EBA/GL/2017/17

12/01/2018

Gairės

dėl saugumo priemonių, susijusių su mokėjimo paslaugų operacine ir saugumo rizika pagal Direktyvą (ES) 2015/2366 (MPD2)

1. Atitiktis gairėms ir informavimo pareiga

Šių gairių statusas

1. Šiame dokumente pateiktos pagal Reglamento (ES) Nr. 1093/2010[1] 16 straipsnį parengtos gairės. Pagal Reglamento Nr. 1093/2010 16 straipsnio 3 dalį kompetentingos institucijos ir finansų įstaigos turi dėti visas pastangas siekdamos laikytis šių gairių.

2. Gairėse išdėstoma EBI nuomonė dėl tinkamos priežiūros praktikos Europos finansų priežiūros institucijų sistemoje arba dėl to, kaip Sąjungos teisė turėtų būti taikoma tam tikroje srityje. Reglamento (ES) Nr. 1093/2010 4 straipsnio 2 dalyje apibrėžtos kompetentingos institucijos, kurioms taikomos šios gairės, turėtų jų laikytis ir atitinkamai jas įtraukti į savo praktiką (pvz., iš dalies pakeisti savo teisinę sistemą arba priežiūros procesus), įskaitant tuos atvejus, kai gairės pirmiausia yra skiriamos įstaigoms.

Pranešimo reikalavimai

3. Pagal Reglamento Nr. 1093/2010 16 straipsnio 3 dalį kompetentingos institucijos iki 12.03.2018 privalo EBI pranešti, ar laikosi arba ketina laikytis šių gairių, arba nurodyti nesilaikymo priežastis. Jeigu kompetentingos institucijos iki šio termino nepateiks jokio pranešimo, EBI laikys, kad jos gairių nesilaiko. Pranešimus reikėtų siųsti adresu compliance@eba.europa.eu užpildžius EBI interneto svetainėje pateiktą formą ir įrašius nuorodą „EBA/GL/2017/17“. Pranešimus turėtų teikti asmenys, turinys įgaliojimus pranešti apie gairių laikymąsi savo kompetentingų institucijų vardu. Apie visus gairių laikymosi pasikeitimus taip pat būtina pranešti EBI.

4. Pranešimai bus skelbiami EBI interneto svetainėje pagal 16 straipsnio 3 dalį.

[1] 2010 m. lapkričio 24 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 1093/2010, kuriuo įsteigiama Europos priežiūros institucija (Europos bankininkystės institucija), iš dalies keičiamas Sprendimas Nr. 716/2009/EB ir panaikinamas Komisijos sprendimas 2009/78/EB (OL L 331, 2010 12 15, p. 12).

2. Dalykas, taikymo sritis ir sąvokų apibrėžtys

Dalykas ir taikymo sritis

5. Paskelbdama šias gaires EBI įgyvendina jai Direktyvos (ES) 2015/2366 [2] 95 straipsnio 3 dalimi pavestus įgaliojimus.

6. Šiose gairėse nustatomi saugumo priemonių, kurių pagal Direktyvos (ES) 2015/2366 95 straipsnio 1 dalį privalo imtis mokėjimo paslaugų teikėjai (MPT) siekdami valdyti su jų teikiamomis mokėjimo paslaugomis susijusią operacinę ir saugumo riziką, sukūrimo, įgyvendinimo ir stebėsenos reikalavimai.

Kam skirtos šios gairės?

7. Šios gairės skirtos mokėjimo paslaugų teikėjams (MPT), kaip apibrėžta Direktyvos (ES) 2015/2366 4 straipsnio 11 punkte ir kaip nurodyta sąvokos „finansų įstaiga“ apibrėžtyje Reglamento (ES) Nr. 1093/2010, ir kompetentingoms institucijoms (KI), kaip apibrėžta to reglamento 4 straipsnio 2 dalies i punkte darant nuorodą į panaikintą Direktyvą 2007/64/EB [3] (dabar – Direktyva (ES) 2015/2366[4]).

Sąvokų apibrėžtys

8. Jei nenurodyta kitaip, Direktyvoje (ES) 2015/2366 vartojamos ir apibrėžtos sąvokos šiose gairėse turi tokią pačią reikšmę. Be to, šiose gairėse vartojamos šios sąvokų apibrėžtys:

Valdymo organas	– MPT, kurie yra kredito įstaigos, atveju šis terminas turi tokią pačią reikšmę, kaip apibrėžta Direktyvos 2013/36/ES [5] 3 straipsnio 1 dalies 7 punkte;

[2] 2015 m. lapkričio 25 d. Europos Parlamento ir Tarybos direktyva (ES) 2015/2366 dėl mokėjimo paslaugų vidaus rinkoje, kuria iš dalies keičiamos direktyvos 2002/65/EB, 2009/110/EB ir 2013/36/ES bei Reglamentas (ES) Nr. 1093/2010 ir panaikinama Direktyva 2007/64/EB (OL L 337, 2015 12 23, p. 35).

[3] 2007 m. lapkričio 13 d. Europos Parlamento ir Tarybos direktyva 2007/64/EB dėl mokėjimo paslaugų vidaus rinkoje, iš dalies keičianti direktyvas 97/7/EB, 2002/65/EB, 2005/60/EB ir 2006/48/EB ir panaikinanti Direktyvą 97/5/EB (OL L 319, 2007 12 5, p. 1).

[4] Remiantis Direktyvos (ES) 2015/2366 114 straipsnio antra pastraipa, bet kokia nuoroda į panaikintą Direktyvą 2007/64/EB laikoma nuoroda į Direktyvą (ES) 2015/2366 ir aiškinama remiantis Direktyvos (ES) 2015/2366 II priede pateikta atitikmenų lentele.

[5] Europos Parlamento ir Tarybos direktyva 2013/36/ES dėl galimybės verstis kredito įstaigų veikla ir dėl riziką ribojančios kredito įstaigų ir investicinių įmonių priežiūros, kuria iš dalies keičiama Direktyva 2002/87/EB ir panaikinamos direktyvos 2006/48/EB bei 2006/49/EB (OL L 176, 2013 6 27, p. 338).

	– MPT, kurie yra mokėjimo įstaigos arba elektroninių pinigų įstaigos, atveju šis terminas reiškia direktorius arba už MPT valdymą atsakingus asmenis ir tam tikrais atvejais asmenis, atsakingus už MPT mokėjimo paslaugų veiklos valdymą; – MPT, nurodytų Direktyvos (ES) 2015/2366 1 straipsnio 1 dalies c, e ir f punktuose, atveju šis terminas turi tokią pačią reikšmę, kaip taikytinuose ES ar nacionalinės teisės aktuose.
Operacinis ar saugumo incidentas	Pavienis įvykis arba tarpusavyje susijusių įvykių grupė, kurių MPT neplanavo ir kurie turi arba, tikėtina, turės neigiamą poveikį su mokėjimu susijusių paslaugų vientisumui, prieinamumui, konfidencialumui, autentiškumui ir (arba) tęstinumui.
Vyresnioji vadovybė	(a) MPT, kurie yra kredito įstaigos, atveju šis terminas turi tokią pačią reikšmę, kaip apibrėžta Direktyvos 2013/36/ES 3 straipsnio 1 dalies 9 punkte; (b) MPT, kurie yra mokėjimo įstaigos ir elektroninių pinigų įstaigos, šis terminas reiškia fizinius asmenis, kurie įstaigoje vykdo vykdomąsias funkcijas, atsako už kasdienį MPT valdymą ir atsiskaito valdymo organui; (c) MPT, nurodytų Direktyvos (ES) 2015/2366 1 straipsnio 1 dalies c, e ir f punktuose, atveju šis terminas turi tokią pačią reikšmę, kaip taikytinuose ES ar nacionalinės teisės aktuose.
Saugumo rizika	Rizika, susijusi su nepakankamais ar nevykusiais vidaus procesais ar išorės įvykiais, kurie turi ar gali turėti neigiamą poveikį informacijos ir ryšių technologijų (IRT) sistemų ir (arba) teikiant mokėjimo paslaugas naudojamos informacijos prieinamumui, vientisumui ir konfidencialumui. Tai apima su kibernetinėmis atakomis ar nepakankamu fiziniu saugumu susijusią riziką.
Priimtina rizika	Bendrasis rizikos, kurią siekdama savo strateginių tikslų įstaiga nori prisiimti, lygis ir tipai, atsižvelgiant į įstaigos pajėgumą prisiimti riziką ir verslo modelį.

3. Įgyvendinimas

Taikymo data

9. Šios gairės taikomos nuo 2018 m. sausio 13 d.

4. Gairės

1 gairė. Bendrieji principai

1.1 Visi MPT turėtų laikytis visų šiose gairėse išdėstytų nuostatų. Informacijos išsamumas turėtų būti proporcingas MPT dydžiui ir konkrečių paslaugų, kurias MPT teikia ar ketina teikti, pobūdžiui, mastui, sudėtingumui ir rizikingumui.

2 gairė. Valdymas

Operacinės ir saugumo rizikos valdymo sistema

2.1 MPT turėtų sukurti veiksmingą operacinės ir saugumo rizikos valdymo sistemą (toliau – rizikos valdymo sistema), kurią bent kartą per metus tvirtintų ir peržiūrėtų valdymo organas ir prireikus vyresnioji vadovybė. Toje sistemoje pagrindinis dėmesys turėtų būti skiriamas saugumo priemonėms, kuriomis siekiama mažinti operacinę ir saugumo riziką, ir ji turėtų būti visiškai integruota į bendruosius MPT rizikos valdymo procesus.

2.2 Rizikos valdymo sistema turėtų:

a) apimti išsamų saugumo politikos dokumentą, kaip numatyta Direktyvos (ES) 2015/2366 5 straipsnio 1 dalies j punkte;

b) atitikti priimtiną MPT riziką;

c) apibrėžti ir priskirti pagrindines funkcijas ir pareigas ir atitinkamas atskaitomybės linijas, būtinas saugumo priemonėms stiprinti ir saugumo ir operacinei rizikai valdyti;

d) sukurti būtinas įvairios su mokėjimais susijusios MPT veiklos ir MPT kylančios rizikos nustatymo, matavimo, stebėsenos ir valdymo procedūras ir sistemas, įskaitant veiklos tęstinumo priemones.

2.3 MPT turėtų užtikrinti, kad rizikos valdymo sistema būtų tinkamai įforminta dokumentais ir atnaujinama remiantis dokumentuota patirtimi ją įgyvendinant ir vykdant jos stebėseną.

2.4 MPT turėtų užtikrinti, kad prieš atliekant esminius infrastruktūros, procesų ar procedūrų pakeitimus ir po kiekvieno svarbaus operacinio ar saugumo incidento, darančio poveikį jų teikiamų mokėjimo paslaugų saugumui, būtų vertinama, ar reikėtų nepagrįstai nedelsiant keisti ar tobulinti rizikos valdymo sistemą.

Rizikos valdymo ir kontrolės modeliai

2.5 MPT turėtų sukurti tris veiksmingas gynybos linijas arba lygiavertį vidaus rizikos valdymo ir kontrolės modelį, kad nustatytų ir valdytų operacinę ir saugumo riziką. MPT turėtų užtikrinti, kad pirmiau nurodytas vidaus kontrolės modelis būtų pakankamai autoritetingas ir nepriklausomas ir

kad jam būtų skiriama pakankamai išteklių ir tiesioginės atskaitomybės linijos sietų jį su valdymo organu ir tam tikrais atvejais vyresniąja vadovybe.

2.6 Šiose gairėse nustatytas saugumo priemones turėtų tikrinti IT saugumo ir mokėjimų srityse patyrę auditoriai, kurių veikla nepriklauso nuo MPT. Nustatant tokių auditų dažnį ir dalyką reikėtų atsižvelgti į atitinkamą saugumo riziką.

Užsakomosios paslaugos

2.7 Naudodamiesi užsakomosiomis paslaugomis, susijusiomis su mokėjimo paslaugų operacinėmis funkcijomis, įskaitant IT sistemas, MPT turėtų užtikrinti šiose gairėse nustatytų saugumo priemonių veiksmingumą.

2.8 MPT turėtų užtikrinti, kad į sutartis ir paslaugų lygio susitarimus su teikėjais, kuriems pavedamos tokios funkcijos, būtų įtraukti tinkami ir proporcingi saugumo tikslai, priemonės ir veiklos rezultatų tikslai. MPT turėtų vykdyti stebėseną ir siekti užtikrinti, kad tie paslaugų teikėjai laikytųsi nustatytų saugumo tikslų, priemonių ir veiklos rezultatų tikslų.

3 gairė. Rizikos vertinimas

Funkcijų, procesų ir išteklių nustatymas

3.1 MPT turėtų nustatyti, apibrėžti ir reguliariai atnaujinti veiklos funkcijų, pagrindinių funkcijų ir pagalbinių procesų sąrašą siekdami apibūdinti kiekvienos funkcijos ir pagalbinių procesų svarbą ir ryšį su operacine ir saugumo rizika.

3.2 MPT turėtų nustatyti, apibrėžti ir reguliariai atnaujinti informacinių išteklių, kaip antai IRT sistemų, jų konfigūracijos, kitų infrastruktūros objektų ir ryšių su kitomis vidaus ir išorės sistemomis, sąrašą siekdami valdyti išteklius, naudojamus svarbiausioms veiklos funkcijoms ir procesams remti.

Funkcijų, procesų ir išteklių klasifikavimas

3.3 MPT turėtų klasifikuoti nustatytas veiklos funkcijas, pagalbinius procesus ir informacinius išteklius pagal jų svarbą.

Funkcijų, procesų ir išteklių rizikos vertinimas

3.4 MPT turėtų nuolat stebėti grėsmes ir pažeidžiamas vietas ir reguliariai peržiūrėti rizikos scenarijus, darančius poveikį jų veiklos funkcijoms, svarbiausiems procesams ir informaciniams ištekliams. Vykdydami savo įsipareigojimus atlikti ir KI pateikti atnaujintą ir išsamų su jų teikiamomis mokėjimo paslaugomis susijusios operacinės ir saugumo rizikos vertinimą ir pranešti apie rizikos mažinimo priemonių ir kontrolės mechanizmų, įgyvendintų reaguojant į tą riziką, pakankamumą, kaip numatyta Direktyvos (ES) 2015/2366 95 straipsnio 2 dalyje, MPT turėtų atlikti ir dokumentais įforminti nustatytų ir klasifikuotų funkcijų, procesų ir informacinių išteklių rizikos vertinimą bent kartą per metus arba dažniau, kaip nustatė KI, siekdami nustatyti ir įvertinti pagrindinę operacinę

ir saugumo riziką. Toks rizikos vertinimas taip pat turėtų būti atliekamas prieš atliekant svarbius infrastruktūros, proceso ar procedūrų pakeitimus, darančius poveikį mokėjimo paslaugų saugumui.

3.5 Remdamiesi rizikos vertinimais, MPT turėtų nustatyti, ar reikia keisti galiojančias saugumo priemones, naudojamas technologijas ir procedūras ar siūlomas mokėjimo paslaugas ir kaip. MPT turėtų atsižvelgti į tai, kiek laiko reikia tiems pakeitimams įgyvendinti ir kiek laiko reikia tinkamoms laikinosioms saugumo priemonėms įgyvendinti siekiant kuo labiau sumažinti operacinius ar saugumo incidentus, sukčiavimą ir galimą neigiamą poveikį teikiant mokėjimo paslaugas.

4 gairė. Apsauga

4.1 Siekdami apsisaugoti nuo nustatytos operacinės ir saugumo rizikos MPT turėtų sukurti ir įgyvendinti prevencines saugumo priemones. Tokiomis priemonėmis turėtų būti užtikrinamas pakankamas saugumo lygis, atitinkantis nustatytą riziką.

4.2 MPT turėtų sukurti ir įgyvendinti nuodugnios apsaugos požiūrį įdiegdami daugiapakopes kontrolės priemones, apimančias asmenis, procesus ir technologijas, kurias taikant kiekviena pakopa yra ankstesnių pakopų apsaugos priemonė. Nuodugnią apsaugą reikėtų suprasti taip, kad tai pačiai rizikai sukuriama daugiau nei viena kontrolės priemonė, pavyzdžiui, taikomas keturių akių principas, dviejų veiksnių autentiškumo patvirtinimas, tinklo skaidymas ir daug užkardų.

4.3 MPT turėtų užtikrinti svarbiausių loginių ir fizinių turto objektų, išteklių ir saugomų, perduodamų ar naudojamų konfidencialių mokėjimo paslaugų vartotojo (MPV) mokėjimo duomenų konfidencialumą, vientisumą ir prieinamumą. Jeigu yra asmens duomenų, tokios priemonės turėtų būti įgyvendinamos laikantis Reglamento (ES) Nr. 2016/679[6] arba, jei taikytina, Reglamento (EB) Nr. 45/2001[7].

4.4 MPT turėtų nuolat vertinti, ar dabartinės veiklos aplinkos pokyčiai daro įtakos įgyvendinamoms saugumo priemonėms arba ar reikia priimti papildomas susijusios rizikos mažinimo priemones. Tokie pakeitimai turėtų būti įtraukti į oficialų MPT pokyčių valdymo procesą, kuriuo turėtų būti užtikrinama, kad pakeitimai būtų tinkamai planuojami, bandomi, įforminami dokumentais ir patvirtinami. Remiantis pastebėtomis grėsmėmis saugumui ir atsižvelgiant į atliktus pakeitimus, reikėtų atlikti bandymus siekiant įtraukti svarbių ir žinomų potencialių atakų scenarijus.

4.5 Projektuodami, kurdami ir teikdami mokėjimo paslaugas MPT turėtų užtikrinti, kad būtų taikomi pareigų atskyrimo ir mažiausių privilegijų principai. MPT turėtų atkreipti ypatingą dėmesį į IT aplinkos dalių, ypač susijusių su kūrimu, bandymais ir gamyba, atskyrimą.

[6] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (OL L 119, 2016 5 4, p. 1).

[7] 2000 m. gruodžio 18 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 45/2001 dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo (OL L 8, 2001 1 12, p. 1).

Duomenų ir sistemų vientisumas ir konfidencialumas

4.6 Projektuodami, kurdami ir teikdami mokėjimo paslaugas, MPT turėtų užtikrinti, kad konfidencialių MPV mokėjimų duomenų rinkimas, perdavimas, tvarkymas, saugojimas ir (arba) archyvavimas ir vizualizavimas būtų pakankami, tinkami ir apriboti tik tuo, kas yra būtina mokėjimo paslaugoms teikti.

4.7 MPT turėtų reguliariai tikrinti, kad mokėjimo paslaugoms teikti naudojama programinė įranga, įskaitant su vartotojų mokėjimais susijusią programinę įrangą, būtų atnaujinta ir kad būtų įdiegtos būtinos saugumo pataisos. MPT turėtų užtikrinti, kad būtų įdiegti vientisumo tikrinimo mechanizmai, kuriais būtų tikrinamas programinės įrangos, gamintojo programinės įrangos ir informacijos apie mokėjimo paslaugas vientisumas.

Fizinis saugumas

4.8 MPT turėtų įsidiegti tinkamas fizinio saugumo priemones, visų pirma siekdami apsaugoti konfidencialius MPV mokėjimų duomenis ir mokėjimo paslaugoms teikti naudojamas IRT sistemas.

Prieigos kontrolė

4.9 Fizinę ir loginę prieigą prie IRT sistemų turėtų turėti tik autorizuoti asmenys. Leidimas turėtų būti suteikiamas atsižvelgiant į darbuotojų užduotis ir atsakomybės sritis tik asmenims, kurie yra tinkamai apmokyti ir stebimi. MPT turėtų įsidiegti kontrolės priemones, kuriomis tokia prieiga prie IRT sistemų būtų patikimai ribojama ir suteikiama tik teisėtų su veikla susijusių poreikių turintiems asmenims. Elektroninė taikomųjų programų prieiga prie duomenų ir sistemų turėtų būti kuo labiau ribojama ir suteikiama tik kai tai būtina tam tikrai paslaugai teikti.

4.10 Privilegijuotajai prieigai prie sistemų MPT turėtų taikyti griežtos kontrolės priemones ir griežtai riboti ir stebėti darbuotojus, turinčius didesnes prieigos prie sistemos teises. Turėtų būti įdiegtos tokios kontrolės priemonės, kaip prieiga atsižvelgiant į pareigas, privilegijuotųjų vartotojų veiksmų sistemoje registravimas ir peržiūra, griežtos autentiškumo patvirtinimo priemonės ir anomalijų stebėsena. MPT turėtų valdyti prieigos prie informacinių išteklių ir pagalbinių sistemų teises remdamiesi principu „būtina žinoti“. Prieigos teises reikėtų reguliariai peržiūrėti.

4.11 Prieigos registracijos žurnalus reikėtų saugoti tiek, kiek proporcinga atsižvelgiant į nustatytų veiklos funkcijų, pagalbinių procesų ir informacinių išteklių svarbą, kaip numatyta GL 3.1 ir GL 3.2, nepažeidžiant ES ir nacionalinės teisės aktuose nustatytų informacijos saugojimo reikalavimų. MPT turėtų naudoti šią informaciją siekdami palengvinti anomalios veiklos, pastebėtos teikiant mokėjimo paslaugas, nustatymą ir tyrimą.

4.12 Siekiant užtikrinti saugų ryšį ir sumažinti riziką, nuotolinę administracinę prieigą prie svarbiausių IRT komponentų reikėtų suteikti tik pagal principą „būtina žinoti“ ir naudojant patikimus autentiškumo patvirtinimo sprendimus.

4.13 Naudojant su prieigos kontrolės procesais susijusius produktus, priemones ir procedūras reikėtų apsaugoti prieigos kontrolės procesus, kad jie nebūtų pažeidžiami ar apeinami. Tai apima atitinkamų produktų, priemonių ir procedūrų atradimą, pateikimą, atšaukimą ir panaikinimą.

5 gairė. Nustatymas

Nuolatinė stebėsena ir nustatymas

5.1 MPT turėtų nustatyti ir įgyvendinti procesus ir pajėgumus, kad nuolat stebėtų veiklos funkcijas, pagalbinius procesus ir informacinius išteklius siekdami nustatyti anomalius veiksmus teikiant mokėjimo paslaugas. Vykdydami tokią nuolatinę stebėseną, MPT turėtų įsidiegti tinkamas ir veiksmingas fizinio ir loginio įsibrovimo ir teikiant mokėjimo paslaugas naudojamų informacinių išteklių konfidencialumo, vientisumo ir prieinamumo pažeidimų nustatymo priemones.

5.2 Nuolatinės stebėsenos ir nustatymo procesai turėtų apimti:

a) svarbius vidaus ir išorės veiksnius, įskaitant veiklos ir IRT administracines funkcijas;

b) operacijas, siekiant nustatyti atvejus, kai paslaugų teikėjai ar kiti subjektai netinkamai naudojasi prieiga, ir

c) galimas vidaus ir išorės grėsmes.

5.3 MPT turėtų įgyvendinti nustatymo priemones, kad galėtų nustatyti galimą informacijos nutekėjimą, kenkėjišką kodą ir kitas grėsmes saugumui, taip pat viešai žinomas pažeidžiamas programinės ir aparatinės įrangos vietas ir tikrinti, ar yra susijusių naujų saugumo atnaujinimo pakeitimų.

Operacinių ar saugumo incidentų stebėsena ir pranešimas apie juos

5.4 MPT turėtų nustatyti tinkamus kriterijus ir ribines vertes, kuriomis remiantis įvykį būtų galima pripažinti operaciniu ar saugumo incidentu, kaip apibrėžta šių gairių skirsnyje „Sąvokų apibrėžtys“, ir ankstyvojo perspėjimo rodiklius, kurie turėtų būti įspėjimas MPT, kad šie galėtų anksti nustatyti operacinius ar saugumo incidentus.

5.5 Siekdami užtikrinti nuoseklią ir integruotą operacinių ar saugumo incidentų stebėseną, tvarkymą ir su jais susijusius tolesnius veiksmus, MPT turėtų sukurti tinkamus procesus ir organizacines struktūras.

5.6 MPT turėtų sukurti pranešimo apie tokius operacinius ar saugumo incidentus ir su saugumu susijusių klientų skundų pateikimo vyresniajai vadovybei procedūrą.

6 gairė. Veiklos tęstinumas

6.1 MPT turėtų parengti patikimą veiklos tęstinumo valdymo planą siekdamos užtikrinti kuo didesnį savo gebėjimą nuolat teikti mokėjimo paslaugas ir apriboti nuostolius veiklai rimtai sutrikus.

6.2 Siekdami parengti patikimą veiklos tęstinumo valdymo planą, MPT turėtų kruopščiai išnagrinėti jiems kylančią rimto verslo sutrikdymo ir prieigos riziką ir (kiekybiškai ir kokybiškai) įvertinti galimą jų poveikį, remdamiesi vidaus ir (arba) išorės duomenimis ir scenarijų analize. Remdamiesi nustatytomis ir klasifikuotomis svarbiausiomis funkcijomis, procesais, sistemomis, operacijomis ir tarpusavio ryšiais, kaip numatyta GL 3.1–GL 3.3, MPT turėtų teikti pirmenybę veiklos tęstinumo veiksmams remdamiesi rizika pagrįstu metodu, kuris gali būti grindžiamas pagal GL 3 atliktu rizikos vertinimu. Priklausomai nuo MPT verslo modelio tai, pavyzdžiui, gali padėti toliau tvarkyti svarbiausias operacijas kartu tęsiant taisomuosius veiksmus.

6.3 Remdamasis pagal GL 6.2 atlikta analize MPT turėtų įdiegti:

a) VTP, siekdamas užtikrinti, kad galėtų tinkamai reaguoti į nenumatytas situacijas ir galėtų toliau vykdyti svarbiausią veiklą, ir

b) rizikos mažinimo priemones, kurių reikia imtis nutraukiant mokėjimo paslaugas ir nutraukiant galiojančias sutartis, siekiant išvengti neigiamo poveikio mokėjimo sistemoms ir MPV ir užtikrinti vykstančių mokėjimo operacijų įvykdymą.

Scenarijais grindžiamas veiklos tęstinumo planavimas

6.4 MPT turėtų apsvarstyti įvairius scenarijus, įskaitant kraštutinius, bet įmanomus, su kuriais jam gali tekti susidurti, ir įvertinti galimą tokių scenarijų poveikį.

6.5 Remdamasis pagal GL 6.2 atlikta analize ir pagal GL 6.4 nustatytais tikėtinais scenarijais, MPT turėtų parengti reagavimo ir atkūrimo planus:

a) sutelkdamas dėmesį į poveikį svarbiausių funkcijų, procesų, sistemų, operacijų ir tarpusavio ryšių įgyvendinimui;

b) kurie būtų įforminti dokumentais, kuriais galėtų naudotis veiklos ir pagalbiniai skyriai ir kuriuos būtų galima skubiai pritaikyti iškilus nenumatytam atvejui, ir

c) kurie būtų atnaujinami atsižvelgiant į patirtį, sukauptą atliekant bandymus, nustatytą riziką ir grėsmes ir pasikeitusius atkūrimo tikslus ir prioritetus.

Veiklos tęstinumo planų bandymai

6.6 MPT turėtų atlikti savo VTP bandymus ir užtikrinti, kad bent kartą per metus būtų atliekami jų svarbiausių funkcijų, procesų, sistemų, operacijų ir tarpusavio ryšių veikimo bandymai. Planais turėtų būti remiami tikslai apsaugoti ir, jei būtina, naujai apibrėžti operacijų vientisumą ir prieinamumą, taip pat informacinių išteklių konfidencialumą.

6.7 Planai turėtų būti atnaujinami bent kartą per metus atsižvelgiant į bandymų rezultatus, turimus žvalgybos duomenis apie grėsmes, informacijos dalijimąsi ir su ankstesniais įvykiais susijusią patirtį, kintančius atkūrimo tikslus, operaciniu ir techniniu požiūriu tikėtinų scenarijų, kurie dar neįvyko, analizę ir tam tikrais atvejais atliktų sistemų ir procesų pakeitimų analizę. Rengdami savo VTP, MPT turėtų konsultuotis ir koordinuoti savo veiksmus su atitinkamais vidaus ir išorės suinteresuotaisiais subjektais.

6.8 MPT VTP bandymai turėtų būti atliekami:

a) remiantis pakankamu scenarijų rinkiniu, kaip numatyta GL 6.4;

b) kvestionuojant prielaidas, kuriomis pagrįsti VTP, įskaitant valdymo priemones ir informavimo krizės atveju planus, ir

c) numatant procedūras, kurias taikant tikrinami darbuotojų ir procesų gebėjimai tinkamai reaguoti į pirmiau nurodytus scenarijus.

6.9 MPT turėtų reguliariai stebėti savo VTP veiksmingumą ir dokumentuoti ir analizuoti bet kokius kylančius sunkumus ar atliekant bandymus nustatytus trūkumus.

Informavimas krizės atveju

6.10 Sutrikus veiklai arba iškilus nenumatytai situacijai, įgyvendindami VTP, MPT turėtų būti įsidiegę veiksmingas informavimo krizės atveju priemones, kad visi svarbūs vidaus ir išorės suinteresuotieji subjektai, įskaitant išorės paslaugų teikėjus, būtų laiku ir tinkamai informuoti.

7 gairė. Saugumo priemonių bandymai

7.1 MPT turėtų sukurti ir įgyvendinti bandymų sistemą, kurioje būtų tikrinami saugumo priemonių patikimumas ir veiksmingumas, ir užtikrinti, kad bandymų sistemoje būtų atsižvelgiama į naujausias atliekant rizikos stebėsenos veiksmus nustatytas grėsmes ir pažeidžiamas vietas.

7.2 MPT turėtų užtikrinti, kad keičiant infrastruktūrą, procesus ar procedūras ir atliekant pakeitimus, susijusius su svarbiais operaciniais ar saugumo incidentais, būtų atliekami bandymai.

7.3 Bandymų sistemoje taip pat turėtų būti saugumo priemonių, susijusių su i) mokėjimo terminalais ir prietaisais, naudojamais mokėjimo paslaugoms teikti, ii) mokėjimo terminalais ir prietaisais, naudojamais MPV autentiškumui patvirtinti, ir iii) prietaisais ir programine įranga, kurią MPT teikia MPV autentiškumo patvirtinimo kodams generuoti (gauti).

7.4 Bandymų sistemoje turėtų būti užtikrinama, kad bandymai:

a) būtų atliekami vykdant oficialų MPT pokyčių valdymo procesą siekiant užtikrinti jų patikimumą ir veiksmingumą;

b) būtų atliekami nepriklausomų bandymų specialistų, turinčių pakankamai žinių, įgūdžių ir patirties bandant mokėjimo paslaugų saugumo priemones, kurie nedalyvauja kuriant atitinkamų mokėjimo paslaugų ar sistemų, kurių bandymus planuojama atlikti, saugumo

priemones, bent jau kai atliekami galutiniai bandymai prieš pradedant taikyti saugumo priemones, ir

c) apimtų pažeidžiamumo vertinimus ir skverbties bandymus, atitinkančius nustatytos su mokėjimo paslaugomis susijusios rizikos lygį.

7.5 MPT turėtų atlikti nuolatinius ir reguliarius mokėjimo paslaugų saugumo priemonių bandymus. Teikiant mokėjimo paslaugas būtinų sistemų (kaip aprašyta GL 3.2) bandymai atliekami bent kartą per metus. Nebūtinos sistemos turėtų būti bandomos reguliariai taikant rizika pagrįstą metodą, bet ne rečiau nei kartą per trejus metus.

7.6 MPT turėtų stebėti ir vertinti vykdomų bandymų rezultatus ir atitinkamai atnaujinti savo saugumo priemones ir, kai tai apima svarbiausių sistemų priemones, tai daryti nepagrįstai nedelsiant.

8 gairė. Informuotumas apie padėtį

Grėsmės ir informuotumas apie padėtį

8.1 MPT turėtų sukurti ir įgyvendinti procesus ir organizacines struktūras, kuriomis siekiama nustatyti ir nuolat stebėti grėsmes saugumui ir veiklai, kurios galėtų padaryti reikšmingą poveikį jų gebėjimui teikti mokėjimo paslaugas.

8.2 MPT turėtų analizuoti operacinius ar saugumo incidentus, kurie buvo nustatyti ar įvyko organizacijoje ir (arba) už jos ribų. MPT turėtų nagrinėti svarbiausią įgytą patirtį, sukauptą atliekant tokią analizę, ir atitinkamai atnaujinti saugumo priemones.

8.3 MPT turėtų aktyviai stebėti technologinę plėtrą siekdami užtikrinti, kad būtų informuoti apie saugumo riziką.

Mokymo ir informuotumo saugumo klausimais užtikrinimo programos

8.4 MPT turėtų parengti visiems darbuotojams skirtą mokymo programą siekdami užtikrinti jų pasirengimą vykdyti savo pareigas laikantis atitinkamos saugumo politikos ir procedūrų, kad būtų sumažintas žmonių klaidų, vagystės, sukčiavimo, piktnaudžiavimo ar nuostolių atvejų skaičius. MPT turėtų užtikrinti, kad pagal mokymo programą būtų numatytas darbuotojų mokymas bent kartą per metus ir, prireikus, dažniau.

8.5 MPT turėtų užtikrinti, kad GL 3.1 išvardytas pagrindines pareigas einantiems darbuotojams būtų kasmet arba, prireikus, dažniau rengiamas tikslinis mokymas informacijos saugumo klausimais.

8.6 MPT turėtų parengti ir įgyvendinti periodines informuotumo saugumo klausimais užtikrinimo programas, kurių tikslas – šviesti darbuotojus ir mažinti su informacijos saugumu susijusią riziką. Pagal tas programas MPT darbuotojai turėtų pranešti apie bet kokius nejprastus veiksmus ir incidentus.

9 gairė. Santykių su mokėjimo paslaugų vartotojais vadyba

Mokėjimo paslaugų vartotojų informavimas apie saugumo riziką ir rizikos mažinimo veiksmus

9.1 MPT turėtų sukurti ir įgyvendinti procesus, kuriais būtų didinamas MPV informuotumas apie su mokėjimo paslaugomis susijusią saugumo riziką ir MPV būtų teikiama pagalba ir patarimai.

9.2 MPV teikiamą pagalbą ir patarimus reikėtų atnaujinti atsižvelgiant į naujas grėsmes ir pažeidžiamas vietas, MPV reikėtų informuoti apie pokyčius.

9.3 Jeigu tai įmanoma pagal produkto funkcionalumą, MPT turėtų leisti MPV išjungti tam tikras mokėjimų funkcijas, susijusias su MPT mokėjimo paslaugų vartotojams teikiamomis mokėjimo paslaugomis.

9.4 Jeigu pagal Direktyvos (ES) 2015/2366 68 straipsnio 1 dalį MPT susitarė su mokėtoju dėl taikant tam tikras mokėjimo priemones vykdomų mokėjimo operacijų sumų apribojimų, MPT turėtų pasiūlyti mokėtojui galimybę koreguoti tas ribas jas padidinant iki didžiausios sutartos ribos.

9.5 MPT turėtų pasiūlyti MPV galimybę gauti pranešimus apie bandymus ir (arba) nepavykusius bandymus inicijuoti mokėjimo operacijas, kad jie galėtų nustatyti sukčiavimo ar piktnaudžiavimo jų sąskaita atvejus.

9.6 MPT turėtų nuolat informuoti MPV apie saugumo procedūrų atnaujinimą, darantį poveikį MPV teikiant mokėjimo paslaugas.

9.7 MPT turėtų teikti MPV pagalbą visais klausimais ir atsiliepti į pagalbos prašymus ir pranešimus apie anomalijas ar su mokėjimo paslaugų saugumo aspektais susijusias problemas. MPV turėtų būti tinkamai informuojami, kaip gauti tokią pagalbą.