töötajaid ja käsitleda infoturbe riske. Need programmid peaksid nõudma, et makseteenuse pakkuja töötajad teatavad ebatavalisest tegevusest ja intsidentidest.

Suunis 9: Makseteenuse kasutajate suhtehaldus

Makseteenuse kasutaja teadlikkus turvariskidest ja riski leevendamisest

9.1 Makseteenuse pakkujad peaksid kehtestama ja rakendama protsessid, millega teadvustatakse makseteenuse kasutajatele makseteenuste turvariske, pakkudes makseteenuse kasutajatele abi ja suuniseid.

9.2 Makseteenuse kasutajatele pakutavad abi ja suunised tuleks uute ohtude ja nõrkuste suhtes ajakohastada ning muudatustest tuleks makseteenuse kasutajat teavitada.

9.3 Kui toote funktsionaalsus võimaldab, peaksid makseteenuse pakkujad võimaldama makseteenuse kasutajatel välja lülitada teatud maksetoiminguid, mis on seotud makseteenuse pakkuja poolt makseteenuse kasutajale pakutavate makseteenustega.

9.4 Kui makseteenuse pakkuja on direktiivi (EL) 2015/2366 artikli 68 lõike 1 kohaselt nõustunud maksja kulutuste limiidiga konkreetsete makseinstrumentide kaudu täidetavate maksetehingute korral, peaks ta andma maksjale võimaluse suurendada limiite kuni maksimaalse kokkulepitud limiidini.

9.5 Makseteenuse pakkujad peaksid pakkuma makseteenuse kasutajale võimalust saada hoiatusteateid maksetehingute alustamise ja/või ebaõnnestunud alustamiskatsete kohta, et nad saaksid tuvastada oma konto petturlikku või pahatahtlikku kasutamist.

9.6 Makseteenuse pakkujad peaksid teatama makseteenuse kasutajaile selliste turvaprotseduuride uuendustest, mis mõjutavad makseteenuse kasutajaid seoses makseteenuse pakkumisega.

9.7 Makseteenuse pakkujad peaksid andma makseteenuse kasutajatele abi kõigi küsimuste, abipalvete ja anomaaliateadete või makseteenuse turvaprobleemide korral. Makseteenuse kasutajatele tuleks asjakohaselt teatada, kuidas sellist abi saada.