EBA/GL/2017/17

12/01/2018

Obecné pokyny

k bezpečnostním opatřením v souvislosti s operačními a bezpečnostními riziky platebních služeb podle směrnice (EU) 2015/2366 (PSD2)

1. Dodržování předpisů a oznamovací povinnost

Status těchto obecných pokynů

1. Tento dokument obsahuje obecné pokyny vydané podle článku 16 nařízení Evropského parlamentu a Rady (EU) č. 1093/2010[1]. V souladu s čl. 16 odst. 3 nařízení Evropského parlamentu a Rady (EU) č. 1093/2010 příslušné orgány a finanční instituce vynaloží veškeré úsilí, aby se těmito obecnými pokyny řídily.

2. Obecné pokyny formulují názor orgánu EBA na náležité postupy dohledu v rámci Evropského systému dohledu nad finančním trhem nebo na to, jak by unijní právní předpisy měly být uplatňovány v konkrétní oblasti. Příslušné orgány ve smyslu čl. 4 odst. 2 nařízení (EU) č. 1093/2010, na které se tyto obecné pokyny vztahují, by s nimi měly být v souladu a začlenit je do svých postupů (např. pozměněním právního rámce nebo dohledových postupů), včetně případů, kdy jsou obecné pokyny zaměřeny v prvé řadě na instituce.

Oznamovací povinnost

3. V souladu s čl. 16 odst. 3 nařízení (EU) č. 1093/2010 musí příslušné orgány do 12.03.2018 orgánu EBA oznámit, zda se těmito obecnými pokyny řídí nebo hodlají řídit, a v opačném případě uvést do tohoto data důvody, proč se jimi neřídí či nehodlají řídit. Neposkytnou-li příslušné orgány oznámení v této lhůtě, bude mít orgán EBA za to, že se těmito obecnými pokyny neřídí nebo nehodlají řídit. Oznámení by měla být zasílána na formuláři, který je k dispozici na internetových stránkách orgánu EBA, na adresu compliance@eba.europa.eu s označením „EBA/GL/2017/17“. Oznámení by měly předkládat osoby s příslušným oprávněním oznamovat, zda se jejich příslušné orgány těmito obecnými pokyny řídí nebo hodlají řídit. Jakoukoli změnu stavu dodržování pokynů je rovněž nutno oznámit orgánu EBA.

4. Oznámení budou zveřejněna na internetových stránkách orgánu EBA v souladu s čl. 16 odst. 3.

[1] Nařízení Evropského parlamentu a Rady (EU) č. 1093/2010 ze dne 24. listopadu 2010 o zřízení Evropského orgánu dohledu (Evropského orgánu pro bankovnictví), o změně rozhodnutí č. 716/2009/ES a o zrušení rozhodnutí Komise 2009/78/ES (Úř. věst. L 331, 15.12.2010, s. 12).

2. Předmět, oblast působnosti a definice

Předmět a oblast působnosti

5. Tyto obecné pokyny vycházejí z mandátu uděleného orgánu EBA v čl. 95 odst. 3 směrnice (EU) 2015/2366[2] (PSD2).

6. V těchto obecných pokynech jsou stanoveny požadavky na stanovení, provádění a sledování bezpečnostních opatření, která musí učinit poskytovatelé platebních služeb v souladu s čl. 95 odst. 1 směrnice (EU) 2015/2366 s cílem řídit operační a bezpečnostní rizika související s platebními službami, které poskytují.

Adresáti

7. Tyto obecné pokyny jsou určeny poskytovatelům platebních služeb ve smyslu čl. 4 odst. 11 směrnice (EU) 2015/2366 a uvedeným v definici „finančních institucí" v čl. 4 odst. 1 nařízení (EU) č. 1093/2010 a příslušným orgánům ve smyslu čl. 4 odst. 2 bodu i) uvedeného nařízení s odkazem na zrušenou směrnici 2007/64/ES[3] (v současnosti směrnice (EU) 2015/2366[4]).

Definice

8. Není-li stanoveno jinak, mají pojmy používané a definované ve směrnici (EU) 2015/2366 v těchto obecných pokynech stejný význam. Kromě toho pro účely těchto obecných pokynů platí tyto definice:

Vedoucí orgán	– Pro poskytovatele platebních služeb, kteří jsou úvěrovými institucemi, má tento pojem stejný význam jako definice v bodě 7 čl. 3 odst. 1 směrnice 2013/36/EU[5], – pro poskytovatele platebních služeb, kteří jsou platebními

[2] Směrnice Evropského parlamentu a Rady (EU) 2015/2366 ze dne 25. listopadu 2015 o platebních službách na vnitřním trhu, kterou se mění směrnice 2002/65/ES, 2009/110/ES a 2013/36/EU a nařízení (EU) č. 1093/2010 a zrušuje směrnice 2007/64/ES (Úř. věst. L 337, 23.12.2015, s. 35).

[3] Směrnice Evropského parlamentu a Rady 2007/64/ES ze dne 13. listopadu 2007 o platebních službách na vnitřním trhu, kterou se mění směrnice 97/7/ES, 2002/65/ES, 2005/60/ES a 2006/48/ES a zrušuje směrnice 97/5/ES (Úř. věst. L 319, 5.12.2007, s. 1).

[4] V souladu s druhým pododstavcem článku 114 směrnice (EU) 2015/2366 se odkazy na zrušenou směrnici 2007/64/ES považují za odkazy na směrnici (EU) 2015/2366 v souladu se srovnávací tabulkou obsaženou v příloze II směrnice (EU) 2015/2366.

[5] Směrnice Evropského parlamentu a Rady 2013/36/EU o přístupu k činnosti úvěrových institucí a o obezřetnostním dohledu nad úvěrovými institucemi a investičními podniky, o změně směrnice 2002/87/ES a zrušení směrnic 2006/48/ES a 2006/49/ES (Úř. věst. L 176, 27.6.2013, s. 338).

	institucemi nebo institucemi elektronických peněz, se pod tímto pojmem rozumí vedoucí pracovníci nebo osoby odpovědné za řízení poskytovatele platebních služeb, případně osoby odpovědné za řízení činností v oblasti platebních služeb poskytovatele platebních služeb, – pro poskytovatele platebních služeb uvedených v čl. 1 odst. 1 písm. c), e) a f) směrnice (EU) 2015/2366 má tento pojem význam, který mu přiznávají platné unijní nebo vnitrostátní právní předpisy.
Operační nebo bezpečnostní incident	Jednorázová událost nebo řada souvisejících událostí neplánovaných poskytovatelem platebních služeb, která má nebo pravděpodobně bude mít nepříznivý dopad na integritu, dostupnost, důvěrnost, autenticitu a/nebo kontinuitu služeb souvisejících s platbami.
Vrcholné vedení	(a) Pro poskytovatele platebních služeb, kteří jsou úvěrovými institucemi, má tento pojem stejný význam jako definice v bodě 9 čl. 3 odst. 1 směrnice 2013/36/EU; (b) pro poskytovatele platebních služeb, kteří jsou platebními institucemi nebo institucemi elektronických peněz, se tímto pojmem rozumí fyzické osoby, které vykonávají výkonné funkce v rámci instituce a které jsou zodpovědné vedoucímu orgánu za každodenní řízení poskytovatele platebních služeb; (c) pro poskytovatele platebních služeb uvedených v čl. 1 odst. 1 písm. c), e) a f) směrnice (EU) 2015/2366 má tento pojem význam, který mu přiznávají platné unijní nebo vnitrostátní právní předpisy.
Bezpečnostní riziko	Riziko vyplývající z nevhodných nebo neúspěšných interních postupů nebo vnějších událostí, které mají nebo mohou mít nepříznivý dopad na dostupnost, integritu a důvěrnost systémů informačních a komunikačních technologií a/nebo informace používané pro poskytování platebních služeb. To zahrnuje riziko kybernetických útoků nebo nedostatečné fyzické zabezpečení.
Ochota podstupovat riziko	Souhrnná míra a druhy rizik, které je instituce ochotná podstupovat v rámci své schopnosti nést riziko v souladu se svým obchodním modelem, aby dosáhla svých strategických cílů.

3. Provádění

Datum použití

9. Tyto obecné pokyny se použijí ode dne 13. ledna 2018.

4. Obecné pokyny

Obecný pokyn 1: Všeobecné zásady

1.1 Všichni poskytovatelé platebních služeb by měli splňovat všechna ustanovení těchto obecných pokynů. Míra podrobnosti by měla odpovídat velikosti poskytovatele platebních služeb a rovněž povaze, rozsahu, složitosti a rizikovosti konkrétních služeb, které poskytovatel platebních služeb poskytuje nebo má v úmyslu poskytovat.

Obecný pokyn 2: Správa a řízení

Rámec řízení operačních a bezpečnostních rizik

2.1 Poskytovatelé platebních služeb by měli vytvořit účinný rámec řízení operačních a bezpečnostních rizik (dále jen „rámec řízení rizik“), který by měl schválit a nejméně jednou ročně přezkoumat vedoucí orgán a případně vrcholné vedení. Tento rámec by měl být zaměřen na bezpečnostní opatření ke zmírnění operačních a bezpečnostních rizik a měl by být poskytovateli platebních služeb plně začleněn do celkových procesů řízení rizik.

2.2 Rámec řízení rizik by měl:

a) zahrnovat komplexní bezpečnostní předpis podle čl. 5 odst. 1 písm. j) směrnice (EU) 2015/2366;

b) být v souladu s ochotou poskytovatele platebních služeb podstupovat riziko;

c) definovat a přiřadit klíčové role a odpovědnosti, a také příslušné hierarchické vztahy hlášení potřebné k posílení bezpečnostních opatření a pro řízení bezpečnostních a operačních rizik;

d) stanovit nezbytné postupy a systémy pro identifikaci, měření, sledování a řízení řady rizik, která vyplývají z činnosti poskytovatele platebních služeb v souvislosti s platbami a kterým jsou poskytovatelé platebních služeb vystaveni, včetně opatření k zajištění kontinuity činnosti.

2.3 Poskytovatelé platebních služeb by měli zajistit, aby rámec řízení rizik byl řádně zdokumentován a doplněn o zdokumentované zkušenosti, které byly získány během jeho provádění a sledování.

2.4 Poskytovatelé platebních služeb by měli zajistit, aby před významnou změnou infrastruktury, procesů nebo postupů a po každém závažném operačním nebo bezpečnostním incidentu, který má dopad na bezpečnost poskytovaných platebních služeb, bylo přezkoumáno, zda je změny nebo zlepšení rámce řízení rizik nutné provést bez zbytečného prodlení.

Modely řízení rizik a kontroly

2.5 Poskytovatelé platebních služeb by měli stanovit tři účinné linie obrany nebo ekvivalentní modely interního řízení rizik a kontroly s cílem identifikovat a řídit operační a bezpečnostní rizika. Poskytovatelé platebních služeb by měli zajistit, aby výše uvedený model vnitřní kontroly disponoval dostatečnými pravomocemi, nezávislostí, zdroji a přímými hierarchickými vztahy hlášení vedoucímu orgánu, případně vrcholnému vedení.

2.6 Bezpečnostní opatření stanovená v těchto obecných pokynech by měla být kontrolována auditory, kteří mají odborné znalosti v oblasti IT bezpečnosti a plateb a jsou provozně nezávislí na poskytovateli platebních služeb. Frekvence a zaměření takových auditů by měly zohledňovat odpovídající bezpečnostní rizika.

Outsourcing

2.7 Poskytovatelé platebních služeb by měli zajistit účinnost bezpečnostních opatření stanovených v těchto obecných pokynech, pokud jsou provozní funkce platebních služeb, včetně informačních systémů, zajišťovány externě.

2.8 Poskytovatelé platebních služeb by měli zajistit, že příslušné a přiměřené bezpečnostní cíle, opatření a provozní úkoly budou zahrnuty do smluv a dohod o úrovni služeb uzavřených s externími poskytovateli těchto služeb. Poskytovatelé platebních služeb by měli sledovat a ověřovat, že tito poskytovatelé zajišťují správnou úroveň bezpečnostních cílů, opatření a provozních úkolů.

Obecný pokyn 3: Posouzení rizik

Identifikace funkcí, procesů a aktiv

3.1 Poskytovatelé platebních služeb by měli identifikovat své obchodní funkce, klíčové role a podpůrné procesy a sestavit a pravidelně aktualizovat jejich soupis, aby zmapovali význam každé funkce, role a podpůrného procesu a jejich vzájemné závislosti s operačními a bezpečnostními riziky.

3.2 Poskytovatelé platebních služeb by měli určit, sestavit a pravidelně aktualizovat soupis informačních aktiv, jako jsou systémy informačních a komunikačních technologií, jejich konfigurace, další infrastruktury a také propojení s jinými interními a externími systémy, aby bylo možné spravovat aktiva, která podporují kritické obchodní funkce a procesy.

Klasifikace funkcí, procesů a aktiv

3.3 Poskytovatelé platebních služeb by měli klasifikovat kritičnost identifikovaných obchodních funkcí, podpůrných procesů a informačních aktiv.

Posouzení rizik funkcí, procesů a aktiv

3.4 Poskytovatelé platebních služeb by měli zajistit, aby byly průběžně sledovány hrozby a zranitelná místa a aby byly pravidelně přezkoumávány scénáře rizik, které mají dopad na jejich obchodní funkce, kritické procesy a informační aktiva. V rámci povinnosti provádět a předkládat příslušným orgánům aktualizované a komplexní posouzení operačních a bezpečnostních rizik spojených s platebními službami, které poskytují, a přiměřenosti opatření ke zmírnění těchto rizik a kontrolních mechanismů zavedených v reakci na tato rizika, jak je stanoveno v čl. 95 odst. 2 směrnice (EU) 2015/2366, by poskytovatelé platebních služeb měli nejméně jednou ročně nebo v kratších intervalech stanovených příslušným orgánem provádět a dokumentovat posouzení rizik funkcí, procesů a informačních aktiv, které byly identifikovány a klasifikovány, aby bylo možné identifikovat a posoudit klíčová operační a bezpečnostní rizika. Takové posouzení rizik by mělo být provedeno také před jakoukoli významnou změnou infrastruktury, procesu nebo postupu, která má dopad na bezpečnost platebních služeb.

3.5 Na základě posouzení rizik by měli poskytovatelé platebních služeb stanovit, zda a do jaké míry jsou nezbytné změny stávajících bezpečnostních opatření, používaných technologií a postupů či nabízených platebních služeb. Poskytovatelé platebních služeb by měli zohlednit čas potřebný k provedení změn a čas na přijetí příslušných prozatímních bezpečnostních opatření, aby byly minimalizovány operační nebo bezpečnostní incidenty, podvody a případné rušivé vlivy při poskytování platebních služeb.

Obecný pokyn 4: Ochrana

4.1 Poskytovatelé platebních služeb by měli stanovit a provádět preventivní bezpečnostní opatření související s identifikovanými operačními a bezpečnostními riziky. Tato opatření by měla zajistit odpovídající úroveň bezpečnosti v souladu s identifikovanými riziky.

4.2 Poskytovatelé platebních služeb by měli stanovit a uplatňovat přístup „hloubkové obrany“ zavedením vícevrstvých kontrol, které zahrnují osoby, procesy a technologie, přičemž každá vrstva bude sloužit jako bezpečnostní síť pro předchozí vrstvy. Pod pojmem hloubková obrana se rozumí určení více než jedné kontroly pokrývající stejné riziko, jako je princip čtyř očí, dvouúrovňové ověření, segmentace sítě a vícečetné firewally.

4.3 Poskytovatelé platebních služeb by měli zajistit důvěrnost, integritu a dostupnost svých kritických logických a fyzických aktiv, zdrojů a citlivých platebních údajů svých uživatelů platebních služeb, ať už se momentálně nevyužívají, přenášejí se, nebo se používají. Pokud data zahrnují osobní

údaje, měla by být tato opatření prováděna v souladu s nařízením (EU) 2016/679[6] nebo případně s nařízením (ES) č. 45/2001.[7]

4.4 Poskytovatelé platebních služeb by měli průběžně zjišťovat, zda změny stávajícího provozního prostředí ovlivňují stávající bezpečnostní opatření nebo vyžadují přijetí dalších opatření, aby se zmírnilo příslušné riziko. Tyto změny by měly být součástí formálního procesu řízení změn poskytovatele platebních služeb, který by měl zajistit, že změny jsou řádně naplánovány, otestovány, zdokumentovány a schváleny. Na základě zjištěných bezpečnostních hrozeb a uskutečněných změn by mělo být provedeno testování, které bude zahrnovat scénáře relevantních a známých potenciálních útoků.

4.5 Při navrhování, vývoji a poskytování platebních služeb by poskytovatelé platebních služeb měli zajistit uplatňování zásady oddělení funkcí a zásady „minimálních práv“. Poskytovatelé platebních služeb by měli věnovat zvláštní pozornost oddělení IT prostředí, zejména vývojářského, testovacího a výrobního prostředí.

Integrita a důvěrnost údajů a systémů

4.6 Při navrhování, vývoji a poskytování platebních služeb by poskytovatelé platebních služeb měli zajistit, aby shromažďování, přesměrování, zpracování, ukládání a/nebo archivace a vizualizace citlivých platebních údajů uživatele platebních služeb byly přiměřené, relevantní a omezené na nezbytnou míru pro poskytování platebních služeb.

4.7 Poskytovatelé platebních služeb by měli pravidelně kontrolovat, zda je software používaný k poskytování platebních služeb, včetně softwaru souvisejícího s platbami uživatelů, aktuální a zda jsou použity bezpečnostní aktualizace pro kritické případy. Poskytovatelé platebních služeb by měli zajistit, aby byly zavedeny mechanismy kontroly k ověření integrity softwaru, firmwaru a informací o platebních službách.

Fyzické zabezpečení

4.8 Poskytovatelé platebních služeb by měli mít zavedena vhodná opatření k fyzickému zabezpečení, zejména k ochraně citlivých platebních údajů uživatelů platebních služeb, jakož i systémů informačních a komunikačních technologií používaných k poskytování platebních služeb.

Kontrola přístupu

4.9 Fyzický a logický přístup k systémům informačních a komunikačních technologií by měl být povolen pouze oprávněným osobám. Oprávnění by mělo být přiděleno v souladu s úkoly

[6] Nařízení Evropského parlamentu a Rady ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně údajů) (Úř. věst. L 119, 4.5.2016, s. 1).

[7] Nařízení Evropského parlamentu a Rady (ES) č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů (Úř. věst. L 8, 12.1.2001, s. 1).

a povinnostmi zaměstnanců a mělo by být omezeno na osoby, které jsou řádně vyškoleny a sledovány. Poskytovatelé platebních služeb by měli zavést kontroly, které spolehlivě omezí přístup k systémům informačních a komunikačních technologií na osoby s legitimními obchodními požadavky. Elektronický přístup prostřednictvím aplikací k datům a systémům by měl být omezen na minimum, které je nutné k poskytování příslušné služby.

4.10 Poskytovatelé platebních služeb by měli zavést silné kontroly privilegovaného přístupu do systému prostřednictvím striktního omezení počtu zaměstnanců s rozšířenými oprávněními k přístupu do systému a pečlivého dohledu nad nimi. Měly by být prováděny kontroly přístupu založeného na rolích, zaznamenávání a přezkoumávání systémových činností privilegovaných uživatelů a silné ověřování a sledování anomálií. Poskytovatelé platebních služeb by měli spravovat přístupová práva k informačním aktivům a jejich podpůrným systémům a poskytovat je pouze těm, kteří dané informace potřebují. Přístupová práva by měla být pravidelně revidována.

4.11 Záznamy o přístupu by měly být uloženy po dobu odpovídající kritičnosti identifikovaných obchodních funkcí, podpůrných procesů a informačních aktiv v souladu s odstavci 3.1 a 3.2 těchto obecných pokynů, aniž by byly dotčeny požadavky na uchovávání údajů stanovené v unijních a vnitrostátních právních předpisech. Poskytovatelé platebních služeb by měli tyto informace používat k usnadnění identifikace a vyšetřování anomálií, které byly zjištěny při poskytování platebních služeb.

4.12 Aby byla zajištěna bezpečná komunikace a snížena rizika, měl by být vzdálený administrativní přístup k důležitým komponentám systému informačních a komunikačních technologií poskytován pouze těm, kteří dané informace potřebují, a uplatňovat při tom řešení silného ověřování.

4.13 Používání produktů, nástrojů a postupů souvisejících s procesy kontroly přístupu by mělo chránit procesy kontroly přístupu před zneužitím nebo obcházením. To zahrnuje registraci, dodání, odvolání a odebrání příslušných produktů, nástrojů a postupů.

Obecný pokyn 5: Odhalování neobvyklé činnosti

Průběžná kontrola a odhalování neobvyklé činnosti

5.1 Poskytovatelé platebních služeb by měli stanovit a uplatňovat postupy a možnosti průběžného sledování obchodních funkcí, podpůrných procesů a informačních aktiv, aby bylo možné odhalit neobvyklé činnosti při poskytování platebních služeb. V rámci tohoto průběžného sledování by poskytovatelé platebních služeb měli mít k dispozici vhodné a účinné možnosti k odhalení fyzického nebo logického narušení, jakož i porušení důvěrnosti, integrity a dostupnosti informačních aktiv používaných při poskytování platebních služeb.

5.2 Průběžné procesy kontroly a odhalování neobvyklé činnosti by se měly zaměřit na:

a) relevantní interní a externí faktory, včetně obchodních a správcovských funkcí v systému informačních a komunikačních technologií;

b) transakce, aby bylo možné odhalit zneužití přístupu poskytovateli služeb nebo jinými subjekty; a

c) potenciální interní a externí hrozby.

5.3 Poskytovatelé platebních služeb by měli zavést opatření k identifikaci možných úniků informací, škodlivých kódů a dalších bezpečnostních hrozeb a veřejně známých zranitelných míst softwaru a hardwaru a měli by kontrolovat odpovídající nové aktualizace zabezpečení.

Sledování a hlášení operačních nebo bezpečnostních incidentů

5.4 Poskytovatelé platebních služeb by měli stanovit příslušná kritéria a prahové hodnoty ke klasifikaci události jako operačního nebo bezpečnostního incidentu, jak je stanoveno v oddíle „Definice“ těchto obecných pokynů, a také indikátory včasného varování, které by pro poskytovatele platebních služeb měly sloužit jako upozornění umožňující včas odhalit operační nebo bezpečnostní incident.

5.5 Poskytovatelé platebních služeb by měli stanovit příslušné postupy a organizační struktury, aby zajistili důsledné a integrované sledování a řešení operačních nebo bezpečnostních incidentů a navazující opatření.

5.6 Poskytovatelé platebních služeb by měli stanovit postup pro hlášení takových operačních nebo bezpečnostních incidentů, jakož i stížností zákazníků, které souvisí se zabezpečením, vrcholnému vedení.

Obecný pokyn 6: Kontinuita činnosti

6.1 Poskytovatelé platebních služeb by měli zavést řádné řízení kontinuity činnosti s cílem maximalizovat svou schopnost průběžně poskytovat platební služby a omezit ztráty v případě vážného narušení činnosti.

6.2 Za účelem vypracování řádného plánu řízení kontinuity činnosti by měli poskytovatelé platebních služeb pečlivě analyzovat svou expozici vůči závažným narušením činnosti a kvantitativně i kvalitativně posoudit jejich možný dopad pomocí analýzy interních anebo externích dat a scénářů. Na základě identifikovaných a klasifikovaných kritických funkcí, procesů, systémů, transakcí a vzájemně závislých činností v souladu s odstavci 3.1 až 3.3 těchto obecných pokynů by poskytovatelé platebních služeb měli upřednostnit opatření týkající se kontinuity činnosti, která využívají rizikově orientovaný přístup, což může být založeno na posouzeních rizik provedených podle oddílu 3 těchto obecných pokynů. V závislosti na obchodním modelu poskytovatele platebních služeb to může například usnadnit další zpracování kritických transakcí, zatímco se pracuje na nápravě.

6.3 Na základě analýzy provedené podle odstavce 6.2 těchto obecných pokynů by poskytovatelé platebních služeb měli zavést:

a) plány pro zajištění kontinuity činnosti, které mají zabezpečit, že poskytovatelé platebních služeb budou schopni náležitě reagovat na mimořádné události a budou schopni udržovat svou kriticky důležitou obchodní činnost; a

b) opatření, která mají být přijata v případě ukončení platebních služeb nebo stávajících smluv, aby se zabránilo nepříznivým účinkům na platební systémy a uživatele platebních služeb a zajistilo se provedení dosud nezpracovaných platebních transakcí.

Plánování kontinuity činnosti na základě scénářů

6.4 Poskytovatelé platebních služeb by měli zvážit řadu různých scénářů, včetně extrémních, ale pravděpodobných, jimž by mohli být vystaveni, a posoudit jejich případný dopad.

6.5 Na základě analýzy provedené podle odstavce 6.2 těchto obecných pokynů a pravděpodobných scénářů identifikovaných podle odstavce 6.4 těchto obecných pokynů by poskytovatelé platebních služeb měli vypracovat plány reakce a obnovy, které:

a) by se měly zaměřit na dopad kritických funkcí, procesů, systémů, transakcí a vzájemně závislých činností;

b) by měly být zdokumentovány a zpřístupněny obchodním a podpůrným jednotkám a snadno dostupné v případě nouze a

c) by měly být aktualizovány v souladu s poznatky získanými z testování, nově identifikovanými riziky či hrozbami a změněnými cíli a prioritami obnovy.

Testování plánů kontinuity činnosti

6.6 Poskytovatelé platebních služeb by měli otestovat své plány pro zajištění kontinuity činnosti a zajistit, aby kritické funkce, procesy, systémy, transakce a vzájemně závislé činnosti byly otestovány nejméně jednou za rok. Plány by měly podporovat cíle, které mají chránit a v případě potřeby obnovit integritu a dostupnost operací a zajistit důvěrnost informačních aktiv.

6.7 Plány by měly být aktualizovány nejméně jednou za rok, a to na základě výsledků testování, informací o současných hrozbách, sdílení zkušeností z předchozích událostí a změn cílů obnovy, a také analýzy provozně a technicky pravděpodobných scénářů, ke kterým dosud nedošlo, případně i po změnách v systémech a procesech. Poskytovatelé platebních služeb by při stanovování svých plánů pro zajištění kontinuity činnosti měli vše konzultovat a koordinovat s příslušnými interními a externími zainteresovanými stranami.

6.8 Poskytovatelé platebních služeb by při testování svých plánů pro zajištění kontinuity činnosti měli:

a) do testování zahrnout odpovídající soubor scénářů, jak je uvedeno v odstavci 6.4 těchto obecných pokynů;

b) testování navrhnout tak, aby prověřilo předpoklady, na nichž spočívají plány pro zajištění kontinuity činnosti, včetně systémů správy a řízení a plánů krizové komunikace; a

c) zahrnout postupy k ověření schopností svých zaměstnanců a procesů, zda dokáží odpovídajícím způsobem reagovat na výše uvedené scénáře.

6.9 Poskytovatelé platebních služeb by měli pravidelně sledovat účinnost svých plánů pro zajištění kontinuity činnosti a zdokumentovat a analyzovat veškeré problémy nebo chyby, které testy odhalí.

Krizová komunikace

6.10 V případě narušení nebo mimořádné situace a během provádění plánů pro zajištění kontinuity činnosti by měli poskytovatelé platebních služeb zajistit, aby byla zavedena účinná komunikační opatření pro případ krize, aby byly včas a vhodným způsobem informovány všechny příslušné interní i externí zainteresované strany, včetně externích poskytovatelů služeb.

Obecný pokyn 7: Testování bezpečnostních opatření

7.1 Poskytovatelé platebních služeb by měli stanovit a zavést rámec testování, který potvrdí spolehlivost a účinnost bezpečnostních opatření, a zajistit, aby rámec testování byl přizpůsoben novým hrozbám a zranitelným místům identifikovaným prostřednictvím činností souvisejících se sledováním rizik.

7.2 Poskytovatelé platebních služeb by měli zajistit, aby testy byly prováděny v případě změn infrastruktury, procesů nebo postupů, a pokud byly změny provedeny v důsledku závažných operačních nebo bezpečnostních incidentů.

7.3 Rámec testování by měl rovněž zahrnovat bezpečnostní opatření týkající se i) platebních terminálů a zařízení používaných k poskytování platebních služeb; ii) platebních terminálů a zařízení používaných k ověřování uživatelů platebních služeb a iii) zařízení a softwaru poskytovaných uživateli poskytovatelem platebních služeb za účelem generování/získání ověřovacího kódu.

7.4 Rámec testování by měl zajistit, že:

a) testy jsou prováděny v rámci formálního procesu řízení změn poskytovatele platebních služeb, aby byla zajištěna jejich spolehlivost a účinnost;

b) přinejmenším závěrečné testy před zavedením bezpečnostních opatření provádějí nezávislé osoby, které mají dostatečné vědomosti, dovednosti a odborné znalosti k testování bezpečnostních opatření platebních služeb a nepodílí se na vývoji bezpečnostních opatření vztahujících se k příslušným platebním službám nebo testovaným systémům; a

c) testy zahrnují kontroly zranitelných míst a penetrační testování přiměřené úrovni rizika identifikovaného u platebních služeb.

7.5 Poskytovatelé platebních služeb by v souvislosti se svými platebními službami měli provádět průběžné a opakované testy bezpečnostních opatření. U systémů, které jsou kritické pro

poskytování platebních služeb (jak je popsáno v odstavci 3.2 těchto obecných pokynů), se tyto testy provádějí alespoň jednou ročně. Ostatní systémy by měly být testovány pravidelně na základě rizikově orientovaného přístupu, nejméně však každé tři roky.

7.6 Poskytovatelé platebních služeb by měli sledovat a vyhodnocovat výsledky provedených testů a odpovídajícím způsobem aktualizovat svá bezpečnostní opatření, v případě kritických systémů bez zbytečného prodlení.

Obecný pokyn 8: Informovanost o situaci a neustálé učení

Hrozby a informovanost o situaci

8.1 Poskytovatelé platebních služeb by měli stanovit a uplatňovat postupy a organizační struktury s cílem identifikovat a neustále sledovat bezpečnostní a operační hrozby, které by mohly podstatně ovlivnit schopnost poskytovat platební služby.

8.2 Poskytovatelé platebních služeb by měli analyzovat operační nebo bezpečnostní incidenty, které byly identifikovány nebo se vyskytly uvnitř organizace a/nebo mimo ni. Poskytovatelé platebních služeb by měli zvážit základní poznatky z těchto analýz a odpovídajícím způsobem aktualizovat bezpečnostní opatření.

8.3 Poskytovatelé platebních služeb by měli aktivně sledovat technologický vývoj, aby zajistili, že jsou si vědomi bezpečnostních rizik.

Programy odborné přípravy a programy zvyšování povědomí o bezpečnosti

8.4 Poskytovatelé platebních služeb by měli zavést program odborné přípravy pro všechny zaměstnance, aby zajistili, že zaměstnanci budou plnit všechny své úkoly a povinnosti v souladu s příslušnými bezpečnostními zásadami a postupy, a eliminovat tak lidské chyby, krádeže, podvody, zneužití nebo ztráty. Poskytovatelé platebních služeb by měli zajistit, aby na základě programu odborné přípravy byli zaměstnanci proškoleni nejméně jednou ročně a v případě potřeby i častěji.

8.5 Poskytovatelé platebních služeb by měli zajistit, aby zaměstnanci na klíčových pozicích podle odstavce 3.1 těchto obecných pokynů byli každoročně nebo v případě potřeby častěji školeni o zabezpečení informací.

8.6 Poskytovatelé platebních služeb by měli stanovit a implementovat pravidelné programy pro zvyšování povědomí o bezpečnosti s cílem vzdělávat své zaměstnance a řešit rizika týkající se bezpečnosti informací. V rámci těchto programů by se od zaměstnanců poskytovatelů platebních služeb mělo požadovat, aby hlásili jakékoli neobvyklé činnosti a incidenty.

Obecný pokyn 9: Řízení vztahů s uživateli platebních služeb

Informovanost uživatelů platebních služeb o bezpečnostních rizicích a opatřeních ke zmírnění rizik

9.1 Poskytovatelé platebních služeb by měli stanovit a uplatňovat postupy za účelem zvýšení povědomí uživatelů platebních služeb o bezpečnostních rizicích spojených s platebními službami, a to prostřednictvím asistenčních služeb a poradenství pro uživatele platebních služeb.

9.2 Asistenční služby a poradenství nabízené uživatelům platebních služeb by měly být aktualizovány s ohledem na nové hrozby a zranitelná místa a uživatelé by měli být informováni o všech změnách.

9.3 V případě, že to umožňuje funkčnost produktu, by poskytovatelé platebních služeb měli umožnit uživatelům deaktivovat konkrétní platební funkce, které souvisí s platebními službami nabízenými uživateli poskytovatelem platebních služeb.

9.4 Pokud se poskytovatel platebních služeb v souladu s čl. 68 odst. 1 směrnice (EU) 2015/2366 dohodl s plátcem na omezení výdajů u platebních transakcí prováděných prostřednictvím zvláštních platebních prostředků, měl by poskytovatel platební služby poskytnout plátci možnost tento stanovený maximální limit upravit.

9.5 Poskytovatelé platebních služeb by měli uživatelům platebních služeb poskytnout možnost dostávat upozornění o provedených a/nebo neúspěšných pokusech o zadání příkazu k platební transakci, což jim umožní odhalit podvodné nebo neoprávněné používání jejich účtu.

9.6 Poskytovatelé platebních služeb by měli uživatele informovat o aktuálních změnách bezpečnostních postupů, které mají vliv na poskytování platebních služeb uživateli.

9.7 Poskytovatelé platebních služeb by měli uživatelům poskytnout pomoc v případě jakéhokoli dotazu, žádosti o podporu a oznámení anomálií nebo potíží týkajících se bezpečnostních záležitostí, které se vztahují na platební služby. Uživatelé platebních služeb by měli být náležitě informováni o tom, jak mohou tuto pomoc získat.