EBA/GL/2014/12_Rev1

19. decembra 2014

Záverečné usmernenia

týkajúce sa bezpečnosti internetových platieb

Obsah

Usmernenia týkajúce sa bezpečnosti internetových platieb

Štatút týchto usmernení

Tento dokument obsahuje usmernenia vydané podľa článku 16 nariadenia 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 (ďalej len „nariadenie o EBA“). V súlade s článkom 16 ods. 3 nariadenia o EBA musia príslušné orgány a finančné inštitúcie vynaložiť všetko úsilie na dodržanie týchto usmernení.

V usmerneniach sa uvádza stanovisko EBA k náležitým postupom dohľadu v rámci európskeho systému orgánov finančného dohľadu alebo spôsob, ktorým sa má uplatňovať právo Únie v konkrétnej oblasti. EBA preto očakáva, že všetky príslušné orgány finančné inštitúcie, ktorým sú tieto usmernenia určené, ich budú dodržiavať. Príslušné orgány, na ktoré sa usmernenia vzťahujú, ich majú dodržiavať tak, že ich primeraným spôsobom začlenia do svojich postupov dohľadu (napr. zmenou svojho právneho rámca alebo svojich procesov dohľadu), vrátane prípadov, keď sú usmernenia zamerané v prvom rade na inštitúcie.

Požiadavky na podávanie správ

Podľa článku 16 ods. 3 nariadenia (EÚ) č. 1093/2010 musia príslušné orgány informovať EBA o tom, či dodržiavajú alebo majú v úmysle dodržiavať tieto usmernenia alebo ak nie, musia uviesť dôvody nedodržiavania, a to do 5. mája 2015. V prípade neposkytnutia oznámenia v tejto lehote bude EBA považovať príslušné orgány za orgány, ktoré nedodržiavajú tieto usmernenia. Oznámenia treba posielať predložením formulára uvedeného v oddiele 5 na adresu compliance@eba.europa.eu s označením „EBA/GL/2014/12“. Oznámenia majú predkladať osoby s náležitým oprávnením na oznamovanie dodržiavania súladu v mene ich príslušných orgánov.

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

Hlava I – Rozsah pôsobnosti a vymedzenie pojmov

Rozsah pôsobnosti

1. V týchto usmerneniach je stanovený súbor minimálnych požiadaviek v oblasti bezpečnosti internetových platieb. Usmernenia vychádzajú z ustanovení smernice 2007/64/ES[1] (ďalej len „smernica o platobných službách“) a týkajú sa požiadaviek na poskytovanie informácií o platobných službách a povinností poskytovateľov platobných služieb v súvislosti s poskytovaním týchto služieb. Okrem toho sa v článku 10 ods. 4 smernice vyžaduje, aby platobné inštitúcie zaviedli rozsiahle riadiace opatrenia a zaviedli primerané mechanizmy vnútornej kontroly.

2. Usmernenia sa vzťahujú na poskytovanie platobných služieb ponúkaných cez internet poskytovateľmi platobných služieb, ako sú vymedzení v článku 1 smernice.

3. Adresátmi usmernení sú finančné inštitúcie podľa vymedzenia v článku 4 ods. 1 nariadenia (EÚ) č. 1093/2010 a príslušné orgány podľa vymedzenia v článku 4 ods. 2 nariadenia (EÚ) č. 1093/2010. Príslušné orgány v 28 členských štátoch Európskej únie majú zabezpečiť uplatňovanie týchto usmernení poskytovateľmi platobných služieb, na ktorých dohliadajú, ako sú vymedzení v článku 1 smernice o platobných službách.

4. Príslušné orgány sa tiež môžu rozhodnúť, že budú od poskytovateľov platobných služieb požadovať, aby im predkladali správy o uplatňovaní týchto usmernení.

5. Usmernenia nemajú vplyv na platnosť Odporúčaní Európskej centrálnej banky týkajúcich sa bezpečnosti internetových platieb (ďalej len „správa“).[2] V správe sa najmä naďalej predstavuje dokument, na základe ktorého centrálne banky majú v rámci funkcie dohľadu nad platobnými systémami a nástrojmi posudzovať dodržiavanie právnych predpisov v oblasti bezpečnosti internetových platieb.

6. V usmerneniach sú sformulované minimálne predpoklady. Nie je nimi dotknutá povinnosť poskytovateľov platobných služieb monitorovať a posudzovať riziká v rámci platobných operácií, vypracovať vlastné podrobné bezpečnostné zásady a prijať primerané opatrenia týkajúce sa bezpečnosti, pohotovostných plánov, krízového riadenia a zabezpečenia kontinuity činností, ktoré budú úmerné rizikám prítomným v poskytovaných platobných službách.

7. Cieľom usmernení je vymedziť spoločné minimálne požiadavky na internetové platobné služby uvedené v nasledujúcom zozname, a to bez ohľadu na použité prístupové zariadenie:

[1] 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.

[2] http://www.ecb.europa.eu/press/pr/date/2013/html/pr130131_1.en.html

- [karty] vykonávanie platieb kartami na internete vrátane platieb virtuálnymi kartami, ako aj registrácia údajov o platbách kartami na použitie v tzv. digitálnych peňaženkách;

- [úhrady] vykonávanie úhrad na internete;

- [elektronický mandát] vydávanie a zmeny elektronických mandátov na inkaso;

- [elektronické peniaze] prevody elektronických peňazí medzi dvoma elektronickými peňažnými účtami prostredníctvom internetu.

8. Ak sa v usmerneniach uvádza výsledok, môže byť dosiahnutý rôznymi prostriedkami. Súčasťou usmernení sú okrem stanovených požiadaviek aj príklady najlepších postupov (v prílohe 1), ktoré by poskytovatelia platobných služieb mali (ale nemusia) nasledovať.

9. Ak sú platobné služby a nástroje poskytované prostredníctvom režimov platieb (napríklad režimy platieb kartami, režimy úhrad, režimy inkasa atď.), príslušné orgány a príslušná centrálna banka, ktorá plní funkciu dohľadu nad platobnými nástrojmi, majú spolupracovať s cieľom zabezpečiť jednotné uplatňovanie usmernení zo strany subjektov zodpovedných za fungovanie daného režimu.

10. Integrátori platieb[3], ponúkajúci služby inicializácie platieb, sa považujú buď za príjemcov internetových platobných služieb (a teda za poskytovateľov platobných služieb), alebo za externých poskytovateľov technických služieb príslušných režimov alebo poskytovateľov platobných služieb. V druhom z uvedených prípadov majú integrátori platieb byť zmluvne zaviazaní, aby dodržiavali usmernenia.

11. Z rozsahu pôsobnosti usmernení sú vyňaté tieto body:

- ostatné internetové služby poskytované poskytovateľom platobných služieb prostredníctvom jeho platobnej webovej lokality (napr. internetové maklérstvo, on-line zmluvy);

- platby, pri ktorých sa pokyn vydáva poštou, telefonickým príkazom, hlasovou poštou alebo použitím technológií založených na správach SMS;

- mobilné platby iné ako platby založené na prehliadači;

- úhrady v prípade, ak tretia strana pristupuje k platobnému účtu zákazníka;

- platobné transakcie realizované podnikom prostredníctvom vyhradených sietí;

[3] Integrátori platieb poskytujú príjemcovi (t. j. internetovému obchodníkovi) normalizované rozhranie pre služby inicializácie platieb poskytované poskytovateľom platobných služieb.

- platby kartou s použitím anonymných a nedobíjacích fyzických alebo virtuálnych predplatených kariet, ak momentálne neexistuje žiadny vzťah medzi vydavateľom a držiteľom karty;

- zúčtovanie a vyrovnanie platobných transakcií.

Vymedzenie pojmov

12. Na účel týchto usmernení a na doplnenie vymedzení pojmov uvedených v smernici o platobných službách sa uplatňujú nasledujúce vymedzenia pojmov:

- *Autentifikácia* je postup, ktorý poskytovateľovi platobných služieb umožňuje overiť totožnosť zákazníka.

- *Prísna autentifikácia zákazníka* je, na účel týchto usmernení, postup založený na použití minimálne dvoch z nasledujúcich prvkov, ktoré sú kategorizované ako poznatok, vlastníctvo a inherencia: i) niečo, čo pozná len používateľ, napr. statické heslo, kód, osobné identifikačné číslo; ii) niečo, čo vlastní len používateľ, napr. kupón, čipová karta, mobilný telefón; iii) niečo, čo je vlastné len používateľovi (napr. biometrické vlastnosti, ako sú odtlačky prstov). Okrem toho platí, že vybrané prvky musia byť navzájom nezávislé, čo znamená, že narušenie jedného prvku nenaruší ostatné prvky. Aspoň jeden z prvkov by nemal umožňovať opätovné použitie a reprodukciu (okrem inherencie) a mal by byť zabezpečený pred utajeným odcudzením prostredníctvom internetu. Postup prísnej autentifikácie zákazníka by mal byť vytvorený takým spôsobom, aby chránil dôvernosť autentifikačných údajov.

- *Povolenie* je postup, prostredníctvom ktorého sa kontroluje, či zákazník alebo poskytovateľ platobných služieb má právo uskutočniť určitú činnosť (napríklad právo na prevod finančných prostriedkov) alebo získať prístup k citlivým údajom.

- *Údaje* sú informácie (vo všeobecnosti dôverné) poskytnuté zákazníkom alebo poskytovateľom platobných služieb na účely autentifikácie. Údajom môže byť aj držanie fyzického nástroja obsahujúceho informácie (napr. nástroj na vytvorenie jednorazového hesla, čipová karta) alebo niečo, čo sa používateľ naučí naspamäť alebo preukáže (napríklad biometrické vlastnosti).

- *Zásadný bezpečnostný incident v oblasti platieb* je incident, ktorý má alebo by mohol mať podstatný vplyv na bezpečnosť, integritu alebo kontinuitu systémov poskytovateľov platobných služieb súvisiacich s platbami a/alebo bezpečnosť citlivých platobných údajov alebo finančných prostriedkoch. Pri posudzovaní významnosti treba zohľadniť počet potenciálne dotknutých zákazníkov, ohrozenú sumu a vplyv na iných poskytovateľov platobných služieb alebo iné platobné infraštruktúry.

- *Analýza rizikovosti transakcie* je posúdenie rizika súvisiaceho s konkrétnou transakciou, pri ktorom sa zohľadnia také kritériá, ako sú napríklad platobné zvyklosti zákazníka (správanie sa), hodnota súvisiacej transakcie, druh produktu a profil príjemcu.

- *Virtuálne karty* sú riešenia platieb založené na kartách, pri ktorých je vytvorené dočasné číslo karty s obmedzenou lehotou platnosti, obmedzeným použitím a vopred stanoveným limitom útrat, ktoré možno použiť pri internetových nákupoch.

- *Digitálne peňaženky* sú riešenia, ktoré zákazníkovi umožňujú registráciu údajov týkajúcich sa jedného alebo viacerých platobných nástrojov s cieľom realizovať platby s viacerým internetovými obchodníkmi.

Hlava II – Usmernenia týkajúce sa bezpečnosti internetových platieb

Všeobecná kontrola a bezpečné prostredie

Správa

1. Poskytovatelia platobných služieb majú zaviesť a pravidelne kontrolovať formálne bezpečnostné zásady týkajúce sa internetových platobných služieb.

1.1 Bezpečnostné zásady treba riadne zdokumentovať a pravidelne revidovať (v súlade s usmernením 2.4). Má ich schváliť vrcholový manažment. Majú sa v nich vymedziť bezpečnostné ciele a ochota podstupovať riziká.

1.2 V rámci bezpečnostných zásad sa majú určiť úlohy a povinnosti vrátane funkcie riadenia rizík s priamym hierarchickým vzťahom až na úroveň predstavenstva, ako aj hierarchické vzťahy súvisiace s poskytovanými internetovými platobnými službami vrátane spravovania citlivých platobných údajov so zreteľom na posudzovanie, kontrolu a zmiernenie rizika.

Posudzovanie rizika

2. Poskytovatelia platobných služieb majú uskutočniť a zdokumentovať dôkladné posudzovanie rizika, pokiaľ ide o bezpečnosť internetových platieb a súvisiacich služieb, a to pred zriadením služby a v pravidelných intervaloch po jej zriadení.

2.1 Poskytovatelia platobných služieb majú prostredníctvom funkcie riadenia rizík uskutočniť a zdokumentovať podrobné posudzovania rizika pre internetové platby a súvisiace služby. Majú zvážiť výsledky prebiehajúceho monitorovania bezpečnostných hrozieb týkajúcich sa internetových platobných služieb, ktoré ponúkajú alebo majú v úmysle ponúkať, pričom majú zohľadniť: i) technologické riešenia, ktoré používajú, ii) služby, ktorých poskytovanie zverili externým poskytovateľom (outsourcing) a iii) technické prostredie zákazníkov. Poskytovatelia platobných služieb majú posúdiť riziká súvisiace so zvolenými technologickými platformami, architektúrou aplikácií, technikami a bežnými postupmi programovania na svojej strane[4] a na strane svojich zákazníkov[5], ako aj výsledky monitorovania bezpečnostných incidentov (pozri usmernenie 3).

2.2 Na základe uvedeného posúdenia majú poskytovatelia platobných služieb určiť, či je nutné zmeniť existujúce bezpečnostné opatrenia, použité technológie a ponúkané

[4] Napríklad náchylnosť systému na zmocnenie sa platobnej relácie, tzv. injekcie SQL (SQL injection), skriptovanie medzi lokalitami, pretečenie medzipamäte atď.

[5] Tieto riziká súvisia s multimediálnymi aplikáciami, doplnkami prehliadačov, rámcami, externými prepojeniami a pod.

postupy alebo služby a v akom rozsahu. Poskytovatelia platobných služieb majú zohľadniť čas potrebný na uskutočnenie zmien (vrátane odstávky zákazníka) a prijať primerané predbežné opatrenia s cieľom minimalizovať bezpečnostné incidenty a podvody, ako aj možné deštruktívne dôsledky.

2.3 Posudzovanie rizík sa má zamerať na potrebu chrániť a zabezpečiť citlivé platobné údaje.

2.4 Poskytovatelia platobných služieb majú revidovať rizikové scenáre a platné bezpečnostné opatrenia po závažných incidentoch, ktoré sa dotkli ich služieb, pred významnou zmenou infraštruktúry alebo postupov a v prípade identifikovania nových hrozieb na základe monitorovania rizík. Okrem toho sa aspoň raz za rok má uskutočniť generálna revízia posudzovania rizika. Výsledky posudzovaní rizika a revízií sa majú predkladať vrcholovému manažmentu na schválenie.

Monitorovanie a ohlasovanie incidentov

3. Poskytovatelia platobných služieb majú zabezpečiť konzistentné a integrované monitorovanie, zvládanie a následnú kontrolu bezpečnostných incidentov vrátane sťažností zákazníkov týkajúcich sa zabezpečenia. Majú stanoviť postup ohlasovania takýchto incidentov manažmentu a v prípade zásadných bezpečnostných incidentov v oblasti platieb aj príslušným orgánom.

3.1 Poskytovatelia platobných služieb majú zaviesť postup monitorovania, riešenia a následnej kontroly bezpečnostných incidentov a sťažností zákazníkov týkajúcich sa bezpečnosti a ohlasovania takýchto incidentov manažmentu.

3.2 Poskytovatelia platobných služieb majú zaviesť postup bezodkladného oznamovania príslušným orgánom (t. j. orgánom dohľadu a orgánom pre ochranu osobných údajov), pokiaľ takéto orgány existujú, v prípade zásadných bezpečnostných incidentov v oblasti platieb so zreteľom na poskytované platobné služby.

3.3 Poskytovatelia platobných služieb majú zaviesť postup spolupráce s príslušnými orgánmi presadzovania práva pri zásadných bezpečnostných incidentoch v oblasti platieb vrátane porušenia ochrany osobných údajov.

3.4 Prijímajúci poskytovatelia platobných služieb majú zmluvne požadovať od internetových obchodníkov, ktorí ukladajú, spracúvajú alebo prenášajú citlivé platobné údaje, aby v prípade zásadných bezpečnostných incidentov v oblasti platieb, vrátane porušenia ochrany osobných údajov, spolupracovali s nimi, ako aj s príslušnými orgánmi presadzovania práva. Ak poskytovateľ platobných služieb zistí, že internetový obchodník nespolupracuje tak, ako sa to vyžaduje v zmluve, má prijať opatrenia na presadenie tohto zmluvného záväzku alebo ukončiť zmluvu.

Kontrola a zmierňovanie rizík

4. Poskytovatelia platobných služieb majú zaviesť bezpečnostné opatrenia v súlade s príslušnými bezpečnostnými zásadami s cieľom zmierniť identifikované riziká. Tieto opatrenia majú zahŕňať viaceré úrovne zaistenia bezpečnosti, kde zlyhanie jednej úrovne ochrany bude zachytené nasledujúcou úrovňou ochrany („ochrana do hĺbky“).

4.1 Poskytovatelia platobných služieb majú pri navrhovaní, vývoji a údržbe internetových platobných služieb venovať osobitnú pozornosť primeranému oddeleniu povinností v prostrediach informačných technológií (IT) (napr. vývojové, testovacie a produkčné prostredia) a riadnemu vykonávaniu zásady „čo najmenších práv“ ako základu pre stabilné riadenie totožnosti a prístupu.[6]

4.2 Poskytovatelia platobných služieb majú mať zavedené primerané bezpečnostné riešenia na ochranu sietí, webových lokalít, serverov a komunikačných prepojení pred zneužitím alebo útokmi. Poskytovatelia platobných služieb majú odobrať zo serverov všetky nadbytočné funkcie v záujme ochrany (posilnenia) serverov a obmedzenia alebo odstránenia ohrozených zraniteľných aplikácií. Prístup rôznych aplikácií k požadovaným údajom a zdrojom treba udržať na najprísnejšej minimálnej úrovni podľa zásady „čo najmenších oprávnení“. V záujme obmedzenia používania „falošných“ webových lokalít (ktoré napodobňujú stránky legitímnych poskytovateľov platobných služieb) sa transakčné webové lokality ponúkajúce internetové platobné služby majú identifikovať pomocou rozšírených povoľovacích certifikátov vystavených v mene poskytovateľa platobných služieb alebo pomocou iných podobných spôsobov autentifikácie.

4.3 Poskytovatelia platobných služieb majú mať zavedené primerané postupy monitorovania, sledovania a obmedzenia prístupu k: i) citlivým platobným údajom a ii) logickým a fyzickým mimoriadne dôležitým zdrojom, ako sú napríklad siete, systémy, databázy, bezpečnostné moduly a pod. Poskytovatelia platobných služieb majú vytvárať, ukladať a analyzovať príslušné denníky a kontrolné záznamy.

4.4 Pri navrhovaní[7], vývoji a údržbe internetových platobných služieb poskytovatelia platobných služieb majú zabezpečiť, aby hlavnou súčasťou základnej funkcie bola minimalizácia údajov[8]: zber, smerovanie, spracovanie, ukladanie a/alebo archivácia a vizualizácia citlivých platobných údajov by mali dosahovať absolútne minimálnu úroveň.

[6] „Každý program a každý oprávnený používateľ systému by mali pracovať s čo najmenším počtom oprávnení nevyhnutne potrebných na splnenie úlohy.“ Pozri Saltzer, J.H. (1974), Protection and the Control of Information Sharing in Multics, Communications of the ACM (Ochrana a kontrola zdieľania informácií v programe Multics, Komunikácia ACM), zv. 17, č. 7, s. 388.

[7] Ochrana súkromia už v štádiu návrhu.

[8] Minimalizácia údajov sa vzťahuje na zásadu zberu čo najmenšieho množstva osobných informácií, nevyhnutne potrebných na prevádzku danej funkcie.

4.5 Bezpečnostné opatrenia pre internetové platobné služby sa majú testovať pod dohľadom funkcie riadenia rizík s cieľom zabezpečiť ich spoľahlivosť a účinnosť. Na všetky zmeny sa má vzťahovať formálny proces riadenia zmien, ktorým sa zabezpečí riadne plánovanie, testovanie, dokumentovanie a povoľovanie zmien. Na základe vykonaných zmien a zistených bezpečnostných hrozieb sa testy majú pravidelne opakovať a zahŕňať scenáre relevantných a známych možných útokov.

4.6 Bezpečnostné opatrenia poskytovateľov platobných služieb týkajúce sa internetových platobných služieb majú pravidelne podliehať auditu, aby sa zabezpečila ich spoľahlivosť a účinnosť. Rovnako má podliehať auditu zavádzanie a fungovanie internetových platobných služieb. Pokiaľ ide o častosť a zameranie týchto auditov, majú byť primerané zohľadneným prítomným bezpečnostným rizikám. Audity majú vykonávať dôveryhodní a nezávislí (medzinárodní alebo externí) odborníci. Títo odborníci sa nemajú žiadnym spôsobom podieľať na vývoji, zavádzaní ani operatívnom riadení poskytovaných internetových platobných služieb.

4.7 Ak poskytovatelia platobných služieb zabezpečujú funkcie týkajúce sa bezpečnosti internetových platobných služieb externe, zmluva má obsahovať ustanovenia vyžadujúce dodržiavanie zásad a usmernení uvedených v týchto usmerneniach.

4.8 Poskytovatelia platobných služieb ponúkajúci služby prijímania majú od internetových obchodníkov zmluvne vyžadovať, aby pri zaobchádzaní s citlivými platobnými údajmi(t. j. ukladaní, spracúvaní alebo prenášaní) uplatňovali bezpečnostné opatrenia v rámci svojej IT infraštruktúry v súlade s usmerneniami 4.1 až 4.7 s cieľom predísť odcudzeniu citlivých platobných údajov prostredníctvom ich systémov. Ak poskytovateľ platobných služieb zistí, že internetový obchodník nezaviedol požadované bezpečnostné opatrenia, má prijať opatrenia na presadenie zmluvného záväzku alebo ukončiť zmluvu.

Vysledovateľnosť

5. Poskytovatelia platobných služieb majú zaviesť postupy, ktorými sa zabezpečí riadne sledovanie všetkých transakcií, ako aj vývoja spracovania elektronických mandátov.

5.1 Poskytovatelia platobných služieb majú zabezpečiť, aby ich služby zahŕňali bezpečnostné mechanizmy na podrobné zapisovanie údajov o transakciách a elektronických mandátoch do denníka vrátane poradového čísla transakcie, časových pečiatok pre transakčné údaje, zmien parametrov, ako aj prístupu k údajom o transakciách a elektronických mandátoch.

5.2 Poskytovatelia platobných služieb majú zaviesť protokolovacie súbory o vykonaných operáciách umožňujúce sledovať doplnenia, zmeny alebo odstránenia údajov o transakciách a elektronických mandátoch.

5.3 Poskytovatelia platobných služieb majú požadovať a analyzovať údaje o transakciách a elektronických mandátoch a dbať na to, aby mali k dispozícii nástroje na hodnotenie súborov o vykonaných operáciách. Príslušné aplikácie majú byť dostupné len pre autorizovaný personál.

Osobitné kontrolné a bezpečnostné opatrenia pre internetové platby

Úvodná identifikácia zákazníka, informácie

6. Zákazníci majú byť riadne identifikovaní v súlade s európskymi právnymi predpismi o boji proti praniu špinavých peňazí [9] a pred udelením prístupu k internetovým platobným službám majú potvrdiť svoju ochotu uskutočňovať internetové platby s použitím týchto služieb. Poskytovatelia majú poskytovať zákazníkom adekvátne „predbežné“, „pravidelné“ alebo (ak je to vhodné) „ad hoc“ informácie o nevyhnutných požiadavkách (napr. zariadenia, postupy) na vykonávanie zabezpečených internetových platobných transakcií, ako aj o prítomných rizikách.

6.1 Poskytovatelia platobných služieb majú zabezpečiť, aby sa zákazníci podrobili postupom povinnej starostlivosti a predložili adekvátne doklady totožnosti [10] a súvisiace informácie pred umožnením prístupu k internetovým platobným službám.[11]

6.2 Poskytovatelia platobných služieb majú zabezpečiť, aby informácie [12] poskytnuté zákazníkovi vopred obsahovali konkrétne podrobnosti týkajúce sa internetových platobných služieb. Podľa okolností má ísť o tieto informácie:

- jasné informácie o akýchkoľvek požiadavkách na zariadenia zákazníka, softvér alebo iné nevyhnutne potrebné nástroje (napr. antivírusový softvér, brány firewall);

- pokyny na správne a bezpečné používanie personalizovaných bezpečnostných údajov;

[9] Napríklad smernica Európskeho parlamentu a Rady 2005/60/ES z 26. októbra 2005 o predchádzaní využívania finančného systému na účely prania špinavých peňazí a financovania terorizmu. Ú. v EÚ L 309, 25.11.2005, s. 15 – 36. Pozri tiež smernicu Komisie 2006/70/ES z 1. augusta 2006, ktorou sa ustanovujú vykonávacie opatrenia smernice Európskeho parlamentu a Rady 2005/60/ES, pokiaľ ide o vymedzenie pojmu „politicky exponovaná osoba“, a technické kritériá postupov zjednodušenej povinnej starostlivosti vo vzťahu ku klientovi a výnimky na základe finančnej činnosti vykonávanej príležitostne alebo vo veľmi obmedzenom rozsahu. Ú. v. EÚ L 214, 4.8.2006, s. 29 – 34.

[10] Napríklad cestovný pas, občiansky preukaz alebo rozšírený elektronický podpis.

[11] Postup identifikácie zákazníka sa netýka prípadných výnimiek stanovených v platných právnych predpisoch o boji proti praniu špinavých peňazí. Poskytovatelia platobných služieb nemusia zavádzať samostatný postup identifikácie zákazníka pre internetové platobné služby, pokiaľ sa identifikácia zákazníka už uskutočnila, napr. v súvislosti s inými existujúcimi službami súvisiacimi s platbami alebo na účely otvorenia účtu.

[12] Tieto informácie dopĺňajú článok 42 smernice o platobných službách spresňujúci informácie, ktoré musí poskytovateľ platobných služieb poskytnúť používateľovi platobných služieb pred tým, ako s ním uzatvorí zmluvu o poskytovaní platobných služieb.

- opis postupu zákazníka v jednotlivých krokoch týkajúci sa zaslania a povolenia platobnej transakcie a/alebo získania informácií vrátane dôsledkov jednotlivých krokov;

- pokyny na správne a bezpečné používanie hardvéru a softvéru, ktoré boli poskytnuté zákazníkovi;

- návody na to, ako postupovať v prípade straty alebo odcudzenia personalizovaných bezpečnostných údajov alebo zákazníckeho hardvéru či softvéru pri prihlasovaní alebo uskutočňovaní transakcií;

- návody ako postupovať v prípade zistenia zneužitia alebo podozrenia na zneužitie;

- opis povinností a záväzkov poskytovateľa platobných služieb a zákazníka so zreteľom na používanie internetovej platobnej služby.

6.3 Poskytovateľ platobných služieb majú zabezpečiť, aby v rámcovej zmluve so zákazníkom bolo špecifikované, že poskytovateľ môže zablokovať konkrétne transakcie alebo platobné nástroje[13] z dôvodu obáv o narušenie bezpečnosti. Má stanoviť spôsob a podmienky oznámenia zákazníkovi a spôsob, akým môže zákazník kontaktovať poskytovateľa platobných služieb na účely „odblokovania“ internetovej platobnej transakcie alebo služby v súlade so smernicou o platobných službách.

[13] Pozri článok 55 smernice o platobných službách obmedzenie použitia platobného nástroja.

Prísna autentifikácia zákazníka

7. Inicializácia internetových platieb, ako aj prístup k citlivým platobným údajom, musia byť chránené prísnou autentifikáciou zákazníka. Poskytovatelia platobných služieb majú zaviesť postup prísnej autentifikácie zákazníka v súlade s vymedzením tohto pojmu uvedeným v týchto usmerneniach.

7.1 [úhrada/elektronický mandát/elektronické peniaze] Poskytovatelia platobných služieb majú vykonávať prísnu autentifikáciu zákazníka pri povoľovaní internetových platobných transakcií zákazníkom (vrátane zoskupených úhrad) a pri vydávaní alebo zmenách elektronických mandátov na inkaso. Poskytovatelia platobných služieb majú zvážiť prijatie alternatívnych opatrení na autentifikáciu zákazníka v súvislosti s:

- odosielanými platbami dôveryhodným príjemcom uvedeným v predbežne zostavených tzv. bielych (overených) zoznamoch pre daného zákazníka;
- transakciami medzi dvoma účtami toho istého zákazníka vedenými u rovnakého poskytovateľa platobných služieb;
- prevodmi v rámci rovnakého poskytovateľa platobných služieb oprávnenými na základe analýzy rizikovosti transakcie;
- platbami nízkej hodnoty, ako sú uvedené v smernici o platobných službách.[14]

7.2 Prísna autentifikácia zákazníka sa vyžaduje na získanie prístupu k citlivým platobným údajom alebo na umožnenie zmeny týchto údajov (vrátane vytvorenia a zmeny „bielych“ zoznamov). Ak poskytovateľ platobných služieb ponúka výlučne poradenské služby, pričom nezobrazuje žiadne citlivé informácie o zákazníkoch alebo citlivé platobné informácie , ako sú napríklad údaje o platobných kartách, ktoré by sa dali ľahko zneužiť na spáchanie podvodu, poskytovateľ platobných služieb môže prijať vlastné autentifikačné požiadavky na základe posudzovania rizika.

7.3 [karty] V prípade transakcií s kartami majú všetci poskytovatelia platobných služieb, ktorí vydávajú platobné karty, podporovať prísnu autentifikáciu držiteľa karty. Všetky vydané karty musia byť technicky pripravené (zaregistrované) na použitie s prísnou autentifikáciou.

7.4 [karty] Poskytovatelia platobných služieb, ktorí ponúkajú služby prijímania, majú podporovať technológie, ktorými sa umožňuje vydavateľovi vykonávať prísnu

[14] Pozri vymedzenie pojmu nástrojov na vykonávanie platieb nízkej hodnoty v článku 34 ods. 1 a článku 53 ods. 1 smernice o platobných službách.

autentifikáciu držiteľa karty v rámci režimov platieb kartami, na ktorých sa prijímajúci podieľa.

7.5 [karty] Poskytovatelia platobných služieb, ktorí ponúkajú služby prijímania, majú požadovať od svojich internetových obchodníkov, aby podporovali riešenia umožňujúce vydavateľovi vykonávať prísnu autentifikáciu držiteľa karty pri transakciách s kartami na internete. O použití alternatívnych autentifikačných opatrení by bolo možné uvažovať pri vopred určených kategóriách nízkorizikových transakcií, t. j. na základe analýzy rizikovosti transakcií, alebo pri transakciách zahŕňajúcich platby nízkej hodnoty, ako sú uvedené v smernici o platobných službách.

7.6 [karty] V prípade režimov platieb kartami prijímanými službou majú poskytovatelia elektronických peňaženiek požadovať prísnu autentifikáciu zo strany vydavateľa pri prvej registrácii údajov o karte oprávneným držiteľom karty.

7.7 Poskytovatelia elektronických peňaženiek majú podporovať prísnu autentifikáciu zákazníkov pri prihlasovaní zákazníkov do služieb platieb prostredníctvom elektronickej peňaženky alebo pri realizácii transakcií s použitím karty na internete. O použití alternatívnych autentifikačných opatrení by bolo možné uvažovať pri vopred určených kategóriách nízkorizikových transakcií, t. j. na základe analýzy rizikovosti transakcií, alebo pri transakciách zahŕňajúcich platby nízkej hodnoty, ako sú uvedené v smernici o platobných službách.

7.8 [karty] Pokiaľ ide o virtuálne karty, úvodná registrácia sa má uskutočniť v bezpečnom a spoľahlivom prostredí.[15] Prísna autentifikácia zákazníka sa má vyžadovať pri postupe vytvorenia údajov o virtuálnej karte, ak sa karta vydáva v internetovom prostredí.

7.9 Poskytovatelia platobných služieb majú zabezpečiť riadnu dvojstrannú autentifikáciu pri komunikácii s internetovými obchodníkmi na účely inicializácie internetových platieb a pri pristupovaní k citlivým platobným údajom.

Registrácia a poskytnutie nástrojov na autentifikáciu a/alebo softvéru dodaného zákazníkovi

8. Poskytovatelia platobných služieb majú zabezpečiť, aby sa registrácia zákazníka a úvodné poskytnutie nástrojov na autentifikáciu požadovaných pri používaní internetovej platobnej služby a/alebo dodanie softvéru súvisiaceho s platbami uskutočnili bezpečným spôsobom.

[15] Prostredia, za ktoré zodpovedajú poskytovatelia platobných služieb, v ktorých je zabezpečená adekvátna autentifikácia zákazníka a poskytovateľa platobných služieb ponúkajúceho službu, ako aj ochrana dôverných/citlivých informácií, zahŕňajú: i) prevádzky poskytovateľov internetových služieb; ii) internetové bankovníctvo alebo inú zabezpečenú webovú lokalitu, napríklad tam, kde riadiaci orgán ponúka porovnateľné bezpečnostné funkcie, okrem iného tie, ktoré sú vymedzené v usmernení 4; iii) služby bankomatov. (V prípade bankomatov sa vyžaduje prísna autentifikácia zákazníka. Túto autentifikáciu zvyčajne umožňuje čip a kód PIN alebo čip a biometrické údaje).

8.1 Registrácia a poskytnutie nástrojov na autentifikáciu a/alebo softvéru súvisiaceho s platbami dodaného zákazníkovi má spĺňať tieto požiadavky:

- Súvisiace postupy sa majú realizovať v bezpečnom a spoľahlivom prostredí, pričom treba zohľadniť možné riziká vyplývajúce zo zariadení, ktoré nie sú pod kontrolou poskytovateľa platobných služieb.

- Majú sa zaviesť účinné a bezpečné postupy týkajúce sa poskytnutia personalizovaných bezpečnostných údajov, softvéru súvisiaceho s platbami a všetkých osobných zariadení súvisiacich s internetovými platbami. Softvér poskytnutý prostredníctvom internetu má byť digitálne podpísaný poskytovateľom platobných služieb s cieľom umožniť zákazníkovi, aby si overil jeho autentickosť a nepoškodenosť.

- [karty] Pokiaľ ide o transakcie s kartami, zákazník má mať možnosť zaregistrovať sa na účely prísnej autentifikácie nezávisle od konkrétneho internetového nákupu. Ak sa ponúka aktivácia v priebehu on-line nákupu, mala by sa uskutočniť presmerovaním zákazníka do bezpečného a spoľahlivého prostredia.

8.2 [karty] Vydavatelia majú aktívne povzbudzovať registráciu držiteľov kariet na účely prísnej autentifikácie a umožniť svojim držiteľom kariet obídenie registrácie len vo výnimočných a obmedzených prípadoch, ktoré sú odôvodnené rizikom súvisiacim s konkrétnou transakciou prostredníctvom karty.

Pokusy o prihlásenie, uplynutie času relácie, platnosť autentifikácie

9. Poskytovatelia platobných služieb majú obmedziť počet pokusov o prihlásenie alebo autentifikáciu, stanoviť pravidlá vypršania času relácie internetových platobných služieb, ako aj časové limity pre platnosť autentifikácie.

9.1 Ak sa na účely autentifikácie využíva jednorazové heslo, poskytovatelia platobných služieb majú zabezpečiť, že čas platnosti takéhoto hesla bude obmedzený na nevyhnutne potrebné minimum.

9.2 Poskytovatelia platobných služieb majú stanoviť maximálny počet neúspešných pokusov o prihlásenie alebo autentifikáciu, po vyčerpaní ktorých bude prístup k internetovej platobnej službe (dočasne alebo trvalo) zablokovaný. Má sa uplatňovať bezpečný postup na opätovnú aktiváciu zablokovaných internetových platobných služieb.

9.3 Poskytovatelia platobných služieb majú stanoviť maximálne obdobie, po uplynutí ktorého sa neaktívne relácie internetových platobných služieb automaticky ukončia.

Monitorovanie transakcií

10. Mechanizmy monitorovania transakcií určené na predchádzanie podvodným platobným transakciám, ich zisťovanie a blokovanie sa majú aplikovať pred záverečným overením poskytovateľa platobných služieb. Na podozrivé alebo vysokorizikové transakcie sa majú vzťahovať osobitné postupy skríningu a hodnotenia. Rovnocenné mechanizmy bezpečnostného monitorovania a overovania sa majú zaviesť aj na vydávanie elektronických mandátov.

10.1 Poskytovatelia platobných služieb majú používať systémy na zisťovanie podvodov a predchádzanie podvodom, a to predtým, než poskytovateľ platobnej služby na záver potvrdí transakcie alebo elektronické mandáty. Takéto systémy majú byť založené napríklad na parametrizovaných pravidlách (ako sú tzv. čierne zoznamy porušených alebo ohrozených údajov o kartách) a monitorovaní nezvyčajného správania sa zákazníka alebo zákazníckeho prístupového zariadenia (ako sú zmena adresy internetového protokolu (IP)[16] alebo rozsahu IP v priebehu relácie internetových platobných služieb, ktorá sa niekedy dá zistiť kontrolami geografického umiestnenia adresy IP[17], atypické kategórie internetových obchodníkov pre konkrétneho zákazníka alebo nezvyčajné údaje o transakcii atď.). Tieto systémy majú tiež byť schopné zistiť príznaky malwarovej infekcie v relácii (napr. prostredníctvom povolenia skriptu oproti človeku) a známych podvodných scenárov. Rozsah, komplexnosť a prispôsobivosť riešení umožňujúcich monitorovanie a zároveň dodržiavanie príslušných právnych predpisov o ochrane osobných údajov majú zodpovedať výsledku posudzovania rizika.

10.2 Prijímajúci poskytovatelia platobných služieb majú zaviesť systémy zisťovania podvodov a predchádzania podvodom s cieľom monitorovať činnosti internetových obchodníkov.

10.3 Poskytovatelia platobných služieb majú vykonávať každý postup skríningu a hodnotenia transakcie v primeranom časovom rámci, aby zbytočne nezdržiavali inicializáciu a/alebo poskytnutie dotknutej platobnej služby.

10.4 Ak sa poskytovateľ platobných služieb na základe svojej politiky rizík rozhodne zablokovať platobnú transakciu, ktorá bola identifikovaná ako potenciálne podvodná, zablokovanie má trvať čo najkratšie, kým sa nevyriešia bezpečnostné otázky.

Ochrana citlivých platobných údajov

11. Citlivé platobné údaje majú byť chránené pri ukladaní, spracúvaní alebo prenášaní.

[16] Adresa IP je jedinečný číselný kód, ktorým sa identifikuje každý počítač pripojený k internetu.

[17] Kontrola Geo-IP overuje, či vydávajúca krajina zodpovedá adrese IP, z ktorej používateľ inicializuje transakciu.

11.1 Všetky údaje použité na identifikáciu a autentifikáciu zákazníkov (napr. pri prihlasovaní, inicializácii internetových platieb a vydávaní, zmenách alebo zrušení elektronických mandátov), ako aj zákazníckeho rozhrania (webová lokalita poskytovateľa platobných služieb alebo elektronického predajcu) majú byť primerane zabezpečené proti odcudzeniu a neoprávnenému prístupu alebo úpravám.

11.2 Poskytovatelia platobných služieb majú zabezpečiť, aby sa pri výmene citlivých platobných údajov medzi komunikujúcimi stranami prostredníctvom internetu v priebehu príslušných komunikačných relácií používalo zabezpečené šifrovanie bez medzifáz[18] s cieľom zabezpečiť dôvernosť a integritu údajov, s použitím spoľahlivých a všeobecne uznávaných šifrovacích techník.

11.3 Poskytovatelia platobných služieb poskytujúci služby prijímania majú nabádať svojich internetových obchodníkov, aby neukladali žiadne citlivé platobné údaje. V prípade, že internetoví obchodníci nakladajú s citlivými platobnými údajmi (t. j. ukladajú ich, spracúvajú alebo prenášajú), poskytovatelia platobných služieb majú zmluvne požadovať, aby internetoví obchodníci prijali nevyhnutne potrebné opatrenia na ochranu takýchto údajov. Poskytovatelia platobných služieb majú vykonávať pravidelné kontroly a ak poskytovateľ platobných služieb zistí, že internetový obchodník zaobchádzajúci s citlivými platobnými údajmi nezaviedol požadované platobné služby, má prijať opatrenia na tohto zmluvného záväzku alebo ukončiť zmluvu.

[18] Šifrovanie bez medzifáz je šifrovanie v rámci zdrojového koncového systému alebo v ňom, pričom k príslušnému rozšifrovaniu dochádza len v rámci cieľového koncového systému alebo v ňom. ETSI EN 302 109 V1.1.1. (2003-06).

Informovanosť zákazníka, vzdelávanie a komunikácia

Vzdelávanie zákazníka a komunikácia

12. Poskytovatelia platobných služieb majú podľa potreby poskytnúť pomoc a usmernenia zákazníkom, pokiaľ ide o bezpečné používanie internetových platobných služieb. Poskytovatelia platobných služieb majú so svojimi zákazníkmi komunikovať takým spôsobom, aby ich ubezpečili o autentickosti doručených správ.

12.1 Poskytovatelia platobných služieb majú poskytnúť aspoň jeden zabezpečený kanál[19] na priebežnú komunikáciu so zákazníkmi týkajúcu sa správneho a bezpečného použitia internetovej platobnej služby. Majú informovať zákazníkov o tomto kanáli a vysvetliť im, že akékoľvek správy týkajúce sa správneho a bezpečného použitia internetových platobných služieb, ktoré boli doručené v mene poskytovateľa platobných služieb inými prostriedkami (napr. e-mailom), nie sú spoľahlivé. Poskytovatelia platobných služieb majú vysvetliť:

- postup, akým majú zákazníci oznamovať poskytovateľovi platobných služieb (podozrivé) podvodné platby, podozrivé incidenty alebo anomálie v priebehu relácie internetových platobných služieb a/alebo možné pokusy o sociálne inžinierstvo[20];
- nadväzujúci postup, t. j. akým spôsobom poskytovatelia platobných služieb odpovedia zákazníkom;
- spôsob, ako poskytovatelia platobných služieb budú informovať zákazníkov o (možných) podvodných transakciách alebo o tom, že neboli inicializované, alebo ako budú varovať zákazníkov pred útokmi (napr. e-maily neoprávnené získavajúce údaje (phishing)).

12.2 Poskytovatelia platobných služieb majú prostredníctvom zabezpečeného kanála informovať zákazníkov o aktualizáciách bezpečnostných postupov týkajúcich sa internetových platobných služieb. Prostredníctvom zabezpečeného kanála sa majú tiež mali poskytovať všetky výstrahy pred podstatnými novými rizikami (napríklad varovania pred sociálnym inžinierstvom).

12.3 Poskytovatelia platobných služieb majú poskytnúť pomoc zákazníkom v prípade otázok, sťažností, žiadostí o podporu a hlásení anomálií alebo incidentov súvisiacich

[19] Napríklad vyhradená poštová schránka na webovej lokalite poskytovateľa platobných služieb alebo zabezpečená webová lokalita.

[20] Sociálne inžinierstvo v tejto súvislosti znamená techniky manipulácie s ľuďmi na účely získania informácií (napr. prostredníctvom e-mailu alebo telefonického hovoru) alebo techniky získavania informácií zo sociálnych sietí na účely podvodu alebo získania neoprávneného prístupu k počítaču či sieti.

s internetovými platbami a príslušnými službami. Zákazníci majú byť náležite informovaní o spôsoboch získania takejto pomoci.

12.4 Poskytovatelia platobných služieb majú dbať na vzdelávanie zákazníkov a informačné programy navrhnuté s cieľom zabezpečiť, aby zákazníci porozumeli aspoň tomu, že je potrebné:

- chrániť si heslá, bezpečnostné kupóny, osobné údaje a ostatné dôverné údaje;
- správnym spôsobom dbať na bezpečnosť osobného zariadenia (napr. počítača) formou inštalácie a aktualizácie bezpečnostných súčastí (antivírusové programy, brány firewall, bezpečnostné opravy);
- zohľadňovať závažné hrozby a riziká súvisiace s preberaním softvéru z internetu, pokiaľ si zákazník nie je istý, že je softvér pravý a nebol porušený;
- používať pravú internetovú platobnú webovú lokalitu poskytovateľa platobných služieb.

12.5 Prijímajúci poskytovatelia platobných služieb majú vyžadovať od internetových obchodníkov, aby jasne oddelili postupy súvisiace s platbami od internetového obchodu s cieľom zjednodušiť zákazníkom orientáciu v tom, kedy komunikujú s poskytovateľom platobných služieb a nekomunikujú s príjemcom (napr. presmerovaním zákazníka a otvorením samostatného okna, aby sa postup platby nezobrazoval v rámci internetového obchodníka).

Oznámenia, nastavenie limitov

13. Poskytovatelia platobných služieb majú stanoviť limity pre internetové platobné služby a mohli by svojim zákazníkom poskytnúť možnosť ďalšieho obmedzenia rizík v rámci stanovených limitov. Môžu tiež poskytovať upozornenia a služby riadenia profilu zákazníka.

13.1 Skôr ako poskytovatelia platobných služieb začnú zákazníkom poskytovať internetové platobné služby, majú stanoviť limity[21] pre tieto služby (napr. maximálnu sumu pre jednotlivé platby alebo celkovú sumu za určité časové obdobie) a majú o tom informovať zákazníkov. Poskytovatelia platobných služieb majú umožniť zákazníkom, aby zakázali funkciu internetových platieb.

[21] Limity sa môžu uplatňovať všeobecne (t. j. na všetky platobné nástroje umožňujúce internetové platby) alebo individuálne.

Prístup zákazníka k informáciám o stave inicializácie a realizácie platby

14. Poskytovatelia platobných služieb majú svojim zákazníkom včas potvrdiť inicializáciu platby a poskytnúť informácie nevyhnutne potrebné na skontrolovanie správnosti inicializácie a realizácie platobnej transakcie.

    14.1 [Úhrada/elektronický mandát] Poskytovatelia platobných služieb majú zákazníkom poskytnúť pomôcku fungujúcu takmer v reálnom čase na kontrolu stavu realizácie transakcií, ako aj zostatkov na účte bez časového obmedzenia[22], v bezpečnom a spoľahlivom prostredí.

    14.2 Všetky podrobné elektronické výpisy majú byť prístupné v bezpečnom a spoľahlivom prostredí. Ak poskytovateľ platobných služieb informuje zákazníkov o dostupnosti elektronického výpisu (napr. pravidelne pri vydaní elektronického výpisu alebo ad hoc po realizácii transakcie) prostredníctvom alternatívneho kanála (napríklad správy SMS, e-mailu alebo listu), do takéto oznámenia nemá zahrnúť citlivé platobné údaje a pokiaľ ich zahrnie, má ich zamaskovať.

Hlava III – Záverečné ustanovenia a vykonávanie

15. Tieto usmernenia nadobudnú účinnosťod 01.08.2015.

[22] Okrem výnimočnej nedostupnosti pomôcky z dôvodu technickej údržby alebo závažného incidentu.

Príloha 1: Príklady najlepších postupov

Okrem požiadaviek uvedených v predchádzajúcom texte sú v týchto usmerneniach opísané niektoré najlepšie postupy, ktoré by poskytovatelia platobných služieb mali prijať (ale nemusia). V záujme prehľadnosti sú výslovne uvedené kapitoly, ktorých sa najlepšie postupy týkajú.

Všeobecná kontrola a bezpečné prostredie

Správa

NP 1: Bezpečnostné zásady môžu byť zhrnuté v samostatnom dokumente.

Kontrola a zmierňovanie rizík

NP 2: Poskytovatelia platobných služieb by mohli poskytnúť nástroje na zabezpečenie (napríklad riadne zabezpečené zariadenia a/alebo prispôsobené prehliadače) na ochranu zákazníckeho rozhrania pred neoprávneným použitím alebo útokmi (napr. útokmi typu „man in the browser“).

Vysledovateľnosť

NP 3: Poskytovatelia platobných služieb ponúkajúci služby prijímania by mohli zmluvne vyžadovať od internetových obchodníkov, ktorí ukladajú informácie o platbách, aby zaviedli primerané postupy na podporu vysledovateľnosti.

Osobitné kontrolné a bezpečnostné opatrenia pre internetové platby

Úvodná identifikácia zákazníka, informácie

NP 4: Namiesto zahrnutia zmluvných podmienok do širšej všeobecnej zmluvy o službách s poskytovateľom platobných služieb môže zákazník podpísať vyhradenú zmluvu o službách na uskutočňovanie internetových platobných transakcií.

NP 5: Poskytovatelia platobných služieb by mohli i takisto zabezpečiť, aby zákazníci dostávali priebežne alebo prípadne ad hoc a vhodnou formou (napr. letáky, internetové stránky) jasné a priame pokyny s vysvetlením ich povinností, pokiaľ ide o bezpečné použitie služby.

Prísna autentifikácia zákazníka

NP 6: [karty] Internetoví obchodníci by mohli podporovať prísnu autentifikáciu držiteľa karty zo strany vydavateľa karty v rámci transakcií s kartami na internete.

NP 7: Poskytovatelia platobných služieb by mali vyjsť v ústrety zákazníkom a zvážiť použitie jediného nástroja na prísnu autentifikáciu zákazníka pri všetkých internetových platobných službách. Tým by sa zvýšila miera prijatia riešenia medzi zákazníkmi a podporilo správne používanie.

NP 8: Do prísnej autentifikácie zákazníka by mohli byť zahrnuté prvky spájajúce autentifikáciu s konkrétnou sumou a príjemcom. Tým by sa zvýšila istota zákazníka pri povoľovaní platieb. Technologické riešenie umožňujúce prepojenie údajov prísnej autentifikácie a údajov o transakcii by malo byť odolné proti poškodeniu.

Ochrana citlivých platobných údajov

NP 9: Je vhodné, aby internetoví obchodníci, ktorí spracúvajú citlivé platobné údaje , riadne školili svojich pracovníkov zodpovedných za riešenie podvodov a pravidelne tieto školenia aktualizovali s cieľom zabezpečiť, aby obsah školení ostal relevantný vzhľadom na dynamické bezpečné prostredie.

Vzdelávanie zákazníka a komunikácia

NP 10: Je vhodné, aby poskytovatelia platobných služieb, ktorí ponúkajú služby prijímania, pripravili vzdelávacie programy o prevencii podvodov pre svojich internetových obchodníkov.

Oznámenia, nastavenie limitov

NP 11: Poskytovatelia platobných služieb by v rámci nastavených limitov mohli svojim zákazníkom poskytnúť pomôcku na spravovanie limitov pre internetové platobné služby v bezpečnom a spoľahlivom prostredí.

NP 12: Poskytovatelia platobných služieb by mohli zaviesť varovania pre zákazníkov, napríklad prostredníctvom telefonátov alebo správ SMS, pred podozrivými alebo vysokorizikovými platobnými transakciami, a to na základe svojich politík riadenia rizík.

NP 13: Poskytovatelia platobných služieb by mohli zákazníkom umožniť, aby spresnili všeobecné osobne prispôsobené pravidlá ako parametre pre svoje správanie so zreteľom na internetové platby a súvisiace služby, napr. pravidlo, že budú inicializovať platby len z určitých konkrétnych krajín a platby inicializované z ostatných krajín by sa mali blokovať, alebo pravidlo, že môžu zahrnúť určitých príjemcov na čierny alebo biely zoznam.