EBA/GL/2017/17

12/01/2018

Pamatnostādnes

par drošības pasākumiem attiecībā uz maksājumu pakalpojumu operacionālajiem un drošības riskiem saskaņā ar Direktīvu (ES) 2015/2366 (MPD 2)

1. Atbilstības un ziņošanas prasības

Pamatnostādņu statuss

1. Šis dokuments ietver pamatnostādnes, kas izdotas saskaņā ar Regulas (EK) Nr. 1093/2010 16. pantu[1]. Kompetentajām iestādēm un finanšu iestādēm saskaņā ar Regulas (EK) Nr. 1093/2010 16. panta 3. punktu jādara viss iespējamais, lai ievērotu šīs pamatnostādnes.

2. Pamatnostādnēs izklāstīts EBI skatījums uz atbilstošām uzraudzības praksēm Eiropas Finanšu uzraudzības sistēmā jeb par to, kā konkrētā jomā jāpiemēro Savienības tiesību akti. Kompetentajām iestādēm, kas minētas Regulas (ES) Nr. 1093/2010 4.panta 2.punktā, uz kurām attiecas šīs pamatnostādnes, tās būtu jāievēro, iekļaujot tās attiecīgi savā praksē (piemēram, veicot grozījumus savā tiesiskajā regulējumā vai uzraudzības procesos), tostarp gadījumos, ja pamatnostādnes ir paredzētas, galvenokārt, iestādēm.

Ziņošanas prasības

3. Saskaņā ar Regulas (ES) Nr. 1093/2010 16. panta 3. punktu kompetentajām iestādēm līdz 12.03.2018 jāpaziņo EBI, vai tās ievēro vai paredz ievērot šīs pamatnostādnes, vai jānorāda to neievērošanas iemesli. Ja šajā termiņā nebūs saņemts šāds paziņojums, EBI uzskatīs, ka kompetentās iestādes šos ieteikumus neievēro. Paziņojumi jāiesniedz, nosūtot EBI tīmekļa vietnē pieejamo veidlapu uz e-pasta adresi compliance@eba.europa.eu ar norādi „EBA/GL/2017/17”. Paziņojumus nosūta personas, kas ir pilnvarotas kompetento iestāžu vārdā ziņot par prasību izpildi. Par jebkurām izmaiņām atbilstības statusā arī ir jāziņo EBI.

4. Paziņojumus publicēs EBI tīmekļa vietnē saskaņā ar 16. panta 3. punktu.

[1] Ar Eiropas Parlamenta un Padomes Regulu (ES) Nr. 1093/2010 (2010. gada 24. novembris), ar ko izveido Eiropas Uzraudzības iestādi (Eiropas Banku iestādi), tiek grozīts Lēmums Nr. 716/2009/EK un atcelts Komisijas Lēmums 2009/78/EK (OV L331, 15.12.2010., 12.lpp).

2. Priekšmets, darbības joma un definīcijas

Priekšmets un darbības joma

5. Šīs pamatnostādnes izriet no pilnvarām, kas EBI piešķirtas saskaņā ar Direktīvas (ES) 2015/2366[2] (MPD 2) 95. panta 3. punktu.

6. Šajās pamatnostādnēs norādītas prasības tādu drošības pasākumu noteikšanai, īstenošanai un uzraudzībai, kas maksājumu pakalpojumu sniedzējiem (MPS) ir jāveic saskaņā ar Direktīvas (ES) 2015/2366 95. panta 1. punktu, lai pārvaldītu operacionālos un drošības riskus, kas saistīti ar to sniegtajiem maksājumu pakalpojumiem.

Adresāti

7. Šīs pamatnostādnes ir adresētas maksājumu pakalpojumu sniedzējiem (MPS), kā noteikts Direktīvas (ES) 2015/2366 4. panta 11. punktā un minēts Regulas (ES) 1093/2010 4. panta 1. punktā sniegtajā "finanšu iestāžu" definīcijā, un kompetentajām iestādēm (KI), kā noteikts šīs regulas 4. panta 2. punkta i) apakšpunktā, izmantojot atsauci uz atcelto Direktīvu 2007/64/EK[3] (pašreizējā Direktīva (ES) 2015/2366[4]).

Definīcijas

8. Ja nav norādīts citādi, terminiem, kas lietoti un definēti Direktīvā (ES) 2015/2366, ir tāda pati nozīme arī šajās pamatnostādnēs. Šajās pamatnostādnēs papildus tiek piemērotas turpmāk sniegtās definīcijas:

[2] Eiropas Parlamenta un Padomes 2015. gada 25. novembra Direktīva (ES) 2015/2366 par maksājumu pakalpojumiem iekšējā tirgū, ar ko groza Direktīvas 2002/65/EK, 2009/110/EK un 2013/36/ES un Regulu (ES) Nr. 1093/2010 un atceļ Direktīvu 2007/64/EK (OV L 337, 23.12.2015., 35. lpp.).

[3] Eiropas Parlamenta un Padomes 2007. gada 13. novembra Direktīva 2007/64/EK par maksājumu pakalpojumiem iekšējā tirgū, ar ko groza Direktīvas 97/7/EK, 2002/65/EK, 2005/60/EK un 2006/48/EK un atceļ Direktīvu 97/5/EK (OV L 319, 5.12.2007., 1. lpp.).

[4] Saskaņā ar Direktīvas (ES) 2015/2366 114. panta otro daļu atsauces uz atcelto Direktīvu 2007/64/EK uzskata par atsaucēm uz Direktīvu (ES) 2015/2366, un tās lasa saskaņā ar atbilstības tabulu Direktīvas (ES) 2015/2366 II pielikumā.

Vadības struktūra	– Attiecībā uz tādiem MPS, kuri ir kredītiestādes, šā termina nozīme ir atbilstīga Direktīvas 2013/36/ES 3. panta 1. punkta 7. apakšpunktā sniegtajai definīcijai[5]; – Attiecībā uz MPS, kuri ir maksājumu iestādes vai elektroniskās naudas iestādes, šis termins nozīmē direktorus vai personas, kas ir atbildīgas par MPS vadību, un attiecīgos gadījumos — personas, kas ir atbildīgas par MPS maksājumu pakalpojumu darbību vadību; – Attiecībā uz Direktīvas (ES) 2015/2366 1. panta 1. punkta c), e) un f) apakšpunktā minētajiem MPS šim terminam ir tāda nozīme, kāda tam piešķirta piemērojamajos ES un valsts tiesību aktos.
Operacionālais vai drošības incidents	Vienreizējs notikums vai vairāki saistīti notikumi, kurus MPS nav plānojis un kuri negatīvi ietekmē vai, iespējams, ietekmēs ar maksājumiem saistīto pakalpojumu integritāti, pieejamību, konfidencialitāti, autentiskumu un/vai nepārtrauktību.
Augstākā vadība	(a) Attiecībā uz tādiem MPS, kuri ir kredītiestādes, šā termina nozīme atbilst Direktīvas 2013/36/ES 3. panta 1. punkta 9. apakšpunktā sniegtajai definīcijai; (b) Attiecībā uz MPS, kas ir maksājumu iestādes vai elektroniskās naudas iestādes, šis termins nozīmē tās fiziskās personas, kuras iestādē veic izpildfunkcijas un ir atbildīgas un pārskatatbildīgas vadības struktūrai par MPS ikdienas pārvaldību; (c) Attiecībā uz Direktīvas (ES) 2015/2366 1. panta 1. punkta c), e) un f) apakšpunktā minētajiem MPS šim terminam ir tāda nozīme, kāda tam piešķirta piemērojamajos ES un valsts tiesību aktos.
Drošības risks	Risks, ko izraisa neatbilstīgi vai nepilnvērtīgi iekšējie procesi vai ārējie notikumi, kuri negatīvi ietekmē vai var negatīvi ietekmēt maksājumu pakalpojumu sniegšanai izmantoto informācijas un komunikācijas tehnoloģiju (IKT) sistēmu un/vai informācijas pieejamību, integritāti, konfidencialitāti. Tas ietver kiberuzbrukumu vai nepiemērotas fiziskās drošības risku.
Vēlme uzņemties risku	Tāda riska kopējais līmenis un veidi, ko iestāde saskaņā ar tās darbības modeli vēlas uzņemties savas riska spējas darījumdarbības jomā, lai sasniegtu savus stratēģiskos mērķus.

[5] Eiropas Parlamenta un Padomes Direktīva 2013/36/ES par piekļuvi kredītiestāžu darbībai un kredītiestāžu un ieguldījumu brokeru sabiedrību prudenciālo uzraudzību, ar ko groza Direktīvu 2002/87/EK un atceļ Direktīvas 2006/48/EK un 2006/49/EK (OV L 176, 27.6.2013., 338. lpp.).

3. Īstenošana

Piemērošanas datums

9. Šīs pamatnostādnes tiek piemērotas no 2018. gada 13. janvāra.

4. Pamatnostādnes

1. pamatnostādne: Vispārējais princips

1.1 Visiem MPS jāatbilst visiem noteikumiem, kas izklāstīti šajās pamatnostādnēs. Detalizācijas pakāpei jābūt samērīgai ar MPS lielumu un ar tādu konkrēto pakalpojumu veidu, jomu, sarežģītību un riska pakāpi, kurus sniedz vai plāno sniegt attiecīgais MPS.

2. pamatnostādne: Pārvaldība

Operacionālo un drošības risku pārvaldības sistēma

2.1 MPS būtu jāizveido efektīva operacionālo un drošības risku pārvaldības sistēma (turpmāk "risku pārvaldības sistēma"), kura vismaz reizi gadā jāapstiprina un jāpārskata vadības struktūrai un attiecīgos gadījumos — augstākajai vadībai. Šai sistēmai būtu jākoncentrējas uz drošības pasākumiem operacionālo un drošības risku mazināšanai un jābūt pilnībā integrētai kopējos MPS risku pārvaldības procesos.

2.2 Risku pārvaldības sistēmai būtu:

a) jāietver visaptverošs drošības politikas dokuments, kas minēts Direktīvas (ES) 2015/2366 5. panta 1. punkta j) apakšpunktā;

b) jābūt saskaņotai ar MPS vēlmi uzņemties risku;

c) jānosaka un jāpiešķir galvenie uzdevumi un pienākumi, kā arī attiecīga ziņojumu sniegšanas kārtība, kas vajadzīga, lai īstenotu drošības pasākumus un pārvaldītu drošības un operacionālos riskus;

d) jāizveido nepieciešamās procedūras un sistēmas, kas paredzētas, lai noteiktu, novērtētu, uzraudzītu un pārvaldītu tādu risku diapazonu, kurus izraisa ar maksājumiem saistītas MPS darbības un kuriem MPS ir pakļauts, ietverot darbības nepārtrauktības kārtību.

2.3 MPS būtu jānodrošina, ka risku pārvaldības sistēma tiek pareizi dokumentēta un informācija tiek atjaunināta, izmantojot dokumentētas "gūtās atziņas", kas uzkrātas sistēmas īstenošanas un uzraudzības gaitā.

2.4 Maksājumu pakalpojumu sniedzējiem būtu jānodrošina, ka pirms būtiskām infrastruktūras, procesu vai procedūru izmaiņām un pēc katra būtiska operacionālā vai drošības incidenta, kas ietekmē to sniegto maksājumu pakalpojumu drošību, MPS pārskata jautājumu par to, vai ir, vai nav bez nepamatotas kavēšanās jāmaina vai jāuzlabo riska pārvaldības sistēma.

Riska pārvaldības un kontroles modeļi

2.5 MPS būtu jāizveido efektīva trīs līniju aizsardzība vai līdzvērtīgs iekšējā riska pārvaldības un kontroles modelis, lai noteiktu un pārvaldītu operacionālos un drošības riskus. MPS būtu jānodrošina, ka iepriekš minētajam modelim ir pietiekamas pilnvaras, neatkarība, resursi un tāda ziņojumu sniegšanas kārtība, ar kuru saskaņā paredzēta tieša ziņošana vadības struktūrai un attiecīgos gadījumos — augstākajai vadībai.

2.6 Šajās pamatnostādnēs norādīto drošības pasākumu revīzija būtu jāveic revidentiem, kuriem ir pieredze IT drošības un maksājumu jomā un kuri ir operacionāli neatkarīgi MPS ietvaros vai kuri ir operacionāli neatkarīgi no MPS. Nosakot šādu revīziju biežumu un koncentrēšanās virzienu, būtu jāņem vērā attiecīgie drošības riski.

Ārpakalpojumi

2.7 MPS būtu jānodrošina šajās pamatnostādnēs norādīto drošības pasākumu efektivitāte, ja maksājumu pakalpojumu darbības funkcijas, ietverot IT sistēmas, tiek uzticētas ārpakalpojumu sniedzējiem.

2.8 MPS būtu jānodrošina, ka līgumos un pakalpojuma līmeņa nolīgumos ar ārpakalpojumu sniedzējiem, kam ir uzticētas šādas funkcijas, tiek ietverti atbilstīgi un samērīgi drošības mērķi, pasākumi un darbības mērķi. MPS būtu jāuzrauga šo pakalpojumu sniedzēju atbilstības līmenis un jāpārliecinās, ka tas ir atbilstīgs drošības mērķiem, pasākumiem un darbības mērķiem.

3. pamatnostādne: Riska novērtējums

Funkciju, procesu un aktīvu identifikācija

3.1 MPS būtu jānosaka, jāizveido un regulāri jāatjaunina savu darbības funkciju, galveno uzdevumu un atbalsta procesu saraksts, lai attēlotu katras funkcijas, lomas un atbalsta procesu nozīmību, kā arī to savstarpējās atkarības saistībā ar operacionālajiem un drošības riskiem.

3.2 MPS būtu jānosaka, jāizveido un regulāri jāatjaunina informācijas aktīvu, tajā skaitā, IKT sistēmu, to konfigurāciju, citas infrastruktūras un arī saikņu ar citām iekšējām un ārējām sistēmām uzskaites saraksts, lai varētu pārvaldīt aktīvus, kas nodrošina MPS kritiski svarīgās darbības funkcijas un procesus.

Funkciju, procesu un aktīvu klasifikācija

3.3 MPS būtu jāklasificē noteiktās darbības funkcijas, atbalsta procesi un informācijas aktīvi pēc to kritiskā svarīguma.

Funkciju, procesu un aktīvu riska novērtējumi

3.4 MPS būtu jānodrošina, ka tie pastāvīgi uzrauga apdraudējumus un ievainojamību un regulāri pārskata tos riska scenārijus, kas ietekmē to darbības funkcijas, kritiski svarīgus procesus un

informācijas aktīvus. Ņemot vērā pienākumu izveidot un sniegt KI atjauninātu, visaptverošu riska novērtējumu par operacionālajiem un drošības riskiem, kas saistīti ar to sniegtajiem maksājumu pakalpojumiem, un par to, vai, reaģējot uz šiem riskiem, ir veikti adekvāti riska mazināšanas pasākumi un ieviesti kontroles mehānismi, kā tas noteikts Direktīvas (ES) 2015/2366 95. panta 2. punktā, maksājumu pakalpojumu sniedzējiem vismaz reizi gadā vai biežāk, kā noteikusi kompetentā iestāde, būtu jāizstrādā un jādokumentē riska novērtējumi par funkcijām, procesiem un informācijas aktīviem, ko tie ir noteikuši un klasificējuši, lai konstatētu un novērtētu būtiskos operacionālos un drošības riskus. Šādi riska novērtējumi būtu jāveic arī pirms jebkurām būtiskām infrastruktūras, procesa vai procedūru izmaiņām, kas ietekmē maksājumu pakalpojumu drošību.

3.5 Pamatojoties uz riska novērtējumiem, MPS būtu jānosaka, vai attiecībā uz esošajiem drošības pasākumiem, izmantotajām tehnoloģijām un procedūrām vai piedāvātajiem maksājumu pakalpojumiem ir jāveic izmaiņas, un kādā mērā to darīt. MPS būtu jāņem vērā izmaiņu ieviešanai nepieciešamais laiks, kā arī laiks, kas vajadzīgs, lai veiktu piemērotus pagaidu drošības pasākumus nolūkā mazināt operacionālo vai drošības incidentu, krāpšanas un iespējamo traucējumu ietekmi maksājumu pakalpojumu sniegšanas jomā.

4. pamatnostādne: Aizsardzība

4.1 MPS būtu jāizstrādā un jāīsteno preventīvi drošības pasākumi, lai cīnītos pret noteiktajiem operacionālajiem un drošības riskiem. Šiem pasākumiem būtu jānodrošina atbilstīgs drošības līmenis saskaņā ar noteiktajiem riskiem.

4.2 MPS būtu jāizstrādā un jāīsteno "pastiprinātas aizsardzības" pieeja, ieviešot daudzpakāpju kontroli, kas aptver cilvēkus, procesus un tehnoloģijas tā, ka katra kontroles pakāpe kalpo kā drošības tīkls tās iepriekšējām pakāpēm. Pastiprināta aizsardzība būtu jāsaprot tā, ka vienam un tam pašam riskam tiek noteikta vairāk nekā viena kontrole, piemēram, "četru acu princips", divfaktoru autentifikācija, tīkla segmentācija un vairāki ugunsmūri.

4.3 MPS būtu jānodrošina konfidencialitāte, integritāte un pieejamība attiecībā uz to kritiskajiem, loģiskajiem un fiziskajiem aktīviem, resursiem un savu maksājumu pakalpojumu lietotāju (MPL) sensitīvajiem maksājumu datiem, neatkarīgi no tā vai dati tiek uzglabāti, pārsūtīti vai apstrādāti. Ja dati ietver personas datus, šādi pasākumi būtu jāīsteno saskaņā ar Regulu (ES) 2016/679[6] vai attiecīgos gadījumos — ar Regulu (EK) 45/2001.[7]

4.4 MPS būtu pastāvīgi jānosaka, vai izmaiņas esošajā darbības vidē ietekmē esošos drošības pasākumus, vai jāpieņem turpmāki pasākumi, lai mazinātu saistīto risku. Šīm izmaiņām būtu jāiekļaujas MPS formālo izmaiņu vadības procesā, kam būtu jānodrošina, ka izmaiņas tiek pareizi plānotas, pārbaudītas, dokumentētas un atļautas. Pamatojoties uz novērotajiem drošības

[6] Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Regula (ES) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (OV L 119, 4.5.2016., 1. lpp.).

[7] Eiropas Parlamenta un Padomes 2000. gada 18. decembra Regula (EK) Nr. 45/2001 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Kopienas iestādēs un struktūrās un par šādu datu brīvu apriti (OV L 8, 12.1.2001., 1. lpp.).

apdraudējumiem un veiktajām izmaiņām, būtu jāveic testēšana nolūkā ietvert būtisku un zināmu iespējamo uzbrukumu scenārijus.

4.5 MPS, izstrādājot, attīstot un sniedzot maksājumu pakalpojumus, būtu jānodrošina, ka tiek piemēroti pienākumu nošķiršanas un "mazāko privilēģiju" principi. MPS būtu jāpievērš īpaša uzmanība nošķiršanai attiecībā uz IT vidēm, jo īpaši izstrādes, pārbaudes un ražošanas vidēm.

Datu un sistēmu integritāte un konfidencialitāte

4.6 MPS, izstrādājot, attīstot un sniedzot maksājumu pakalpojumus, būtu jānodrošina, ka MPL sensitīvo maksājumu datu apkopošana, maršrutēšana, apstrāde, glabāšana un/vai arhivēšana un vizualizēšana ir piemērota, atbilstīga un tiek ierobežota līmenī, kas nepieciešams maksājumu pakalpojumu sniegšanai.

4.7 MPS būtu regulāri jāpārliecinās, ka maksājumu pakalpojumu sniegšanai izmantotā programmatūra, tostarp ar lietotāju maksājumiem saistītā programmatūra, ir atjaunināta un ka ir uzstādīti kritiskie drošības ielāpi. MPS būtu jānodrošina, ka ir ieviesti integritātes pārbaudes mehānismi nolūkā pārbaudīt integritāti attiecībā uz programmatūru, aparātprogrammatūru un informāciju par MPS maksājumu pakalpojumiem.

Fiziskā drošība

4.8 MPS vajadzētu būt ieviestiem piemērotiem fiziskās drošības pasākumiem, jo īpaši, lai aizsargātu MPL sensitīvos maksājumu datus, kā arī maksājumu pakalpojumu sniegšanai izmantotās IKT sistēmas.

Piekļuves kontrole

4.9 Fizisku un loģisku piekļuvi IKT sistēmām būtu jāatļauj tikai atļauju saņēmušām personām. Atļauja būtu jāpiešķir saskaņā ar darbinieku uzdevumiem un pienākumiem, un — tikai personām, kas ir atbilstīgi apmācītas un uzraudzītas. MPS būtu jāievieš kontrole, kas uzticami ierobežo šādu piekļuvi IKT sistēmām, nosakot piekļuvi tikai tiem, kuri atbilst likumīgas darbības prasībai. Lietojumprogrammu elektroniskā piekļuve datiem un sistēmām būtu jāierobežo līdz minimālajam līmenim, kas nepieciešams attiecīgā pakalpojuma sniegšanai.

4.10 MPS būtu jāievieš spēcīga kontrole attiecībā uz priviliģētu piekļuvi sistēmai, stingri ierobežojot un cieši uzraugot personālu, kam ir palielinātas pilnvaras attiecībā uz piekļuvi sistēmai. Būtu jāīsteno tādas kontroles kā, piemēram, "uz funkcijām pamatota piekļuve", priviliģēto lietotāju sistēmā veikto darbību reģistrēšana un pārskatīšana, stingrā autentifikācija un sistēmas noviržu uzraudzība. MPS būtu jāpārvalda piekļuves tiesības informācijas aktīviem un to atbalsta sistēmām, pamatojoties uz "nepieciešamība zināt" principu. Piekļuves tiesības būtu regulāri jāpārskata.

4.11 Piekļuves žurnālierakstu glabāšanas ilgumam vajadzētu būt atbilstīgam konstatēto darbības funkciju, atbalsta procesu un informācijas aktīvu kritiskumam saskaņā ar šo pamatnostādņu 3.1. un 3.2. punktu (GL 3.1 un GL 3.2), neskarot ES un valsts tiesību aktos noteiktās saglabāšanas

prasības. MPS būtu jāizmanto šī informācija, lai sekmētu maksājumu pakalpojumu sniegšanā konstatēto netipisku darbību identifikāciju un izmeklēšanu.

4.12 Lai nodrošinātu drošu saziņu un samazinātu risku, attālinātā administratīvā piekļuve kritiski svarīgiem IKT komponentiem būtu jāpiešķir tikai, pamatojoties uz "nepieciešamību zināt", un, ja tiek izmantoti spēcīgi autentifikācijas risinājumi.

4.13 Ar piekļuves kontroles procesiem saistītu produktu, rīku un procedūru darbībai būtu jāaizsargā piekļuves kontroles procesi, lai tie netiktu apdraudēti vai apieti. Tas ietver atbilstīgo produktu, rīku un procedūru reģistrāciju, piegādi, atsaukšanu un izņemšanu.

5. pamatnostādne: Konstatēšana

Pastāvīga uzraudzība un konstatēšana

5.1 MPS būtu jāizstrādā un jāievieš procesi un iespējas ar mērķi pastāvīgi uzraudzīt darbības funkcijas, atbalsta procesus un informācijas aktīvus, lai atklātu un konstatētu netipiskas darbības saistībā ar maksājumu pakalpojumu sniegšanu. Šīs pastāvīgās uzraudzības ietvaros MPS būtu jāievieš atbilstīgas un efektīvas iespējas, kas ļautu konstatēt fizisku vai loģisku ielaušanos, kā arī pārkāpumus attiecībā uz konfidencialitāti, integritāti un maksājumu pakalpojumu sniegšanā izmantoto informācijas aktīvu pieejamību.

5.2 Pastāvīgas uzraudzības un konstatēšanas procesos būtu jāietver šādi aspekti:

a) būtiski iekšējie un ārējie faktori, tostarp darbības un IKT administratīvās funkcijas;

b) darījumi, lai konstatētu pakalpojumu sniedzēju vai citu personu ļaunprātīgu piekļuvi; un

c) iespējamie iekšējie un ārējie apdraudējumi.

5.3 MPS būtu jāīsteno atklāšanas pasākumi, lai konstatētu iespējamo informācijas noplūdi, ļaunprātīgu kodu un citus drošības apdraudējumus un publiski zināmas ievainojamības attiecībā uz programmatūru un aparatūru, kā arī, lai pārliecinātos par atbilstīgiem jauniem drošības atjauninājumiem.

Uzraudzība un ziņošana par operacionālajiem un drošības incidentiem

5.4 MPS būtu jānosaka piemēroti kritēriji un robežvērtības, lai notikumu klasificētu kā operacionālo vai drošības incidentu, kā noteikts šo pamatnostādņu sadaļā "Definīcijas", kā arī jānosaka agrīnas brīdināšanas rādītāji, kas MPS dotu iespēju agrīni atklāt operacionālos vai drošības incidentus.

5.5 MPS būtu jāizveido atbilstoši procesi un organizatoriskās struktūras, lai attiecībā uz operacionālajiem vai drošības incidentiem nodrošinātu saskaņotu un integrētu uzraudzību, apstrādi un turpmākos pasākumus.

5.6 Maksājumu pakalpojumu sniedzējiem būtu jāizveido procedūra, kas paredz ziņošanu augstākajai vadībai par šādiem operacionālajiem vai drošības incidentiem, kā arī par klientu sūdzībām, kas saistītas ar drošību.

6. pamatnostādne: Darbības nepārtrauktība

6.1 MPS būtu jāizveido stabila darbības nepārtrauktības vadība, lai palielinātu maksājumu pakalpojumu pastāvīgas sniegšanas spēju un ierobežotu zaudējumus būtisku darbības traucējumu gadījumā.

6.2 Lai izveidotu stabilu darbības nepārtrauktības vadību, MPS būtu rūpīgi jāanalizē būtisku darbības traucējumu iedarbība un kvantitatīvi un kvalitatīvi jānovērtē to iespējamā ietekme, veicot iekšējo un/vai ārējo datu un scenāriju analīzi. Pamatojoties uz konstatētām un klasificētām kritiski svarīgām funkcijām, procesiem, sistēmām, darījumiem un savstarpējām atkarībām saskaņā ar GL 3.1 – GL 3.3, MPS būtu jānosaka prioritātes darbības nepārtrauktības pasākumiem, izmantojot uz risku balstītu pieeju, kuras pamatā var būt riska novērtēšana, kas veikta saskaņā ar GL 3. Atkarībā no MPS darījumdarbības modeļa šādi var, piemēram, veicināt kritiski svarīgo darījumu turpmāku apstrādi, vienlaikus novēršot ārkārtas situāciju.

6.3 Pamatojoties uz analīzi, kas veikta saskaņā ar GL 6.2, MPS būtu jāievieš:

a) Darbības nepārtrauktības plāni (DNP), lai nodrošinātu, ka MPS var pienācīgi reaģēt uz ārkārtas situācijām un spēj uzturēt savus kritiski svarīgos darbības pasākumus; un

b) ietekmes mazināšanas pasākumi, kas maksājumu pakalpojumu pārtraukšanas un esošo līgumu pārtraukšanas gadījumā ir jāpieņem, lai izvairītos no nelabvēlīgas ietekmes uz maksājumu sistēmām un uz maksājumu pakalpojumu lietotājiem (MPL) un lai nodrošinātu nenokārtotu maksājumu darījumu izpildi.

Uz scenārijiem pamatota darbības nepārtrauktības plānošana

6.4 MPS būtu jāapsver virkne dažādu scenāriju, ar kuriem tas varētu saskarties, ietverot ārkārtējus, bet iespējamus scenārijus, un jānovērtē šo scenāriju iespējamā ietekme.

6.5 Pamatojoties uz analīzi, ko veic saskaņā ar GL 6.2 un iespējamiem scenārijiem, kas noteikti saskaņā ar GL 6.4, MPS būtu jāizstrādā reaģēšanas un atjaunošanas plāni, kuri:

a) jākoncentrē uz ietekmi, kas skar kritiski svarīgu funkciju, procesu, sistēmu, darījumu un savstarpējo atkarību darbību;

b) jādokumentē un jānodrošina, ka tie ir pieejami darbības un atbalsta vienībām un tiem ir viegli piekļūt avārijas gadījumā; un

c) jāatjaunina, ņemot vērā pārbaudēs gūto pieredzi, identificētos jaunos riskus un apdraudējumus, kā arī precizētos atjaunošanas mērķus un prioritātes.

Darbības nepārtrauktības plānu pārbaudes

6.6 Maksājumu pakalpojumu sniedzējiem būtu jāpārbauda savi darījumdarbības nepārtrauktības plāni (DNP) un jānodrošina, ka ne retāk kā reizi gadā tiek pārbaudīta MPS kritiski svarīgo funkciju, procesu, sistēmu, darījumu un savstarpējo atkarību darbība. Plānos būtu jāietver atbalsts mērķiem

aizsargāt un, ja nepieciešams, atjaunot MPS darbības integritāti un pieejamību, kā arī MPS informācijas aktīvu konfidencialitāti.

6.7 Plāni būtu jāatjaunina ne retāk kā reizi gadā, pamatojoties uz pārbaužu rezultātiem, pašreizējo apdraudējumu izlūkošanu, informācijas apmaiņu un iepriekšējo notikumu pieredzi, un mainīgiem atjaunošanas mērķiem, kā arī analīzi par funkcionāli un tehniski iespējamiem scenārijiem, kas vēl nav piepildījušies, kā arī attiecīgos gadījumos pēc izmaiņām sistēmās un procesos. MPS, izstrādājot savu DNP, būtu jākonsultējas un tas jāsaskaņo ar attiecīgajām iekšējām un ārējām ieinteresētajām personām.

6.8 Attiecībā uz MPS darbības nepārtrauktības plānu (DNP) pārbaudēm:

a) tajās būtu jāietver atbilstīgs scenāriju kopums saskaņā ar GL 6.4;

b) tās būtu jāizstrādā tā, lai pārbaudītu pieņēmumus, uz kuriem DNP balstās, ietverot pārvaldības režīmu un plānus saziņai krīzes laikā; un

c) tajās būtu jāietver procedūras nolūkā pārbaudīt MPS personāla un procesu spēju atbilstīgi reaģēt uz minētajiem scenārijiem.

6.9 MPS būtu regulāri jāuzrauga savu DNP efektivitāte un jādokumentē, kā arī jāanalizē visas problēmas vai kļūmes, kas radušās pārbaužu rezultātā.

Saziņa krīzes laikā

6.10 Maksājumu pakalpojumu sniedzējiem būtu jānodrošina, ka traucējumu vai ārkārtas situācijas gadījumā, kā arī darbības nepārtrauktības plānu īstenošanas laikā tiem vajadzētu būt sagatavotiem efektīviem krīzes saziņas pasākumiem, lai visas attiecīgās iekšējās un ārējās ieinteresētās personas, tostarp ārējie pakalpojumu sniedzēji tiktu savlaicīgi un atbilstošā veidā informēti.

7. pamatnostādne: Drošības pasākumu pārbaude

7.1 MPS būtu jāizveido un jāievieš tāda pārbaudes sistēma, kas apstiprina drošības pasākumu noturību un efektivitāti un nodrošina, ka pārbaudes sistēma ir pielāgota riska uzraudzības pasākumu gaitā noteikto jauno apdraudējumu un ievainojamību izskatīšanai.

7.2 MPS būtu jānodrošina, ka pārbaudes tiek veiktas, ja notiek infrastruktūras, procesu vai procedūru izmaiņas un ja izmaiņas ir veiktas būtisku operacionālo vai drošības incidentu rezultātā.

7.3 Pārbaužu sistēmā būtu jāietver arī drošības pasākumi, kas attiecas uz i) maksājumu termināliem un ierīcēm, ko izmanto maksājumu pakalpojumu sniegšanai, ii) maksājumu termināliem un ierīcēm, ko izmanto MPL autentifikācijai, un iii) ierīcēm un programmatūru, ar ko MPS nodrošina MPL, lai izveidotu/saņemtu autentifikācijas kodu.

7.4 Pārbaužu sistēmai būtu jānodrošina, ka pārbaudes:

a) tiek veiktas MPS formālo izmaiņu pārvaldības procesa gaitā, lai nodrošinātu to noturību un efektivitāti;

b) veic neatkarīgi pārbaudītāji, kuriem ir pietiekamas zināšanas, prasmes un pieredze maksājumu pakalpojumu drošības pasākumu pārbaužu veikšanā un kuri nav iesaistīti attiecīgo pārbaudāmo maksājumu pakalpojumu vai sistēmu drošības pasākumu izstrādē (vismaz attiecībā uz gala pārbaudēm pirms drošības pasākumu darbības uzsākšanas); un

c) ietver ievainojamību skenēšanu un drošības pārbaudes testus, kas ir atbilstīgi maksājumu pakalpojumiem konstatētajam risku līmenim.

7.5 MPS būtu jāveic savu maksājumu pakalpojumu drošības pasākumu pastāvīgas un atkārtotas pārbaudes. Sistēmām, kas ir kritiski svarīgas MPS maksājumu pakalpojumu sniegšanai (kā aprakstīts GL 3.2), šīs pārbaudes veic vismaz reizi gadā. Sistēmas, kas nav kritiski svarīgas, būtu jāpārbauda regulāri, izmantojot uz risku balstītu pieeju, bet ne retāk kā reizi trīs gados.

7.6 MPS būtu jāuzrauga un jāvērtē veikto pārbaužu rezultāti un attiecīgi jāuzlabo drošības pasākumi atbilstošā veidā un bez nepamatotas kavēšanās attiecībā uz kritiski svarīgām sistēmām.

8. pamatnostādne: Informētība par situāciju un nepārtraukta mācīšanās

Apdraudējumi un informētība par situāciju

8.1 MPS būtu jāizstrādā un jāīsteno procesi un organizatoriskās struktūras, lai noteiktu un pastāvīgi uzraudzītu drošības un operacionālos apdraudējumus, kas varētu būtiski ietekmēt to spēju sniegt maksājumu pakalpojumus.

8.2 MPS būtu jāanalizē konstatētie operacionālie vai drošības incidenti, kas notikuši organizācijas iekšienē un/vai ārpus tās. MPS būtu jāapsver galvenās atziņas, kas gūtas no šīm analīzēm, un jāveic attiecīgie drošības pasākumu atjauninājumi.

8.3 MPS būtu aktīvi jāuzrauga tehnoloģiskā attīstība, lai nodrošinātu to, ka tie ir informēti par drošības riskiem.

Programmas apmācībai un informētībai par drošību

8.4 MPS būtu jāizstrādā apmācības programma visiem darbiniekiem, lai nodrošinātu, ka viņi ir apmācīti veikt savus pienākumus un atbildīgos uzdevumus saskaņā ar attiecīgo drošības politiku un attiecīgajām procedūrām, lai mazinātu cilvēku kļūdas, zādzības, krāpšanu, ļaunprātīgu izmantošanu vai zaudējumus. MPS būtu jānodrošina, ka apmācības programma paredz darbinieku apmācību vismaz reizi gadā vai biežāk, ja nepieciešams.

8.5 MPS būtu jānodrošina, ka darbinieki, kuru pārziņā ir galvenie uzdevumi, kas noteikti saskaņā ar GL 3.1, saņem mērķtiecīgu informācijas drošības apmācību reizi gadā vai biežāk, ja nepieciešams.

8.6 MPS būtu jāveido un jāīsteno regulāras programmas informētībai par drošību, lai izglītotu savus darbiniekus un pievērstos riskiem, kas saistīti ar informācijas drošību. Šajās programmās būtu jānosaka prasība MPS darbiniekiem ziņot par jebkuru neparastu darbību vai incidentu.

9. pamatnostādne: Maksājumu pakalpojumu lietotāja attiecību pārvaldība

Maksājumu pakalpojumu lietotāja informētība par drošības riskiem un riska mazināšanas pasākumiem

9.1 MPS būtu jāizveido un jāievieš procesi ar mērķi uzlabot MPL informētību par drošības riskiem, kas saistīti ar maksājumu pakalpojumiem, nodrošinot palīdzību un norādījumus maksājumu pakalpojumu lietotājiem (MPL).

9.2 Maksājumu pakalpojumu lietotājiem (MPL) piedāvātā palīdzība un norādījumi būtu jāatjaunina, ņemot vērā jaunus apdraudējumus un ievainojamību, un izmaiņas jāpaziņo MPL.

9.3 Ja produkta funkcionalitāte to pieļauj, MPS būtu jāļauj MPL atspējot konkrētas maksājumu funkcijas, kas saistītas ar maksājumu pakalpojumiem, ko MPS piedāvā MPL.

9.4 Ja saskaņā ar Direktīvas (ES) 2015/2366 68. panta 1. punktu MPS ir vienojies ar maksātāju par tērēšanas limitu maksājumu darījumiem, kas veikti, izmantojot konkrētu maksājumu instrumentu, MPS būtu jānodrošina maksātājam iespēja koriģēt šos ierobežojumus līdz maksimālajai robežai, par kuru ir notikusi vienošanās.

9.5 MPS būtu jānodrošina MPL iespēja saņemt brīdinājumus par sāktiem maksājumu darījumiem un/vai neveiksmīgiem mēģinājumiem sākt maksājumu darījumus, kas ļauj tiem konstatēt krāpniecisku vai ļaunprātīgu sava konta izmantošanu.

9.6 MPS būtu pastāvīgi jāinformē MPL par drošības procedūru atjauninājumiem, kas ietekmē MPL saistībā ar maksājumu pakalpojumu sniegšanu.

9.7 MPS būtu jānodrošina MPL palīdzība attiecībā uz visiem jautājumiem, pieprasījumiem par atbalstu un paziņojumiem par novirzēm vai problēmām attiecībā uz drošības jautājumiem, kas saistīti ar maksājumu pakalpojumiem. MPL vajadzētu būt pienācīgi informētiem par to, kā var saņemt šādu palīdzību.