EBA/GL/2017/17

12/01/2018

Usmernenia

k bezpečnostným opatreniam vzťahujúcim sa na prevádzkové a bezpečnostné riziká platobných služieb podľa smernice (EÚ) 2015/2366 (PSD2)

1. Povinnosti týkajúce sa dodržiavania súladu (compliance) s predpismi a ohlasovacia povinnosť

Štatút týchto usmernení

1. Tento dokument obsahuje usmernenia vydané podľa článku 16 nariadenia (EÚ) č. 1093/2010[1]. Podľa článku 16 ods. 3 nariadenia č. 1093/2010 príslušné orgány a finančné inštitúcie vynaložia všetko úsilie na dodržanie týchto usmernení a odporúčaní.

2. Tieto usmernenia zahŕňajú názor EBA na príslušné postupy dohľadu v rámci Európskeho systému finančného dohľadu alebo na spôsob uplatňovania právnych predpisov Únie v konkrétnej oblasti. Príslušné orgány, ako sú vymedzené v článku 4 ods. 2 nariadenia (EÚ) č. 1093/2010, na ktoré sa tieto usmernenia vzťahujú, ich majú dodržiavať tak, že ich začlenia do svojich postupov dohľadu podľa potreby (napr. zmenou svojho právneho rámca alebo postupov dohľadu), a to aj v prípade, keď sú tieto usmernenia zamerané prevažne na banky.

Požiadavky na vykazovanie

3. Podľa článku 16 ods. 3 nariadenia (EÚ) č. 1093/2010 musia príslušné orgány oznámiť EBA, či tieto usmernenia dodržiavajú alebo majú v úmysle dodržať, alebo musia uviesť dôvody ich nedodržania do 12.03.2018. Ak do tohto dátumu nebude doručené žiadne oznámenie, EBA sa bude domnievať, že ich príslušné orgány nedodržiavajú. Oznámenia sa majú zaslať prostredníctvom formulára dostupného na adrese compliance@eba.europa.eu spolu s označením „EBA/GL/2017/17“. Tieto oznámenia majú príslušnému orgánu predkladať osoby, ktoré sú oprávnené podávať správy o dodržaní v mene svojich príslušných orgánov. Akúkoľvek zmenu stavu dodržiavania ustanovení treba takisto oznámiť EBA.

4. Oznámenia budú uverejnené na webovej stránke EBA v súlade s článkom 16 ods. 3.

[1] Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1093/2010 z 24. novembra 2010, ktorým sa zriaďuje Európsky orgán dohľadu (Európsky orgán pre bankovníctvo) a ktorým sa mení a dopĺňa rozhodnutie č. 716/2009/ES a zrušuje rozhodnutie Komisie 2009/78/ES (Ú. v. EÚ L 331, 15.12.2010. s. 12).

2. Predmet úpravy, rozsah pôsobnosti a vymedzenie pojmov

Predmet úpravy a rozsah pôsobnosti

5. Tieto usmernenia vychádzajú z mandátu, ktorý bol orgánu EBA udelený podľa článku 95 ods. 3 smernice (EÚ) 2015/2366[2] (ďalej len „smernica PSD2“).

6. V týchto usmerneniach sa stanovujú požiadavky na zavedenie, vykonávanie a monitorovanie bezpečnostných opatrení, ktoré poskytovatelia platobných služieb musia prijať v súlade s článkom 95 ods. 1 smernice (EÚ) 2015/2366 na riadenie prevádzkových a bezpečnostných rizík súvisiacich s platobnými službami, ktoré poskytujú.

Adresáti

7. Tieto usmernenia sú určené poskytovateľom platobných služieb v zmysle článku 4 ods. 11 smernice (EÚ) 2015/2366 a uvedených vo vymedzení pojmu „finančné inštitúcie“ v článku 4 ods. 1 nariadenia (EÚ) č. 1093/2010 a príslušným orgánom v zmysle článku 4 ods. 2 písm. i) uvedeného nariadenia s odkazom na zrušenú smernicu 2007/64/ES[3] (v súčasnosti smernica (EÚ) 2015/2366[4]).

Vymedzenie pojmov

8. Pokiaľ nie je uvedené inak, pojmy používané a vymedzené v smernici (EÚ) 2015/2366 majú v týchto usmerneniach rovnaký význam. Na účely týchto usmernení okrem toho platí toto vymedzenie pojmov:

[2] Smernica Európskeho parlamentu a Rady (EÚ) 2015/2366 z 25. novembra 2015 o platobných službách na vnútornom trhu, ktorou sa menia smernice 2002/65/ES, 2009/110/ES a 2013/36/EÚ a nariadenie (EÚ) č. 1093/2010 a ktorou sa zrušuje smernica 2007/64/ES (Ú. v. EÚ L 337, 23.12.2015, s. 35).

[3] Smernica Európskeho parlamentu a Rady 2007/64/ES z 13. novembra 2007 o platobných službách na vnútornom trhu, ktorou sa menia a dopĺňajú smernice 97/7/ES, 2002/65/ES, 2005/60/ES a 2006/48/ES a ktorou sa zrušuje smernica 97/5/ES (Ú. v. EÚ L 319, 5.12.2007, s. 1).

[4] V súlade s článkom 114 druhým pododsekom smernice (EÚ) 2015/2366 sa každý odkaz na zrušenú smernicu 2007/64/ES považuje za odkaz na smernicu (EÚ) 2015/2366 a vykladá sa v súlade s tabuľkou zhody uvedenou v prílohe II k smernici (EÚ) 2015/2366.

Riadiaci orgán	– v prípade poskytovateľov platobných služieb, ktorí sú úverovými inštitúciami, má tento pojem rovnaký význam ako vymedzenie pojmu v článku 3 ods. 1 bode 7 smernice 2013/36/EÚ[5], – v prípade poskytovateľov platobných služieb, ktorí sú platobnými inštitúciami alebo inštitúciami elektronických peňazí, sa pod týmto pojmom rozumejú členovia predstavenstva a osoby zodpovedné za riadenie poskytovateľa platobnej služby a v relevantných prípadoch aj osôb zodpovedných za riadenie činností súvisiacich s platobnými službami poskytovateľa platobnej služby, – v prípade poskytovateľov platobných služieb uvedených v článku 1 ods. 1 písm. c), e) a f) smernice (EÚ) 2015/2366 má tento pojem význam, ktorý mu priznáva platné právo Únie alebo vnútroštátne právo.
Prevádzkový alebo bezpečnostný incident	Jednorazová udalosť alebo rad navzájom súvisiacich udalostí, ktoré poskytovateľ platobných služieb neplánoval a ktoré majú alebo pravdepodobne budú mať nepriaznivý vplyv na integritu, dostupnosť, dôvernosť, autentickosť a/alebo kontinuitu služieb súvisiacich s platbami.
Vrcholový manažment	(a) v prípade poskytovateľov platobných služieb, ktorí sú úverovými inštitúciami, má tento pojem rovnaký význam ako vymedzenie pojmu v článku 3 ods. 1 bode 9 smernice 2013/36/EÚ, (b) v prípade poskytovateľov platobných služieb, ktorí sú platobnými inštitúciami a inštitúciami elektronických peňazí, sa pod týmto pojmom rozumejú fyzické osoby, ktoré vykonávajú výkonné funkcie v rámci inštitúcie a ktoré sa zodpovedajú riadiacemu orgánu za každodenné riadenie poskytovateľa platobných služieb, (c) v prípade poskytovateľov platobných služieb uvedených v článku 1 ods. 1 písm. c), e) a f) smernice (EÚ) 2015/2366 má tento pojem význam, ktorý mu priznáva platné právo Únie alebo vnútroštátne právo.
Bezpečnostné riziko	Riziko vyplývajúce z neprimeraných alebo zlyhaných interných postupov alebo externých udalostí, ktoré majú alebo môžu mať nepriaznivý vplyv na dostupnosť, integritu, dôvernosť systémov informačných a komunikačných technológií (IKT) a/alebo informácií používaných na poskytovanie platobných služieb. Sem patrí aj riziko kybernetických útokov alebo nedostatočnej fyzickej bezpečnosti.

[5] Smernica Európskeho parlamentu a Rady 2013/36/EÚ o prístupe k činnosti úverových inštitúcií a prudenciálnom dohľade nad úverovými inštitúciami a investičnými spoločnosťami, o zmene smernice 2002/87/ES a o zrušení smerníc 2006/48/ES a 2006/49/ES (Ú. v. EÚ L 176, 27.6.2013, s. 338).

Ochota podstupovať riziká	Agregovaná úroveň a typy rizík, ktoré je inštitúcia ochotná znášať v rámci svojej schopnosti znášať riziko a v súlade so svojím obchodným modelom, aby dosiahla svoje strategické ciele.

3. Vykonávanie

Dátum začiatku uplatňovania

9. Tieto usmernenia sa uplatňujú od 13. januára 2018.

4. Usmernenia

Usmernenie 1: Všeobecná zásada

1.1 Všetci poskytovatelia platobných služieb by mali dodržiavať všetky ustanovenia uvedené v týchto usmerneniach. Miera podrobnosti by mala zodpovedať veľkosti poskytovateľa platobných služieb, ako aj povahe, rozsahu, komplexnosti a rizikovosti konkrétnych služieb, ktoré poskytovateľ platobných služieb poskytuje alebo zamýšľa poskytovať.

Usmernenie 2: Správa a riadenie

Rámec riadenia prevádzkových a bezpečnostných rizík

2.1 Poskytovatelia platobných služieb by mali zaviesť účinný rámec riadenia prevádzkových a bezpečnostných rizík (ďalej len „rámec riadenia rizík“), ktorý by aspoň raz ročne mal schváliť a preskúmať riadiaci orgán a prípadne vrcholový manažment. Tento rámec by sa mal zameriavať na bezpečnostné opatrenia na zmiernenie prevádzkových a bezpečnostných rizík a mal by sa plne začleniť do celkových postupov riadenia rizík poskytovateľa platobných služieb.

2.2 Rámec riadenia rizík by mal:

a) obsahovať komplexný dokument o bezpečnostnej politike uvedený v článku 5 ods. 1 písm. j) smernice (EÚ) 2015/2366;

b) byť v súlade so schopnosťou a potenciálom poskytovateľa platobných služieb podstupovať riziká;

c) definovať a priradiť kľúčové úlohy a zodpovednosti, ako aj príslušné línie oznamovania, ktoré sú potrebné na presadzovanie bezpečnostných opatrení a na riadenie bezpečnostných a prevádzkových rizík;

d) zaviesť potrebné postupy a systémy na identifikáciu, meranie, monitorovanie a riadenie rizík obsiahnutých v činnostiach poskytovateľa platobných služieb súvisiacich s platbami, ktorým je poskytovateľ platobných služieb vystavený, vrátane mechanizmov na zabezpečenie kontinuity činností.

2.3 Poskytovatelia platobných služieb by mali zabezpečiť riadne zdokumentovanie a aktualizáciu rámca riadenia rizík so zdokumentovanými skúsenosťami, ktoré boli získané pri jeho implementácii a monitorovaní.

2.4 Poskytovatelia platobných služieb by mali zabezpečiť, aby pred rozsiahlou zmenou infraštruktúry, procesov alebo postupov a po každom veľkom prevádzkovom alebo bezpečnostnom incidente, ktorý ovplyvňuje bezpečnosť poskytovaných platobných služieb, preskúmali, či zmeny alebo zlepšenia rámca riadenia rizík je alebo nie je potrebné vykonať bez zbytočného odkladu.

Modely riadenia rizík a kontroly

2.5 Poskytovatelia platobných služieb by mali stanoviť tri účinné línie obrany alebo ekvivalentný model vnútorného riadenia rizík a kontroly s cieľom identifikovať a riadiť prevádzkové a bezpečnostné riziká. Poskytovatelia platobných služieb by mali zabezpečiť, aby uvedený model vnútornej kontroly disponoval dostatočnou právomocou, nezávislosťou, zdrojmi a priamymi líniami oznamovania vo vzťahu k riadiacemu orgánu a v prípade potreby vrcholovému manažmentu.

2.6 Bezpečnostné opatrenia stanovené v týchto usmerneniach by mali overiť audítori s odbornými znalosťami v oblasti bezpečnosti IT a platieb, ktorí sú prevádzkovo nezávislí v rámci poskytovateľa platobných služieb alebo sú od neho nezávislí. Frekvencia a zameranie takýchto auditov by mali zohľadňovať príslušné bezpečnostné riziká.

Externé vykonávanie činností

2.7 Poskytovatelia platobných služieb by mali zabezpečiť účinnosť bezpečnostných opatrení stanovených v týchto usmerneniach, ak sú prevádzkové funkcie platobných služieb vrátane systémov IT vykonávané externe.

2.8 Poskytovatelia platobných služieb by mali zabezpečiť, aby sa adekvátne a primerané bezpečnostné ciele, opatrenia a výkonnostné ciele zahrnuli do zmlúv a dohôd o úrovni poskytovaných služieb uzatvorených s externými poskytovateľmi, ktorým boli tieto činnosti zverené. Poskytovatelia platobných služieb by mali monitorovať a zaisťovať, aby títo poskytovatelia zabezpečovali požadovanú úroveň bezpečnostných cieľov, bezpečnostných opatrení a výkonnostných cieľov.

Usmernenie 3: Posúdenie rizík

Identifikácia funkcií, procesov a aktív

3.1 Poskytovatelia platobných služieb by mali určiť, zostaviť a pravidelne aktualizovať súpis svojich obchodných funkcií, kľúčových úloh a podporných procesov s cieľom zmapovať dôležitosť každej funkcie, úlohy a podporných procesov a ich prepojenie s prevádzkovými a bezpečnostnými rizikami.

3.2 Poskytovatelia platobných služieb by mali určiť, zostaviť a pravidelne aktualizovať súpis informačných aktív, ako sú systémy IKT, ich konfigurácie, ďalšie infraštruktúry a takisto prepojenia s inými vnútornými a vonkajšími systémami, aby mohli spravovať aktíva, ktoré podporujú ich kritické obchodné funkcie a procesy.

Klasifikácia funkcií, procesov a aktív

3.3 Poskytovatelia platobných služieb by mali klasifikovať identifikované obchodné funkcie, podporné procesy a informačné prostriedky z hľadiska kritickej povahy.

Hodnotenie rizika funkcií, procesov a aktív

3.4 Poskytovatelia platobných služieb by mali zabezpečiť, aby sa neustále monitorovali hrozby a zraniteľné miesta a pravidelne preskúmali rizikové scenáre, ktoré majú vplyv na ich obchodné funkcie, kritické procesy a informačné aktíva. V rámci povinnosti vykonávať a predkladať príslušným orgánom aktualizované a komplexné posúdenie rizík, pokiaľ ide o operačné a bezpečnostné riziká súvisiace s platobnými službami, ktoré poskytujú, a o primeranosť opatrení na zmiernenie rizík a kontrolných mechanizmov zavedených v rámci reakcie na tieto riziká, ako je uvedené v článku 95 ods. 2 smernice (EÚ) 2015/2366, by poskytovatelia platobných služieb mali aspoň raz ročne alebo v kratších intervaloch stanovených príslušným orgánom, vykonať a zdokumentovať posúdenie rizík funkcií, procesov a informačných aktív, ktoré identifikovali a klasifikovali, aby bolo možné určiť a posúdiť kľúčové prevádzkové a bezpečnostné riziká. Takéto hodnotenia rizík by sa mali vykonať aj pred akoukoľvek rozsiahlou zmenou infraštruktúry, procesu alebo postupov, ktoré majú vplyv na bezpečnosť platobných služieb.

3.5 Na základe posúdenia rizík by poskytovatelia platobných služieb mali určiť, či a do akej miery sú potrebné existujúce bezpečnostné opatrenia, používané technológie a postupy alebo ponúkané platobné služby. Poskytovatelia platobných služieb by mali vziať do úvahy čas potrebný na vykonanie zmien a čas potrebný na prijatie príslušných predbežných bezpečnostných opatrení s cieľom minimalizovať prevádzkové alebo bezpečnostné incidenty, podvody a potenciálne rušivé vplyvy pri poskytovaní platobných služieb.

Usmernenie 4: Ochrana

4.1 Poskytovatelia platobných služieb by mali stanoviť a implementovať preventívne bezpečnostné opatrenia proti identifikovaným prevádzkovým a bezpečnostným rizikám. Tieto opatrenia by mali zabezpečiť primeranú úroveň bezpečnosti v súlade s identifikovanými rizikami.

4.2 Poskytovatelia platobných služieb by mali stanoviť a implementovať prístup „hĺbkovej ochrany“ zavedením viacvrstvových kontrol, ktoré zahŕňajú ľudí, procesy a technológiu, pričom každá vrstva má slúžiť ako záchranná sieť pre predchádzajúce vrstvy. Pod pojmom hĺbková ochrana sa rozumie určenie viac ako jednej kontroly zameranej na rovnaké riziko, ako je napríklad zásada štyroch očí, dvojstupňové overenie, segmentácia siete a viaceré brány firewall.

4.3 Poskytovatelia platobných služieb by mali zabezpečiť dôvernosť, integritu a dostupnosť svojich kritických logických a fyzických aktív, zdrojov a citlivých platobných údajov používateľov platobných služieb, či už sú tieto údaje v pokoji, v tranzite alebo sa používajú. Ak údaje zahŕňajú osobné údaje, takéto opatrenia by sa mali vykonať v súlade s nariadením (EÚ) 2016/679[6] alebo prípadne s nariadením (ES) č. 45/2001.[7]

[6] Nariadenie Európskeho parlamentu a Rady (EÚ) z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (Ú. v. EÚ L 119, 4.5.2016, s. 1).

[7] Nariadenie Európskeho parlamentu a Rady (ES) č. 45/2001 z 18. decembra 2000 o ochrane jednotlivcov so zreteľom na spracovanie osobných údajov inštitúciami a orgánmi Spoločenstva a o voľnom pohybe takýchto údajov (Ú. v. ES L 8, 12.1.2001, s. 1).

4.4 Poskytovatelia platobných služieb by mali priebežne určovať, či zmeny v existujúcom prevádzkovom prostredí ovplyvňujú existujúce bezpečnostné opatrenia alebo si vyžadujú prijatie ďalších opatrení na zmiernenie príslušného rizika. Tieto zmeny by mali byť súčasťou formálneho procesu riadenia zmien poskytovateľa platobných služieb, ktorý by mal zabezpečiť správne naplánovanie, testovanie, zdokumentovanie a povolenie zmien. Na základe pozorovaných bezpečnostných hrozieb a vykonaných zmien by sa malo vykonať testovanie tak, aby zahrnulo scenáre relevantných a známych potenciálnych útokov.

4.5 Pri navrhovaní, vývoji a poskytovaní platobných služieb by mali poskytovatelia platobných služieb zabezpečiť oddelenie úloh a uplatnenie zásady tzv. najnižších práv (least privilege). Poskytovatelia platobných služieb by mali venovať osobitnú pozornosť oddeleniu prostredí IT, a to najmä vývojového, testovacieho a produkčného prostredia.

Integrita a dôvernosť údajov a systémov

4.6 Pri navrhovaní, vývoji a poskytovaní platobných služieb by poskytovatelia platobných služieb mali zabezpečiť, aby zhromažďovanie, presmerovanie, spracovanie, ukladanie a/alebo archivovanie a zobrazovanie citlivých platobných údajov používateľov platobných služieb boli primerané, relevantné a obmedzené na to, čo je nevyhnutné na poskytnutie ich platobných služieb.

4.7 Poskytovatelia platobných služieb by mali pravidelne kontrolovať, či je softvér používaný na poskytovanie platobných služieb vrátane softvéru súvisiaceho s platbami používateľov aktuálny a či sú nasadené kritické bezpečnostné záplaty. Poskytovatelia platobných služieb by mali zabezpečiť, aby boli zavedené mechanizmy kontroly integrity s cieľom overiť integritu softvéru, firmvéru a informácií o platobných službách.

Fyzická bezpečnosť

4.8 Poskytovatelia platobných služieb by mali mať zavedené vhodné fyzické bezpečnostné opatrenia, a to najmä na ochranu citlivých platobných údajov používateľov platobných služieb, ako aj systémov IKT používaných na poskytovanie platobných služieb.

Kontrola prístupu

4.9 Fyzický a logický prístup k systémom informačných a komunikačných technológií (IKT) by sa mal povoliť iba oprávneným osobám. Oprávnenie by sa malo prideliť v súlade s úlohami a povinnosťami zamestnancov a obmedziť na osoby, ktoré sú primerane vyškolené a sledované. Poskytovatelia platobných služieb by mali zaviesť kontroly, ktoré spoľahlivo obmedzujú prístup k systémom IKT na osoby s legitímnymi obchodnými požiadavkami. Elektronický prístup prostredníctvom aplikácií k údajom a systémom by sa mal obmedziť na minimum, ktoré je potrebné na poskytovanie príslušnej služby.

4.10 Poskytovatelia platobných služieb by mali zaviesť prísne kontroly nad privilegovaným prístupom do systému tak, že prísne obmedzia zamestnancov a budú dôkladne vykonávať dohľad nad zamestnancami s rozšírenými oprávneniami na prístup do systému. Mali by sa vykonávať kontroly,

ako sú kontroly prístupu založeného na úlohách, záznamy do denníka a preskúmanie systémových činností privilegovaných používateľov, prísne overovanie a monitorovanie anomálií. Poskytovatelia platobných služieb by mali spravovať prístupové práva k informačným aktívam a ich podporným systémom na základe tzv. potreby poznať (need-to-know). Prístupové práva by sa mali pravidelne preskúmavať.

4.11 Záznamy do denníka je potrebné uchovávať počas obdobia zodpovedajúceho kritickosti identifikovaných obchodných činností, podporných procesov a informačných aktív v súlade s usmerneniami 3.1 a 3.2 bez toho, aby boli dotknuté požiadavky na uchovávanie stanovené v práve Únie a vo vnútroštátnom práve. Poskytovatelia platobných služieb by mali tieto informácie použiť na uľahčenie identifikácie a vyšetrovania nezvyčajných činností zistených pri poskytovaní platobných služieb.

4.12 S cieľom zabezpečiť bezpečnú komunikáciu a znížiť riziko by sa mal správcovský prístup na diaľku ku kritickým komponentom IKT poskytovať iba na základe potreby poznať a pri použití riešení prísneho overenia.

4.13 Prevádzka produktov, nástrojov a postupov súvisiacich s postupmi kontroly prístupu by mala chrániť postupy kontroly prístupu pred ohrozením alebo obchádzaním. Zahŕňa to registráciu, doručenie, zrušenie a stiahnutie príslušných produktov, nástrojov a postupov z obehu.

Usmernenie 5: Odhaľovanie

Nepretržité monitorovanie a odhaľovanie

5.1 Poskytovatelia platobných služieb by mali stanoviť a implementovať procesy a možnosti na nepretržité monitorovanie obchodných funkcií, podporných procesov a informačných aktív s cieľom odhaliť nezvyčajné činnosti pri poskytovaní platobných služieb. V rámci tohto nepretržitého monitorovania by poskytovatelia platobných služieb mali mať k dispozícii vhodné a účinné možnosti na detekciu fyzického alebo logického narušenia, ako aj porušenia dôvernosti, integrity a dostupnosti informačných aktív používaných pri poskytovaní platobných služieb.

5.2 Procesy nepretržitého monitorovania a odhaľovania by mali zahŕňať:

a) príslušné interné a externé faktory vrátane obchodných funkcií a správcovských funkcií IKT;

b) transakcie s cieľom odhaliť zneužitie prístupu poskytovateľmi služieb alebo inými subjektmi a

c) potenciálne vnútorné a vonkajšie hrozby.

5.3 Poskytovatelia platobných služieb by mali zaviesť opatrenia na odhaľovanie možných únikov informácií, škodlivého kódu a iných bezpečnostných hrozieb, ako aj verejne známych zraniteľností softvéru a hardvéru a kontrolovať, či majú zodpovedajúce nové bezpečnostné aktualizácie.

Monitorovanie a oznamovanie prevádzkových alebo bezpečnostných incidentov

5.4 Poskytovatelia platobných služieb by mali určiť vhodné kritériá a prahové hodnoty na klasifikáciu udalosti ako prevádzkového alebo bezpečnostného incidentu, ako je stanovené vo Vymedzení pojmov týchto usmernení, ako aj ukazovatele včasného varovania, ktoré by mali pre poskytovateľa platobných služieb slúžiť ako upozornenie, aby bol schopný včas odhaliť prevádzkové alebo bezpečnostné incidenty.

5.5 Poskytovatelia platobných služieb by mali vytvoriť vhodné postupy a organizačné štruktúry na zabezpečenie konzistentného a integrovaného monitorovania a riešenia prevádzkových alebo bezpečnostných incidentov, ako aj vykonávania nadväzujúcich činností.

5.6 Poskytovatelia platobných služieb by mali zaviesť postup, ktorým sa budú vrcholovému manažmentu oznamovať takéto prevádzkové alebo bezpečnostné incidenty, ako aj sťažnosti zákazníkov súvisiace s bezpečnosťou.

Usmernenie 6: Kontinuita činností

6.1 Poskytovatelia platobných služieb by mali vytvoriť spoľahlivé riadenie kontinuity činností, aby sa maximalizovala ich schopnosť priebežne poskytovať platobné služby a obmedziť straty v prípade vážneho prerušenia činnosti.

6.2 Na vytvorenie spoľahlivého riadenia kontinuity činností by poskytovatelia platobných služieb mali dôkladne analyzovať svoju expozíciu závažným prerušeniam činnosti a mali by zhodnotiť (kvantitatívne aj kvalitatívne) ich možný dosah pomocou analýzy interných a/alebo externých údajov a scenárov. Na základe identifikovaných a klasifikovaných kritických funkcií, procesov, systémov, transakcií a vzájomných závislostí v súlade s usmerneniami 3.1 až 3.3 by poskytovatelia platobných služieb mali uprednostňovať opatrenia súvisiace s kontinuitou činností pomocou prístupu založeného na riziku, ktorý sa môže zakladať na hodnoteniach rizík vykonaných podľa usmernenia 3. V závislosti od obchodného modelu poskytovateľa platobných služieb to môže, napríklad, uľahčiť ďalšie spracovanie kritických transakcií, zatiaľ čo úsilie o nápravu bude pokračovať.

6.3 Na základe analýzy vykonanej podľa usmernenia 6.2 by poskytovateľ platobných služieb mal zaviesť:

a) plány na zabezpečenie kontinuity činností, aby mohol primerane reagovať na núdzové situácie a udržiavať svoje kritické obchodné činnosti a

b) opatrenia na zmiernenie rizík, ktoré sa majú prijať v prípade ukončenia platobných služieb a ukončenia existujúcich zmlúv, aby sa zabránilo nepriaznivým účinkom na platobné systémy a používateľov platobných služieb a aby sa zabezpečilo vykonávanie platobných transakcií čakajúcich na spracovanie.

Plánovanie zabezpečenia kontinuity činností podľa scenára

6.4 Poskytovateľ platobných služieb by mal zvážiť celý rad rôznych scenárov vrátane extrémnych, ale vierohodných scenárov, ktorým by mohol byť vystavený, a posúdiť ich prípadný vplyv.

6.5 Na základe analýzy vykonanej podľa usmernenia 6.2 a vierohodných scenárov identifikovaných podľa usmernenia 6.4 by poskytovateľ platobných služieb mal vypracovať plány reakcie a obnovy, ktoré by mali byť:

a) zamerané na vplyv na prevádzku kritických funkcií, procesov, systémov, transakcií a vzájomných závislostí;

b) zdokumentované a prístupné obchodným a podporným jednotkám a byť ľahko dostupné v prípade núdze a

c) aktualizované v súlade so skúsenosťami získanými z testov, identifikovanými novými rizikami a hrozbami, ako aj so zmenenými cieľmi a s prioritami obnovy.

Testovanie plánov na zabezpečenie kontinuity činností

6.6 Poskytovatelia platobných služieb by mali svoje plány na zabezpečenie kontinuity činností testovať a zabezpečiť, aby sa prevádzka ich kritických funkcií, procesov, systémov, transakcií a vzájomné závislosti testovali najmenej raz ročne. Plány by mali podporovať ciele, ktoré majú chrániť, a v prípade potreby obnoviť, integritu a dostupnosť ich prevádzky a dôvernosť ich informačných aktív.

6.7 Plány by sa mali aktualizovať najmenej raz ročne na základe výsledkov testovania, aktuálnych informácií o hrozbách, výmeny informácií a získaných skúseností z predchádzajúcich udalostí a zmien cieľov obnovy, ako aj analýzy prevádzkovo a technicky prijateľných scenárov, ktoré sa ešte nevyskytli, a v prípade potreby po zmenách v systémoch a procesoch. Poskytovatelia platobných služieb by počas zostavovania svojich plánov na zabezpečenie kontinuity činností mali viesť konzultácie a koordinovať postup s príslušnými internými a externými zainteresovanými stranami.

6.8 Testovanie plánov na zabezpečenie kontinuity činností poskytovateľmi platobných služieb by:

a) malo zahŕňať primeraný súbor scenárov, ako je uvedené v usmernení 6.4;

b) malo byť navrhnuté tak, aby overilo predpoklady, na ktorých stoja plány na zabezpečenie kontinuity činností vrátane dohôd o riadení a plánov krízovej komunikácie a

c) malo zahŕňať postupy na overenie schopnosti zamestnancov a procesov primerane reagovať na vyššie uvedené scenáre.

6.9 Poskytovatelia platobných služieb by mali pravidelne monitorovať účinnosť svojich plánov na zabezpečenie kontinuity činností a dokumentovať a analyzovať všetky problémy alebo neúspešné výsledky, ktoré odhalili testy.

Komunikácia v prípade krízy

6.10 V prípade prerušenia prevádzky alebo núdzového stavu a počas vykonávania plánov na zabezpečenie kontinuity činností by poskytovatelia platobných služieb mali zabezpečiť, aby boli zavedené účinné opatrenia pre komunikáciu v prípade krízy, aby boli všetky príslušné interné

a externé zainteresované strany vrátane externých poskytovateľov služieb včas a primerane informované.

Usmernenie 7: Testovanie bezpečnostných opatrení

7.1 Poskytovatelia platobných služieb by mali stanoviť a implementovať rámec testovania na potvrdenie stability a účinnosti bezpečnostných opatrení a zabezpečiť prispôsobenie rámca testovania tak, aby zohľadňoval nové hrozby a zraniteľné miesta identifikované prostredníctvom činností monitorovania rizík.

7.2 Poskytovatelia platobných služieb by mali zabezpečiť vykonanie testov v prípade zmien infraštruktúry, procesov alebo postupov a ak v dôsledku závažných prevádzkových alebo bezpečnostných incidentov boli vykonané zmeny.

7.3 Rámec testovania by mal zahŕňať aj bezpečnostné opatrenia týkajúce sa i) platobných terminálov a zariadení používaných na poskytovanie platobných služieb; ii) platobných terminálov a zariadení používaných na autentifikáciu používateľa platobných služieb; a iii) zariadení a softvéru poskytnutých poskytovateľom platobných služieb používateľovi platobných služieb za účelom generovania/prijatia autentifikačného kódu.

7.4 Rámec testovania by mal zabezpečiť, že testy:

a) sa vykonávajú ako súčasť formálneho procesu riadenia zmien poskytovateľa platobných služieb, aby sa zabezpečila ich stabilita a účinnosť ;

b) vykonávajú nezávislí testovací pracovníci, ktorí majú dostatočné vedomosti, zručnosti a odborné znalosti v testovaní bezpečnostných opatrení platobných služieb a nepodieľajú sa na vývoji bezpečnostných opatrení pre príslušné platobné služby alebo systémy, ktoré sa majú testovať, a to aspoň v prípade záverečných testov pred uvedením bezpečnostných opatrení do prevádzky a

c) zahŕňajú kontroly zamerané na zraniteľné miesta a penetračné testy primerané úrovni rizika identifikovaného v platobných službách.

7.5 Poskytovatelia platobných služieb by pre svoje platobné služby mali vykonávať priebežné a opakované testy bezpečnostných opatrení V prípade systémov, ktoré sú kriticky dôležité pre poskytovanie ich platobných služieb (ako je uvedené v usmernení 3.2), sa tieto testy musia vykonať aspoň raz ročne. Nekritické systémy by sa mali pravidelne testovať pomocou prístupu založeného na rizikách, najmenej však každé tri roky.

7.6 Poskytovatelia platobných služieb by mali monitorovať a vyhodnocovať výsledky vykonaných testov a aktualizovať podľa toho svoje bezpečnostné opatrenia a v prípade kritických systémov bez zbytočného odkladu.

Usmernenie 8: Informovanosť o situácii a priebežné vzdelávanie

Prostredie hrozieb a informovanosť o situácii

8.1 Poskytovatelia platobných služieb by mali stanoviť a implementovať procesy a organizačné štruktúry, aby sa identifikovali a neustále monitorovali bezpečnostné a prevádzkové hrozby, ktoré by mohli významne ovplyvniť ich schopnosť poskytovať platobné služby.

8.2 Poskytovatelia platobných služieb by mali analyzovať prevádzkové alebo bezpečnostné incidenty, ktoré boli identifikované alebo ktoré sa vyskytli v rámci a/alebo mimo organizácie. Poskytovatelia platobných služieb by mali zvážiť kľúčové poznatky získané z týchto analýz a zodpovedajúcim spôsobom aktualizovať bezpečnostné opatrenia.

8.3 Poskytovatelia platobných služieb by mali aktívne monitorovať technologický vývoj s cieľom, aby boli informovaní o bezpečnostných rizikách.

Odborná príprava a programy zvyšovania informovanosti o bezpečnosti

8.4 Poskytovatelia platobných služieb by mali vytvoriť program odbornej prípravy pre všetkých zamestnancov, aby zabezpečili ich prípravu na vykonávanie povinností a úloh v súlade s príslušnými bezpečnostnými politikami a postupmi v záujme zníženia počtu chýb spôsobených ľudským faktorom, krádeží, podvodov, zneužití alebo strát. Poskytovatelia platobných služieb by mali zabezpečiť, aby sa program odbornej prípravy poskytoval zamestnancom najmenej raz ročne a v prípade potreby aj častejšie.

8.5 Poskytovatelia platobných služieb by mali zabezpečiť, aby zamestnanci, ktorí zastávajú kľúčové úlohy určené podľa usmernenia 3.1, každý rok alebo v prípade potreby aj častejšie absolvovali cielenú odbornú prípravu o informačnej bezpečnosti.

8.6 Poskytovatelia platobných služieb by mali stanoviť a vykonávať pravidelné programy na zvyšovanie informovanosti o bezpečnosti s cieľom vzdelávať svojich zamestnancov a riešiť riziká súvisiace s bezpečnosťou informácií. Tieto programy by mali od zamestnancov poskytovateľa platobných služieb vyžadovať oznámenie každej nezvyčajnej činnosti a incidentov.

Usmernenie 9: Riadenie vzťahov s používateľmi platobných služieb

Informovanosť používateľov platobných služieb o bezpečnostných rizikách a opatreniach na zmiernenie rizík

9.1 Poskytovatelia platobných služieb by mali stanoviť a implementovať procesy na zvýšenie povedomia používateľov platobných služieb o bezpečnostných rizikách spojených s platobnými službami tak, že poskytnú asistenčné služby a usmernenia pre používateľov platobných služieb.

9.2 Pomoc a usmernenia ponúkané používateľom platobných služieb by sa mali aktualizovať vzhľadom na nové hrozby a zraniteľné miesta, pričom používatelia platobných služieb by mali byť o zmenách informovaní.

9.3 Ak to umožňuje funkčnosť produktu, poskytovatelia platobných služieb by mali umožniť používateľom platobných služieb zakázať konkrétne platobné funkcie súvisiace s platobnými službami, ktoré poskytovateľ platobných služieb ponúka používateľovi platobných služieb.

9.4 Ak sa poskytovateľ platobných služieb v súlade s článkom 68 ods. 1 smernice (EÚ) 2015/2366 s platiteľom dohodne na výdavkových limitoch na platobné transakcie vykonávané prostredníctvom osobitných platobných nástrojov, poskytovateľ platobných služieb by mal poskytnúť platiteľovi možnosť upraviť tieto limity až do maximálneho dohodnutého limitu.

9.5 Poskytovatelia platobných služieb by mali používateľom platobných služieb poskytnúť možnosť prijímať upozornenia o iniciovaných a/alebo neúspešných pokusoch o iniciovanie platobných transakcií, čo im umožní odhaliť podvodné alebo škodlivé používanie ich účtu.

9.6 Poskytovatelia platobných služieb by mali informovať používateľov platobných služieb o aktualizáciách bezpečnostných postupov, ktoré majú vplyv na používateľov platobných služieb v súvislosti s poskytovaním platobných služieb.

9.7 Poskytovatelia platobných služieb by mali poskytnúť používateľom platobných služieb pomoc pri všetkých otázkach, žiadostiach o podporu a upozorneniach na anomálie alebo problémy týkajúce sa bezpečnostných záležitostí súvisiacich s platobnými službami. Používatelia platobných služieb by mali byť primerane informovaní o tom, ako možno takúto pomoc získať.