

**Odvetvie platobných kariet   
Norma na ochranu údajov  
Samohodnotiaci dotazník D   
a preukazovanie zhody obchodníkov**

**Všetci ostatní obchodníci oprávnení využívať systém SAQ**

**Na použitie s PCI DSS verzia 3.2**

Vydanie 1.1

10. januára 2017 **Zmeny v dokumente**

|  |  |  |  |
| --- | --- | --- | --- |
| **Dátum** | **PCI DSS verzia** | **SAQ vydanie** | **Popis** |
| Október 2008 | 1.2 |  | Zosúladenie obsahu s novou verziu 1.2 PCI DSS a implementácia menších zmien zaznamenaných od pôvodnej verzie 1.1. |
| Október 2010 | 2.0 |  | Zosúladenie obsahu s novými požiadavkami na skúšobné postupy verzie 2.0 PCI DSS. |
| Február 2014 | 3.0 |  | Zosúladenie obsahu s novými požiadavkami na skúšobné postupy verzie 3.0 PCI DSS a zahrnutie dodatočných možností odozvy. |
| Apríl 2015 | 3.1 |  | Zosúladenie s PCI DSS v3.1. Podrobné informácie o zmenách PCI DSS sú uvedené v *PCI DSS - Súhrn zmien medzi verziami 3.0 a 3.1 PCI DSS.* |
| Júl 2015 | 3.1 | 1.1 | Odstránené odkazy na „osvedčené postupy" pred 30. júnom 2015 a odstránená možnosť podávania správ z v2 PCI DSS v bode 11.3 Požiadavky. |
| Apríl 2016 | 3.2 | 1.0 | Zosúladenie s PCI DSS v3.2. Podrobné informácie o zmenách PCI DSS sú uvedené v *PCI DSS - Súhrn zmien medzi verziami 3.1a 3.2PCI DSS.* |
| Január 2017 | 3.2 | 1.1 | Aktualizované číslovanie verzií na zosúladenie s inými SAQ |

**Obsah**

Zmeny dokumentu

Úvod

Samohodnotiaci postup PCI DCC

Vysvetlenie samohodnotiaceho dotazníku

Očakávané skúšky

Vyplnenie samohodnotiaceho dotazníku

Nepoužiteľnosť určitých špecifických požiadaviek

Vysvetlenie rozdielu medzi „nevzťahuje sa" a „netestované"

Právne výnimky

**Sekcia 1:** Informácie o hodnotení

**Sekcia 2:** Samohodnotiaci dotazník D pre obchodníkov

Vytváranie a udržiavanie bezpečnej siete a systémov

*Požiadavka 1:* Inštalácia a udržiavanie firewallového systému na ochranu dát

*Požiadavka 2:* Nepoužívanie predvolených nastavení systémových hesiel a iných bezpečnostných parametrov

Ochrana údajov držiteľa karty

*Požiadavka 3:* Ochrana uložených údajov držiteľa karty

*Požiadavka 4:* Šifrovanie prenosových údajov držiteľa karty pri použití v otvorených verejných sietiach

Udržiavanie programu na riadenie zraniteľnosti

*Požiadavka 5:* Ochrana všetkých systémov voči škodlivým softvérom a pravidelná aktualizácia antivírusových programov alebo softvéru

*Požiadavka 6:* Vytváranie a udržiavanie bezpečných systémov a aplikácií

Implementácia prísnych opatrení na kontrolu prístupu

*Požiadavka 7:* Obmedzenie prístupu k údajom držiteľa karty v nevyhnutnom rozsahu

*Požiadavka 8:* Identifikácia a autentifikácia prístupu k systémovým komponentom

*Požiadavka 9:* Obmedzenie fyzického prístupu k údajom držiteľa karty

Pravidelné sledovanie a testovanie siete

*Požiadavka 10:*  Sledovanie a monitorovanie každého prístupu do sieťových zdrojov a údajov držiteľa karty

*Požiadavka 11:* Pravidelné testovanie bezpečnostných systémov a procesov

Udržiavanie politiky zabezpečenia informácií

*Požiadavka 12:* Udržiavanie politiky, ktorá rieši bezpečnosť informácií všetkých pracovníkov

**Dodatok A:** Dodatočné požiadavky PCI DSS

*Dodatok A1:*  Dodatočné požiadavky PCI DSS pre spoločných poskytovateľov hostingu

*Dodatok A2:*  Dodatočné požiadavky PCI DSS pre subjekty používajúce SSL/staršie TLS

*Dodatok A3:*  Dodatočná validácia určených subjektov (DESV)

**Dodatok B:** Hárok kompenzácií ovládacích prvkov

**Dodatok C:** Vysvetlenie pojmu „nevzťahuje sa"

**Dodatok D:** Vysvetlenie požiadaviek „netestované"

**Odsek 3:** Podrobnosti o overovaní a osvedčovaní

**Úvod**

Systém SAQ D pre obchodníkov sa vzťahuje na obchodníkov, ktorí sú oprávnení využívať SAQ a ktorí nespĺňajú kritéria pre žiaden iný typ SAQ. Príklady takýchto obchodníkov sú (vrátane, ale nielen):

 Elektronickí obchodníci, ktorí prijímajú údaje držiteľov karty na svojich webových stránkach.

 Obchodníci s elektronickým ukladaním údajov držiteľov karty

 Obchodníci, ktorí údaje držiteľa karty neukladajú elektronicky a zároveň nespĺňajú kritéria iného typu SAQ

 Obchodníci podnikajúci v prostredí, ktoré môže spĺňať kritéria iného typu SAQ ale ktoré má dodatočné požiadavky PCI DSS vzťahujúce sa na dané prostredie

Zatiaľčo množstvo organizácií vykonávajúcich SAQ D potrebuje overovať súlad s každou požiadavkou PCI DSS, niektoré organizácie s veľmi špecifickým obchodným modelom dokážu rozpoznať, že nie všetky požiadavky sa na ne vzťahujú. Pozrite pokyny nižšie pre podrobné informácie o vylúčení určitých špecifických požiadaviek.

**Samohodnotiaci postup PCI DCC**

1. Určite príslušné SAQ pre vaše prostredie - pre postup si pozrite dokument o pokynoch a usmerneniach k samohodnotiacemu dotazníku na webovej stránke PCI SSC.

2. Potvrďte, že vaše prostredie je správne zaradené a spĺňa kritéria oprávnenosti typu SAQ, ktorý používate.

3. Vyhodnoťte súlad vášho prostredia s požiadavkami PCI DSS.

4. Vyplňte všetky sekcie tohto dokumentu:

* Sekcia 1 (časti 1 a 2 AOC) - Informácie o hodnotení a zhrnutie.
* Sekcia 2 - Samohodnotiaci dotazník PCI DSS (SAQ D)
* Sekcia 3 (časti 3 a 4 AOC) - Údaje o overovaní a osvedčovaní a akčný plán pre nesplnené požiadavky (ak existujú)

5. Predložte vášmu nadobúdateľovi, kartovej spoločnosti alebo inému žiadateľovi SAQ osvedčenie o súlade (AOC) spolu s akoukoľvek ďalšou potrebnou dokumentáciou, ako sú naskenované správy ASV.

**Vysvetlenie samohodnotiaceho dotazníka**

Otázky obsiahnuté v stĺpci „otázka PCI DSS" v tomto samohodnotiacom dotazníku vychádzajú z požiadavky PCI DSS.

Odkazy na užitočné informácie o požiadavkách PCI DSS a spôsobe vyplnenia samohodnotiaceho dotazníka Vám boli zaslané spolu na uľahčenie hodnotiaceho procesu. Prehľad týchto odkazov je uvedený nižšie:

|  |  |
| --- | --- |
| **Dokument** | **Obsahuje:** |
| PCI DSS  *(Štandardné požiadavky na zabezpečenie údajov PCI a postupy hodnotenia bezpečnosti)* |  Pokyny na priraďovanie   Vysvetlenie zámeru všetkých požiadaviek PCI DSS   Podrobnosti o testovacích postupoch   Pokyny ku kompenzačným kontrolám |
| Dokumenty o pokynoch a usmerneniach SAQ |  Informácie o všetkých SAQ a kritériách oprávnenosti   Ako zistiť, ktorý SAQ sa vzťahuje na vašu organizáciu |
| *Slovník pojmov, skratky a akronymy PCI DSS a PA-DSS* |  Popis a definície pojmov použitých v PCI DSS a samohodnotiacich dotazníkoch |

Tieto a ďalšie zdroje je možné nájsť na webovej stránke PCI SSC *(www.pcisecuritystandards.org*). Odporúča sa, aby si organizácie preštudovali PCI DSS a iné podporné dokumenty pred začiatkom hodnotiaceho procesu.

***Očakávané testovanie***

Pokyny uvedené v stĺpci „očakávané testovanie" vychádzajú zo skúšobných postupov PCI DSS a poskytujú podrobný popis typov potrebných skúšobných činností na verifikáciu súladu s požiadavkami. Podrobné informácie o skúšobných postupoch pre každú požiadavku je možné nájsť v PCI DSS.

**Vyplnenie samohodnotiaceho dotazníka**

Pre každú otázku máte možnosť výberu odpovedí na označenie stavu vašej spoločnosti v súvislosti s touto požiadavkou. ***Vyberte len jednu odpoveď pre každú otázku.***

Popis významu každej odpovede je uvedený v nasledujúcej tabuľke:

|  |  |
| --- | --- |
| **Odpoveď** | **Kedy používať túto odpoveď:** |
| **Áno** | Očakávané testovanie bolo vykonané a všetky prvky požiadavky boli riadne splnené. |
| **Áno s CCW**  (Hárok kompenzačného riadenia) | Očakávané testovanie bolo vykonané a požiadavky boli splnené pomocou kompenzačného riadenia.  Všetky odpovede v tomto stĺpci vyžadujú vyplnenie hárku kompenzačného riadenia (CCW) obsiahnutého v prílohe B k SAQ.  Informácie o použití kompenzačných prvkov a pokyny o vyplnení hárku sú uvedené v PCI DSS. |
| **Nie** | Niektoré alebo všetky prvky požiadavky neboli splnené alebo sú v procese implementácie alebo vyžadujú dodatočné testovanie než je možné zistiť ich súlad. |
| **N/A**  (nevzťahuje sa) | Táto požiadavka sa nevzťahuje na prostredie organizácie. (Pozrite *Pokyny o neuplatňovaní špecifických požiadaviek* - príklady uvedené nižšie)  Všetky odpovede v tomto stĺpci vyžadujú dodatočné vysvetlenie podľa prílohy C k SAQ. |
| **Netestované** | Táto požiadavka nebola preskúmavaná v hodnotiacom procese a nebola žiadnym spôsobom testovaná. (Pozrite *Vysvetlenie rozdielu medzi pojmom „nevzťahuje sa" a „netestované"* - príklady, kedy je možné využiť túto možnosť).  Všetky odpovede v tomto stĺpci vyžadujú dodatočné vysvetlenie podľa prílohy D k SAQ. |

**Nepoužiteľnosť určitých špecifických požiadaviek**

Pričom množstvo organizácií vykonávajúcich SAQ D potrebuje overovať súlad s každou požiadavkou PCI DSS, niektoré organizácie s veľmi špecifickým obchodným modelom dokážu rozpoznať, že nie všetky požiadavky sa na ne vzťahujú. Napríklad od spoločnosť, ktorá nepoužíva bezdrôtovú technológiu v žiadnom rozsahu, sa neočakáva, že splní súlad so sekciami PCI DSS, ktoré sa špecificky venujú riadeniu bezdrôtovej technológie. Podobne organizácia, ktorá neukladá elektronicky žiadne údaje držiteľa karty, nemusí overovať požiadavky súvisiace s bezpečným ukladaním údajov držiteľa karty (napríklad požiadavky 3.4).

Príklady požiadaviek so špecifickou použiteľnosťou zahŕňajú:

 Otázky špecifické pre zabezpečenie bezdrôtových technológií (napríklad požiadavky 1.2.3, 2.1.1 a 4.1.1) musia byť zodpovedané len vtedy, ak je vo vašej sieti využívaná bezdrôtová technológia. Upozorňujeme, že požiadavka 11.1 (použitie procesov na identifikáciu neoprávnených bezdrôtových prístupových bodov) musí byť zodpovedaná, napriek tomu, že nevyužívate bezdrôtovú technológiu, keďže tento proces dokáže odhaliť akékoľvek neoprávnené alebo nepoctivé zariadenia nasadené bez vášho vedomia.

 Otázky týkajúce sa vývoja aplikácie a bezpečného kódovania (požiadavky 6.3 a 6.5) musia byť zodpovedané len, ak vaša organizácia vyvíja vlastné aplikácie.

 Otázky týkajúce sa požiadaviek 9.1.1 a 9.3 musia byť zodpovedané len pre zariadenia s „citlivými oblasťami" podľa tejto definície: „Citlivé oblasti" označujú akékoľvek dátové centrum, serverovú miestnosť alebo akúkoľvek oblasť, v ktorej sú umiestnené systémy na uchovávanie, spracovanie alebo prenášanie údajov držiteľa karty. Tým sa vylučujú oblasti, kde sú nainštalované predajné terminály, ako sú priestory pokladne v maloobchodnej predajni, avšak zahrnuté sú priestory serverových miestností, ktoré uchovávajú údaje držiteľa karty a iné priestory slúžiace na uchovávanie väčšieho množstva údajov držiteľov karty.

V prípade, že niektoré požiadavky sa považujú za neuplatniteľné vo vašom prostredí, vyberte možnosť „N/A" pre danú špecifickú požiadavku a vyplňte hárok „Vysvetlenie neuplatnenia" obsiahnutý v dodatku C pre každú odpoveď „N/A".

***Vysvetlenie rozdielu medzi „nevzťahuje sa" a „netestované"***

Neuplatnenie požiadavky na dané prostredie je nutné overiť samo o sebe. Použitím vyššie uvedeného príkladu, organizácia na to, aby vybrala „N/A" pre požiadavky 1.2.3, 2.1.1 a 4.1.1 musí najprv potvrdiť, že nepoužíva žiadnu bezdrôtovú komunikáciu vo svojej CDE a že žiadna taká sa nepripája na CDE. Po tomto potvrdení môže organizácia vybrať možnosť „N/A" pre tieto špecifické požiadavky.

V prípade, že požiadavka je úplne vylúčená z hodnotenia, bez akéhokoľvek skúmania o tom, či má byť uplatnená alebo nie, je nutné vybrať odpoveď „netestované". Príklady takýchto situácií môžu zahŕňať:

 Organizácia môže byť požiadaná svojim nadobúdateľom, aby overila skupinu požiadaviek, napríklad za pomoci prioritizovaného prístupu overovania určitých míľnikov.

 Organizácia chce potvrdiť novú bezpečnostnú kontrolu, ktorá ovplyvňuje iba určitú podmnožinu požiadaviek, napríklad implementáciu novej metodiky šifrovania, ktorá vyžaduje hodnotenie súladu s požiadavkami 2, 3 a 4 PCI DSS.

 Poskytovateľ služby môže ponúkať službu, ktorá pokrýva len určite množstvo požiadaviek PCI DSS, napríklad poskytovateľ fyzického skladovania môže vyžadovať validáciu fyzických bezpečnostných prvkov každej požiadavky 9 PCI DSS pre svoje skladovacie zariadenie.

V takýchto prípadoch môže organizácia overovať len určité požiadavky PCI DSS napriek tomu, že sa môžu na jej prostredie vzťahovať aj iné požiadavky.

**Právna výnimka**

V prípade, že vaša organizácia podlieha právnemu obmedzeniu, ktoré zabraňuje organizácii splniť požiadavky PCI DCC, zaškrtnite odpoveď „nie" pre danú požiadavku a vyplňte zodpovedajúce potvrdenie v časti 3.

**Sekcia 1:** **Informácie o hodnotení**

***Pokyny na predloženie***

Tento dokument musí byť vyplnený ako vyhlásenie o výsledkoch sebahodnotenia obchodníka so *Štandardnými* *bezpečnostnými požiadavkami platobných kariet a postupmi hodnotenia bezpečnosti (PCI DSS).* Vyplňte všetky sekcie: Obchodník je povinný zabezpečiť, aby každá sekcia bola vyplnená príslušnými stranami, podľa potreby. Obráťte sa na svojho nadobúdateľa (banku obchodníka) alebo kartové spoločnosti na určenie postupov podávania správ a predkladania.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Časť 1. Informácie o obchodníkovi a oprávnenom overovateľovi bezpečnosti** | | | | | | |
| **Časť 1a. Informácie o organizácii obchodníka** | | | | | | |
| Názov spoločnosti: | ........... | | DBA (obchodné meno): | ........... | | |
| Meno kontaktnej osoby: | ........... | | Titul: | ........... | | |
| Telefón: | ........... | | E-mail: | ........... | | |
| Obchodné sídlo: | ........... | | Mesto: | ........... | | |
| Štát / provincia: | ........... | Krajina: | ........... | | Poštové číslo: | ........... |
| URL: | ........... | | | | | |
| **Časť 1b. Informácie o oprávnenom overovateľovi bezpečnosti (podľa potreby)** | | | | | | |
| Názov spoločnosti: | ........... | | | | | |
| Meno kontaktnej osoby QSA: | ........... | | Titul: | ........... | | |
| Telefón: | ........... | | E-mail: | ........... | | |
| Obchodné sídlo: | ........... | | Mesto: | ........... | | |
| Štát / provincia: | ........... | Krajina: | ........... | | Poštové číslo: | ........... |
| URL: | ........... | | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Časť 2. Súhrnná správa** | | | |
| **Časť 2a. Podnikateľská činnosť obchodníka (začiarknite všetky, ktoré sa vzťahujú)** | | | |
| Maloobchodník  Telekomunikácie  Potraviny a supermarkety | | | |
| Ropné výrobky  Elektronický predaj  Poštový / telefonický predaj (MOTO) | | | |
| Iné (uveďte): | | | |
| Aké platobné metódy využíva vaša spoločnosť?  Poštové / telefonické objednávky (MOTO)  Elektronický predaj  Fyzická prítomnosť karty (kamenný predaj) | | Aké platobné metódy sú pokryté v tomto SAQ?  Poštové / telefonické objednávky (MOTO)  Elektronický predaj  Fyzická prítomnosť karty (kamenný predaj) | |
| ***Poznámka:*** *V prípade, že vaša spoločnosť využíva platobnú metódu alebo postup, ktoré nie sú obsiahnuté v tomto SAQ, obráťte sa na vášho nadobúdateľa alebo kartovú spoločnosť o validáciu ostatných metód.* | | | |
| **Časť 2b. Popis spracovania platobných kariet** | | | |
| Ako a v akom rozsahu vaša spoločnosť ukladá, spracováva a/alebo prenáša údaje držiteľa karty? | ........... | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Časť 2c. Miesta** | | | | |
| Uveďte zoznam všetkých zariadení (napríklad maloobchodné predajne, firemné kancelárie, dátové centrá, call centrá, atď.) a súhrn miest obsiahnutých v posudku PCI DSS. | | | |
| **Spôsob zariadenia** | **Počet zariadení tohto typu** | **Miesto zariadenia (mesto, krajina)** |
| *Príklad: Maloobchodné predajne* | *3* | *Boston, MA, USA* |
| ........... | ........... | ........... |
| ........... | ........... | ........... |
| ........... | ........... | ........... |
| ........... | ........... | ........... |
| ........... | ........... | ........... |
| ........... | ........... | ........... |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Časť 2d. Platobná aplikácia** | | | | | |
| Využíva vaša spoločnosť jednu alebo viacero platobných aplikácií? Áno Nie | | | | |
| Uveďte nasledujúce informácie týkajúce sa platobných aplikácií používaných vašou spoločnosťou: | | | | | |
| **Názov platobnej aplikcáie** | **Číslo verzie** | **Dodávateľ aplikácie** | **Je aplikácia v zozname PA-DSS?** | **Dátum skončenia platnosti PA-DSS (ak existuje)** | |
| ........... | ........... | ........... | Áno  Nie | ........... | |
| ........... | ........... | ........... | Áno  Nie | ........... | |
| ........... | ........... | ........... | Áno  Nie | ........... | |
| ........... | ........... | ........... | Áno  Nie | ........... | |
| ........... | ........... | ........... | Áno  Nie | ........... | |

|  |  |  |
| --- | --- | --- |
| **Časť 2e. Popis prostredia** | | |
| Uveďte ***podrobný*** popis prostredia posudzovaného v tomto hodnotení.  *Napríklad:*  • *Spojenia s dátovým prostredím držiteľa karty (CDE).*  • *Kritické súčasti systému v rámci CDE, ako sú POS, zariadenia, databázy, webové servery, atď. a akékoľvek ďalšie potrebné platobné komponenty, podľa potreby.* | ........... | | |
| Využíva vaša spoločnosť segmentáciu siete na zmenu rozsahu vášho prostredia PCI DSS?  *(Pozri sekciu „segmentácia siete" PCI DSS pre inštrukcie k segmentácii siete)* | | Áno  Nie | |

|  |  |  |
| --- | --- | --- |
| **Časť 2f. Poskytovateľ služieb v úlohe tretej strany** | | |
| Využíva vaša spoločnosť QIR (Kvalifikovaný integrátor a predajca)?  Ak áno:  Názov spoločnosti QIR:  Samostatné meno QIR:  Popis služieb poskytovaných QIR: | | Áno  Nie | |
| Zdieľa vaša spoločnost údaje držiteľa karty s inými poskytovateľmi tretej strany (napríklad: QIR, poskytovatelia brán, spracovateľkých platobných služieb, platobných služieb (PSP) a webhostingových služieb, zástupcovia rezervačných leteckých služieb, zástupcovia vernostných programov, atď.)? | | Áno  Nie | |
| ***Ak áno:*** | | |
| **Meno poskytovateľa:** | **Popis poskytovnaých služieb:** | |
| ........... | ........... | |
| ........... | ........... | |
| ........... | ........... | |
| ........... | ........... | |
| ........... | ........... | |
| ........... | ........... | |
| ***Poznámka:*** *Požiadavky 12.8 sa vzťahujú na všetky subjekty v tomto zozname.* | | |

**Sekcia 2:** **Samohodnotiaci dotazník D pre obchodníkov**

***Poznámka:***Nasledujúce otázky sú očíslované podľa požiadavky PCI DSS a skúšobných postupov, ako sú definované v dokumente Požiadavky PCI DSS a postup hodnotenia bezpečnosti.

**Dátum dokončenia samohodnotenia:**

**Vybudovanie a udržiavanie bezpečnostnej siete a systémov**

***Požiadavka 1:*** ***Inštalácia a udržiavanie firewallového systému na ochranu dát***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Otázka PCI DSS** | | **Očakávané testovanie** | **Odpoveď**  ***(Zaškrtnite jednu odpoveď pre každú otázku)*** | | | | |
| **Áno** | **Áno s CCW** | **Nie** | **N/A** | **Netestované** |
| 1.1 | Obsahujú vaše zavedené štandardy o konfigurácii firewallu a routeru nasledujúce prvky: |  |  |  |  |  |  |
| 1.1.1 | Je zavedený formálny postup na schvaľovanie a testovanie všetkých sieťových pripojení a zmien konfigurácií firewallu a routeru? |  Kontrola zavedeného procesu   Rozhovor s personálom   Preskúmanie sieťových konfigurácií |  |  |  |  |  |
| 1.1.2 | (a) Existuje aktuálny sieťový diagram, ktorý obsahuje informácie o všetkých pripojeniach medzi dátovým prostredím držiteľa karty a ostatnými sieťami, vrátane bezdrôtových sietí? |  Kontrola súčasného sieťového diagramu   Preskúmanie sieťových konfigurácií |  |  |  |  |  |
| (b) Je zavedený proces na zabezpečenie aktualizácii diagramu? |  Rozhovor so zodpovedným personálom |  |  |  |  |  |
| 1.1.3 | (a) Máte aktualizovaný diagram, ktorý zobrazuje všetky prechádzajúce údaje držiteľa karty v systéme a sietiach? |  Kontrola súčasného diagramu dátového toku   Preskúmanie sieťových konfigurácií |  |  |  |  |  |
| (b) Je zavedený proces na zabezpečenie aktualizácii diagramu? |  Rozhovor s personálom |  |  |  |  |  |
| 1.1.4 | (a) Vyžaduje sa firewall a je zavedený pre každé internetové pripojenie a medzi demilitarizovanou zónou (DMZ) a vnútornou sieťovou zónou? |  Preskúmanie štandardov konfigurácie firewallu   Skontrolujte sieťové konfigurácie na overenie, či firewall je nainštalovaný |  |  |  |  |  |
|  | (b) Je súčasný sieťový diagram v súlade so štandardami firewallovej konfigurácie? |  Porovnajte štandardy firewallovej konfigurácie s aktuálnym sieťovým diagramom |  |  |  |  |  |
| 1.1.5 | Sú priradené skupiny, úlohy a zodpovednosti logického riadenia sieťových komponentov obsiahnuté v štandardoch konfigurácie firewallu a routeru? |  Preskúmanie štandardov konfigurácie firewallu a routeru   Rozhovor s personálom |  |  |  |  |  |
| 1.1.6 | (a) Obsahujú vaše štandardy konfigurácie firewallu a routeru zoznam služieb, protokolov a portov, vrátane obchodného odôvodnenia a schválenia každého z nich? |  Preskúmanie štandardov konfigurácie firewallu a routeru |  |  |  |  |  |
| (b) Máte zavedené a zdokumentované bezpečnostné funkcie pre všetky nezabezpečené služby, prokotoly a porty? |  Preskúmanie štandardov konfigurácie firewallu a routeru   Kontrola konfigurácie firewallu a routeru |  |  |  |  |  |
| 1.1.7 | (a) Vyžaduje váš štandard konfigurácie firewallu a routeru pravidelnú kontrolu nastavených pravidiel firewallu a routeru najmenej každých šesť mesiacov? |  Preskúmanie štandardov konfigurácie firewallu a routeru |  |  |  |  |  |
| (b) Sú vaše nastavené pravidla firewallu a routeru kontrolované najmenej raz za šesť mesiacov? |  Preskúmanie dokumentácie z kontrol firewallu |  |  |  |  |  |
| 1,2 | Je konfigurácia firewallu a routeru nastavená tak, aby obmedzovala pripojenia medzi neoverenými sieťami a akýmkoľvek systémom z dátového prostredia držiteľa kartý, pričom:  ***Poznámka:*** *„Neoverená sieť" je akákoľvek sieť, ktorá nepatrí do siete posudzovaného subjektu a ktorá je mimo kontroly alebo riadenia daného subjektu.* |  | | | | | |
| 1.2.1 | (a) Sú prichádzajúce a odchádzajúce prenosy obmedzené na nevyhnutný rozsah, pokiaľ ide o dátové prostredie držiteľa karty? |  Preskúmanie štandardov konfigurácie firewallu a routeru   Kontrola konfigurácie firewallu a routeru |  |  |  |  |  |
|  | (b) Sú všetky ostatné prichádzajúce a odchádzajúce prenosy špecificky zamietnuté (napríklad použitím explicitného príkazu „zamietnuť všetky" alebo implicitného zamietnutia povoľujúceho príkazu)? |  Preskúmanie štandardov konfigurácie firewallu a routeru   Kontrola konfigurácie firewallu a routeru |  |  |  |  |  |
| 2.2.1 | Sú konfiguračné súbory routera chránené voči neoprávnenému prístupu a synchronizované - napríklad spustená (alebo aktívna) konfigurácia zodpovedá konfigurácii pri spustení (používaná pri spustení zariadenia)? |  Preskúmanie štandardov konfigurácie firewallu a routeru   Preskúmanie konfiguračných súborov routera a routerovej konfigurácie |  |  |  |  |  |
| 1.2.3 | Sú medzi všetkými bezdrôtovými sieťami a dátovým prostredím držiteľa karty nainštalované obvodové firewally a sú tieto firewally nainštalované tak, aby zamietali alebo (v prípade, že je to potrebné na obchodné účely) schvaľovali len oprávnenú komunikáciu medzi bezdrôtovým prostredím a dátovým prostredím držiteľa karty. |  Preskúmanie štandardov konfigurácie firewallu a routeru   Kontrola konfigurácie firewallu a routeru |  |  |  |  |  |
| 1.3 | Je priamy verejný prístup zákazaný medzi internetom a akýmkoľvek komponentom v systéme dátového prostredia držiteľa karty, a to nasledovne: |  |  |  |  |  |  |
| 1.3.1 | Je DMZ zavedené tak, aby obmedzovalo prichádzajúcu komunikáciu len na systémové komponenty, ktoré umožňujú oprávnené verejné prístupové služby, protokoly a porty? |  Kontrola konfigurácie firewallu a routeru |  |  |  |  |  |
| 1.3.2 | Je prichádzajúca internetová komunikácia s IP adresami v rámci DMZ? |  Kontrola konfigurácie firewallu a routeru |  |  |  |  |  |
| 1.3.3 | Sú zavedené opatrenia proti falšovaniu zamerané na odhaľovanie a blokovanie falošných vstupných IP adries pri prístupe na sieť?  (Napríklad, blokovanie prichádzajúcej komunikácie z internetu s internou adresou). |  Kontrola konfigurácie firewallu a routeru |  |  |  |  |  |
| 1.3.4 | Je odchádzajúca komunikácia z dátového prostredia držiteľa karty na internet explicitne autorizovaná? |  Kontrola konfigurácie firewallu a routeru |  |  |  |  |  |
| 1.3.5 | Majú k sieti prístup len zavedené pripojenia? |  Kontrola konfigurácie firewallu a routeru |  |  |  |  |  |
| 1.3.6 | Sú systémové komponenty, ktoré ukladajú údaje držiteľa karty (ako je databáza) umiestnené v internej sieťovej zóne oddelenej od DMZ a iných neoverených sietí? |  Kontrola konfigurácie firewallu a routeru |  |  |  |  |  |
| 1.3.7 | (a) Sú zavedené postupy na zabránenie neoprávneného odhalenia súkromných IP adries a informácií o trasovaní?  ***Poznámka:*** *Metódy na zakrytie IP adresy môžu zahŕňať nasledovné:*   Maskovanie sieťovej adresy NAT   Umiestnenie serverov s údajmi držiteľa kary za proxy servery / firewally,   Odstránenie alebo filtrovanie reklám o trasovaní pre súkromné siete, ktoré využívajú registrované adresy,   Interné použitie adresy RFC1918 namiesto registrovanej adresy. |  Kontrola konfigurácie firewallu a routeru |  |  |  |  |  |
| (b) Môže dochádzať k oprávnenému odtajňovaniu súkromných IP adries a informácií o trasovaní zo strany externých subjektov? |  Kontrola konfigurácie firewallu a routeru   Rozhovor s personálom |  |  |  |  |  |
| 1.4 | (a) Je nainštalovaný firewall (alebo softvér s ekvivalentnou účinnosťou) a aktívny na každom prenosnom počítačovom zariadení (či už vo vlastníctve spoločnosti a/alebo zamestnancov), ktoré sa pripája na internet mimo siete (napríklad, notebooky používané zamestnancami), ktoré sa takisto využívajú na prístup do CDE? |  Preskúmanie politík a štandardov konfigurácie firewallu   Kontrola prenosných zariadení a/alebo zariadení zamestnancov |  |  |  |  |  |
|  | (b) Je firewall (alebo softvér s ekvivalentnou účinnosťou) nastavený na špecifickú konfiguráciu, aktívny a zabezpečený voči neoprávnenému zásahu zo strany užívateľov mobilných zariadení alebo zariadení zamestnancov? |  Preskúmanie politík a štandardov konfigurácie firewallu   Kontrola prenosných zariadení a/alebo zariadení zamestnancov |  |  |  |  |  |
| 1,5 | Sú bezpečnostné pravidlá a operačné postupy pre správu firewallov:   zdokumentované   používané   oznámené dotknutým stranám? |  Kontrola bezpečnostných pravidiel a operačných postupov   Rozhovor s personálom |  |  |  |  |  |

***Požiadavka 2:*** ***Nepoužívanie predvolených nastavení systémových hesiel a iných bezpečnostných parametrov***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Otázka PCI DSS** | | **Očakávané testovanie** | **Odpoveď**  ***(Zaškrtnite jednu odpoveď pre každú otázku)*** | | | | |
| **Áno** | **Áno s CCW** | **Nie** | **N/A** | **Netestované** |
| 2.1 | (a) Sú pred inštaláciou systému na sieť vždy zmenené predvolené nastavenia dodávateľa?  *Toto sa týka všetkých predvolených hesiel, vrátane (ale nie výlučne) tých, ktoré využívajú operačné systémy, bezpečnostného softvéru, systémových účtov a účtov aplikácií, platobných terminálov v mieste predaja (POS), platobných aplikácií, jednoduchého sieťového riadiaceho protokolu (SNMP), komunitých reťazcov, atď.).* |  Kontrola pravidiel a postupov   Kontrola dokumentácie dodávateľa   Preskúmanie systémového nastavenia a nastavenia účtu   Rozhovor s personálom |  |  |  |  |  |
|  | (b) Pred inštaláciou systému do siete sú odstránené alebo zakázané zbytočné predvolené účty? |  Kontrola pravidiel a postupov   Kontrola dokumentácie dodávateľa   Preskúmanie systémového nastavenia a nastavenia účtu   Rozhovor s personálom |  |  |  |  |  |
| 2.1.1 | V prípade bezdrôtového prostredia pripojeného k dátovému prostrediu držiteľa karty alebo prenose údajov držiteľa karty, sú VŠETKY bezdrôtové predvolené nastavenia zmenené počas inštalácie nasledovným spôsobom: |  |  |  |  |  |  |
|  | (a) Sú šifrovacie kľúče zmenené pri inštalácii z predvolených hodnôt a vždy v prípade, kedy zamestnanec, ktorý pozná tieto kľúče odíde zo spoločnosti alebo zmení pozíciu? |  Kontrola pravidiel a postupov   Kontrola dokumentácie dodávateľa   Rozhovor s personálom |  |  |  |  |  |
|  | (b) Sú predvolené komunitné reťazce SNMP na bezdrôtových zariadeniach zmenené pri inštalácii? |  Kontrola pravidiel a postupov   Kontrola dokumentácie dodávateľa   Rozhovor s personálom   Preskúmanie systémových konfigurácií |  |  |  |  |  |
|  |
|  | (c) Sú predvolené heslá / prístupové frázy v prístupových bodoch zmenené pri inštalácii? |  Kontrola pravidiel a postupov   Rozhovor s personálom   Preskúmanie systémových konfigurácií |  |  |  |  |  |
|  | (d) Bol aktualizovaný firmvér na bezdrôtových zariadeniach na podporu silného šifrovania na účely autentifikácie a prenosu prostredníctvom bezdrôtových sieti? |  Kontrola pravidiel a postupov   Kontrola dokumentácie dodávateľa   Preskúmanie systémových konfigurácií |  |  |  |  |  |
|  | (e) Boli zmenené všetky ostatné bezpečnostné bezdrôtové predvolené nastavenia? |  Kontrola pravidiel a postupov   Kontrola dokumentácie dodávateľa   Preskúmanie systémových konfigurácií |  |  |  |  |  |
| 2.2 | (a) Boli pre všetky systémové komponenty vyvinuté konfiguračné štandardy a sú v súlade s priemyselne akceptovanými systémovými bezpečnostnými štandardami?  *Zdroje priemyselne akceptovaných bezpečnostných štandardov môžu zahŕňať (ale nie len) inštitút SysAdmin Audit Network Security (SANS) Institute, Národný inštitút technologických noriem (NIST), Medzinárodnú organizáciu pre normalizáciu (ISO) a Centrum pre internetovú bezpečnost (CIS).* |  Preskúmanie systémových konfiguračných štandardov   Preskúmanie priemyselne akceptovaných bezpečnostných štandardov   Kontrola pravidiel a postupov   Rozhovor s personálom |  |  |  |  |  |
|  | (b) Sú systémové konfiguračné štandardy aktualizované, vždy po odhalení nových problémov zraniteľnosti tak, ako je definované v požiadavke 6.1? |  Kontrola pravidiel a postupov   Rozhovor s personálom |  |  |  |  |  |
|  | (c) Sú systémové konfiguračné štandardy použité pri nastavovaní nových systémov? |  Kontrola pravidiel a postupov   Rozhovor s personálom |  |  |  |  |  |
|  | (d) Obsahujú systémové konfiguračné štandardy všetky nasledovné prvky:   Dochádza k zmene všetkých predvolených nastavení a odstráneniu nepotrebných predvolených účtov?   Je na každý server implementovaná len jedna primárna funkcia na zabránenie toho, aby funkcie s rozdielnymi bezpečnostnými úrovňami nemohli pracovať súčasne na rovnakom serveri?   Majú povolenie len potrebné služby, protokoly, démonov atď, tak, ako to vyžaduje daná funkcia systému?   Dochádza k implementácii dodatočných bezpečnostných funkcií pre všetky potrebné služby, protokoly a démonov, ktoré sú považované za nezabezpečené?   Sú systémové bezpečnostné parametre nastavené tak, aby zabránili neoprávnenému použitiu?   Dochádza k odstraňovaniu nepotrebných funkcionalít, ako sú skripty, ovládače, funkcie, podsystémy, systémy súborov a nepotrebné webové servery? |  Preskúmanie systémových konfiguračných štandardov |  |  |  |  |  |
| 2.2.1 | (a) Je na každý server implementovaná len jedna primárna funkcia na zabránenie toho, aby funkcie s rozdielnymi bezpečnostnými úrovňami nemohli pracovať súčasne na rovnakom serveri?  *Napríklad webové servery, databázové servery a DNS musia byť nainštalované na samostatných serveroch.* |  Preskúmanie systémových konfigurácií |  |  |  |  |  |
|  | (b) V prípade použitia virtualizačných technológií, je na každý virtuálny systémový komponent alebo zariadenie použitá len jedna primárna funkcia? |  Preskúmanie systémových konfigurácií |  |  |  |  |  |
| 2.2.2 | (a) Majú povolenie len potrebné služby, protokoly, démoni atď, tak, ako to vyžaduje daná funkcia systému (sú vypnuté služby a protokoly, ktoré nie sú priamo potrebné na vykonanie funkcie zariadenia)? |  Preskúmanie konfiguračných štandardov   Preskúmanie systémových konfigurácií |  |  |  |  |  |
|  | (b) Sú všetky povolené nezabezpečené služby, démoni alebo protokoly odôvodnené a zdokumentované v konfiguračných štandardoch? |  Preskúmanie konfiguračných štandardov   Rozhovor s personálom   Preskúmanie konfiguračných nastavení   Porovnanie povolených služieb, atď. so záznamami |  |  |  |  |  |
| 2.2.3 | Dochádza k implementácii dodatočných bezpečnostných funkcií pre všetky potrebné služby, protokoly a démonov, ktorí sú považovaní za nezabezpečení?  ***Poznámka:*** *Pri použití SSL/starších TLS je nutné vyplniť požiadavky dodatku A2.* |  Preskúmanie konfiguračných štandardov   Preskúmanie konfiguračných nastavení |  |  |  |  |  |
| 2.2.4 | (a) Boli systémoví administrátori a/alebo zamestnanci, ktorí nastavujú systémové komponenty, oboznámení so spoločnými bezpečnostnými parametrami a nastaveniami pre tieto systémové komponenty? |  Rozhovor s personálom |  |  |  |  |  |
|  | (b) Sú spoločné systémové bezpečnostné parametre a nastavenia zahrnuté v systémových konfiguračných štandardoch? |  Preskúmanie systémových konfiguračných štandardov |  |  |  |  |  |
|  | (c) Sú bezpečnostné parametre a nastavenia nastavené vhodne na dané systémové komponenty? |  Preskúmanie systémových komponentov   Preskúmanie bezpečnostných parametrov a nastavení   Porovnanie nastavení so systémovými konfiguračnými štandardami |  |  |  |  |  |
| 2.2.5 | (a) Dochádza k odstraňovaniu nepotrebných funkcionalít, ako sú skripty, ovládače, funkcie, podsystémy, systémy súborov a nepotrebné webové servery? |  Preskúmanie bezpečnostných parametrov pre systémové komponenty |  |  |  |  |  |
| (b) Sú povolené funkcie zdokumentované a podporujú bezpečnú konfiguráciu? |  Kontrola dokumentácie   Preskúmanie bezpečnostných parametrov pre systémové komponenty |  |  |  |  |  |
| (c) Je na systémových komponentoch prítomná len riadne zdokumentovaná funkcionalita? |  Kontrola dokumentácie   Preskúmanie bezpečnostných parametrov pre systémové komponenty |  |  |  |  |  |
| 2.3 | Je správcovský prístup bez konzoly zašifrovaný nasledovným spôsobom:  ***Poznámka:*** *Pri použití SSL/starších TLS je nutné vyplniť požiadavky dodatku A2.* |  |  |  |  |  |  |
|  | (a) Je správcovský prístup bez konzoly riadne zašifrovaný a je silná metóda šifrovania vyvolaná predtým, než sa vyžaduje heslo administrátora? |  Preskúmanie systémových komponentov   Preskúmanie systémových konfigurácií   Kontrola prihlasovania správcu |  |  |  |  |  |
|  | (b) Sú systémové služby a súbory parametrov nakonfigurované tak, aby zabránili používaniu príkazov Telnet a iných nezabezpečených vzdialených prihlasovacích príkazov? |  Preskúmanie systémových komponentov   Kontrola služieb a súborov |  |  |  |  |  |
|  | (c) Je správcovský prístup k webovému riadiacemu rozhraniu riadne zašifrovaný? |  Preskúmanie systémových komponentov   Kontrola prihlasovania správcu |  |  |  |  |  |
|  | (d) Pri používanej technológii, je šifrovanie riadne implementované v súlade s osvedčenými postupmi a/alebo odporúčaní predajcu? |  Preskúmanie systémových komponentov   Kontrola dokumentácie dodávateľa   Rozhovor s personálom |  |  |  |  |  |
| 2.4 | (a) Je udržiavaný inventár pre systémové komponenty, ktoré spadajú do pôsobnosti PCI DSS, vrátané zoznamu hardvérových a softvérových komponentov s opisom funkcionality/použitia každého z nich? |  Preskúmanie systémového inventára |  |  |  |  |  |
| (b) Je tento inventár aktualizovaný? |  Rozhovor s personálom |  |  |  |  |  |
| 2.5 | Sú bezpečnostné pravidlá a prevádzkové postupy na riadenie predvolených parametrov a iných bezpečnostných parametrov:   zdokumentované   používané   oznámené dotknutým stranám? |  Kontrola bezpečnostných pravidiel a operačných postupov   Rozhovor s personálom |  |  |  |  |  |
| 2.6 | *Táto požiadavka sa vzťahuje výlučne na poskytovateľov služieb.* |  |  |  |  |  |  |

**Ochrana údajov držiteľa karty**

***Požiadavka 3:*** ***Ochrana uložených údajov držiteľa karty***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Otázka PCI DSS** | | **Očakávané testovanie** | **Odpoveď**  ***(Zaškrtnite jednu odpoveď pre každú otázku)*** | | | | |
| **Áno** | **Áno s CCW** | **Nie** | **N/A** | **Netestované** |
| 3.1 | Sú zásady, postupy a pravidlá na uchovávanie a likvidáciu údajov implementované nasledovne: |  |  |  |  |  |  |
| (a) Je uchovávanie údajov limitované časovo a množstvom tak, aby bol takýto postup v súlade so zákonnými, regulačnými a/alebo obchodnými požiadavkami? |  Preskúmanie pravidiel a postupov na uchovávanie a likvidáciu údajov   Rozhovor s personálom |  |  |  |  |  |
| (b) Sú zadefinované postupy na zabezpečenie zničenia údajov držiteľa karty, ktoré nie sú už ďalej potrebné z právnych, regulačných a/alebo obchodných dôvodov? |  Kontrola pravidiel a postupov   Rozhovor s personálom   Kontrola mechanizmu mazania a likvidácie |  |  |  |  |  |
| (c) Existujú špeciálne požiadavky na uchovávanie údajov držiteľov kariet?  *Napríklad, údaje držiteľa karty musia byť uchovávané po dobu X kvôli obchodným dôvodom Y.* |  Kontrola pravidiel a postupov   Rozhovor s personálom   Kontrola požiadaviek na uchovávanie |  |  |  |  |  |
| (d) Existuje štvrťročný proces identifikácie a bezpečnostného mazania údajov držiteľov kariet, ktoré presahujú definované požiadavky na uchovávanie údajov? |  Kontrola pravidiel a postupov   Rozhovor s personálom   Kontrola postupu mazania |  |  |  |  |  |
| (e) Spĺňajú všetky uložené údaje držiteľov kariet požiadavky uvedené v pravidlách uchovávania údajov? |  Kontrola súborov a systémových záznamov |  |  |  |  |  |
| 3.2 | (a) *Tento postup testovania sa týka len vydávateľov.* |  |  |  |  |  |  |
| (b) *Tento postup testovania sa týka len vydávateľov.* |  |  |  |  |  |  |
|  | (c) Sú po dokončení autorizačného procesu citlivé autentifikačné údaje neobnoviteľné po ich vymazaní? |  Kontrola pravidiel a postupov   Preskúmanie systémových konfigurácií   Kontrola postupov mazania |  |  |  |  |  |
|  | (d) Spĺňajú všetky systémy nasledovné požiadavky týkajúce sa neuchovávania citlivých autentifikačných údajov po autorizačnom procese (aj keď sú zašifrované): |  |  |  |  |  |  |
| 3.2.1 | Neuchováva sa po autorizácii celý obsah akejkoľvek stopy (či už z magnetického prúžku umiestneného na zadnej strane karty, ekvivalentné údaje obsiahnuté na čipe alebo inak)?  *Tieto údaje sa alternatívne nazývajú celá stopa, stopa, stopa 1, stopa 2 a údaje z magnetického prúžku.*  ***Poznámka:*** *Pri bežnom podnikaní môže byť potrebné uchovať nasledujúce údaje z magnetického prúžku:*   *meno držiteľa karty,*   *číslo primárneho účtu (PAN),*   *dátum expirácie a*   *servisný kód*  *Na minimalizáciu rizika sú obvykle potrebné len tieto údaje.* |  Kontrola zdrojov údajov, vrátane:   údajov o prichádzajúcich transakciách   všetkých záznamoch   súborov histórie   súborov trasy   databázovej schémy   databázového obsahu |  |  |  |  |  |
| 3.2.2 | Overovací kód alebo hodnota na karte (trojmiestny alebo štvormiestny kód na prednej alebo zadnej strane platobnej karty) sa neukladá po autorizácii? |  Kontrola zdrojov údajov, vrátane:   údajov o prichádzajúcich transakciách   všetkých záznamoch   súborov histórie   súborov trasy   databázovej schémy   databázového obsahu |  |  |  |  |  |
| 3.2.3 | Osobné identifikačné číslo (PIN) alebo šifrovaný blok PIN sa neukladá po autorizácii? |  Kontrola zdrojov údajov, vrátane:   údajov o prichádzajúcich transakciách   všetkých záznamoch   súborov histórie   súborov trasy   databázovej schémy   databázového obsahu |  |  |  |  |  |
| 3.3 | Dochádza k maskovaniu kódu PAN pri jeho zobrazení (maximálne môže byť zobrazených prvých 6 čísiel a posledné 4 čísla) tak, aby boli zamestnanci schopní vidieť len prvých 6/posledné 4 čísla kódu PAN?  ***Poznámka:*** *Táto požiadavka nenahrádza prísnejšie požiadavky na zobrazovanie údajov držiteľov kariet - napríklad zákonné požiadavky alebo požiadavky kartovej spoločnosti na používanie kariet v mieste predaja (POS).* |  Kontrola pravidiel a postupov   Kontrola úloh, ktoré potrebujú prístup na zobrazenie plného kódu PAN   Preskúmanie systémových konfigurácií   Kontrola zobrazovania kódu PAN |  |  |  |  |  |
| 3.4 | Je kód PAN nečitateľný pri uložení (vrátane dátových skladov, prenosných digitálnych médií, záložných médií a kontrolných záznamov) pomocou niektorého z nasledujúcich metód?   Jednosmerné hašovanie (celý kód PAN musí byť zahašovaný)   Skrátenie (hašovanie sa nesmie použiť na nahradenie skráteného segmentu kódu PAN)   Indexové tokeny a pady (pady musia byť bezpečne uložené)   Šifrovanie so súvisiacimi procesmi a postupmi správy kľúčov.  ***Poznámka:*** *Je pomerne triviálne pre neoprávnené osoby rekonštruovať originálny kód PAN, ak majú prístup ku skrátenej a hašovanej verzii kódu PAN. V prípade, že má subjekt prístup k hašovanej a skrátenej verzii rovnakého kódu PAN, je nutné mať zavedené dodatočné kontrolné mechanizmy na zabezpečenie toho, aby nedošlo k spojeniu hašovanej a skrátenej verzii originálneho kódu PAN, a tým zabráneniu jeho možnej rekonštrukcii.* |  Kontrola dokumentácie dodávateľa   Kontrola dátových úložísk   Kontrola vymeniteľných médií   Kontrola kontrolných záznamov, vrátane záznamov platobných aplikácií |  |  |  |  |  |
| 3.4.1 | V prípade, že sa používa šifrovanie disku (namiesto šifrovania databázy na úrovni súbora alebo stĺpca), jeho prístup je riadený nasledovne:  ***Poznámka:*** *Táto požiadavka je nad rámec ostatných požiadaviek PCI DSS na šifrovanie a správu kľúčov.* |  |  |  |  |  |  |
| (a) Je logický prístup k zašifrovaným systémovým súborom riadený samostatne a nezávisle od pôvodnej autentifikácie operačného systému a prístupových kontrolných mechanizmov (napríklad tým, že sa nepoužíva databáza miestnych užívateľov alebo všeobecné sieťové prihlasovacie údaje)? |  Preskúmanie systémových konfigurácií   Kontrola procesu autentifikácie |  |  |  |  |  |
|  | (b) Sú šifrovacie kľúče ukladané samostatne (napríklad, uložené na odstrániteľných médiách, ktoré sú primerane chránené pomocou silných prístupových bezpečnostných prvkov)? |  Kontrola procesov   Rozhovor s personálom |  |  |  |  |  |
|  | (c) Sú údaje držiteľa karty na vymeniteľnom médiu zašifrované vždy, keď sú uložené?  ***Poznámka:*** *V prípade, že sa nepoužíva šifrovanie disku na zašifrovanie vymeniteľného disku, musia byť dáta uložené na takomto disku zabezpečené inou metódou.* |  Preskúmanie systémových konfigurácií   Kontrola procesov |  |  |  |  |  |
| 3.5 | Sú kľúče použité na zabezpečenie uložených údajov držiteľa karty chránené voči zverejneniu a zneužitiu nasledovným spôsobom:  ***Poznámka:*** *Táto požiadavka sa týka len kľúčov použitých na zašifrovanie uložených údajov držiteľov kariet a takisto na kľúče použité na ochranu zašifrovacích kľúčov. Takéto kľúče na šifrovanie kľúčov musia byť aspoň tak silné, ako kľúče na šifrovanie údajov.* |  |  |  |  |  |  |
| 3.5.1 | *Táto požiadavka sa vzťahuje výlučne na poskytovateľov služieb* |  | | | | | |
| 3.5.2 | Je prístup šifrovacích kľúčov obmedzený pre čo najmenší počet správcov? |  Kontrola zoznamu prístupových účtov |  |  |  |  |  |
| 3.5.3 | Sú tajné a súkromné šifrovacie kľúče používané na zašifrovanie/odšifrovanie údajov držiteľov kariet uložené nasledujúcim (alebo nasledujúcimi) spôsobmi?   Šifrovanie kľúčov pomocou šifrovacích kľúčov, ktoré sú aspoň tak silné ako kľúč na šifrovanie údajov a uložené samostatne od kľúčov na šifrovanie údajov   V rámci zabezpečeného šifrovacieho zariadenia (ako je hardvérový (hostiteľský) bezpečnostný modul (HSM) alebo schválené zariadenia PTS s miestom interakcie)   Najmenej dva kľúčové komponenty v plnej dĺžke alebo kľúčové časti v súlade s priemyselne akceptovanou metódou.  ***Poznámka:*** *Nie je potrebné, aby boli verejné kľúče uložené pomocou týchto foriem.* |  Kontrola zdokumentovaných postupov   Preskúmanie systémových konfigurácií a miest skladovania kľúčov, vrátane kľúčov na šifrovanie kľúčov |  |  |  |  |  |
| 3.5.4 | Sú šifrovacie kľúče uložené v čo najmenšom počte rôznych miest? |  Preskúmanie miest skladovania kľúčov   Kontrola procesov |  |  |  |  |  |
| 3.6 | (a) Sú všetky postupy a procesy správy kľúčov plne zdokumentované a realizované pokiaľ ide o šifrovacie kľúče používané na šifrovanie údajov držiteľov kariet? |  Kontrola postupov riadenia kľúčov |  |  |  |  |  |
| (b) *Tento postup testovania sa týka len poskytovateľov služieb.* |  |  |  |  |  |  |
|  | (c) Sú postupy a procesy riadenia kľúčov realizované tak, aby vyžadovali nasledovné: |  |  |  |  |  |  |
| 3.6.1 | Zahŕňajú šifrovacie postupy tvorbu silných šifrovacích kľúčov? |  Kontrola postupov riadenia kľúčov   Kontrola šifrovacieho postupu |  |  |  |  |  |
| 3.6.2 | Obsahujú šifrovacie postupy bezpečnú distribúciu šifrovacích kľúčov? |  Prečítajte si postupy riadenia kľúčov   Kontrola postupov distribúcie kľúčov |  |  |  |  |  |
| 3.6.3 | Obsahujú postupy šifrovacích kľúčov bezpečné skladovanie šifrovacích kľúčov? |  Kontrola postupov riadenia kľúčov   Kontrola metódy bezpečného skladovania kľúčov |  |  |  |  |  |
| 3.6.4 | Obsahujú postupy šifrovacích kľúčov zmenu šifrovacích kľúčov, ktoré dosiahli koniec svojej stanovenej doby šifrovania (napríklad po uplynutí stanovenej doby a/alebo po vytvorení určitého množstva zašifrovaného textu pomocou daného kľúča) tak, ako je stanovené dodávateľom danej aplikácie alebo vlastníkom kľúča a založené na osvedčených postupoch a usmerneniach (napríklad NIST Special Publication 800-57)? |  Kontrola postupov riadenia kľúčov   Rozhovor s personálom |  |  |  |  |  |
| 3.6.5 | (a) Obsahujú postupy šifrovacích kľúčov ich zmazanie alebo výmenu (napríklad archivácia, zničenie a/alebo zrušenie) šifrovacích kľúčov v prípade, že došlo k narušeniu integrity daného kľúča (napríklad odchod zamestnanca so znalosťou daného postupu)? |  Kontrola postupov riadenia kľúčov   Rozhovor s personálom |  |  |  |  |  |
| (b) Obsahujú postupy šifrovacích kľúčov výmenu tých kľúčov, ktorých bezpečnosť je ohrozená? |  Kontrola postupov riadenia kľúčov   Rozhovor s personálom |  |  |  |  |  |
|  | (c) V prípade obnovenia zrušených alebo vymenených šifrovacích kľúčov, sú tieto kľúče využívané len na šifrovacie/overovacie účely a nie na šifrovacie operácie? |  Kontrola postupov riadenia kľúčov   Rozhovor s personálom |  |  |  |  |  |
| 3.6.6 | V prípade použitia manuálnych operácií na riadenie nekódovaných kľúčov obsahujú tieto šifrovacie postupy nasledovné rozdelenie vedomostí a dvojitú kontrolu šifrovacích kľúčov:   Vyžadujú postupy rozdelenia vedomostí, aby časti daného kľúča boli spravované najmenej dvomi osobami, z ktorých každá má vedomosť len o svojej časti?  A   Vyžaduje dvojitá kontrola, aby najmenej dve osoby, ktoré nemajú prístup k autentifikačným materiálom (napríklad heslám a kľúčom) ostatných osôb, vykonali riadiace operácie?  ***Poznámka:*** *Príklady manuálnych operácií na riadenie nekódovaných kľúčov zahŕňajú (ale nielen): tvorba, prenos, nahrávanie, uschovávanie a zničenie kľúčov.* |  Kontrola postupov riadenia kľúčov   Rozhovor s personálom a/alebo   Kontrola procesov |  |  |  |  |  |
| 3.6.7 | Obsahujú šifrovacie postupy prevenciu neoprávnenej výmeny šifrovacích kľúčov? |  Kontrola postupov   Rozhovor s personálom a/alebo   Kontrola procesov |  |  |  |  |  |
| 3.6.8 | Je od správcov šifrovacích kľúčov vyžadované, aby formálne potvrdili (písomne alebo elektronicky), že boli oboznámení a súhlasia so zodpovednosťami a úlohami kladenými na správcov šifrovacích kľúčov |  Kontrola postupov   Kontrola dokumentácie a iných dokladov |  |  |  |  |  |
| 3,7 | Sú bezpečnostné pravidlá a operačné postupy na ochranu uložených údajov držiteľov kariet:   zdokumentované   používané   oznámené dotknutým stranám? |  Kontrola bezpečnostných pravidiel a operačných postupov   Rozhovor s personálom |  |  |  |  |  |

***Požiadavka 4:*** ***Šifrovanie prenosových údajov držiteľa karty pri použití v otvorených verejných sietiach***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Otázka PCI DSS** | | **Očakávané testovanie** | **Odpoveď**  ***(Zaškrtnite jednu odpoveď pre každú otázku)*** | | | | |
| **Áno** | **Áno s CCW** | **Nie** | **N/A** | **Netestované** |
| 4.1 | (a) Používajú sa silné šifrovacie a zabezpečovacie protokoly na ochranu citlivých údajov držiteľov kariet počas prenosu cez otvorené verejné siete?  ***Poznámka:*** *Pri použití SSL/starších TLS je nutné vyplniť požiadavky dodatku A2.*  *Príklady otvorených verejných sietí sú (ale nielen): internet, bezdrôtové technológie, vrátane 802.11 a Bluetooth, bunkové technológie, napríklad Globálny systém pre mobilné komunikácie (GSM), viacnásobný prístup kódovým delením (CDMA) a službu General Packet Radio Service (GPRS).* |  Preskúmanie zdokumentovaných štandardov   Kontrola pravidiel a postupov   Kontrola všetkých miest, kde dochádza k prenosu alebo príjmu CHD   Preskúmanie systémových konfigurácií |  |  |  |  |  |
|  | (b) Sú akceptované len dôveryhodné kľúče a/alebo certifikáty? |  Kontrola prichádzajúcich a odchádzajúcich komunikácií   Kontrola kľúčov a certifikátov |  |  |  |  |  |
|  | (c) Sú bezpečnostné protokoly realizované tak, aby využívali len bezpečné konfigurácie a aby neodporovali nezabezpečené verzie alebo konfigurácie? |  Preskúmanie systémových konfigurácií |  |  |  |  |  |
|  | (d) Je použitá vhodná šifrovacia úroveň použitého šifrovania (kontrola odporúčaní / odporúčaných postupov dodávateľa)? |  Kontrola dokumentácie dodávateľa   Preskúmanie systémových konfigurácií |  |  |  |  |  |
|  | (e) Pokiaľ ide o implementácie TLS, je TLS povolené vždy, keď sa prenášajú alebo prijímajú údaje držiteľa karty?  *Napríklad pokiaľ ide o browserové implementácie:*   *„HTTPS” sa zobrazí ako protokol pre lokalizáciu univerzálneho záznamu prehliadača (URL) a*   Údaje držiteľa karty sú požadované len, ak sa ako súčasť URL objaví „HTTPS". |  Preskúmanie systémových konfigurácií |  |  |  |  |  |
| 4.1.1 | Používajú sa osvedčené postupy pri implementácii šifrovania autentifikácie a bezdrôtových komunikácií odosielajúcich údaje držiteľa karty alebo alebo pripojených k dátovému prostrediu držiteľa karty? |  Preskúmanie zdokumentovaných štandardov   Kontrola bezdrôtových sietí   Preskúmanie systémových konfiguračných nastavení |  |  |  |  |  |
| 4.2 | (a) Sú kódy PAN riadne zašifrované alebo zabezpečené vždy, keď sa posielajú prostredníctvom systému odosielania správ koncového užívateľa (napríklad email, okamžité správy, SMS, chat, atď.)? |  Kontrola procesov   Kontrola odchádzajúcich komunikácií |  |  |  |  |  |
|  | (b) Sú zavedené pravidlá, ktoré stanovujú, aby nechránené kódy PAN nemohli byť posielané prostredníctvom systému odosielania správ koncového užívateľa? |  Kontrola pravidiel a postupov |  |  |  |  |  |
| 4.3 | Sú bezpečnostné pravidlá a operačné postupy na šifrovanie uložených údajov držiteľov kariet:   zdokumentované   používané   oznámené dotknutým stranám? |  Kontrola bezpečnostných pravidiel a operačných postupov   Rozhovor s personálom |  |  |  |  |  |

**Udržiavanie programu na riadenie zraniteľnosti**

***Požiadavka 5:*** ***Ochrana všetkých systémov voči škodlivým softvérom a pravidelná aktualizácia antivírusových programov alebo softvéru***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Otázka PCI DSS** | | **Očakávané testovanie** | **Odpoveď**  ***(Zaškrtnite jednu odpoveď pre každú otázku)*** | | | | |
| **Áno** | **Áno s CCW** | **Nie** | **N/A** | **Netestované** |
| 5.1 | Používa sa antivírusový systém u všetkých systémov, ktoré sú pravidelne vystavované škodlivým softvérom? |  Preskúmanie systémových konfigurácií |  |  |  |  |  |
| 5.1.1 | Sú všetky antivírusové programy schopné odhaľovať, odstraňovať a ochraňovať systém voči všetkým známym typom škodlivého softvéru (napríklad vírusy, trójske kone, červy, spyware, adware a rootkity)? |  Kontrola dokumentácie dodávateľa   Preskúmanie systémových konfigurácií |  |  |  |  |  |
| 5.1.2 | Sú antivírusové programy pravidelne kontrolované a vyhodnocované podľa vyvíjajúcich sa hrozieb škodlivého softvéru, aby sa potvrdilo, či je antivírusový program stále účinný voči škodlivým softvérom? |  Rozhovor s personálom |  |  |  |  |  |
| 5.2 | Sú všetky antivírové mechanizmy uchovávané nasledovným spôsobom: |  |  |  |  |  |  |
| (a) Sú všetky antivírusové programy a definície aktuálne? |  Kontrola pravidiel a postupov   Kontrola antivírusových konfigurácií, vr. hlavnej inštalácie   Preskúmanie systémových komponentov |  |  |  |  |  |
| (b) Sú povolené a vykonávajú sa automatické aktualizácie a pravidelné skenovania? |  Kontrola antivírusových konfigurácií, vr. hlavnej inštalácie   Preskúmanie systémových komponentov |  |  |  |  |  |
| (c) Vytvárajú všetky antivírusové mechanizmy protokoly o kontrole a sú tieto protokoly uchovávané v súlade s požiadavkou 10.7 PCI DSS? |  Preskúmanie antivírusových konfigurácií   Kontrola procesov na uchovávanie protokolov |  |  |  |  |  |
| 5.3 | Sú všetky antivírusové mechanizmy:   Aktívne spustené?   Chránené voči ich zablokovaniu alebo zmene zo strany užívateľa?  ***Poznámka:*** *Antivírusové riešenia môžu byť dočasne zakázané len v prípade legitímnej technickej potreby autorizovanej zo strany manažmentu posudzovanej samostatne. V prípade, že antivírusová ochrana musí byť z určitého dôvodu vypnutá, je nutné tento postup formálne autorizovať. Môže byť nutné implementovať dodatočné bezpečnostné opatrenia počas doby, kedy je antivírusová ochrana vypnutá.* |  Preskúmanie antivírusových konfigurácií   Preskúmanie systémových komponentov   Kontrola procesov   Rozhovor s personálom |  |  |  |  |  |
| 5.4 | Sú bezpečnostné pravidlá a operačné postupy na ochranu systémov voči škodlivému softvéru:   zdokumentované   používané   oznámené dotknutým stranám? |  Kontrola bezpečnostných pravidiel a operačných postupov   Rozhovor s personálom |  |  |  |  |  |

***Požiadavka 6:*** ***Vytváranie a udržiavanie bezpečných systémov a aplikácií***

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Otázka PCI DSS** | | | **Očakávané testovanie** | **Odpoveď**  ***(Zaškrtnite jednu odpoveď pre každú otázku)*** | | | | |
| **Áno** | **Áno s CCW** | **Nie** | **N/A** | **Netestované** |
| 6.1 | Je zavedený postup na odhalenie bezpečnostných zraniteľností, vrátane:   Použitia dôveryhodných externých zdrojov pri odhaľovaní zraniteľností?   Priradenia rizikovej klasifikácie zraniteľnosti, ktorá zahŕňa odhaľovanie vysokorizikových a kritických zraniteľností?  ***Poznámka:*** *Posudzovanie rizík by malo vychádzať z osvedčených postupov v odvetví, rovnako ako aj z hľadiska možného dopadu. Napríklad, kritéria na zoradenie zraniteľností môžu zohľadňovať základné skóre CVSS a/alebo klasifikáciu zo strany dodávateľa a/alebo typy dotknutých systémov.*  *Metódy hodnotenia zraniteľností a priradenia rizík sa budú líšiť v závislosti od stratégie organizácie v oblasti ochrany životného prostredia a stratégie posudzovania rizík. Posudzovanie rizík by malo minimálne stanovovať všetky zraniteľnosti, ktoré sa považujú za vysokorizikové voči životnému prostrediu. Okrem rizík môžu byť aj zraniteľnosti hodnotené za vysokorizikové, ak predstavujú bezprostrednú hrozbu pre životné prostredie, ovplyvňujú kritické systémy a/alebo vedú k potenciálnemu ohrozeniu systému, ak by sa neriešili. Príklady kritických systémov zahŕňajú bezpečnostné systémy, zariadenia a systémy orientované na verejnosť, databázy a iné systémy, ktoré ukladajú, spracovávajú alebo prenášajú dáta držiteľov kariet.* | |  Kontrola pravidiel a postupov   Rozhovor s personálom   Kontrola procesov |  |  |  |  |  |
| 6.2 | (a) Sú všetky systémové komponenty a softvéry chránené voči známym zraniteľnostiam nainštalovanými bezpečnostnými záplatami vydaných dodávateľom? | |  Kontrola pravidiel a postupov |  |  |  |  |  |
| (b) Sú kritické bezpečnostné záplaty inštalované do jedného mesiaca od vydania?  ***Poznámka:*** *Kritické systémové záplaty by sa mali identifikovať podľa hodnotenia rizík uvedeného v požiadavke 6.1.* | |  Kontrola pravidiel a postupov   Preskúmanie systémových komponentov   Porovnanie zoznamu inštalovaných bezpečnostných záplat so zoznamom vydaných záplat od dodávateľa |  |  |  |  |  |
| 6.3 | (a) Sú procesy vývoja softvéru založené na priemyselných normách a/alebo osvedčených postupoch? | |  Kontrola procesu vývoja softvéru   Kontrola procesov   Rozhovor s personálom |  |  |  |  |  |
| (b) Je zabezpečená informačná bezpečnosť počas celého životného cyklu vývoja softvéru? | |  Kontrola procesu vývoja softvéru   Kontrola procesov   Rozhovor s personálom |  |  |  |  |  |
| (c) Sú softvérové aplikácie vyvíjané v súlade s PCI DSS (napríklad, bezpečná autentifikácia a protokolovanie)? | |  Kontrola procesu vývoja softvéru   Kontrola procesov   Rozhovor s personálom |  |  |  |  |  |
| (d) Je vývoj softvéru v súlade s požiadavkami 6.3.1 - 6.3.2: | |  |  |  |  |  |  |
| 6.3.1 | Je potrebné, aby vývoj, skúšky a/alebo účty k vlastným aplikáciám, užívateľské mená a heslá boli zmazané pred uvedením aplikácie na trh? | |  Kontrola procesu vývoja softvéru   Rozhovor s personálom |  |  |  |  |  |
| 6.3.2 | Sú všetky vlastné kódy kontrolované pred vydaním do výroby alebo zákazníkom, aby sa zistila akákoľvek možná zraniteľnosť (buď manuálnymi alebo automatizovanými procesmi:   Sú zmeny kódov kontrolované inými zamestnancami, než je autor ich zmien a zamestnancami, ktorí sú oboznámení s technikami preskúmavania kódu a bezpečnostnými kódovacími postupmi?   Zabezpečuje kontrolu kódov to, aby boli kódy vyvíjané v zmysle bezpečnostných kódovacích pokynov?   Sú pred vydaním vykonávané príslušné opravy?   Sú výsledky z kontroly kódov schválené manažmentom pred vydaním?  ***Poznámka:*** *Táto požiadavka na kontrolu kódov sa vzťahuje na všetky vlastné kódy (interné a orientované na verejnosť), ktoré sú súčasťou životného cyklu vývoja systému. Kontroly kódov môžu byť vykonávané kvalifikovanými internými zamestnancami alebo tretími stranami. Webové aplikácie orientované na verejnosť takisto podliehajú dodatočným kontrolám, na odhaľenie možných hrozieb a zraniteľností po implementácii tak, ako je stanovené v požiadavke 6.6 PCI DSS.* | |  Kontrola pravidiel a postupov   Rozhovor s personálom   Kontrola nedávnych zmien a záznamov o zmenách |  |  |  |  |  |
| 6.4 | Sú procesy a postupy kontroly zmien dodržiavané pre všetky systémové komponenty tak, aby zahŕňali nasledovné: | |  |  |  |  |  |  |
| 6.4.1 | (a) Sú vývojové / testovacie prostredia oddelené od výrobného prostredia? | |  Kontrola procesov a postupov kontroly zmien   Preskúmanie dokumentácie siete a konfigurácií sieťového zariadenia |  |  |  |  |  |
|  | (b) Je zavedená kontrola prístupu na podporu oddeľovania vývojového/testovacie prostredia od výrobného prostredia? | |  Kontrola procesov a postupov kontroly zmien   Kontrola nastavení riadenia prístupu |  |  |  |  |  |
| 6.4.2 | Rozlišuje sa medzi povinnosťami zamestnancov priradených vo vývojovom/testovacom prostredí a tých, ktorí boli priradený do výrobného prostredia? | |  Kontrola procesov a postupov kontroly zmien   Kontrola procesov   Rozhovor s personálom |  |  |  |  |  |
| 6.4.3 | Sú výrobné dáta (živé PAN) ***nepoužívané*** na testovanie alebo vývoj? | |  Kontrola procesov a postupov kontroly zmien   Kontrola procesov   Rozhovor s personálom   Kontrola údajov z testov |  |  |  |  |  |
| 6.4.4 | Sú údaje z testov a účty odstraňované zo systému pred aktiváciou systému / uvedením systému do výroby? | |  Kontrola procesov a postupov kontroly zmien   Kontrola procesov   Rozhovor s personálom   Preskúmanie výrobných systémov |  |  |  |  |  |
| 6.4.5 | (a) Sú postupy kontroly zmien zdokumentované a vyžadujú nasledovné?   Zdokumentovanie dopadov   Zdokumentované schválenie kontroly zmeny oprávnenými stranami   Testovanie funkčnosti na overenie, že zmena nemala negatívny dopad na bezpečnosť systému   Spätné postupy | |  Kontrola procesov a postupov kontroly zmien |  |  |  |  |  |
| (b) Sú nasledujúce činnosti vykonávané a zdokumentované pre každú zmenu: | |  |  |  |  |  |  |
| 6.4.5.1 | Zdokumentovanie dopadov? | |  Sledovanie zmien na dokumentáciu kontroly zmeny   Kontrola dokumentácie kontroly zmeny |  |  |  |  |  |
| 6.4.5.2 | Zdokumentované schválenie oprávnenými stranami? | |  Sledovanie zmien na dokumentáciu kontroly zmeny   Kontrola dokumentácie kontroly zmeny |  |  |  |  |  |
| 6.4.5.3 | Testovanie funkčnosti na overenie, že zmena nemala negatívny dopad na bezpečnosť systému? | |  Sledovanie zmien na dokumentáciu kontroly zmeny   Kontrola dokumentácie kontroly zmeny |  |  |  |  |  |
| (b) Pre zmeny vlastného kódu, sú aktualizácie testované na potvrdenie súladu s požiadavkou 6.5 PCI DSS pred nasadením do výroby? | |  Sledovanie zmien na dokumentáciu kontroly zmeny   Kontrola dokumentácie kontroly zmeny |  |  |  |  |  |
| 6.4.5.4 | Spätné postupy? | |  Sledovanie zmien na dokumentáciu kontroly zmeny   Kontrola dokumentácie kontroly zmeny |  |  |  |  |  |
| 6.4.6 | Po dokončení významnej zmeny, sú všetky súvisiace požiadavky PCI DSS implementované na všetky nové alebo zmenené systémy a siete a je dokumentácia aktualizovaná, v prípade potreby?  ***Poznámka:*** *Táto požiadavka patrí medzi osvedčené postupy až do 31. januára 2018, odkedy sa stáva požiadavkou.* | |  Sledovanie zmien na dokumentáciu kontroly zmeny   Kontrola dokumentácie kontroly zmeny   Rozhovor s personálom   Kontrola dotknutých systémov a sietí |  |  |  |  |  |
| 6.5 | (a) Adresujú softvérové vývojové procesy spoločné zraniteľnosti kódovania? | |  Kontrola pravidiel a postupov vývoja softvéru |  |  |  |  |  |
|  | (b) Prechádzajú vývojári najmenej ročne školením na najnovšie bezpečnostné kódovacie techniky, vrátane spôsobov na minimalizáciu bežných kódovacích chýb? | |  Kontrola pravidiel a postupov vývoja softvéru   Kontrola záznamov zo školení |  |  |  |  |  |
|  | (c) Sú vyvíjané aplikácie založené na bezpečných kódovacích pokynoch na ochranu aplikácií aspoň pred týmito zraniteľnosťami:  ***Poznámka:*** *Zraniteľnosti uvedené v 6.5.1 až 6.5.10 boli aktuálne a patrli medzi osvedčené postupy v čase vydania tejto verzie PCI DSS. Avšak, osvedčené postupy sú pravidelne aktualizované (napríklad: príručka OWASP, SANS CWE Top 25, Bezpečné programovanie CERT Secure Coding, atď.), a teda je nutné vychádzať z aktuálnych osvedčených postupov.* | |  |  |  |  |  |  |
| 6.5.1 | Adresujú spôsoby kódovania možné chyby týkajúce sa tzv. *injection*, a to predovšetkým SQL *injection*?  ***Poznámka:*** *Takisto, okrem iných, berte do úvahy aj injection chyby v OS Command, LDAP a XPath.* | |  Kontrola pravidiel a postupov vývoja softvéru   Rozhovor so zodpovedným personálom |  |  |  |  |  |
| 6.5.2 | Riešia postupy kódovania zraniteľnosti pretečenia vyrovnávajúcej pamäte? | |  Kontrola pravidiel a postupov vývoja softvéru   Rozhovor so zodpovedným personálom |  |  |  |  |  |
| 6.5.3 | Riešia postupy kódovania nezabezpečené šifrovacie pamäte? | |  Kontrola pravidiel a postupov vývoja softvéru   Rozhovor so zodpovedným personálom |  |  |  |  |  |
| 6.5.4 | Riešia postupy kódovania nezabezpečené komunikácie? | |  Kontrola pravidiel a postupov vývoja softvéru   Rozhovor so zodpovedným personálom |  |  |  |  |  |
| 6.5.5 | Riešia postupy kódovania nesprávne spracovanie chýb? | |  Kontrola pravidiel a postupov vývoja softvéru   Rozhovor so zodpovedným personálom |  |  |  |  |  |
| 6.5.6 | Riešia postupy kódovania vysokorizikové zraniteľnosti stanovené v postupe stanovenia zraniteľností (ako je uvedené v požiadavke 6.1 PCI DSS)? | |  Kontrola pravidiel a postupov vývoja softvéru   Rozhovor so zodpovedným personálom |  |  |  |  |  |
| Pre webové aplikácie a aplikačné rozhrania (interné alebo externé), sú aplikácie vyvíjané na základe bezpečnostných kódovacích pokynov na ochranu aplikácií pred nasledujúcimi zraniteľnosťami: | | | |  |  |  |  |  |
| 6.5.7 | | Riešia postupy kódovania útoky XSS? |  Kontrola pravidiel a postupov vývoja softvéru   Rozhovor so zodpovedným personálom |  |  |  |  |  |
| 6.5.8 | | Riešia postupy kódovania nesprávne riadenie prístupu, ako sú nezabezpečené priame odkazy na objekty, neobmedzenie URL prístupu, prienik do adresárov (directory traversal) a neobmedzenie užívateľského prístupu k funkciám? |  Kontrola pravidiel a postupov vývoja softvéru   Rozhovor so zodpovedným personálom |  |  |  |  |  |
| 6.5.9 | | Riešia postupy kódovania útoky CSRF? |  Kontrola pravidiel a postupov vývoja softvéru   Rozhovor so zodpovedným personálom |  |  |  |  |  |
| 6.5.10 | | Riešia postupy kódovania narušené autentifikačné a prihlasovacie riadenie? |  Kontrola pravidiel a postupov vývoja softvéru   Rozhovor so zodpovedným personálom |  |  |  |  |  |
| 6.6 | | Pre webové aplikácie orientované na verejnosť, sú nové hrozby a zraniteľnosti neustále riešené a sú tieto aplikácie chránené voči známym útokom použitím jednej z nasledujúcich metód?   Kontrola webových aplikácií orientovaných na verejnosť prostredníctvom manuálnych alebo automatizovaných hodnotiacich nástrojov alebo metód zraniteľností aplikácii alebo, a to nasledovne:  - Najmenej raz ročne  - Po každej zmene  - Zo strany organizácie, ktorá sa špecializuje na bezpečnosť aplikácií  - Zohľadnenie v hodnotení minimálne tých zraniteľností, ktoré sú uvedené v požiadavke 6.5  - Všetky zraniteľnosti opravené  - Opätovné hodnotenie aplikácie po hodnotení  ***Poznámka:*** *Toto hodnotenie nie je totožné so skenovaním zraniteľností v zmysle požiadavky 11.2.*  – **ALEBO** –   Inštalácia automatizovaných technických riešení na odhaľovanie a zabraňovanie webových útokov (napríklad, brána firewall pre webové aplikácie), a to nasledovne:  - Umiestnené pred verejne orientovanými webovými aplikáciami na odhaľovanie a zabraňovanie webových útokov.  - Aktívne a aktualizované, v prípade potreby.  - Vytváranie protokolov z auditu.  - Konfigurácia, ktorá blokuje webové útoky alebo vydáva upozornenia, ktoré sú okamžite preskúmané. |  Kontrola zdokumentovaného procesu   Rozhovor s personálom   Kontrola záznamov o hodnotení bezpečnosti aplikácie   Preskúmanie systémových konfiguračných nastavení |  |  |  |  |  |
| 6.7 | | Sú bezpečnostné politiky a prevádzkové postupy na vývoj a udržiavanie bezpečnostných systémov a aplikácií:   Zdokumentované   Používané   Oznámené dotknutým stranám? |  Kontrola bezpečnostných pravidiel a operačných postupov   Rozhovor s personálom |  |  |  |  |  |

**Implementácia prísnych opatrení na kontrolu prístupu**

***Požiadavka 7:*** ***Obmedzenie prístupu k údajom držiteľa karty v nevyhnutnom rozsahu***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Otázka PCI DSS** | | **Očakávané testovanie** | **Odpoveď**  ***(Zaškrtnite jednu odpoveď pre každú otázku)*** | | | | |
| **Áno** | **Áno s CCW** | **Nie** | **N/A** | **Netestované** |
| 7.1 | Je prístup k systémovým komponentom a údajom držiteľov kariet obmedzený len na tých oprávnených zamestnancov, a to nasledovne: |  |  |  |  |  |  |
|  |  Existujú písomné pravidlá riadenia prístupu, ktorý zahŕňa nasledovné?   Stanovenie prístupových potrieb a priradenie privilégií pre každú funkciu   Obmedzenie prístupu k privilegovaným užívateľským ID len v nevyhnutnom rozsahu,   Priradenie prístupu na základe klasifikácie a funkcie jednotlivých zamestnancov   Zdokumentované schválenie (elektronické alebo písomné) oprávnenými stranami, vrátane zoznamu špecifických schválených privilégií |  Kontrola písomných pravidiel riadenia prístupu |  |  |  |  |  |
| 7.1.1 | Sú prístupové potreby zadefinované pre každú funkciu, vrátane:   systémových komponentov a dátových zdrojov, ktoré každá úloha potrebuje na prístup v rámci svojej pracovnej funkcie?   požadovanej úrovne privilégií (napríklad používateľ, administrátor, atď.) potrebnej k rôznym typom prístupov? |  Kontrola úloh a prístupových potrieb |  |  |  |  |  |
| 7.1.2 | Je prístup k privilegovaným užívateľským ID obmedzeným nasledovne:   Najmenší potrebný rozsah na vykonávanie svojej pracovnej funkcie?   Priradený len na úlohy, ktoré špecificky vyžadujú privilegovaný prístup? |  Rozhovor s personálom   Rozhovor s manažmentom   Kontrola privilegovaných užívateľských ID |  |  |  |  |  |
| 7.1.3 | Priradenie prístupu na základe klasifikácie a funkcie jednotlivých zamestnancov? |  Rozhovor s manažmentom   Kontrola užívateľských ID |  |  |  |  |  |
| 7.1.4 | Je požadované zdokumentované schválenie autorizovanými stranami, stanovujúce požadované privilégia? |  Kontrola užívateľských ID   Porovnanie so zdokumentovanými schváleniami   Porovnanie priradených privilégií so zdokumentovanými schváleniami |  |  |  |  |  |
| 7.2 | Je zavedený systém riadenia prístupu pre systémové komponenty na obmedzenie prístupu na základe toho, čo užívateľ potrebuje vedieť a je nastavený tak, aby „blokoval všetko", pokiaľ to nie je výslovne povolené, a to nasledovne: |  |  |  |  |  |  |
| 7.2.1 | Je zavedený systém riadenia prístupu pre všetky systémové komponenty? |  Kontrola dokumentácie dodávateľa   Preskúmanie konfiguračných nastavení |  |  |  |  |  |
| 7.2.2 | Je systém riadenia prístupu nastavený tak, aby podporoval privilégia priradené jednotlivcom na základe pracovnej klasifikácie a funkcie? |  Kontrola dokumentácie dodávateľa   Preskúmanie konfiguračných nastavení |  |  |  |  |  |
| 7.2.3 | Má systém riadenia prístupu predvolené nastavenie „deny-all"? |  Kontrola dokumentácie dodávateľa   Preskúmanie konfiguračných nastavení |  |  |  |  |  |
| 7.3 | Sú bezpečnostné pravidlá a prevádzkové postupy na obmedzovanie prístupu k údajom držiteľov kariet:   Zdokumentované   Používané   Oznámené dotknutým stranám? |  Kontrola bezpečnostných pravidiel a prevádzkových postupov   Rozhovor s personálom |  |  |  |  |  |

***Požiadavka 8:*** ***Identifikácia a autentifikácia prístupu k systémovým komponentom***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Otázka PCI DSS** | | **Očakávané testovanie** | **Odpoveď**  ***(Zaškrtnite jednu odpoveď pre každú otázku)*** | | | | |
| **Áno** | **Áno s CCW** | **Nie** | **N/A** | **Netestované** |
| 8.1 | Sú pravidlá a postupy na kontrolu riadenia identifikácie užívateľa zadefinované a zavedené pre užívateľov a administrátorov, ktorí nie sú zákazníkmi, a to pre všetky systémové komponenty nasledovne: |  |  |  |  |  |  |
| 8.1.1 | Je všetkým užívateľom priradené jedinečné ID, kým získajú prístup k systémovým komponentom alebo údajom držiteľov kariet? |  Kontrola postupov pre užívateľské heslá   Rozhovor s personálom |  |  |  |  |  |
| 8.1.2 | Je upravovanie, mazanie alebo dopĺňanie užívateľských ID, identifikátorov alebo iných informácií riadené tak, aby boli užívateľské ID implementované tak, ako sú autorizované (vrátane špecifických privilégií)? |  Kontrola postupov pre užívateľské heslá   Kontrola privilegovaných a všeobecných užívateľských ID a súvisiacich oprávnení   Kontrola systémových nastavení |  |  |  |  |  |
| 8.1.3 | Je prístup pre všetkých zrušených užívateľov okamžite deaktivovaný alebo odstránený? |  Kontrola postupov pre užívateľské heslá   Kontrola zrušených užívateľských účtov   Preskúmanie aktuálnych prístupových zoznamov   Kontrola vrátených fyzických autentifikačných zariadení |  |  |  |  |  |
| 8.1.4 | Sú neaktívni užívatelia odstránení alebo zakázaní do 90 dní? |  Kontrola postupov pre užívateľské heslá   Kontrola užívateľských účtov |  |  |  |  |  |
| 8.1.5 | (a) Sú účty používané tretími stranami na prístup, podporu alebo údržbu systémových komponentov prostredníctvom vzdialeného prístupu povolené len počas potrebnej doby a inokedy vypínané, keď nie sú potrebné? |  Kontrola postupov pre užívateľské heslá   Rozhovor s personálom   Kontrola procesov |  |  |  |  |  |
| (b) Sú účty tretích strán so vzdialeným prístupom sledované počas ich používania? |  Rozhovor s personálom   Kontrola procesov |  |  |  |  |  |
| 8.1.6 | (a) Sú opakované pokusy o prístup obmedzené zablokovaním užívateľského ID po maximálne šiestich pokusoch? |  Kontrola postupov pre užívateľské heslá   Preskúmanie systémových konfiguračných nastavení |  |  |  |  |  |
| (b) *Tento postup testovania sa týka len poskytovateľov služieb.* |  |  |  |  |  |  |
| 8.1.7 | Po zablokovaní užívateľa je táto doba nastavená minimálne na 30 minút alebo kým administátor nepovolí ID užívateľa? |  Kontrola postupov pre užívateľské heslá   Preskúmanie systémových konfiguračných nastavení |  |  |  |  |  |
| 8.1.8 | V prípade, že je prihlásenie nečinné dlhšie ako 15 minút, je nutné, aby sa užívateľ znovu prihlásil (napríklad zadaním hesla) na opätovnú aktiváciu terminálu alebo služby? |  Kontrola postupov pre užívateľské heslá   Preskúmanie systémových konfiguračných nastavení |  |  |  |  |  |
| 8.2 | Okrem priradenia jedinečného ID, využíva sa jedna alebo viacero nasledujúcich služieb na autentifikáciu užívateľov?   Niečo, čo poznáte, heslo alebo prístupová fráza   Niečo, čo máte, tokenové zariadenie alebo čipovú kartu   Niečo, čo ste, napríklad biometrika |  Kontrola postupov pre užívateľské heslá   Kontrola postupu autentifikácie |  |  |  |  |  |
| 8.2.1 | (a) Používa sa silné šifrovanie na maskovanie všetkých autentifikačných údajov počas prenosu a uskladnenia vo všetkých systémových komponentoch? |  Kontrola postupov pre užívateľské heslá   Kontrola dokumentácie dodávateľa   Preskúmanie systémových konfiguračných nastavení   Kontrola súborov s heslami   Kontrola prenosov dát |  |  |  |  |  |
| (b) *Tento postup testovania sa týka len poskytovateľov služieb.* |  |  |  |  |  |  |
| 8.2.2 | Je užívateľ overený pred možnou úpravou svojich údajov (napríklad pri resetovaní hesla, poskytovaní nových tokenov alebo vytváraní nových kľúčov)? |  Kontrola autentifikačných postupov   Kontrola personálu |  |  |  |  |  |
| 8.2.3 | (a) Sú užívateľské heslá obmedzené nasledovným spôsobom?   Heslo musí mať najmenej sedem znakov   Musí obsahovať ako číselné tak aj abecedné znaky  Prípadne heslá/prístupové frázy musia mať minimálnu komplexitu a pevnosť rovnocennú s parametrami uvedenými vyššie. |  Preskúmanie systémových nastavení na overovanie parametrov hesiel |  |  |  |  |  |
| (b) *Tento postup testovania sa týka len poskytovateľov služieb.* |  |  |  |  |  |  |
| 8.2.4 | (a) Sú heslá/prihlasovacie frázy menené aspoň raz za každých 90 dní? |  Kontrola postupov pre užívateľské heslá   Preskúmanie systémových konfiguračných nastavení |  |  |  |  |  |
| (b) *Tento postup testovania sa týka len poskytovateľov služieb.* |  |  |  |  |  |  |
| 8.2.5 | (a) Musí každý užívateľ zaslať nové heslo/prístupovú frázu odlišnú od jeho posledných štyroch hesiel/fráz? |  Kontrola postupov pre užívateľské heslá   Preskúmanie vzorky systémových komponentov   Preskúmanie systémových konfiguračných nastavení |  |  |  |  |  |
| (b) *Tento postup testovania sa týka len poskytovateľov služieb.* |  |  |  |  |  |  |
| 8.2.6 | Sú heslá/prístupové frázy nastavené na jedinečnú hodnotu pre každého užívateľa a po resete musí každý užívateľ zmeniť svoje heslo ihneď po prvom použití? |  Kontrola postupov pre užívateľské heslá   Preskúmanie systémových konfiguračných nastavení   Kontrola bezpečnostného personálu |  |  |  |  |  |
| 8.3 | Sú všetky prístupy bez konzoly a každý vzdialený prístup k CDE zabezpečovaný prostredníctvom viacúrovňovej autentifikácie, a to nasledovne:  ***Poznámka:*** *Viacúrovňová autentifikácia vyžaduje, aby boli použité najmenej dve z troch autentifikačných metód (pozri požiadavku 8.2 PCI DSS pre popis autentifikačných metód) počas autentifikácie. Použitie jedného faktora dvakrát (napríklad dve samostatné heslá) nie je považované za viacúrovňovú autentifikáciu.* |  | | | | | |
| 8.3.1 | Je viacúrovňová autentifikácia zahrnutá vo všetkých prístupoch bez konzoly do CDE pre zamestnancov s administratívnym prístupom?  ***Poznámka:*** *Táto požiadavka patrí medzi osvedčené postupy až do 31. januára 2018, odkedy sa stáva požiadavkou.* |  Preskúmanie systémových konfigurácií   Kontrola prihlasovania administrátora do CDE |  |  |  |  |  |
| 8.3.2 | Je viacúrovňová autentifikácia zahrnutá vo všetkých vzdialených prístupoch (užívateľa a administrátora, vrátane prístupu tretích strán na podporu alebo údržbu) pochádzajúcich mimo siete subjektu? |  Preskúmanie systémových konfigurácií   Kontrola vzdialeného pripojovania zamestnancami |  |  |  |  |  |
| 8.4 | (a) Sú autentifikačné pravidlá a postupy zdokumentované a oznámené všetkým užívateľom? |  Kontrola pravidiel a postupov   Kontrola distribučnej metódy   Rozhovor s personálom   Rozhovor s užívateľmi |  |  |  |  |  |
| (b) Obsahujú autentifikačné postupy a pravidlá nasledovné?   Pokyny na výber silných prihlasovacích údajov   Pokyny pre užívateľov na ochranu svojich prihlasovacích údajov   Pokyny na opätovné použitie predtým používaných hesiel   Pokyny pre užívateľov na zmenu svojich hesiel, ak existuje podozrenie, že ich heslo môže byť ohrozené |  Kontrola pravidiel a postupov   Kontrola dokumentácie poskytnutej užívateľom |  |  |  |  |  |
| 8.5 | Akékoľvek skupinové, zdieľané alebo generické účty, heslá a iné autentifikačné metódy sú zakázané nasledovne:   Generické užívateľské ID a účty sú zablokované alebo odstránené,   Zdieľané užívateľské ID pre činnosti správy systému a iné kritické funkcie nie sú zavedené a   Zdieľané a generické užívateľské ID nie sú používané na správu systémových komponentov? |  Kontrola pravidiel a postupov   Kontrola zoznamov užívateľských ID   Rozhovor s personálom |  |  |  |  |  |
| 8.5.1 | *Táto požiadavka sa vzťahuje výlučne na poskytovateľov služieb.* |  |  |  |  |  |  |
| 8.6 | Pri používaní iných autentifikačných mechanizmov (napríklad fyzické alebo logické bezpečnostné tokeny, čipové karty a certifikáty, atď.), je použitie takýchto mechanizmov nasledovné:   Autentifikačné mechanizmy musia byť priradené k jednotlivým účtom a nesmú byť zdieľané viacerými účtami   Fyzické a/alebo logické kontrolné prvky musia mať zavedené kontroly na to, aby mohol daný účet využívať tieto mechanizmy na získanie prístupu |  Kontrola pravidiel a postupov   Rozhovor s personálom   Preskúmanie systémových konfiguračných nastavení a/alebo fyzických kontrolných prvkov |  |  |  |  |  |
| 8.7 | Je prístup ku každej databáze obsahujúcej údaje držiteľov kariet (vrátane prístupu aplikácií, správcov a iných užívateľov) obmedzený nasledovne: |  |  |  |  |  |  |
| (a) Je každý prístup užívateľa, užívateľské vyhľadávania a užívateľské akcie (napríklad presúvanie, kopírovanie, mazanie) v databáze vykonávané výhradne prostredníctvom programových metód (napríklad prostredníctvom uložených procedúr)? |  Kontrola pravidiel a postupov databázovej autentifikácie   Preskúmanie konfiguračných nastavení databázy a aplikácie |  |  |  |  |  |
|  | (b) Je prístup alebo vyhľadávanie užívateľa v databáze obmedzený len na databázových správcov? |  Kontrola pravidiel a postupov databázovej autentifikácie   Kontrola nastavení riadenia prístupu do databázy   Preskúmanie konfiguračných nastavení databázovej aplikácie |  |  |  |  |  |
| (c) Sú ID aplikácie použiteľné len aplikáciami (a nie individuálnymi užívateľmi alebo inými procesmi)? |  Kontrola pravidiel a postupov databázovej autentifikácie   Kontrola nastavení riadenia prístupu do databázy   Preskúmanie konfiguračných nastavení databázovej aplikácie |  |  |  |  |  |
| 8.8 | Sú bezpečnostné pravidlá a operačné postupy na identifikáciu a autentifikáciu:   Zdokumentované   Používané   Oznámené dotknutým stranám? |  Kontrola bezpečnostných pravidiel a prevádzkových postupov   Rozhovor s personálom |  |  |  |  |  |

***Požiadavka 9:*** ***Obmedzenie fyzického prístupu k údajom držiteľa karty***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Otázka PCI DSS** | | **Očakávané testovanie** | **Odpoveď**  ***(Zaškrtnite jednu odpoveď pre každú otázku)*** | | | | |
| **Áno** | **Áno s CCW** | **Nie** | **N/A** | **Netestované** |
| 9.1 | Existujú vhodné vstupné kontrolné prvky k zariadeniam na obmedzenie a sledovanie fyzického prístupu k systémom v dátovom prostredí držiteľa karty? |  Kontrola fyzických prístupových kontrolných prvkov   Kontrola personálu |  |  |  |  |  |
| 9.1.1 | (a) Sú využívané videokamery alebo mechanizmy kontroly prístupu (alebo oboje) na monitorovanie individuálneho fyzického prístupu k citlivým oblastiam?  ***Poznámka:*** *„Citlivé oblasti" označujú akékoľvek dátové centrum, serverovú miestnosť alebo akúkoľvek oblasť, v ktorej sú umiestnené systémy na uchovávanie, spracovanie alebo prenášanie údajov držiteľa karty. Toto nezahŕňa miestnosti orientované na verejnosť, kde sú v mieste predaja prítomné len platobné terminály, ako sú napríklad pokladničné priestory v maloobchodnej predajni.* |  Kontrola pravidiel a postupov   Kontrola fyzických monitorovacích mechanizmov   Kontrola bezpečnostných prvkov |  |  |  |  |  |
| (b) Sú videokamery alebo mechanizmy kontroly prístupu (alebo oboje) chránené voči neoprávnenému zásahu alebo zablokovaniu? |  Kontrola procesov   Rozhovor s personálom |  |  |  |  |  |
| (c) Sú údaje zhromaždené z videokamier a/alebo mechanizmov kontroly prístupu kontrolované a porovnávané s inými údajmi? |  Kontrola pravidiel a postupov   Rozhovor s bezpečnostným personálom |  |  |  |  |  |
| (d) Sú údaje zhromažďované z videokamier a/alebo mechanizmov kontroly prístupu ukladané po dobu najmenej troch mesiacov, ak zákon neustanovuje inak? |  Kontrola procesov na uchovávanie údajov   Kontrola skladovania dát   Rozhovor s bezpečnostným personálom |  |  |  |  |  |
| 9.1.2 | Sú zavedené fyzické a/alebo logické kontrolné prvky na obmedzenie prístupu k verejne prístupným sieťovým konektorom?  *Napríklad, sieťové konektory umiestnené vo verejných priestoroch a priestoroch prístupných pre návštevníkov môžu byť zablokované, pričom prístup k nim je možné odblokovať výslovne po autorizácii prístupových údajov. Prípadne môžu byť zavedené procesy, ktoré zabezpečia, aby boli návštevníci sprevádzaní zamestnancom vo všetkých priestoroch s aktívnymi sieťovými konektormi.* |  Kontrola pravidiel a postupov   Rozhovor s personálom   Kontrola lokácií |  |  |  |  |  |
| 9.1.3 | Je fyzický prístup k bezdrôtovým prístupovým miestam, bránam, prenosným zariadeniam, sieťovým / komunikačným hardvérom a telekomunikačným linkám obmedzený? |  Kontrola pravidiel a postupov   Rozhovor s personálom   Kontrola zariadení |  |  |  |  |  |
| 9.2 | (a) Boli vyvinuté postupy, ktoré dokážu jednoducho rozlišovať medzi zamestnancom daného pracoviska a návštevníkom, a to nasledovne:   Identifikácia zamestnancov pracoviska a návštevníkov (napríklad prideľovanie odznakov)   Zmena prístupových požiadaviek a   Zrušenie prístupu pre prepustených zamestnancov a návštevníkov, ktorým vypršala platnosť prístupu (ako sú ID odznaky)  *Na účely požiadavky 9 sú „zamestnanci pracoviska" zamestnanci na plný úväzok alebo čiastočný úväzok, dodávatelia a konzultanti, ktorí sú fyzicky prítomní v priestoroch subjektu. „Návštevník" je dodávateľ, návštevník alebo hosť zamestnancov pracoviska, servisní pracovníci alebo ktokoľvek, kto potrebuje na krátku dobu vstúpiť na pracovisko, obyvkle na dobu nie dlhšie ako jeden deň.* |  Kontrola pravidiel a postupov   Rozhovor s personálom   Kontrola metód identifikácie (napr. odznaky)   Kontrola postupu riadenia návštevníkov |  |  |  |  |  |
| (b) Obsahujú metódy identifikácie (napr. odznaky) jasné rozlišovanie návštevníkov od zamestnancov? |  Kontrola metód identifikácie |  |  |  |  |  |
| (c) Má prístup k systému odznakov len autorizovaný personál? |  Preskúmanie fyzických kontrolných a prístupových prvkov systému odznaku |  |  |  |  |  |
| 9.3 | Je fyzický prístup k citlivým oblastiam kontrolovanými zamestnancami pracoviska, a to nasledovne:   Je udeľovaný prístup na základe individuálnych pracovných funkcií?   Je prístup ihneď zrušený po skončení zamestnaneckého pomeru   Sú po skončení zamestnaneckého pomeru odobraté / deaktivované všetky prístupové fyzické mechanizmy, napr. kľúče, prístupové karty, atď? |  Rozhovor s personálom   Kontrola zoznamov prístupových kontrolných prvkov   Kontrola zamestnancov pracoviska   Porovnanie zoznamov bývalých zamestnancov so zoznamami prístupových kontrolných prvkov |  |  |  |  |  |
| 9.4 | Dochádza k identifikácii a spracovaniu prístupu nasledovným spôsobom: |  |  |  |  |  |  |
| 9.4.1 | Dochádza k autorizácií návštevníka pred vstupom a je sprevádzaný zamestnancom počas celej doby a vo všetkých priestoroch, kde dochádza k spracovaniu alebo skladovaniu údajov držiteľov kariet? |  Kontrola pravidiel a postupov   Kontrola procesov riadenia návštevníkov, vrátane riadenia prístupov   Rozhovor s personálom   Kontrola návštevníkov a používanie odznakov |  |  |  |  |  |
| 9.4.2 | (a) Dostanú návštevníci odznaky alebo iné identifikačné znaky, ktoré ich zreteľne odlišujú od zamestnancov pracoviska? |  Kontrola používania odznakov zamestnancami a návštevníkmi   Preskúmanie identifikácie |  |  |  |  |  |
| (b) Dochádza k zrušeniu platnosti odznakov/inej identifikácie návštevníkov? |  Kontrola procesu   Preskúmanie identifikácie |  |  |  |  |  |
| 9.4.3 | Sú návštevníci vyzvaní, aby odovzdali svoj odznak alebo inú identifikáciu pri odchode zo zariadenia alebo po dátume vypršania jej platnosti? |  Kontrola procesov   Kontrola procesu odchodu návštevníkov zo zariadenia |  |  |  |  |  |
| 9.4.4 | (a) Používajú sa záznamy o návštevníkoch na zaznamenávanie fyzického prístupu osôb do zariadenia, rovnako ako aj počítačových miestností a iných dátových centier, kde sa uskladňujú alebo prenášajú údaje držiteľov kariet? |  Kontrola pravidiel a postupov   Kontrola záznamov o návštevníkoch   Kontrola postupu riadenia návštevníkov   Preskúmanie procesu uchovávania záznamov |  |  |  |  |  |
| (b) Obsahujú záznamy o návštevníkoch meno návštevníka, spoločnosť, ktorú zastupuje a meno zamestnanca pracoviska, ktorý udelil prístup danému návštevníkovi? |  Kontrola pravidiel a postupov   Kontrola záznamov o návštevníkoch |  |  |  |  |  |
|  | (c) Sú záznamy o návštevníkoch uchovávané najmenej po dobu troch mesiacov? |  Kontrola pravidiel a postupov   Preskúmanie procesu uchovávania záznamov o návštevníkoch |  |  |  |  |  |
| 9.5 | Sú všetky médiá fyzicky zabezpečené (vrátane, ale nielen, počítačov, vymeniteľných elektronických médií, písomných dokladov, písomných správ a faxov)?  *Na účely požiadavky 9 „médiá" znamenajú písomné a elektronické média obsahujúce údaje držiteľov kariet.* |  Preskúmanie pravidiel a postupov fyzického zabezpečovania médií   Rozhovor s personálom |  |  |  |  |  |
| 9.5.1 | Prechádza miesto, kde sa uchovávajú zálohy médií, pravidelnou kontrolou najmenej raz ročne na overenie bezpečnosti skladovania? |  Preskúmanie pravidiel a postupov overovania bezpečnosti priestorov, kde sa skladujú médiá   Rozhovor s bezpečnostným personálom |  |  |  |  |  |
| 9.6 | (a) Je udržiavaná prísna kontrola nad internou alebo externou distribúciou akéhokoľvek média? |  Preskúmanie pravidiel a postupov distribúcie médií |  |  |  |  |  |
| (b) Obsahujú kontroly nasledovné prvky: |  |  |  |  |  |  |
| 9.6.1 | Je médium klasifikované podľa citlivosti svojich údajov? |  Preskúmanie pravidiel a postupov klasifikácie médií   Rozhovor s bezpečnostným personálom |  |  |  |  |  |
| 9.6.2 | Sú média zasielané bezpečnou kuriérskou službou alebo iným spôsobom doručenia, ktorý je možné presne sledovať? |  Rozhovor s personálom   Kontrola sledovacích protokolov a dokumentácie distribúcie médií |  |  |  |  |  |
| 9.6.3 | Dochádza k schvaľovaniu prenosu médií zo strany manažmentu (predovšetkým, ak sú médiá distribuované jednotlivcom)? |  Rozhovor s personálom   Kontrola sledovacích protokolov a dokumentácie distribúcie médií |  |  |  |  |  |
| 9.7 | Je zachovaná prísna kontrola sledovania a dostupnosti médií? |  Kontrola pravidiel a postupov |  |  |  |  |  |
| 9.7.1 | (a) Je riadne vedený inventár všetkých médií? |  Kontrola inventáru |  |  |  |  |  |
|  | (b) Dochádza k pravidelnej inventarizácií najmenej raz ročne? |  Kontrola inventáru   Rozhovor s personálom |  |  |  |  |  |
| 9.8 | (a) Dochádza k zničeniu médií, keď už nie sú potrebné z obchodných alebo právnych dôvodov? |  Kontrola pravidiel a postupov týkajúcich sa pravidelných likvidácií nepotrebných médií |  |  |  |  |  |
|  | (b) Je zavedená politika likvidácie nepotrebných médií, ktorá stanovuje nasledovné požiadavky?   Vytlačené písomné kópie musia byť rozrezané, spálené alebo rozdrvené tak, aby nebolo možné tieto písomné kópie žiadnym spôsobom rekonštruovať.   Skladové kontajnery daných materiálov musia byť zabezpečené proti neoprávnenému prístupu.   Údaje držiteľa karty uložené na elektronickom médiu musia byť neobnoviteľne vymazané (napr. prostredníctvom programu na vyčistenie disku v zmysle osvedčených postupoch v oblasti bezpečného mazania alebo pomocou fyzického zničenia média). |  Kontrola pravidiel a postupov týkajúcich sa pravidelných likvidácií nepotrebných médií |  |  |  |  |  |
|  | (c) Likvidácia médií prebieha nasledovne: |  |  |  |  |  |  |
| 9.8.1 | (a) Sú písomné materiály rozrezané, spálené alebo rozdrvené tak, aby nebolo možné tieto písomné kópie žiadnym spôsobom rekonštruovať? |  Rozhovor s personálom   Preskúmanie procesov   Kontrola procesov |  |  |  |  |  |
| (b) Sú skladové kontajnery použité na skladovanie materiálov s informáciami zabezpečené voči neoprávnenému prístupu k obsahu? |  Kontrola bezpečnosti skladových kontajnerov |  |  |  |  |  |
| 9.8.2 | Sú údaje držiteľa karty uložené na elektronickom médiu neobnoviteľne vymazané (napr. prostredníctvom programu na vyčistenie disku v zmysle osvedčených postupoch v oblasti bezpečného mazania alebo pomocou fyzického zničenia média) tak, aby nebolo možné ich rekonštruovať? |  Kontrola procesov   Rozhovor s personálom |  |  |  |  |  |
| 9.9 | Sú zariadenia, ktoré zhromažďujú údaje držiteľov kariet prostredníctvom fyzickej interakcie s kartou chránené pred neoprávneným zásahom a nahradením, a to nasledovným spôsobom?  ***Poznámka:*** *Táto požiadavka sa týka zariadení na čítanie kariet, ktoré sa používajú pri transakciách s fyzickou kartou (vloženie alebo priloženie karty) v mieste predaja. Táto požiadavka sa neuplatňuje na ručné vstupné komponenty, ako sú počítačové klávesnice alebo klávesnice v mieste predaja.* |  |  |  |  |  |  |
| (a) Uvádzajú pravidlá a postupy nutnosť viesť zoznam takýchto zariadení? |  Kontrola pravidiel a postupov |  |  |  |  |  |
| (b) Uvádzajú pravidlá a postupy nutnosť vykonávania pravidelnej kontroly takýchto zariadení na odhalenie neoprávneného zásahu alebo výmeny? |  Kontrola pravidiel a postupov |  |  |  |  |  |
| (c) Uvádzajú pravidlá a postupy nutnosť zaškolenia personálu, aby vedel rozpoznávať podozrivé správanie a ohlasovať neoprávnené zásahy do zariadení? |  Kontrola pravidiel a postupov |  |  |  |  |  |
| 9.9.1 | (a) Obsahuje zoznam zariadení nasledovné položky?   Názov, model zariadenia   Umiestnenie zariadenia (napríklad adresa pracoviska alebo závodu, kde je zariadenie umiestnené)   Sériové číslo zariadenia alebo iný jedinečný identifikačný údaj |  Kontrola zoznamu zariadení |  |  |  |  |  |
| (b) Je zoznam presný a aktuálny? |  Kontrola zariadení a umiestnení zariadenia a porovnanie so zoznamom |  |  |  |  |  |
| (c) Je zoznam zariadení aktualizovaný po pridaní, premiestnení alebo vyradení zariadenia, atď.? |  Rozhovor s personálom |  |  |  |  |  |
| 9.9.2 | (a) Sú povrchy zariadení pravidelne kontrolované na odhalenie neoprávnených zásahov (napríklad pridaním skimmerov k zariadeniam) alebo výmene (napríklad kontrolou sériového čísla alebo inej identifikácie zariadenia, či nedošlo k jeho výmene), a to nasledovne?  ***Poznámka:*** *Príklady znakov, ktoré poukazujú na prípadné neoprávnené zásahy alebo výmeny, môžu zahŕňať podozrivé prípojné zariadenia alebo káble vsunuté do zariadenia, chýbajúce alebo zmenené bezpečnostné značky, poškodený alebo farebne odlišný kryt alebo nezrovnalosti v sériovom čísle zariadenia alebo iných vonkajších značiek.* |  Rozhovor s personálom   Preskúmanie kontrolných procesov a porovnanie so stanovenými postupmi |  |  |  |  |  |
| (b) Bol personál oboznámený s postupmi na kontrolu zariadení? |  Rozhovor s personálom |  |  |  |  |  |
| 9.9.3 | Bol personál vyškolený, aby vedel rozpoznať prípadné pokusy o neoprávnené zásahy alebo výmeny zariadení, a to nasledovne? |  |  |  |  |  |  |
| (a) Obsahujú školiace materiály pre pracovníkov v mieste predaja nasledovné informácie?   Verifikácia totožnosti tretích osôb, ktoré tvrdia, že vykonávajú servisné alebo údržbárske služby, predtým, než získajú prístup k zariadeniu.   Nemontujte, nevymieňajte a nevracajte zariadenia bez predošlého overenia.   Všímajte si podozrivé správanie okolo zariadení (napríklad pokusy o odpojenie alebo otvorenie zariadení neznámymi osobami).   Ohláste podozrivé chovanie a náznaky neoprávnených zásahov alebo výmien zariadení príslušným zamestnancom (napríklad manažérovi alebo bezpečnostnému pracovníkovi). |  Preskúmajte školiace materiály |  |  |  |  |  |
|  | (b) Prešiel personál predajného miesta školením o postupoch na odhaľovanie a hlásenie neoprávnených zásahov a výmien (alebo ich pokusov) zariadení? |  Rozhovor so zamestnancami na predajných miestach |  |  |  |  |  |
| 9.10 | Sú bezpečnostné pravidlá a prevádzkové postupy na obmedzovanie prístupu k údajom držiteľov kariet:   Zdokumentované   Používané   Oznámené dotknutým stranám? |  Kontrola bezpečnostných pravidiel a prevádzkových postupov   Rozhovor s personálom |  |  |  |  |  |

**Pravidelné sledovanie a testovanie siete**

***Požiadavka 10:***  ***Sledovanie a monitorovanie každého prístupu do sieťových zdrojov a údajov držiteľa karty***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Otázka PCI DSS** | | **Očakávané testovanie** | **Odpoveď**  ***(Zaškrtnite jednu odpoveď pre každú otázku)*** | | | | |
| **Áno** | **Áno s CCW** | **Nie** | **N/A** | **Netestované** |
| 10.1 | (a) Sú kontrolné stopy povolené a aktívne pre komponenty systému? |  Kontrola procesov   Rozhovor so správcom systému |  |  |  |  |  |
| (b) Je prístup k systémovým komponentom prepojený s jednotlivými užívateľmi? |  Kontrola procesov   Rozhovor so správcom systému |  |  |  |  |  |
| 10.2 | Sú implementované automatizované kontrolné stopy pre všetky systémové komponenty na rekonštrukciu nasledujúcich udalostí: |  |  |  |  |  |  |
| 10.2.1 | Všetky jednotlivé prístupy užívateľov k údajom držiteľov kariet? |  Rozhovor s personálom   Kontrola záznamov a auditu   Kontrola nastavení kontrolných záznamov |  |  |  |  |  |
| 10.2.2 | Sú všetky činnosti vykonávané jednotlivcom s právami správcu? |  Rozhovor s personálom   Kontrola záznamov a auditu   Kontrola nastavení kontrolných záznamov |  |  |  |  |  |
| 10.2.3 | Prístup ku všetkým kontrolným stopám? |  Rozhovor s personálom   Kontrola záznamov a auditu   Kontrola nastavení kontrolných záznamov |  |  |  |  |  |
| 10.2.4 | Neplatné pokusy o logický prístup? |  Rozhovor s personálom   Kontrola záznamov a auditu   Kontrola nastavení kontrolných záznamov |  |  |  |  |  |
| 10.2.5 | Používanie a zmena identifikačných a autentifikačných mechanizmov, vrátane ale nielen, vytvárania nových účtov a zvyšovania práv a všetkých zmien, doplnení alebo odstránení účtov s právami správcu? |  Rozhovor s personálom   Kontrola záznamov a auditu   Kontrola nastavení kontrolných záznamov |  |  |  |  |  |
| 10.2.6 | Spustenie, zastavenie alebo pozastavenie kontrolných záznamov? |  Rozhovor s personálom   Kontrola záznamov a auditu   Kontrola nastavení kontrolných záznamov |  |  |  |  |  |
| 10.2.7 | Vytváranie a odstraňovanie objektov na úrovni systému? |  Rozhovor s personálom   Kontrola záznamov a auditu   Kontrola nastavení kontrolných záznamov |  |  |  |  |  |
| 10.3 | Sú nasledujúce vstupy kontrolných stôp zaznamenávané pre všetky systémové komponenty a pre každú udalosť? |  |  |  |  |  |  |
| 10.3.1 | Identifikácia užívateľa? |  Rozhovor s personálom   Kontrola záznamov a auditu   Kontrola nastavení kontrolných záznamov |  |  |  |  |  |
| 10.3.2 | Typ udalosti? |  Rozhovor s personálom   Kontrola záznamov a auditu   Kontrola nastavení kontrolných záznamov |  |  |  |  |  |
| 10.3.3 | Dátum a čas? |  Rozhovor s personálom   Kontrola záznamov a auditu   Kontrola nastavení kontrolných záznamov |  |  |  |  |  |
| 10.3.4 | Hlásenie o úspechu alebo poruche? |  Rozhovor s personálom   Kontrola záznamov a auditu   Kontrola nastavení kontrolných záznamov |  |  |  |  |  |
| 10.3.5 | Pôvod udalosti? |  Rozhovor s personálom   Kontrola záznamov a auditu   Kontrola nastavení kontrolných záznamov |  |  |  |  |  |
| 10.3.6 | Identita alebo meno dotknutých údajov, systémového komponentu alebo zdroja? |  Rozhovor s personálom   Kontrola záznamov a auditu   Kontrola nastavení kontrolných záznamov |  |  |  |  |  |
| 10.4 | Sú všetky kritické systémové hodiny a časy synchronizované použitím technológie na synchronizáciu času a je táto technológia aktualizovaná?  ***Poznámka:*** *Jeden príklad technológie na synchronizáciu je sieťový časový protokol NTP.* |  Kontrola štandardov a postupov nastavovania času |  |  |  |  |  |
| 10.4.1 | Sú nasledujúce procesy implementované pre kritické systémy, aby mali správny a konzistentný čas: |  |  |  |  |  |  |
|  | (a) Získava určený centrálny časový server časové signály z externých zdrojov a sú tieto externé zdroje založené na medzinárodnom atómovom čase alebo UTC? |  Kontrola štandardov a postupov nastavovania času   Preskúmanie časových parametrov systému |  |  |  |  |  |
|  | (b) Ak je viac ako jeden určený časový server, sú tieto viaceré servery nastavené tak, aby sa spoločne zhodovali a uchovávali presný čas? |  Kontrola štandardov a postupov nastavovania času   Preskúmanie časových parametrov systému |  |  |  |  |  |
|  | (c) Získavajú systémy čas len z určených centrálnych časových serverov? |  Kontrola štandardov a postupov nastavovania času   Preskúmanie časových parametrov systému |  |  |  |  |  |
| 10.4.2 | Sú dáta chránené nasledovným spôsobom:  (a) Je prístup k údajom obmedzený len na personál, ktorý na základe obchodných potrieb vyžaduje prístup k časovým údajom? |  Preskúmanie systémového nastavenia a nastavenia synchronizácie času |  |  |  |  |  |
| (b) Sú zmeny nastavenia času pre kritické systémy zaznamenávané, monitorované a kontrolované? |  Preskúmanie systémového nastavenia a nastavenia a záznamov synchronizácie času |  |  |  |  |  |
| 10.4.3 | Sú časové nastavenia získavané od špecifických, priemyselne akceptovaných časových zdrojov? (To zabráni neoprávnenej osobe zmeniť čas).  *Voliteľne môžu byť tieto aktualizácie šifrované symetrickým kľúčom a môžu byť vytvorené prístupové kontrolné zoznamy, ktoré špecifikujú IP adresy klientských počítačov, ktoré budú poskytované s časovými aktualizáciami (na zabránenie neoprávnenému použitiu interného časového servera).* |  Preskúmanie systémových konfigurácií |  |  |  |  |  |
| 10.5 | Sú kontrolné stopy zabezpečované tak, aby nebolo možné s nimi manipulovať, a to nasledovne: |  |  |  |  |  |  |
| 10.5.1 | Je prezeranie kontrolných stôp obmedzené len na tie osoby, ktoré to majú v pracovnej náplni? |  Rozhovor so správcami systému   Preskúmanie systémového nastavenia a povolení |  |  |  |  |  |
| 10.5.2 | Sú kontrolné stopy chránené voči neoprávneným zásahom prostredníctvom prístupového kontrolného mechanizmu, fyzického oddelenia a/alebo sieťového oddelenia? |  Rozhovor so správcami systému   Preskúmanie systémového nastavenia a povolení |  |  |  |  |  |
| 10.5.3 | Sú kontrolné stopy rýchlo zálohované na centralizovaný protokolový server alebo médium, ktoré je náročne zmeniť? |  Rozhovor so správcami systému   Preskúmanie systémového nastavenia a povolení |  |  |  |  |  |
| 10.5.4 | Sú záznamy pre technológie orientované externe (napríklad bezdrôtové firewally, DNS, mail) zapísané na bezpečný, centralizovaný alebo interný záznam, server alebo médium? |  Rozhovor so správcami systému   Preskúmanie systémového nastavenia a povolení |  |  |  |  |  |
| 10.5.5 | Dochádza k sledovaniu integrity súborov alebo používa sa softvér na detekciu zmien, aby sa zabezpečilo to, že akákoľvek zmena v záznamoch je ihneď signalizovaná (netýka sa zápisu nových údajov)? |  Kontrola nastavení, monitorovaných súborov a výsledkov z monitorovacích činností |  |  |  |  |  |
| 10.6 | Sú záznamy a bezpečnostné udalosti pre všetky systémové komponenty kontrolované na odhalenie anomálií alebo podozrivých aktivít, a to nasledovne?  ***Poznámka:*** *Na dosiahnutie súladu s požiadavkou 10.6 je možné použiť nástroje na signalizáciu, zber alebo analyzovanie záznamov.* |  |  |  |  |  |  |
| 10.6.1 | (a) Sú všetky pravidlá a postupy týkajúce sa kontroly nasledovných prvkov vykonávanej najmenej denne, a to manuálne alebo pomocou denníkov?   Všetky bezpečnostné udalosti   Záznamy všetkých systémových komponentov, ktoré ukladajú, spracovávajú alebo prenášajú CHD a/alebo SAD   Záznamy všetkých kritických systémových komponentov   Záznamy všetkých serverových a systémových komponentov, ktoré vykonávajú bezpečnostné funkcie (napríklad firewally, systémy na detekciu narušenia / systémy na zabránenie preniknutiu (IDS/IPS), autentifikačné servery, servery na premiestňovanie elektronického obchodu, atď.) |  Kontrola bezpečnostných pravidiel a postupov |  |  |  |  |  |
| (b) Sú vyššie uvedené záznamy a bezpečnostné udalosti kontrolované najmenej raz denne? |  Kontrola procesov   Rozhovor s personálom |  |  |  |  |  |
| 10.6.2 | (a) Sú všetky pravidlá a postupy, týkajúce sa kontroly nasledovných prvkov vykonávané najmenej denne, a to manuálne alebo pomocou denníkov, založené na pravidlách a postupoch a stratégii riadenia rizík organizácie? |  Kontrola bezpečnostných pravidiel a postupov |  |  |  |  |  |
|  | (b) Sú kontroly všetkých systémových komponentov vykonávané v súlade s pravidlami a postupmi a stratégiou riadenia rizík organizácie? |  Kontrola dokumentácie hodnotenia rizík   Rozhovor s personálom |  |  |  |  |  |
| 10.6.3 | (a) Sú písomné pravidlá a postupy na sledovanie výnimiek a anomálii stanovené počas procesu kontroly? |  Kontrola bezpečnostných pravidiel a postupov |  |  |  |  |  |
|  | (b) Dochádza k sledovaniu výnimiek a anomálií? |  Kontrola procesov   Rozhovor s personálom |  |  |  |  |  |
| 10.7 | (a) Sú zavedené pravidlá a postupy týkajúce sa uchovávania záznamov a vyžaduje sa, aby boli záznamy uchovávané najmenej po dobu jedného roka s tým, že najmenej tri mesiace sú dostupné na okamžitú analýzu (napríklad online archív alebo obnoviteľné zo zálohy)? |  Kontrola bezpečnostných pravidiel a postupov |  |  |  |  |  |
| (b) Sú kontrolné záznamy uchovávané najmenej jeden rok? |  Rozhovor s personálom   Preskúmanie kontrolných záznamov |  |  |  |  |  |
| (c) Sú záznamy najmenej tri mesiace okamžite k dispozícií na analýzu? |  Rozhovor s personálom   Kontrola procesov |  |  |  |  |  |
| 10.8 | *Táto požiadavka sa vzťahuje výlučne na poskytovateľov služieb* |  | | | | | |
| 10.9 | Sú bezpečnostné pravidlá a prevádzkové postupy na sledovanie prístupu k sieťovým zdrojom a údajom držiteľov kariet:   Zdokumentované   Používané   Oznámené dotknutým stranám? |  Kontrola bezpečnostných pravidiel a operačných postupov   Rozhovor s personálom |  |  |  |  |  |

***Požiadavka 11:*** ***Pravidelné testovanie bezpečnostných systémov a procesov***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Otázka PCI DSS** | | **Očakávané testovanie** | **Odpoveď**  ***(Zaškrtnite jednu odpoveď pre každú otázku)*** | | | | |
| **Áno** | **Áno s CCW** | **Nie** | **N/A** | **Netestované** |
| 11.1 | (a) Sú implementované procesy na detekciu a identifikáciu autorizovaných aj neautorizovaných bezdrôtových prístupových bodov?  ***Poznámka:*** *Metódy, ktoré je možné použiť v procese, zahŕňajú, ale nielen, skenovanie bezdrôtových sietí, fyzické/logické kontroly systémových komponentov a infraštruktúry, riadenie prístupu k sieti (NAC) alebo bezdrôtové IDS/IPS.*  *Bez ohľadu na to, ktorá metóda je použitá, musí byť schopná odhaľovať a identifikovať neoprávnené zariadenia.* |  Kontrola pravidiel a postupov |  |  |  |  |  |
| (b) Dokáže postup odhaľovať a identifikovať neoprávnené bezdrôtové prístupové miesta, vrátane minimálne nasledujúceho?   Karty WLAN vložené do systémových komponentov   Prenosné alebo mobilné zariadenia pripojené k systémovým komponentom na vytvorenie bezdrôtového prístupového bodu (napríklad pomocou USB, atď.) a   Bezdrôtové zariadenia pripojené k sieťovému portu alebo sieťovému zariadeniu. |  Hodnotenie postupu |  |  |  |  |  |
| (c) V prípade, že bezdrôtové skenovanie je použité na identifikáciu autorizovaných a neautorizovaných bezdrôtových prístupových bodov, dochádza k skenovaniu najmenej štvrťročne pre všetky systémové komponenty a zariadenia? |  Kontrola výstupu z predchádzajúcich bezdrôtových skenov |  |  |  |  |  |
| (d) V prípade použitia automatizovaného monitoringu (napríklad bezdrôtové IDS/IPS, NAC, atď.) je monitorovanie nastavené tak, aby generovalo upozornenia pre zodpovedných pracovníkov? |  Preskúmanie konfiguračných nastavení |  |  |  |  |  |
| 11.1.1 | Sú inventár alebo autorizované bezdrôtové prístupové body udržiavané a je zdokumentovaný obchodný účel všetkých autorizovaných bezdrôtových prístupových bodov? |  Kontrola inventáru |  |  |  |  |  |
| 11.1.2 | (a) Vyžaduje a stanovuje plán reakcie odozvu v prípade zistenia neoprávneného bezdrôtového prístupového bodu? |  Kontrola plánu odozvy na incident (pozri požiadavku 12.10) |  |  |  |  |  |
|  | (b) Vykoná sa akcia v prípade zistenia neoprávneného bezdrôtového prístupového bodu? |  Rozhovor so zodpovedným personálom   Kontrola nedávnych bezdrôtových skenov a súvisiacich akcií |  |  |  |  |  |
| 11.2 | Dochádza k skenovaniu interných a externých zraniteľností najmenej štvrťročne a po implementovaní významných zmien v sieti (napríklad inštalácie nových systémových komponentov, zmeny v topológii siete, zmeny pravidiel brány firewallu, aktualizácie produktov), a to nasledovne?  ***Poznámka:*** *Viaceré výstupy zo skenov je možné skombinovať do jednej správy, ktorá obsahuje informácie o skenovaných systémoch, zraniteľnostiach a následných akcií. Môže byť vyžadovaná dodatočná dokumentácia na overenie, či zostávajúce zraniteľnosti sú v procese ich riešenia.*  *Pri počiatočnej zhode s PCI DSS, nie je potrebné, aby štyri štvrtiny všetkých skenov boli dokončené v prípade, že hodnotiteľ overí, že (1) posledný sken bol vyhovujúci, (2) subjekt zdokumentoval postupy a pravidlá vyžadujúce štvrťročné skenovanie a (3) zraniteľnosti zaznamenané vo výsledkoch zo skenu boli opravené a ich odstránenie bolo potvrdené opätovných skenom. Počas nasledujúcich rokov po počiatočnej kontrole PCI DSS musí dôjsť k uskutočneniu štyroch štvrtín skenu.* |  |  |  |  |  |  |
| 11.2.1 | (a) Dochádza k uskutočňovaniu štvrťročných interných skenov zraniteľnosti? |  Kontrola správ zo skenu |  |  |  |  |  |
| (b) Riešia štvrťročné interné skenovacie procesy vysokorizikové zraniteľnosti a obsahujú požiadavky na opätovné skenovanie na overenie odstránenia vysokorizikových zraniteľností (tak, ako je uvedené v požiadavke 6.1 PCI DSS)? |  Kontrola správ zo skenu |  |  |  |  |  |
| (c) Sú štvrťročné interné skeny vykonávané kvalifikovanými internými zdrojmi alebo kvalifikovanými tretími stranami a, v prípade potreby, je zabezpečená organizačná nezávislosť testovacieho subjektu (nie je požadované QSA alebo ASV)? |  Rozhovor s personálom |  |  |  |  |  |
| 11.2.2 | (a) Dochádza k uskutočňovaniu externých štvrťročných interných skenov zraniteľnosti?  ***Poznámka:*** *Štvrťročné externé skenovanie zraniteľnosti musí byť vykonávané poskytovateľom skenov (ASV) schválených radou pre štandardy bezpečnosti platobných kariet (PCI SSC).*  *Pozri príručku programov ASV zverejnenú na webovej stránke PCI SSC na kontrolu povinností týkajúcich sa skenov, prípravy skenov, atď.* |  Kontrola výsledkov z posledných štyroch štvrťročných externých skenov zraniteľností |  |  |  |  |  |
| (b) Vyhovujú výsledky externých štvrťročných skenov a opätovných skenov požiadavky príručky programov ASV (napríklad neboli odhalené žiadne zraniteľnosti s hodnotou 4,0 alebo vyššou CVSS alebo nedošlo k automatickým zlyhaniam)? |  Preskúmanie výsledkom každého externého štvrťročného skenu alebo opätovného skenu |  |  |  |  |  |
| (c) Sú štvrťročné externé skeny zraniteľnosti vykonávané poskytovateľom skenov schválené zo strany PCI SSC (ASV)? |  Preskúmanie výsledkom každého externého štvrťročného skenu alebo opätovného skenu |  |  |  |  |  |
| 11.2.3 | (a) Sú interné a externé skeny a opätovné skeny vykonávané vždy po každej významnej zmene?  ***Poznámka:*** *Skenovanie musí byť vykonávané kvalifikovaným personálom.* |  Preskúmajte a porovnajte dokumentáciu k riadeniu zmien so správami zo skenov |  |  |  |  |  |
| (b) Obsahuje skenovací proces opätovné skenovanie, až kým:   Neexistujú žiadne zraniteľnosti s hodnotou 4,0 a viac CVSS v prípade externých skenov?   Je dosiahnuté vyhovujúce skóre zo skenu pre všetky vysokorizikové zraniteľnosti tak, ako je to stanovené v požiadavke 6.1 PCI DSS v prípade interných skenov? |  Kontrola správ zo skenu |  |  |  |  |  |
| (c) Sú skeny vykonávané kvalifikovanými internými zdrojmi alebo kvalifikovanými tretími stranami a, v prípade potreby, je zabezpečená organizačná nezávislosť testovacieho subjektu (nie je požadované QSA alebo ASV)? |  Rozhovor s personálom |  |  |  |  |  |
| 11.3 | Obsahuje metóda testovania prieniku nasledovné?   Vychádza z osvedčených postupov a metód testovania prieniku (napríklad, NIST SP800-115)   Zahŕňa pokrytie celého obvodu CDE a kritických systémov   Zahŕňa testovanie z vnútra siete aj mimo nej   Zahŕňa testovanie na overenie kontroly akejkoľvek segmentácie a obmedzovania rozsahu   Stanovuje testy prieniku aplikačnej vrstvy, ktorá zahŕňa najmenej zraniteľnosti uvedené v požiadavke 6.5   Stanovuje testy prieniku aplikačnej vrstvy, ktorá zahŕňa komponenty na podporu sieťových funkcií a operačných systémov   Zahŕňa kontroly a posudky hrozieb a zraniteľností odhalených za posledných 12 mesiacov   Stanovuje uchovávanie výsledkov z testovania prieniku a výsledkov nápravných činností |  Kontrola metodiky testu prieniku   Rozhovor so zodpovedným personálom |  |  |  |  |  |
| 11.3.1 | (a) Je externé testovanie prieniku vykonávané na základe stanovenej metodiky, a to najmenej ročne a po každej významnej zmene infraštruktúry alebo prostredia danej aplikácie (ako je aktualizácia operačného systému, pridanie podsiete alebo pridanie webového servera)? |  Kontrola rozsahu prác   Kontrola výsledkov z posledných externých testov prieniku |  |  |  |  |  |
|  | (b) Sú testy vykonávané kvalifikovanými internými zdrojmi alebo kvalifikovanými externými tretími stranami a, v prípade potreby, je zabezpečená organizačná nezávislosť testera (nie je požadované pre QSA a ASV)? |  Rozhovor so zodpovedným personálom |  |  |  |  |  |
| 11.3.2 | (a) Je externé testovanie prieniku vykonávané na základe stanovenej metodiky, a to najmenej ročne a po každej významnej zmene infraštruktúry alebo prostredia danej aplikácie (ako je aktualizácia operačného systému, pridanie podsiete alebo pridanie webového servera)? |  Kontrola rozsahu prác   Kontrola výsledkov z posledných interných testov prieniku |  |  |  |  |  |
|  | (b) Sú testy vykonávané kvalifikovanými internými zdrojmi alebo kvalifikovanými externými tretími stranami a, v prípade potreby, je zabezpečená organizačná nezávislosť testera (nie je požadované pre QSA a ASV)? |  Rozhovor so zodpovedným personálom |  |  |  |  |  |
| 11.3.3 | Sú zraniteľnosti zistené počas testu prieniku opravené a je vykonané následné testovanie na overenie ich odstránenia? |  Kontrola výsledkov testovania prieniku |  |  |  |  |  |
| 11.3.4 | Ak sa používa segmentácia na izoláciu CDE od ostatných sietí: |  |  |  |  |  |  |
| (a) Sú testovacie postupy prieniku stanovené vo všetkých postupoch segmentácie na potvrdenie ich funkčnosti a účinnosti a izolovanie všetkých systémov mimo rozsahu zo systémov v CDE? |  Preskúmanie kontrolných prvkov segmentácie   Kontrola metodiky testu prieniku |  |  |  |  |  |
|  | (b) Spĺňa testovanie prieniku na overenie kontrolných prvkov segmentácie nasledovné?   Vykonáva sa najmenej raz ročne a po každej zmene kontrolných prvkov/metód segmentácie   Týka sa všetkých používaných kontrolných prvkov/metód segmentácie   Overuje, že metóda segmentácie je funkčná a účinná a že izoluje všetky systémy mimo rozsahu od systémov v CDE. |  Kontrola výsledkov z posledných interných testov prieniku |  |  |  |  |  |
|  | (b) Sú testy vykonávané kvalifikovanými internými zdrojmi alebo kvalifikovanými externými tretími stranami a, v prípade potreby, je zabezpečená organizačná nezávislosť testera (nie je požadované pre QSA a ASV)? |  Rozhovor so zodpovedným personálom |  |  |  |  |  |
| 11.3.4.1 | *Táto požiadavka sa vzťahuje výlučne na poskytovateľov služieb* |  | | | | | |
| 11,4 | (a) Sú techniky detekcie narušenia a/alebo prevencie narušenia, ktoré detekujú a/alebo zabraňujú vniknutiu do siete, používané na monitorovanie všetkej komunikácie:   Na obvode dátového prostredia držiteľa karty a   Na kritických miesta dátového prostredia držiteľa karty. |  Preskúmanie systémových konfigurácií   Preskúmanie sieťových konfigurácií |  |  |  |  |  |
| (b) Sú techniky detekcie narušenia a/alebo prevencie narušenia nastavené tak, aby upozorňovali zamestnancov o podozrivých narušeniach? |  Preskúmanie systémových konfigurácií   Rozhovor so zodpovedným personálom |  |  |  |  |  |
| (c) Sú všetky programy, podpisy a základné prvky na detekciu a prevenciu narušení pravidelne aktualizované? |  Kontrola nastavení IDS/IPS   Kontrola dokumentácie dodávateľa |  |  |  |  |  |
| 11.5 | (a) Je mechanizmus detekcie zmeny (napríklad nástroje na monitorovanie integrity súborov) inštalovaný a používaný na detekciu neoprávnených zásahov (vrátane zmien, doplnení a odstránení) kritických systémových súborov, konfiguračných súborov alebo obsahových súborov?  *Príklady súborov, ktoré je potrebné monitorovať:*   *Systémové spustiteľné súbory*   *Spustiteľné súbory aplikácií*   *Súbory konfigurácie a parametrov*   *Centrálne uložené, historické alebo archivované záznamy a kontrolné denníky*   *Dodatočné kritické súbory určené subjektom (napríklad na základe hodnotenia rizík alebo inými metódami)* |  Kontrola systémových nastavení a monitorovaných súborov   Preskúmanie systémových konfiguračných nastavení |  |  |  |  |  |
|  | (a) Je mechanizmus detekcie zmeny nastavený, aby upozorňoval zamestnancov na neoprávnené zásahy (vrátane zmien, doplnení a odstránení) kritických systémových súborov, konfiguračných súborov alebo obsahových súborov a vykonávajú nástroje porovnávania kritických súborov na týždennej báze?  ***Poznámka:*** *Na účely detekcie zmien sú kritické súbory obvykle tie, ktoré sa pravidelne nemenia, úprava ktorých však môže indikovať ohrozenie systému alebo riziko ohrozenia. Mechanizmus detekcie zmeny, ako sú produkty na monitorovanie integrity súborov, obvykle sú dodávané predstavené s kritickým súbormi pre príslušný operačný systém. Iné kritické súbory, ako sú tie určené pre špeciálne aplikácie, musia byť hodnotené a stanovené subjektom (t.j. dodávateľom alebo poskytovateľom služby).* |  Kontrola systémových nastavení a monitorovaných súborov   Kontrola výsledkov z monitorovania |  |  |  |  |  |
| 11.5.1 | Je zavedený proces, ktorý reaguje na všetky upozornenia generované mechanizmom na detekciu zmien? |  Preskúmanie systémových konfiguračných nastavení |  |  |  |  |  |
| 11.6 | Sú bezpečnostné pravidlá a prevádzkové postupy na bezpečné monitorovanie a testovanie:   Zdokumentované   Používané   Oznámené dotknutým stranám? |  Kontrola bezpečnostných pravidiel a prevádzkových postupov   Rozhovor s personálom |  |  |  |  |  |

**Udržiavanie politiky**

**zabezpečenia informácií**

***Požiadavka 12:*** ***Udržiavanie politiky, ktorá rieši bezpečnosť informácií všetkých pracovníkov***

***Poznámka:*** *Na účely požiadavky 12 sa pod pojmom „personál" rozumejú zamestnanci na plný úväzok alebo čiastočný úväzok, zamestnanci na dohodu, dodávatelia a konzultanti, ktorí vykonávajú svoju činnosť v priestoroch subjektu alebo ktorí majú iný prístup k dátovému prostrediu držiteľov kariet.*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Otázka PCI DSS** | | **Očakávané testovanie** | **Odpoveď**  ***(Zaškrtnite jednu odpoveď pre každú otázku)*** | | | | |
| **Áno** | **Áno s CCW** | **Nie** | **N/A** | **Netestované** |
| 12.1 | Je zavedená, zverejnená, udržiavaná a rozširovaná bezpečnostná politika pre celý personál? |  Kontrola informačnej bezpečnostnej politiky |  |  |  |  |  |
| 12.1.1 | Je bezpečnostná politika revidovaná raz ročne a aktualizovaná pri zmene prostredia? |  Kontrola informačnej bezpečnostnej politiky   Rozhovor so zodpovedným personálom |  |  |  |  |  |
| 12.2 | (a) Je zavedený proces ročného posudzovania rizík, ktorý:   Identifikuje kritické aktíva, hrozby a slabé miesta a   Vedie k stanoveniu formálne zdokumentovanej analýzy rizík?  *Príklady postupov posudzovania rizík zahŕňajú, ale nielen, OCTAVE, ISO 27005 and NIST SP 800-30.* |  Revízia ročného postupu hodnotenia rizík   Rozhovor s personálom |  |  |  |  |  |
| (b) Je proces posudzovania rizík vykonávaný najmenej raz ročne a v prípade akejkoľvek významnej zmeny prostredia (napríklad akvizícia, zlúčenie, premiestnenie, atď.)? |  Kontrola dokumentácie hodnotenia rizík   Rozhovor so zodpovedným personálom |  |  |  |  |  |
| 12.3 | Sú použité pravidlá pre kritické technológie vypracované tak, aby stanovovali použitie týchto technológií a vyžadovali:  ***Poznámka:*** *Príklady kritických technológií zahŕňajú, ale nie sú obmedzené na vzdialené prístupy a bezdrôtové technológie, notebooky, tablety, vymeniteľné elektronické médiá, či používanie emailov a internetu.* |  |  |  |  |  |  |
| 12.3.1 | Výslovný súhlas autorizovaným stranám na použitie technológií? |  Kontrola pravidiel používania   Rozhovor so zodpovedným personálom |  |  |  |  |  |
| 12.3.2 | Autentifikácia použitia technológie? |  Kontrola pravidiel používania   Rozhovor so zodpovedným personálom |  |  |  |  |  |
| 12.3.3 | Zoznam zariadení a personálu s prístupom? |  Kontrola pravidiel používania   Rozhovor so zodpovedným personálom |  |  |  |  |  |
| 12.3.4 | Spôsob presného a jednoduchého určovania vlastníka, kontaktných informácií a účelu (napríklad označovanie, kódovanie a/alebo inventarizácia zariadení)? |  Kontrola pravidiel používania   Rozhovor so zodpovedným personálom |  |  |  |  |  |
| 12.3.5 | Prijateľne používanie technológií? |  Kontrola pravidiel používania   Rozhovor so zodpovedným personálom |  |  |  |  |  |
| 12.3.6 | Prijateľné sieťové miesta pre tieto technológie? |  Kontrola pravidiel používania   Rozhovor so zodpovedným personálom |  |  |  |  |  |
| 12.3.7 | Zoznam produktov schválených spoločnosťou? |  Kontrola pravidiel používania   Rozhovor so zodpovedným personálom |  |  |  |  |  |
| 12.3.8 | Automatické odpojovanie prihlásení pre technológie vzdialeného prístupu po určitom období nečinnosti? |  Kontrola pravidiel používania   Rozhovor so zodpovedným personálom |  |  |  |  |  |
| 12.3.9 | Aktivácia technológií vzdialeného prístupu pre dodávateľov a obchodných partnerov len, keď je takýto prístup nutný pre dodávateľov a obchodných partnerov s okamžitou deaktiváciou prístupu po použití? |  Kontrola pravidiel používania   Rozhovor so zodpovedným personálom |  |  |  |  |  |
| 12.3.10 | (a) Pre personál s prístupom k údajom držiteľov kariet prostredníctvom technológií vzdialeného prístupu, určujú tieto pravidlá zákaz kopírovania, presúvania a uchovávania údajov držiteľov kariet na lokálne pevné disky a vymeniteľné elektronické média, pokiaľ k tomu nie je vydaný výslovný súhlas na stanovené obchodné účely?  *V prípade oprávnenej obchodnej potreby, pravidlá používania musia vyžadovať, aby boli údaje chránené v súlade so všetkými príslušnými požiadavkami PCI DSS.* |  Kontrola pravidiel používania   Rozhovor so zodpovedným personálom |  |  |  |  |  |
|  | (b) Pre personál s riadnym oprávneným, vyžadujú tieto pravidlá ochranu údajov držiteľov kariet v súlade s požiadavkami PCI DSS? |  Kontrola pravidiel používania   Rozhovor so zodpovedným personálom |  |  |  |  |  |
| 12.4 | Sú v bezpečnostnej politike a postupoch jasne stanovené zodpovednosti za bezpečnosť informácií pre všetkých pracovníkov? |  Kontrola informačnej bezpečnostnej politiky a postupov   Rozhovor s náhodnými zodpovednými zamestnancami |  |  |  |  |  |
| 12.4.1 | *Táto požiadavka sa vzťahuje výlučne na poskytovateľov služieb* |  |  |  |  |  |  |
| 12.5 | (a) Je formálne priradená zodpovednosť za informačnú bezpečnosť hlavnému bezpečnostnému riaditeľovi alebo inému manažérovi v oblasti bezpečnosti? |  Kontrola informačnej bezpečnostnej politiky a postupov |  |  |  |  |  |
| (b) Sú nasledujúce zodpovednosti informačného bezpečnostného manažmentu priradené jednotlivcovi alebo tímu: |  |  |  |  |  |  |
| 12.5.1 | Zriaďovanie, dokumentovanie a distribúcia bezpečnostných politík a postupov? |  Kontrola informačnej bezpečnostnej politiky a postupov |  |  |  |  |  |
| 12.5.2 | Monitorovanie a analyzovanie bezpečnostných upozornení a informácií a ich distribúcia príslušným zamestnancom? |  Kontrola informačnej bezpečnostnej politiky a postupov |  |  |  |  |  |
| 12.5.3 | Zriaďovanie, dokumentovanie a distribúcia odoziev na bezpečnostné incidenty a postupov eskalácie na zabezpečenie včasného a efektívneho zvládnutia všetkých situácií? |  Kontrola informačnej bezpečnostnej politiky a postupov |  |  |  |  |  |
| 12.5.4 | Spravovanie užívateľských účtov, vrátane doplnení, odstránení a úprav? |  Kontrola informačnej bezpečnostnej politiky a postupov |  |  |  |  |  |
| 12.5.5 | Monitorovanie a kontrola všetkých prístupov k údajom? |  Kontrola informačnej bezpečnostnej politiky a postupov |  |  |  |  |  |
| 12.6 | (a) Je zavedený formálny program na zvyšovanie povedomia o bezpečnosti tak, aby bol celý personál oboznámený o bezpečnostnej politike a postupoch v oblasti ochrany dát držiteľov kariet? |  Kontrola programu na zvyšovanie povedomia o bezpečnosti |  |  |  |  |  |
| (b) Obsahujú programy na zvyšovanie povedomia o bezpečnosti nasledovné? |  |  |  |  |  |  |
| 12.6.1 | (a) Poskytuje program na zvyšovanie povedomia o bezpečnosti viaceré spôsoby informovania a školenia personálu (napríklad plagáty, listy, emaily, webové kurzy, stretnutia a propagačné akcie)?  ***Poznámka:*** *Tieto metódy sa môžu líšiť v závislosti od úlohy personálu a úrovne prístupu k údajom držiteľov kariet.* |  Kontrola programu na zvyšovanie povedomia o bezpečnosti   Kontrola postupov programu na zvyšovanie povedomia o bezpečnosti   Kontrola záznamov o účasti na programe na zvyšovanie povedomia o bezpečnosti |  |  |  |  |  |
| (b) Prechádzajú novo prijatí zamestnanci odbornou prípravou a následne vždy aspoň raz za rok? |  Kontrola dokumentov a postupov programu na zvyšovanie povedomia o bezpečnosti |  |  |  |  |  |
| (c) Dokončili zamestnanci školenie na zvýšenie informovanosti a boli oboznámení s dôležitosťou bezpečnosti údajov držiteľov kariet? |  Rozhovor s personálom |  |  |  |  |  |
| 12.6.2 | Požaduje sa od personálu, aby najmenej raz za rok potvrdil, že si prečítal a porozumel bezpečnostnú politiku a postupy? |  Kontrola dokumentov a postupov programu na zvyšovanie povedomia o bezpečnosti |  |  |  |  |  |
| 12.7 | Je potenciálny nový personál (pozri definíciu „personálu" vyššie) preverený pred prijatím, aby sa minimalizovalo riziko útokov z interných zdrojov?  *Príklady takéhoto preverenia zahŕňajú kontroly predchádzajúcich zamestnaní, trestného záznamu, histórie úverov a referencií.*  ***Poznámka:*** *Potenciálni zamestnanci, ktorí majú byť prijatí na určité pozície, ako napríklad pracovníci pri pokladni, ktorí majú prístup len k jednému číslu karty v čase transakcie, je táto požiadavka len odporúčaním.* |  Rozhovor s vedením oddelenia ľudských zdrojov |  |  |  |  |  |
| 12.8 | Sú udržiavané a implementované pravidlá a postupy tak, aby adresovali poskytovateľov služieb, s ktorými zdieľate údaje držiteľov kariet alebo ktorí by mohli narušiť bezpečnosť údajov držiteľov kariet, a to nasledovne: |  |  |  |  |  |  |
| 12.8.1 | Je udržiavaný zoznam poskytovateľov služieb, vrátane popisu poskytovaných služieb? |  Kontrola pravidiel a postupov   Kontrola procesov   Kontrola zoznamu poskytovateľov služieb |  |  |  |  |  |
| 12.8.2 | Sú udržiavané písomné dohody obsahujúce potvrdenie o tom, že poskytovatelia služieb nesú zodpovednosť za bezpečnosť údajov držiteľov kariet, ktoré sú im poskytnuté a ktoré uschovávajú, spracovávajú alebo zasielajú v mene zákazníka, alebo v rozsahu, v ktorom môžu narušiť bezpečnosť dátového prostredia držiteľov kariet?  ***Poznámka:*** *Presné znenie tohto potvrdenia záleží od dohody medzi oboma stranami, podrobností poskytovaných služieb a zodpovedností pridelených každej strane. Toto potvrdenie nemusí obsahovať presné znenie uvedené v tejto požiadavke.* |  Kontrola písomných dohôd   Kontrola pravidiel a postupov |  |  |  |  |  |
| 12.8.3 | Je zavedený postup na zabezpečenie dodržiavania bezpečnostných pravidiel zo strany poskytovateľov služieb, vrátane náležitej starostlivosti? |  Kontrola procesov   Preskúmanie pravidiel a postupov a podpornú dokumentáciu |  |  |  |  |  |
| 12.8.4 | Je udržiavaný program na monitorovanie súladu poskytovateľov služieb s požiadavkami PCI DSS najmenej raz ročne? |  Kontrola procesov   Preskúmanie pravidiel a postupov a podpornú dokumentáciu |  |  |  |  |  |
| 12.8.5 | Sú uchovávané informácie o tom, ktoré požiadavky PCI DSS sú riadené poskytovateľmi a ktoré sú riadené daným subjektom? |  Kontrola procesov   Preskúmanie pravidiel a postupov a podpornú dokumentáciu |  |  |  |  |  |
| 12.9 | *Táto požiadavka sa vzťahuje výlučne na poskytovateľov služieb.* |  |  |  |  |  |  |
| 12.10 | Je zavedený plán okamžitej reakcie na incidenty v prípade narušenia systému, a to nasledovne: |  |  |  |  |  |  |
| 12.10.1 | (a) Bol vytvorený plán reakcie na incidenty v prípade narušenia systému? |  Kontrola plánu reakcie na incidenty   Kontroly postupov plánu reakcie na incidenty |  |  |  |  |  |
|  | (b) Stanovuje tento plán, minimálne: |  |  |  |  |  |  |
|  |  Úlohy, zodpovednosti a komunikácie a kontaktné stratégie v prípade narušenia systému, vrátane systému oznamovania takýchto prípadov kartovej spoločnosti? |  Kontroly postupov plánu reakcie na incidenty |  |  |  |  |  |
|  |  Špecifické postupy reakcie na incidenty? |  Kontroly postupov plánu reakcie na incidenty |  |  |  |  |  |
|  Postupy na obnovu a kontinuitu podnikateľskej činnosti? |  Kontroly postupov plánu reakcie na incidenty |  |  |  |  |  |
|  Postupy zálohovania údajov? |  Kontroly postupov plánu reakcie na incidenty |  |  |  |  |  |
|  |  Analýza právnych požiadaviek na ohlasovanie narušení? |  Kontroly postupov plánu reakcie na incidenty |  |  |  |  |  |
|  |  Pokrytie a odozvy všetkých kritických systémových komponentov |  Kontroly postupov plánu reakcie na incidenty |  |  |  |  |  |
|  |  Zahrnutie alebo uvedenie reakčných postupov platobných značiek? |  Kontroly postupov plánu reakcie na incidenty |  |  |  |  |  |
| 12.10.2 | Je tento plán revidovaný a testovaný najmenej raz ročne, vrátane všetkých prvkov uvedených v požiadavke 12.10.1? |  Kontroly postupov plánu reakcie na incidenty   Rozhovor so zodpovedným personálom |  |  |  |  |  |
| 12.10.3 | Sú priradené osoby na riešenie takýchto situácií 24 hodín denne a 7 dní v týždni? |  Kontrola procesov   Kontrola pravidiel   Rozhovor so zodpovedným personálom |  |  |  |  |  |
| 12.10.4 | Je zamestnancom, ktorí nesú zodpovednosť za narušenie bezpečnosti, poskytovaná primeraná odborná príprava? |  Kontrola procesov   Kontroly postupov plánu reakcie na incidenty   Rozhovor so zodpovedným personálom |  |  |  |  |  |
| 12.10.5 | Sú súčasťou plánu reakcie na incidenty výstrahy z bezpečnostných monitorovacích systémov? |  Kontrola procesov   Kontroly postupov plánu reakcie na incidenty |  |  |  |  |  |
| 12.10.6 | Bol vyvinutý a je implementovaný proces na úpravu a vývoj plánu reakcie na incidenty založený na získaných skúsenostiach a nových poznatkoch v danom odvetví? |  Kontrola procesov   Kontroly postupov plánu reakcie na incidenty   Rozhovor so zodpovedným personálom |  |  |  |  |  |
| 12.11 | *Táto požiadavka sa vzťahuje výlučne na poskytovateľov služieb* |  | | | | | |

**Dodatok A:** **Dodatočné požiadavky PCI DSS**

***Dodatok A1:***  ***Dodatočné požiadavky PCI DSS pre spoločných poskytovateľov hostingu***

Tento dodatok sa nepoužíva na hodnotenie obchodníkov.

***Dodatok A2:***  ***Dodatočné požiadavky PCI DSS pre subjekty používajúce SSL/staršie TLS***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Otázka PCI DSS** | | **Očakávané testovanie** | **Odpoveď**  ***(Zaškrtnite jednu odpoveď pre každú otázku)*** | | | | |
| **Áno** | **Áno s CCW** | **Nie** | **N/A** | **Netestované** |
| A2.1 | *Pre terminály POS POI (a koncové body SSL/TLS, ku ktorým sa pripájajú) používajúce SSL a/alebo staršie TLS:*   Došlo k overeniu zariadenia, že nie je zraniteľné voči známym útokom do SSL/starších TLS  *Alebo:*   Je zavedený formálny plán zmierňovania rizika a plán migrácie v zmysle požiadavky A2.2? |  Kontrola dokumentácie (napríklad dokumentácie dodávateľa, systémové/sieťové konfiguračné podrobnosti, atď.), ktorá potvrdzuje, že zariadenia POS POI nie sú zraniteľné voči známym útokom do SSL/staršieho TLS. |  |  |  |  |  |
| A2.2 | Je zavedený formálny plán zmierňovania rizika a plán migrácie pre všetky implementácie, ktoré používajú SSL a/alebo staršie TLS (okrem tých, ktoré sú uvedené v A2.1), predovšetkým:   Popis používania, vrátane informácií o tom, aké údaje sú prenášané, typy a počty systémov používajúce SSL/staršie TLS, typ prostredia   Výsledky zavedených kontrolných postupov posudzovania rizika a zmierňovania rizika   Popis postupov na monitorovanie nových zraniteľných miest spojených s SSL / starším TLS   Popis procesov riadenia zmien, ktoré sa implementujú s cieľom zabezpečiť, že SSL / staršie TLS nie je implementované do nových prostredí   Prehľad projektového plánu migrácie, vrátane cieľového dátumu dokončenia migrácie najneskôr do 30. júna 2018? |  Kontrola zdokumentovaného plánu migrácie a plánu zmierňovania rizika |  |  |  |  |  |
| A2.3 | *Táto požiadavka sa vzťahuje výlučne na poskytovateľov služieb* |  |  |  |  |  |  |

***Dodatok A3:***  ***Dodatočná validácia určených subjektov (DESV)***

Tento dodatok sa vzťahuje iba na subjekty vybrané kartovou spoločnosťou alebo nadobúdateľom, od ktorých sa vyžaduje dodatočné overenie požiadaviek PCI DSS. Subjekty, ktoré sú povinné overiť súlad podľa tohto dodatku by mali používať dodatočnú oznamovaciu šablónu DESV a dodatočné preukazovanie zhody a konzultovať proces predkladania s príslušnou kartovou spoločnosťou a/alebo nadobúdateľom.

**Dodatok B:** **Hárok kompenzačného riadenia**

*Použite tento hárok na stanovenie kompenzačného riadenia všetkých požiadaviek, kde ste vybrali „ÁNO s CCW".*

***Poznámka:*** *Len spoločnosti, ktoré vykonali analýzu rizík a ktoré majú oprávnené technologické alebo obchodné obmedzenia, môžu zvážiť použitie kompenzačného riadenia na dosiahnutie súladu.*

*Pozri dodatky B, C a D dokumentu PCI DSS pre informácie o kompenzačnom riadení a pokynoch na vyplnenie tohto hárku.*

**Číslo a popis požiadavky:** ...........

|  |  |  |
| --- | --- | --- |
|  | **Potrebné informácie** | **Vysvetlenie** |
| **1.** **Obmedzenia** | Zoznam obmedzení, ktoré zabraňujú dosiahnutie súladu s pôvodnou požiadavkou. | ........... |
| **2.** **Cieľ** | Stanoviť cieľ pôvodnej kontroly, identifikovať cieľ splnený kompenzačným riadením. | ........... |
| **3.** **Identifikácia rizika** | Identifikovať dodatočné riziká vyplývajúce z nedostatku pôvodnej kontroly. | ........... |
| **4.** **Stanovenie kompenzačného riadenia** | Stanovenie kompenzačného riadenia a vysvetlenie, akým spôsobom rieši cieľe pôvodnej kontroly a prípadné zvýšené riziká, ak existujú. | ........... |
| **5.** **Overenie kompenzačného riadenia** | Vysvetlenie spôsobu overenia a testovania kompenzačného riadenia. | ........... |
| **6.** **Údržba** | Stanovenie zavedených postupov a riadiacich prvkov na udržanie kompenzačného riadenia. | ........... |

**Dodatok C:** **Vysvetlenie pojmu „nevzťahuje sa"**

*V prípade zaškrtnutia stĺpca N/A („nevzťahuje sa") v dotazníku, použite hárok na vysvetlenie, prečo sa táto požiadavka nevzťahuje na vašu organizáciu.*

|  |  |
| --- | --- |
| **Požiadavka** | **Odôvodnenie, prečo sa požiadavka nevzťahuje** |
| *Príklad:* | |
| 3.4 | Údaje držiteľov kariet sa neukladajú elektronicky | |
| ........... | ........... |
| ........... | ........... |
| ........... | ........... |
| ........... | ........... |
| ........... | ........... |
| ........... | ........... |
| ........... | ........... |
| ........... | ........... |
| ........... | ........... |
| ........... | ........... |
| ........... | ........... |
| ........... | ........... |
| ........... | ........... |
| ........... | ........... |
| ........... | ........... |
| ........... | ........... |

**Dodatok D:** **Vysvetlenie požiadaviek „netestované"**

*V prípade zaškrtnutia stĺpca „netestované") v dotazníku, použite hárok na vysvetlenie, prečo táto požiadavka nebola skúmaná ako súčasť hodnotenie.*

|  |  |  |
| --- | --- | --- |
| **Požiadavka** | **Uvedenie častí požiadavky, ktoré neboli testované** | **Odôvodnenie, prečo požiadavky neboli testované** |
| *Príklady:* | | |
| *Požiadavka 12* | *Bod 12.2 bola jediná testovaná požiadavka. Všetky ostatné body požiadavky 12 neboli testované.* | *Toto hodnotenie pokrýva len požiadavky uvedené v míľniku 1 Prioritného prístupu* |
| *Požiadavky 1-8, 10-12* | *V tomto hodnotení bola skúmaná len požiadavka 9. Všetky ostatné požiadavky boli vylúčené.* | *Spoločnosť je poskytovateľom fyzického hosťovania (CO-LO) a len fyzické bezpečnostné prvky boli posudzované v rámci tohto hodnotenia.* |
| ........... | ........... | ........... |
| ........... | ........... | ........... |
| ........... | ........... | ........... |
| ........... | ........... | ........... |
| ........... | ........... | ........... |
| ........... | ........... | ........... |
| ........... | ........... | ........... |
| ........... | ........... | ........... |
| ........... | ........... | ........... |
| ........... | ........... | ........... |
| ........... | ........... | ........... |
| ........... | ........... | ........... |
| ........... | ........... | ........... |
| ........... | ........... | ........... |
| ........... | ........... | ........... |

**Odsek 3:** **Podrobnosti o overovaní a osvedčovaní**

|  |
| --- |
| **Časť 3. Overenie PCI DSS** |

**Tento AOC vychádza z výsledkov zaznamenaných v SAQ D (sekcia 2) zo dňa (*dátum dokončenia SAQ*).**

Na základe výsledkov zaznamenaných v SAQ D, signatári uvedení v častiach 3b-3d, podľa potreby, potvrdzujú nasledujúci súlad subjektu uvedeného v časti 2 tohto dokumentu: (***zaškrtnite jedno***):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Súlad:** Všetky sekcie PCI DSS SAQ sú dokončené, všetky otázky zodpovedané kladne, čo dáva výsledok **SÚLAD**, a preto (*meno spoločnosti obchodníka*) preukázal plný súlad s PCI DSS. | | | |
|  | **Nesúlad:** Nie všetky sekcie PCI DSS SAQ sú dokončené alebo nie všetky otázky zodpovedané kladne, čo dáva **NESÚLAD**, a preto (*meno spoločnosti obchodníka*) nepreukázal plný súlad s PCI DSS.  **Cieľový dátum** na dosiahnutie súladu:  Od subjektu, ktorý predložil tento formulár so stavom Nesúlad, može byť požadované, aby dokončil akčný plán 4 v časti 4 tohto dokumentu. *Obráťte sa na svojho nadobúdateľa alebo kartovú spoločnosť pred vyplnením časti 4.* | | | |
|  | **Súlad s právnou výnimkou:** Jedna alebo viacero požiadaviek boli zaškrtnuté ako „Nie" v dôsledku zákonných obmedzení, ktoré zabránili splniť tieto požiadavky. Táto možnosť vyžaduje dodatočnú kontrolu zo strany nadobúdateľa alebo kartovej spoločnosti.  *Ak zaškrtnuté, vykonajte nasledovné:* | | | |
|  | **Dotknutá požiadavka** | **Podrobný opis zákonných obmedzení, ktoré zabraňujú dosiahnutie súladu s požiadavkou** |  |
| ........... | ........... |  |
| ........... | ........... |
|  | | |

|  |  |
| --- | --- |
| **Časť 3a. Potvrdenie stavu** | |
| **Podpis zodpovedných osôb:**  ***(hodiace sa zaškrtnite)*** | |
|  | Samohodnotiaci dotazník D PCI DSS, verzia (verzia SAQ) bol dokončený v zmysle uvedených pokynov. |
|  | Všetky informácie v rámci vyššie uvedeného SAQ a táto atestácia spravodlivo predstavujú výsledky hodnotenia vo všetkých významných aspektoch. |
|  | So svojim dodávateľom platobnej aplikácie som potvrdil, že môj platobný systém neukladá citlivé autentifikačné údaje po autentifikácií. |
|  | Prečítal som si PCI DSS a beriem na vedomie, že musím neustále dodržiavať požiadavky PCI DSS, ktoré sa vzťahujú na moje prostredie. |
|  | V prípade zmeny môjho prostredia beriem na vedomie, že musím prehodnotiť moje prostredie a implementovať dodatočné požiadavky PCI DSS, ktoré sa na neho môžu vzťahovať. |
| **Časť 3a. Potvrdenie stavu** (pokračovanie) | |
|  | V priebehu tohto hodnotenia nebol nájdený žiaden dôkaz o uchovávaných celých trasovacích údajoch alebo údajoch CAV2, CVC2, CID alebo CVV2 alebo PIN po autentifikácií transakcie na ŽIADNOM systéme posudzovanom v rámci tohto hodnotenia. |
|  | Kontroly ASV boli dokončené so schváleným skenovaním dodávateľa PCI SSC (*názov ASV*) |

|  |  |
| --- | --- |
| **Časť 3b. Atestácia obchodníka** | |
|  | |
| *Podpis výkonného riaditeľa obchodníka*  | *Dátum:* ........... |
| *Meno výkonného riaditeľa obchodníka:* ........... | *Titul:* ........... |

|  |  |  |
| --- | --- | --- |
| **Časť 3c. Informácie o oprávnenom overovateľovi bezpečnosti (QSA) (podľa potreby)** | | |
| V prípade, že do tohto hodnotiaceho procesu bol zapojený QSA, uveďte jeho úlohu: | ........... | |
|  | | |
| *Podpis riadne splnomocneného zástupcu spoločnosti QSA*  | | *Dátum:*  ........... |
| *Meno riadne splnomocneného zástupcu:* ........... | | *Spoločnosť QSA:* ........... |

|  |  |
| --- | --- |
| **Časť 3d. Zapojenie interného overovateľa bezpečnosti (ISA) (podľa potreby)** | |
| V prípade, že do tohto hodnotiaceho procesu bol zapojený ISA, uveďte meno tohto zamestnanca a jeho úlohu: | ........... |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Časť 4. Akčný plán pre nevyhovujúce požiadavky** | | | | |
| Vyberte vhodnú akciu pre „Súlad s požiadavkami PCI DSS" pre každú požiadavku V prípade, že na niektorú z požiadaviek odpoviete „Nie", môže byť od vás požadované uviesť dátum, kedy vaša spoločnosť očakáva dosiahnutie súladu s touto požiadavkou a krátky popis krokov, ktoré podniknete na jej splnenie.  *Obráťte sa na svojho nadobúdateľa alebo kartovú spoločnosť pred vyplnením časti 4.* | | | | |
| **Požiadavka PCI DSS** | **Popis požiadavky** | **Súlad s požiadavkami PCI DSS**  (Vyberte jedno) | | **Dátum a iné opravné kroky** (Ak ste vybrali „nie" k akejkoľvek požiadavke) |
| **ÁNO** | **NIE** |
| 1 | Inštalácia a uchovávanie firewallovej konfigurácie na ochranu údajov držiteľov kariet |  |  | ........... |
| 2 | Nepoužívanie predvolených nastavení systémových hesiel a iných bezpečnostných parametrov |  |  | ........... |
| 3 | Ochrana uložených údajov držiteľa karty |  |  | ........... |
| 4 | Šifrovanie prenosových údajov držiteľa karty pri použití v otvorených verejných sietiach |  |  | ........... |
| 5 | Ochrana všetkých systémov voči škodlivým softvérom a pravidelná aktualizácia antivírusových programov alebo softvéru |  |  | ........... |
| 6 | Vytváranie a udržiavanie bezpečných systémov a aplikácií |  |  | ........... |
| 7 | Obmedzenie prístupu k údajom držiteľa karty v nevyhnutnom rozsahu |  |  | ........... |
| 8 | Identifikácia a autentifikácia prístupu k systémovým komponentom |  |  | ........... |
| 9 | Obmedzenie fyzického prístupu k údajom držiteľa karty |  |  | ........... |
| 10 | Sledovanie a monitorovanie každého prístupu do sieťových zdrojov a údajov držiteľa karty |  |  | ........... |
| 11 | Pravidelné testovanie bezpečnostných systémov a procesov |  |  | ........... |
| 12 | Udržiavanie politiky, ktorá rieši bezpečnosť informácií všetkých pracovníkov |  |  | ........... |
| Dodatok A2 | Dodatočné požiadavky PCI DSS pre subjekty používajúce SSL/staršie TLS |  |  | ........... |

