

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

**Obchodníci s platnou aplikáciou pripojenou priamo na internet – nearchivujú údaje držiteľa platobnej karty**

**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"

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

**Úvod**

Systém SAQ C pre obchodníkov sa vzťahuje na obchodníkov, ktorí sú oprávnení využívať SAQ a ktorí nespĺňajú kritéria pre žiaden iný typ SAQ. Príklady takýto 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

Pričom množstvo organizácií vykonávajúcich SAQ C 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 C)
* 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 C 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 vzozname 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 C 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** |
| 1,2 | 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 | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |
| 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: |  |  |  |  |  |  |
| 1.3.4 | 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 | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |

***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 | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |
| 2.5 | 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 | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |

**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** |
|  | (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 | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |

***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 | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |

**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 | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |

***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 | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |
| 6.4.6 | 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 | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |

**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 | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |
| 7.1.2 | 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 | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |
| 7.2 | 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 | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |

***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 | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |
| 8.1.5 | (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 | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |
| 8.2.3 | (a) Sú užívateľské heslá obmedzené nasledovným spôsobom? Heslo musí mať najmenej sedem znakov Musí obsahovať ako číselné tak aj abecedné znakyPrípadne 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 | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |
| 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 | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |
| 8.8 | 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  | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |
| 9.5 | 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 | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |
| 9.6 | (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 | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |
| 9.8 | (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 | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |
|  | (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 | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |
| 9.9 | 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 | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |

**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** |
| 10.2 | Sú implementované automatizované kontrolné stopy pre všetky systémové komponenty na rekonštrukciu nasledujúcich udalostí: |  |  |  |  |  |  |
| 10.2.2 | Sú všetky činnosti vykonávané jednotlivcom s právami správcu? |  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 | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |
| 10.3 | 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 | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |
| 10.6 | 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 |  |  | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |
| (b) Sú vyššie uvedené záznamy a bezpečnostné udalosti kontrolované najmenej raz denne? |  Kontrola procesov Rozhovor s personálom | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |
| 10.6.2 |  |  | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |
|  | (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 |  |  | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |
|  | (b) Dochádza k sledovaniu výnimiek a anomálií?  |  Kontrola procesov Rozhovor s personálom | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |
| 10.7 |  |  | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |
| (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 | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |

***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 | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |
| 11.3.4 | 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 | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |
|  | (c) 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 | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |
| 11.5 | (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 | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |
|  | (b) 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 | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |

**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 | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |
| 12.3 | 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 | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |
| 12.3.5 | 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 | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |
| 12.3.8 | 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 | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |
| 12.4 | 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 | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |
| 12.5 | (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: |  |  |  |  |  |  |
| 12.5.3 | 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 | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |
| 12.6 | (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 | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |
| 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 | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |
| 12.10.1 | (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 | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |

**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 | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |

***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  |
| ........... | ........... |
| ........... | ........... |
| ........... | ........... |
| ........... | ........... |
| ........... | ........... |
| ........... | ........... |
| ........... | ........... |
| ........... | ........... |
| ........... | ........... |
| ........... | ........... |
| ........... | ........... |
| ........... | ........... |
| ........... | ........... |
| ........... | ........... |
| ........... | ........... |
| ........... | ........... |

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

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

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

Na základe výsledkov zaznamenaných v SAQ C, 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 | [ ]  | [ ]  | ........... |

