

Odvětví platebních karet (PCI)

Standard bezpečnosti dat (DSS)  
  
Dotazník pro sebehodnocení D   
a Osvědčení o shodě

pro obchodníky

Všichni ostatní obchodníci způsobilí k SAQ

Pro užití s PCI DSS verze 3.2.1  
  
Revize 1.0.

Červen 2018

# Změny dokumentu

| **Datum** | **Verze** | **Revize SAQ** | **Popis** |
| --- | --- | --- | --- |
| říjen 2008 | 1.2 |  | Sjednocení obsahu dokumentu s novým PCI DSS v. 1.2 a implementování menší změny zaznamenané od vydání původní verze v. 1.1. |
| říjen 2010 | 2.0 |  | Sjednocení obsahu dokumentu s požadavky nového PCI DSS v. 2.0 a testovacími postupy. |
| únor 2014 | 3.0 |  | Sjednocení obsahu dokumentu s požadavky nového PCI DSS v. 3.0, testovacími postupy a zahrnutí další možnosti odpovědi. |
| duben 2015 | 3.1 |  | Aktualizace dokumentu za účelem sjednocení s verzí PCI DSS 3.1. Detaily změn PCI DSS jsou k dispozici v dokumentu Summary of Changes from PCI DSS Version 3.0 to 3.1 (PCI DSS – Seznam změn PCI DSS verze 3.0 do 3.1). |
| červenec 2015 | 3.1 | 1.1 | Aktualizace za účelem odstranění odkazů na „osvědčené postupy“ před 30. červnem 2015 a odstranění možnosti v2 pro požadavek 11.3 |
| duben 2016 | 3.2 | 1.0 | Aktualizace dokumentu za účelem sjednocení s verzí PCI DSS v3.2. Detaily změn PCI DSS jsou k dispozici v dokumentu Summary of Changes from PCI DSS Version 3.1 to 3.2. (PCI DSS – Seznam změn PCI DSS verze 3.1 do 3.2). |
| leden 2017 | 3.2 | 1.1 | Aktualizace číslování verzí v rámci shody s ostatními SAQ |
| červen 2018 | 3.2.1 | 1.0 | Aktualizace dokumentu za účelem sjednocení s verzí PCI DSS v3.2.1. Detaily změn PCI DSS jsou k dispozici v dokumentu Summary of Changes from PCI DSS Version 3.2 to 3.2.1 (PCI DSS – Seznam změn PCI DSS verze 3.2 do 3.2.1). |

# Obsah

[Změny dokumentu 1](#_Toc13755732)

[Obsah 2](#_Toc13755733)

[Než začnete 3](#_Toc13755734)

[PCI DSS – Postup vyplnění sebehodnotícího dotazníku 3](#_Toc13755735)

[Jak porozumět sebehodnotícímu dotazníku 4](#_Toc13755736)

[Očekávané testování 4](#_Toc13755737)

[Vyplnění sebehodnotícího dotazníku 5](#_Toc13755738)

[Postup v případech, kdy nelze aplikovat určité specifické požadavky 5](#_Toc13755739)

[Pochopení rozdílu mezi „Nevztahuje se (N/A)“ a „Netestováno“ 6](#_Toc13755740)

[Výjimky ze zákona 6](#_Toc13755741)

[Oddíl 1: Informace o hodnocení 7](#_Toc13755742)

[Oddíl 2: Dotazník pro sebehodnocení D pro obchodníky 10](#_Toc13755743)

[Vybudovat a udržovat bezpečné sítě a systémy 10](#_Toc13755744)

[Požadavek 1: Instalovat a udržovat konfiguraci firewallů za účelem ochrany dat držitelů karet 10](#_Toc13755745)

[Požadavek 2: Nepoužívat výchozí nastavení od dodavatele pro systémová hesla a jiné bezpečnostní parametry 14](#_Toc13755746)

[Ochrana dat držitelů karet 19](#_Toc13755747)

[Požadavek 3: Chránit uchovávaná data držitelů karet 19](#_Toc13755748)

[Požadavek 4: Zašifrovat přenos dat držitelů karet po otevřených veřejných sítích 25](#_Toc13755749)

[Udržování programu kontroly zranitelnosti 27](#_Toc13755750)

[Požadavek 5: Chránit všechny systémy proti malware a pravidelně aktualizovat antivirový software nebo programy 27](#_Toc13755751)

[Požadavek 6: Vyvíjet a udržovat bezpečné systémy a aplikace 29](#_Toc13755752)

[Zavedení silných opatření pro řízení přístupu 36](#_Toc13755753)

[Požadavek 7: Omezit přístup k datům držitelů karet jen podle oprávněné potřeby 36](#_Toc13755754)

[Požadavek 8: Identifikovat a autentizovat přístup k systémovým komponentám 38](#_Toc13755755)

[Požadavek 9: Omezit fyzický přístup k datům držitelů karet 43](#_Toc13755756)

[Pravidelné monitorování a testování sítí 50](#_Toc13755757)

[Požadavek 10: Sledovat a monitorovat všechny přístupy k síťovým zdrojům a datům držitelů karet 50](#_Toc13755758)

[Požadavek 11: Pravidelně testovat bezpečnostní systémy a procesy 55](#_Toc13755759)

[Udržování politiky informační bezpečnosti 62](#_Toc13755760)

[Požadavek 12: Udržovat politiku zaměřenou na informační bezpečnost pro všechen personál 62](#_Toc13755761)

[Příloha A1: Dodatečné požadavky PCI DSS na poskytovatele sdíleného hostingu 68](#_Toc13755762)

[Příloha A2: Dodatečné požadavky na subjekty používající SSL/dříve TLS pro transakce za fyzické přítomnosti platební karty u POS POI terminálových připojení 68](#_Toc13755763)

[Příloha A3: Dodatečné hodnocení pro specifické subjekty DESV (Designated Entities Supplemental Validation) 68](#_Toc13755764)

[Příloha B: Pracovní list náhradního řešení 69](#_Toc13755765)

[Příloha C: Vysvětlení pro „Nevztahuje se”(N/A) 70](#_Toc13755766)

[Příloha D: Vysvětlení Požadavku „Netestováno” 71](#_Toc13755767)

[Oddíl 3: Validace a podrobnosti o osvědčení 72](#_Toc13755768)

# Než začnete

SAQ D pro obchodníky použijí všichni obchodníci způsobilí k vyplnění SAQ, pro které se nehodí kritéria ostatních typů dotazníků SAQ. Příklady obchodníků, kteří by měli použít SAQ D, mohou být následující (výčet neobsahuje všechny příklady obchodníků):

* E-commerce obchodníci, kteří přijímají data držitelů karet na svých webových stránkách;
* Obchodníci s elektronickým úložištěm dat držitelů karet;
* Obchodníci, kteří neuchovávají data držitelů karet, ale nesplňují kritéria pro jiný typ dotazníku;
* Obchodníci, kteří mohou splňovat kritéria pro jiný typ dotazníku, ale na jejichž prostředí lze aplikovat i další požadavky PCI DSS.

Zatímco mnoho společností vyplňujících SAQ D bude muset deklarovat shodu se všemi požadavky PCI DSS, některé společnosti mající vlastní specifický obchodní model mohou zjistit, že některé požadavky nejsou pro ně použitelné. Podívejte se na následující návod, který obsahuje informace o vyjmutí konkrétních specifických požadavků.

## PCI DSS – Postup vyplnění sebehodnotícího dotazníku

1. Nalezněte příslušný SAQ pro vaše prostředí – více naleznete v dokumentu Návody a pokyny k dotazníku pro vlastní hodnocení (*Self-Assessment Questionnaire Instructions and Guidelines)* na webových stránkách PCI SSC.
2. Potvrďte, že vaše prostředí je správně definováno a splňuje kritéria způsobilosti pro SAQ, který je použit.
3. Posuďte, zda je vaše prostředí v souladu s příslušnými požadavky PCI DSS.
4. Vyplňte všechny části tohoto dokumentu:

* Oddíl 1 (Část 1 & 2 AOC) – Informace o hodnocení a Shrnutí.
* Oddíl 2 – PCI DSS sebehodnotící dotazník (SAQ D)
* Oddíl 3 (Část 3 & 4 AOC) – validace a podrobnosti o osvědčení, akční plán pro ty požadavky, které nebyly splněny (v případě potřeby)

1. Předložte Dotazník SAQ a Osvědčení o shodě (Attestation of Compliance) spolu s další požadovanou dokumentací – jako je například „ASV scan report“ – vaší zpracovatelské bance, kartovým asociacím nebo dalším žadatelům.

## Jak porozumět sebehodnotícímu dotazníku

Otázky obsažené ve sloupci „PCI DSS Otázka“ v tomto sebehodnotícím dotazníku jsou založeny na požadavcích PCI DSS.

Na pomoc s procesem hodnocení slouží další zdroje, které poskytují návod k PCI DSS požadavkům a k vyplnění sebehodnotícího dotazníku. Přehled některých zdrojů je uveden níže:

|  |  |
| --- | --- |
| **Dokument** | **Zahrnuje:** |
| PCI DSS  Požadavky a postupy posouzení bezpečnosti Standardu bezpečnosti dat v odvětví platebních karet  *(PCI Data Security Standard Requirements and Security Assessment Procedures)* | * Návod pro stanovení rozsahu * Pokyny k záměru všech PCI DSS požadavků * Podrobnosti testovacích postupů * Pokyny týkající se Náhradních řešení |
| Návody a pokyny k dotazníku pro sebehodnocení SAQ  *(Self-Assessment Questionnaire Guidelines and Instructions)* | * Informace o všech SAQ a jejich kritériích způsobilosti * Jak určit, který SAQ je správný pro vaši společnost |
| Slovník pojmů, zkratek a akronymů PCI DSS a PCI PA-DSS  *(PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms)* | * Popis a definice pojmů používaných v PCI DSS a v sebehodnotících dotaznících |

Tyto a další zdroje jsou k naleznutí na webových stránkách PCI SSC ([www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)). Společnosti jsou nabádány, aby prozkoumaly PCI DSS a další podpůrné dokumenty před začátkem vlastního hodnocení.

### Očekávané testování

Instrukce, které jsou poskytnuté ve sloupci „Očekávané testování“, jsou založeny na testovacích postupech v PCI DSS a obsahují tzv. high-level popis testovacích postupů, které by měly být vykonány za účelem ověření, zda byl konkrétní požadavek splněn. Plné znění testovacích postupů pro každý požadavek je k naleznutí v PCI DSS.

## Vyplnění sebehodnotícího dotazníku

Pro každou otázku existuje výběr odpovědí naznačující stav Vaší společnosti týkající se daného požadavku. ***Může být vybrána pouze jedna odpověď pro každou otázku***.

Popis významu každé odpovědi je poskytnut v této tabulce:

| **Odpověď** | **Popis** |
| --- | --- |
| **Ano** | Očekávané testování bylo provedeno a všechny části požadavku byly splněny. |
| **Ano s CCW** (Pracovní list náhradního řešení) | Očekávané testování bylo provedeno a všechny části požadavků byly splněny s pomocí náhradního řešení.  Všechny odpovědi v tomto sloupci je zapotřebí vyplnit v Pracovní list náhradního řešení (CCW) v příloze B dotazníku (SAQ).  Informace o využití náhradního řešení a návod, jak vyplnit pracovní list, jsou poskytnuty v PCI DSS. |
| **Ne** | Některé nebo žádné části požadavku nebyly splněny nebo jsou v procesu implementace nebo vyžadují další testování předtím, než bude známo, jestli jsou již implementovány. |
| **N/A**  (“Nevztahuje se“) | Požadavky, které se nevztahují na vaše prostředí. (Více k nalezení v: *„Guidance for Non-Applicability of Certain, specific Requirements below for examples“)*  Všechny odpovědi v tomto sloupci vyžadují další vysvětlení v příloze C dotazníku SAQ. |
| **Netestováno** | Požadavek nebyl zahrnut do posouzení v tomto ohodnocení a nebyl testován *(příklady rozdílů mezi N/A a Netestováno, kdy jaký požadavek má být použitý jsou k naleznutí dále).*  Všechny odpovědi v tomto sloupci vyžadují doplňující vysvětlení v příloze D dotazníku SAQ. |

## Postup v případech, kdy nelze aplikovat určité specifické požadavky

Zatímco mnohé organizace vyplňující SAQ D budou muset potvrdit shodu se všemi požadavky PCI DSS, některé subjekty se specifickými obchodními modely mohou zjistit, že některé požadavky nelze aplikovat. Například od společnosti, která nevyužívá bezdrátové technologie ve své síti, se neočekává, že bude dokazovat shodu s požadavky, které se týkají právě bezdrátové technologie. Podobně organizace, která nikdy neuchovává data držitelů karet v elektronické podobě, nemusí vyhodnocovat shodu s požadavky týkajícími se bezpečného uchovávání dat držitelů karet (např. požadavek 3.4).

Příklady požadavků se specifickým uplatněním mohou být:

* Otázky týkající se zabezpečení bezdrátové technologie (jako např. požadavky 1.2.3, 2.1.1 a 4.1.1) je třeba zodpovědět pouze v případech, kdy se tyto technologie vyskytují kdekoli ve vaší síti. Vezměte prosím na vědomí, že Požadavek 11.1 (využití procesů k identifikaci neautorizovaných přístupových bodů) musí být zodpovězen i v případě, že nevyužíváte bezdrátové technologii ve vaší síti, protože postup odhalí jakékoli kolizní či neschválená zařízení, která mohla být nainstalována bez Vašeho vědomí.
* Otázky týkající se vývoje aplikací a bezpečného programování (Požadavky 6.3 a 6.5) by měly být zodpovězeny pouze v případě, pokud Vaše organizace vyvíjí vlastní aplikace.
* Otázky vztahující se k Požadavkům 9.1.1 a 9.3 musí vyplnit pouze subjekty, které disponují prostory s tzv. „citlivými oblastmi“. Citlivou oblastí se rozumí datové centrum, serverovna nebo jakákoli oblast, kde jsou umístěny systémy, ve kterých jsou uchovávány, zpracovávány nebo přenášeny údaje držitelů platebních karet. Do citlivých oblastí nejsou zahrnuta místa, kde jsou umístěny pouze POS terminály, jako pokladny v obchodě, ale patří tam zázemí obchodníka, kde jsou servery s uchovávanými daty držitelů platebních karet a úložiště velkého objemu dat držitelů platebních karet.

V případě, že některý z požadavků nelze aplikovat na vaše prostředí, vyberte u daného požadavku možnosti „N/A“ a vyplňte „Explanation of Non-Applicability“ (Vysvětlení pro „Nevztahuje se“) v odpovídající části formuláře Přílohy C.

### Pochopení rozdílu mezi „Nevztahuje se (N/A)“ a „Netestováno“

U požadavků, které obchodník považuje za N/A, musí dojít k prověření této skutečnosti. Příkladem mohou být výše uvedené Požadavky 1.2.3, 2.1.1 a 4.1.1 týkající se bezdrátových technologií, kdy organizace musí před vyplněním N/A nejprve ověřit, že žádná bezdrátová technologie není používána v jejím prostředí dat držitelů karet (CDE) nebo není propojena s prostředím dat držitelů karet (CDE). Jakmile dojde k tomuto ověření, organizace může vyplnit „N/A“ u odpovídajících požadavků.

V případě, kdy bude rozhodnuto o nezahrnutí konkrétních požadavků do hodnocení bez ohledu na skutečnost, zda jsou tyto požadavky aplikovatelné, bude u nich zaškrtnuto „Netestováno“. Příklady, kdy mohou takové situace nastat, jsou následující:

* Zpracovatelská banka může požadovat po organizaci prověření sady požadavků, např. využití principu Prioritního přístupu k prověření určitých milníků.
* Organizace by ráda prověřila novou bezpečnostní kontrolu, která má vliv pouze na podmnožinu požadavků, např. zavedení nové metodologie šifrování, dle požadavků 2, 3 a 4.
* Poskytovatel služeb může nabízet pouze službu, která pokrývá omezený počet PCI DSS požadavků, např. poskytovatel úložiště tištěných účtenek prověřuje pouze dodržení zajištění fyzické bezpečnosti úložiště dle požadavku PCI DSS 9.

V těchto případech se společnost rozhodne prověřit pouze určité požadavky bez ohledu na skutečnost, že se na její prostředí mohou vztahovat i další požadavky.

## Výjimky ze zákona

V případě, že vaše společnost podléhá právním omezením, které znemožňují dodržování požadavků PCI DSS, uveďte u daného požadavku „No“ a vyplňte odpovídající osvědčení v Části 3.

# Oddíl 1: Informace o hodnocení

***Pokyny pro předložení***

Tento dokument musí být vyplněn jako deklarace výsledků sebehodnocení obchodníka podle *Požadavků a postupů posouzení bezpečnosti Standardu bezpečnosti dat v odvětví platebních karet (PCI DSS)*. Vyplňte všechny části: Obchodník je zodpovědný za to, aby každá část byla vyplněna relevantními stranami. Kontaktujte acquirera (zpracovatelskou banku obchodníka) nebo kartové společnosti, aby stanovily reporting a způsob předložení.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Část 1. Informace o obchodníkovi a společnosti kvalifikovaných hodnotitelů bezpečnosti** | | | | | | |
| **Část 1a. Informace o společnosti obchodníka** | | | | | | |
| Název společnosti: |  | | Obch. jméno: |  | | |
| Kontaktní jméno: |  | | Funkce: |  | | |
| Jméno interního auditora (ISA): |  | | Funkce: |  | | |
| Telefon: |  | | E-mail: |  | | |
| Sídlo společnosti: |  | | Město: |  | | |
| Stát / kraj: |  | Země: |  | | PSČ: |  |
| URL: |  | | | | | |
|  | | | | | | |
| **Část 1b. Informace o společnosti kvalifikovaných hodnotitelů bezpečnosti QSA (lze-li aplikovat)** | | | | | | |
| Název společnosti: |  | | | | | |
| Kontaktní jméno hlavního hodnotitele: |  | | Funkce: |  | | |
| Telefon: |  | | E-mail: |  | | |
| Sídlo společnosti: |  | | Město: |  | | |
| Stát / kraj: |  | Země: |  | | PSČ: |  |
| URL: |  | | | | | |

|  |  |  |
| --- | --- | --- |
| **Část 2. Shrnutí:** | | |
| **Část 2a. Druh podnikání obchodníka (zatrhněte vše, co lze aplikovat):** | | |
| Maloobchod  Telekomunikace  Obchody a supermarkety | | |
| Pohonné hmoty  E-Commerce  Písemné / telefonické objednávky (MOTO) | | |
| Jiné (specifikujte): | | |
| Který typ/typy platebních kanálů je/jsou využívány ve Vašem podnikání?  Písemná / telefonická objednávka (MOTO)  E-Commerce  Přítomnost platební karty (face-to-face) | | Na které typy platebních kanálů se vztahuje tento dotazník SAQ?  Písemná / telefonická objednávka (MOTO)  E-Commerce  Přítomnost platební karty (face-to-face) |
| ***Poznámka:*** *Využívá-li vaše organizace platební kanál či proces, na který se nevztahuje tento dotazník SAQ, zkonzultujte se svou acquirerskou bankou nebo kartovou asociací ověření pro ostatní kanály.* | | |
|  | | |
| **Část 2b. Popis typu podnikání s ohledem na platební karty** | | |
| Jak a v jakém množství při Vašem podnikání uchováváte, zpracováváte a/nebo přenášíte data držitelů karet? |  | |

|  |  |  |
| --- | --- | --- |
| **Část 2c. Lokace (umístění)** | | |
| Seznam všech typů zařízení a shrnutí všech lokací zahrnutých v PCI DSS posudku (např. prodejny, firemní kanceláře, datová centra, call centra atd.) | | |
| **Druh zařízení** | **Počet zařízení tohoto typu** | **Umístění zařízení (město, země)** |
| Příklad: maloobchodní prodejny | 3 | Boston, MA, USA |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Část 2d. Platební aplikace** | | | | |
| Používá společnost jednu nebo více platebních aplikací?  Ano  Ne | | | | |
| Poskytněte následující informace týkající se platebních aplikací, které vaše společnost používá: | | | | |
| **Název platební aplikace** | **Číslo verze** | **Dodavatel aplikace** | **Je aplikace na seznamu PA-DSS?** | **Expirace PA-DSS (je-li to relevantní)** |
|  |  |  | Ano  Ne |  |
|  |  |  | Ano  Ne |  |
|  |  |  | Ano  Ne |  |
|  |  |  | Ano  Ne |  |
|  |  |  | Ano  Ne |  |

|  |  |  |
| --- | --- | --- |
| **Část 2e. Popis prostředí** | | |
| Poskytněte „**high-level**“ popis vašeho prostředí, na které se vztahuje toto hodnocení.  *Například:*   * *Spojení do a z prostředí dat držitelů karet (CDE)* * *Kritické komponenty systému v rámci CDE, jako například POS zařízení, databáze, webový server atd., a další nezbytné komponenty, podle potřeby.* |  | |
| Používá Vaše společnost síťovou segmentaci za účelem ovlivnění rozsahu prostředí PCI DSS?  *(Viz Pokyny týkající se části „Síťová segmentace“ v PCI DSS)* | | Ano  Ne |

|  |  |  |
| --- | --- | --- |
| **Část 2f. Poskytovatelé služeb – třetí strany** | | |
| Používá Vaše společnost kvalifikovaného integrátora či prodejce (QIR)? | | Ano  Ne |
| **V případě, že Ano:** | | |
| **Jméno QIR společnosti:** |  | |
| **Jméno zástupce QIR společnosti:** |  | |
| **Popis poskytovaných služeb QIR:** |  | |

|  |  |  |
| --- | --- | --- |
| Sdílí Vaše společnost kartová data s třetími stranami – poskytovateli služeb (např. kvalifikovaní integrátoři a prodejci (QIR), platební brány, zpracovatelé plateb, poskytovatelé platebních služeb (PSP), poskytovatelé webového hostingu, agentury poskytující letecké rezervace, společnosti zabývající se věrnostním programem apod.)? | | Ano  Ne |
| **V případě, že Ano:** | | |
| **Jméno poskytovatele služeb:** | **Popis poskytovaných služeb:** | |
|  |  | |
|  |  | |
|  |  | |
|  |  | |
| ***Poznámka:*** *Požadavek 12.8 se vztahuje na všechny subjekty v tomto seznamu.* | | |

# Oddíl 2: Dotazník pro sebehodnocení D pro obchodníky

|  |
| --- |
| ***Poznámka:*** *Následující otázky jsou očíslovány podle Požadavků a testovacích postupů PCI DSS, jak jsou definovány v dokumentu Požadavky a postupy posouzení bezpečnosti Standardu bezpečnosti dat v odvětví platebních karet.* |

**Datum vyplnění:**

## Vybudovat a udržovat bezpečné sítě a systémy

### Požadavek 1: Instalovat a udržovat konfiguraci firewallů za účelem ochrany dat držitelů karet

| **PCI DSS Otázka** | | **Očekávané Testování** | **Odpověď**  **(zaškrtněte jednu odpověď pro každou otázku)** | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ANO** | **ANO s „CCW“** | | **NE** | **N/A** | **Netestováno** |
| 1.1 | Jsou konfigurační standardy pro routery a firewally zavedeny, implementovány a zahrnují následující? |  | | | | | | |
| 1.1.1 | Existuje formální proces schvalování a testování všech síťových připojení a změn konfigurací firewallů a routerů? | * Zkontrolujte dokumentovatelné procesy * Rozhovor s personálem * Sledujte síťové konfigurace |  |  | |  |  |  |
| 1.1.2 | (a) Existuje aktuální diagram sítě identifikující všechna spojení mezi prostředím dat držitelů karet a dalšími sítěmi, včetně bezdrátových sítí? | * Zkontrolujte aktuální síťový diagram * Sledujte síťové konfigurace |  |  | |  |  |  |
| (b) Je diagram udržován aktuální? | * Rozhovor s odpovědným personálem |  |  | |  |  |  |
| 1.1.3 | (a) Existuje aktuální diagram zobrazující všechny toky dat držitelů karet napříč systémy a sítěmi? | * Zkontrolujte diagram datových toků * Sledujte síťové konfigurace |  |  | |  |  |  |
| (b) Existuje proces zajištující, že diagram je aktuální? | * Rozhovor s personálem |  |  | |  |  |  |
| 1.1.4 | (a) Jsou požadavky na firewall na každém internetovém připojení a mezi každou demilitarizovanou zónou (DMZ) a zónou vnitřní sítě? | * Zkontrolujte konfigurace firewallových standardů * Sledujte síťové konfigurace k ověření, zda je aplikován firewall |  |  | |  |  |  |
|  | (b) Je aktuální síťový diagram konzistentní s konfiguračními standardy firewallů? | * Porovnejte firewallová konfigurační pravidla s aktuálním síťovým diagramem |  |  | |  |  |  |
| 1.1.5 | Jsou skupiny, role a odpovědnosti pro správu síťových komponent přiřazeny a dokumentovány ve standardech firewallové a routerové konfigurace? | * Zkontrolujte firewallové a routerové konfigurační standardy * Rozhovor s personálem |  |  | |  |  |  |
| 1.1.6 | (a) Zahrnují konfigurační standardy firewallů a routerů dokumentovaný seznam všech služeb, protokolů a portů a jsou všechny zdůvodněny? | * Zkontrolujte firewallové a routerové konfigurační standardy |  |  | |  |  |  |
| (b) Jsou známy všechny nezabezpečené služby, protokoly a porty? Jsou dokumentovány všechna bezpečnostní opatření pro každou službu? | * Zkontrolujte firewallové a routerové konfigurační standardy * Přezkoumejte firewallové a routerové konfigurační standardy |  |  | |  |  |  |
| 1.1.7 | (a) Obsahují konfigurační standardy firewallů a routerů požadavek na přezkum těchto standardů a to nejméně každých šest měsíců? | * Zkontrolujte firewallové a routerové konfigurační standardy |  |  | |  |  |  |
| (b) Jsou firewallová a routerová pravidla revidována nejméně každých šest měsíců? | * Přezkoumejte dokumentace revizí firewallu |  |  | |  |  |  |
| 1.2 | Je vytvořená firewallová a routerová konfigurace, která omezuje připojení mezi nedůvěryhodnými sítěmi a jakýmikoliv systémovými komponentami v prostředí dat držitelů karet?  ***Poznámka****: „Nedůvěryhodná síť je jakákoliv síť, která je externí pro sítě náležející posuzovanému subjektu a/nebo která se vymyká subjektu z možností kontroly nebo řízení.* |  | | | | | | |
| 1.2.1 | (a) Jsou omezeny příchozí i odchozí přenosy na ty, které jsou nezbytné pro prostředí dat držitelů karet? | * Zkontrolujte firewallové a routerové konfigurační standardy * Přezkoumejte firewallové a routerové konfigurace |  |  | |  |  |  |
|  | (b) Jsou další příchozí a odchozí přenosy odmítnuty; například s použitím příkazu „zakázat všechno“ nebo implicitním odmítnutím po příkazu „povolit“? | * Zkontrolujte firewallové a routerové konfigurační standardy * Přezkoumejte firewallové a routerové konfigurace |  |  | |  |  |  |
| 1.2.2 | Jsou konfigurační standardy routerů zabezpečeny před neautorizovaným přístupem a synchronizovány – například běžící (nebo aktivní) konfigurace se shoduje s konfigurací při startu (start-up konfigurace, používaná při bootování, spouštění zařízení). | * Zkontrolujte firewallové a routerové konfigurační pravidla * Přezkoumejte firewallová a routerová konfigurační pravidla |  |  | |  |  |  |
| 1.2.3 | Jsou instalovány perimetrové (hraniční) firewally mezi všemi bezdrátovými sítěmi a prostředím dat držitelů karet a jsou konfigurovány tyto firewally tak, aby odmítaly nebo povolovaly (pokud jsou takové přenosy nutné z provozních důvodů) pouze autorizované přenosy mezi bezdrátovým prostředím a prostředím dat držitelů karet? | * Zkontrolujte firewallová a routerová konfigurační pravidla * Přezkoumejte routerové a firewallové konfigurace |  |  | |  |  |  |
| 1.3 | Je zakázán přímý veřejný přístup mezi internetem a jakoukoliv systémovou komponentou v prostředí dat držitelů karet, dle následujícího: |  | | | | | | |
| 1.3.1 | Je implementována demilitarizovaná zóna (DMZ), aby omezila příchozí přenosy jen na systémové komponenty, které poskytují autorizované veřejně přístupné služby, protokoly a porty? | * Přezkoumejte routerové a firewallové konfigurace |  |  |  | |  |  |
| 1.3.2 | Jsou omezeny příchozí internetové přenosy na IP adresy v rámci demilitarizované zóny (DMZ)? | * Přezkoumejte routerové a firewallové konfigurace |  |  |  | |  |  |
| 1.3.3 | Jsou implementována anti-spoofingová opatření k detekci a blokování padělaných zdrojových IP adres před vstupem do sítě? (Pozn. překl.: Spoofing je vytvoření falešné zdrojové IP adresy.)  (Například, blokování provozu pocházejícího z internetu prostřednictvím interní adresy) | * Přezkoumejte routerové a firewallové konfigurace |  |  | |  |  |  |
| 1.3.4 | Jsou odchozí přenosy z prostředí dat držitelů platebních karet na internet explicitně autorizovány? | * Přezkoumejte routerové a firewallové konfigurace |  |  | |  |  |  |
| 1.3.5 | Jsou do sítě připuštěna pouze „navázaná připojení“? | * Přezkoumejte routerové a firewallové konfigurace |  |  | |  |  |  |
| 1.3.6 | Jsou umístěny systémové komponenty uchovávající data držitelů karet (jako jsou databáze) do interní zóny sítě oddělené od DMZ a jiných nedůvěryhodných sítí? | * Přezkoumejte routerové a firewallové konfigurace |  |  | |  |  |  |
| 1.3.7 | (a) Jsou aplikovány metody, které zabraňují vyzrazení privátní IP adresy a informací o směrování (routing)?  ***Poznámka****: Metody k maskování IP adresování mohou zahrnovat, kromě jiného:*   * *Network Address Translation (NAT) (překlad síťových paketů)* * *Umístěním serverů, obsahujících data držitelů karet za proxy servery / firewally nebo schránky obsahu (content cages)* * *Odstranění nebo filtrování cest nabídky (reklamy) pro soukromé sítě, které využívají registrované adresování* * *Interní použití pomocí adresového prostoru RFC 1918 místo registrovaných adres.* | * Přezkoumejte routerové a firewallové konfigurace |  |  | |  |  |  |
|  | (b) Je autorizováno poskytnutí interní IP adresy a routovacích informací externím subjektům? | * Přezkoumejte routerové a firewallové konfigurace * Rozhovor s personálem |  |  | |  |  |  |
| 1.4 | (a) Je instalován a aktivní osobní firewallový software (nebo rovnocenné funkcionality) na všech přenosných zařízeních s výpočetní technikou (včetně vlastněných společností a/ nebo zaměstnanci), které se připojují na internet mimo síť (například laptopy používané zaměstnanci), a které jsou také užívány k přístupu do prostředí dat držitelů karet? | * Zkontrolujte politiky a konfigurační standardy * Přezkoumejte mobilní a/nebo zaměstnanci vlastněná zařízení |  |  | |  |  |  |
| (b) Je osobní firewallový software (nebo rovnocenné funkcionality) konfigurován na konkrétní konfigurační nastavení, je aktivní a nezměnitelný uživateli mobilních a/nebo zaměstnanci vlastněných zařízení? | * Zkontrolujte politiky a konfigurační standardy * Přezkoumejte mobilní a/nebo zaměstnanci vlastněná zařízení |  |  | |  |  |  |
| 1.5 | Jsou bezpečnostní politiky a operační postupy pro řízení firewallů:   * dokumentovány * používány * známy všem dotčeným stranám? | * Zkontrolujte bezpečnostní politiky a operační postupy * Rozhovor s personálem |  |  | |  |  |  |

### Požadavek 2: Nepoužívat výchozí nastavení od dodavatele pro systémová hesla a jiné bezpečnostní parametry

| **PCI DSS Otázka** | | **Očekávané Testování** | **Odpověď**  **(zaškrtněte jednu odpověď pro každou otázku)** | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **ANO** | **ANO s „CCW“** | **NE** | **N/A** | **Netestováno** |
| 2.1 | (a) Jsou vždy změněna výchozí (defaultní) nastavení od dodavatelů před instalací systémů do sítě?  *To se vztahuje na VŠECHNA výchozí (defaultní) hesla, kromě jiných i na ta, používaná pro operační systémy, software poskytující bezpečnostní služby, aplikační a systémové účty, point-of-sale (POS) terminály, platební aplikace, Simple Network Management Protocol (CNMP) Community strings (Pozn. překl.: Obdoba hesel pro přístup do statistik routeru.) apod.* | * Zkontrolujte politiky a postupy * Přezkoumejte dokumentace dodavatelů * Sledujte systémové konfigurace a nastavení účtů * Rozhovor s personálem |  |  |  |  |  |
| (b) Jsou všechny zbytečné výchozí (defaultní) účty odstraněny nebo deaktivovány před instalací systémů do sítě? | * Zkontrolujte politiky a postupy * Přezkoumejte dokumentace dodavatelů * Přezkoumejte konfigurace systému a nastavení účtů * Rozhovor s personálem |  |  |  |  |  |
| 2.1.1 | U bezdrátových technologií připojených do prostředí dat držitelů karet nebo přenášejících data držitelů karet, jsou změněna VŠECHNA výchozí nastavení od dodavatelů, dle následujícího: |  | | | | | |
|  | (a) Jsou změněny výchozí (defaultní) šifrovací klíče při instalaci a pokaždé, když někdo se znalostí klíčů opustí společnost nebo změní funkci? | * Zkontrolujte politiky a postupy * Zkontrolujte dokumentace dodavatelů * Rozhovor s personálem |  |  |  |  |  |
|  | (b) Je při instalaci vyžadována změna výchozích (defaultních) řetězců SNMP community strings na bezdrátových zařízeních? | * Zkontrolujte politiky a postupy * Zkontrolujte dokumentace dodavatelů * Rozhovor s personálem * Přezkoumejte konfigurace systémů |  |  |  |  |  |
|  | (c) Je při instalaci vyžadována změna výchozích (defaultních) hesel/heslových frází na přístupových bodech? | * Zkontrolujte politiky a postupy * Rozhovor s personálem * Přezkoumejte konfigurace systémů |  |  |  |  |  |
|  | (d) Je firmware na bezdrátových zařízeních aktualizován tak, aby podporoval silné šifrování pro ověření (autentizaci) a přenos prostřednictvím bezdrátových sítí? | * Zkontrolujte politiky a postupy * Zkontrolujte dokumentace dodavatelů * Přezkoumejte konfigurace systémů |  |  |  |  |  |
| (e) Jsou všechna další bezpečnostní nastavení u bezdrátových zařízení změněna z výchozího nastavení (v případě potřeby)? | * Zkontrolujte politiky a postupy * Zkontrolujte dokumentace dodavatelů * Přezkoumejte konfigurace systémů |  |  |  |  |  |
| 2.2 | (a) Jsou konfigurační standardy vyvinuty pro všechny systémové komponenty a jsou konzistentní s všeobecně platnými zpřísněnými standardy ochrany systémů v odvětví?  *Zdroje zpřísněných standardů ochrany systémů v odvětví zahrnují mimo jiné: SysAdmin Audit Network Security (SANS) Institute, National Institute of Standards Technology (NIST), International Organization for Standardization (ISO) a Center for Internet Security (CIS)* | * Zkontrolujte konfigurační standardy systémů * Zkontrolujte odvětvím přijaté zpřísňující standardy * Zkontrolujte politiky a postupy * Rozhovor s personálem |  |  |  |  |  |
|  | (b) Jsou konfigurační standardy systémů aktualizovány při identifikaci nových zranitelností, jak je definováno v Požadavku 6.1? | * Zkontrolujte politiky a postupy * Rozhovor s personálem |  |  |  |  |  |
|  | (c) Jsou konfigurační standardy systémů aplikovány při konfiguraci nových systémů? | * Zkontrolujte politiky a postupy * Rozhovor s personálem |  |  |  |  |  |
|  | (d) Zahrnují konfigurační standardy systémů vše následující:   * Jsou změněna všechna defaultní (výchozí) nastavení dodané dodavateli a odstraněny nepotřebné defaultní (výchozí) účty? * Je implementována na každém serveru pouze jedna primární funkce, aby se zabránilo současné existenci funkcí, které požadují různé bezpečnostní úrovně, na stejném serveru? * Jsou umožněny pouze nezbytné služby, protokoly, daemony apod., které jsou potřebné pro funkci systému (Pozn. překl.: daemon je program běžící v pozadí.)? * Jsou implementovány další bezpečnostní prvky pro všechny požadované služby, protokoly nebo daemony pokládané za nezabezpečené? * Jsou konfigurovány bezpečnostní parametry systému tak, aby se zabránilo zneužití? * Jsou odstraněny všechny zbytečné funkcionality, jako jsou skripty, drivery, prvky, subsystémy, souborové systémy a zbytečné webové servery? | * Zkontrolujte konfigurační standardy systémů |  |  |  |  |  |
| 2.2.1 | (a) Je implementována pouze jedna primární funkce na každém serveru, aby se na jednom serveru zabránilo spolupráci funkcím, které vyžadují různé úrovně bezpečnosti?  *Např. webové servery, databázové servery a DNS by měly být implementovány na oddělených serverech.* | * Přezkoumejte konfigurace systémů |  |  |  |  |  |
| (b) Jsou-li použity virtualizační technologie, je pouze jedna primární funkce na každé virtuální systémové komponentě nebo zařízení? | * Přezkoumejte konfigurace systémů |  |  |  |  |  |
| 2.2.2 | (a) Jsou umožněny pouze nezbytné služby, protokoly, daemony apod., které jsou zapotřebí k funkci systému (služby a protokoly, které nejsou přímo potřebné k provedení zadané funkce, jsou vypnuty)? | * Zkontrolujte konfigurační standardy * Přezkoumejte konfigurace systémů |  |  |  |  |  |
|  | (b) Jsou jakékoli aktivované nezabezpečené služby, daemony nebo protokoly, oprávněné podle dokumentovaných konfiguračních standardů? | * Zkontrolujte konfigurační standardy * Rozhovor s personálem * Přezkoumejte konfigurační nastavení * Porovnejte povolené služby, atd. s dokumentovanými zdůvodněními |  |  |  |  |  |
| 2.2.3 | Jsou implementované dodatečné bezpečnostní prvky na jakékoli požadované služby, protokoly nebo daemony, které jsou považovány za nezabezpečené? | * Zkontrolujte konfigurační standardy * Přezkoumejte konfigurační nastavení |  |  |  |  |  |
| 2.2.4 | (a) Jsou správci systému a/nebo osoby konfigurující systémové komponenty seznámeni s obvyklými nastaveními bezpečnostních parametrů pro systémové komponenty? | * Rozhovor s personálem |  |  |  |  |  |
| (b) Jsou zkontrolovány konfigurační standardy systémů a ověřeny, zda obsahují obvyklé bezpečnostní parametry? | * Zkontrolujte konfigurační standardy |  |  |  |  |  |
| (c) Jsou bezpečnostní parametry nastaveny vhodně na systémové komponenty? | * Přezkoumejte komponenty systémů * Přezkoumejte nastavení parametrů zabezpečení * Porovnejte nastavení se standardy konfigurace systému. |  |  |  |  |  |
| 2.2.5 | (a) Jsou odstraněny všechny nepotřebné funkce, jako skripty, drivery (řadiče), prvky, subsystémy, souborové systémy a nepotřebné webové servery? | * Přezkoumejte nastavení parametrů zabezpečení systémových komponent |  |  |  |  |  |
|  | (b) Jsou povolené funkce dokumentovány a podporují bezpečnou konfiguraci? | * Zkontrolujte dokumentace * Přezkoumejte nastavení parametrů zabezpečení systémových komponent |  |  |  |  |  |
|  | (c) Jsou na komponentách systému přítomny pouze zdokumentované funkce | * Zkontrolujte dokumentace * Přezkoumejte nastavení parametrů zabezpečení systémových komponent |  |  |  |  |  |
| 2.3 | Jsou šifrované všechny nekonzolové administrativní přístupy následujícím způsobem? |  | | | | | |
| (a) Jsou všechny nekonzolové přístupy šifrované za použití silného šifrování a je metoda použití silného šifrování vyžádána před tím, než je požadováno administrátorské heslo? | * Přezkoumejte komponenty systémů * Přezkoumejte konfigurace systémů * Sledujte přihlášení administrátora |  |  |  |  |  |
| (b) Jsou všechny služby a parametry souborů konfigurovány tak, aby znemožnily použití protokolu/služby Telnet a dalších nebezpečných vzdálených přístupů/protokolů? | * Přezkoumejte komponenty systémů * Přezkoumejte služby a soubory |  |  |  |  |  |
| (c) Je využito silné kryptografie k šifrování pro administrátorský přístup prostřednictvím webového rozhraní? | * Přezkoumejte komponenty systémů * Sledujte přihlášení administrátora |  |  |  |  |  |
| (d) Je implementována silná kryptografie pro použitou technologii v souladu s odvětvovými osvědčenými postupy a/nebo doporučeními dodavatele? | * Přezkoumejte komponenty systémů * Zkontrolujte dokumentace dodavatele * Rozhovor s personálem |  |  |  |  |  |
| 2.4 | (a) Je udržován soupis systémových komponent, které jsou v rozsahu PCI DSS včetně hardware a software a obsahuje pro každou položku její popis funkce nebo použití? | * Přezkoumejte soupis systémů |  |  |  |  |  |
| (b) Je dokumentovaný soupis udržován aktuální? | * Rozhovor s personálem |  |  |  |  |  |
| 2.5 | Jsou bezpečnostní politiky a provozní postupy pro správu defaultního (výchozího) nastavení od dodavatelů a další bezpečnostní parametry:   * dokumentovány * používají se * jsou známy všem dotčeným stranám? | * Zkontrolujte bezpečnostní politiky a provozní postupy * Rozhovor s personálem |  |  |  |  |  |
| 2.6 | *Tento požadavek je platný pouze pro poskytovatele služeb* |  | | | | | |

## Ochrana dat držitelů karet

### Požadavek 3: Chránit uchovávaná data držitelů karet

| **PCI DSS Otázka** | | **Očekávané Testování** | **Odpověď**  **(zaškrtněte jednu odpověď pro každou otázku)** | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **ANO** | **ANO s „CCW“** | **NE** | **N/A** | **Netestováno** |
| 3.1 | Jsou politiky, postupy a procesy držení a mazání dat implementovány dle následujícího: |  | | | | | |
| (a) Je množství dat a doba jejich držení omezeno na nezbytně nutné z právních, regulačních a/nebo provozních důvodů? | * Zkontrolujte politiky a postupy pro držení a likvidaci dat * Rozhovor s personálem |  |  |  |  |  |
| (b) Jsou definovány procesy bezpečného mazání dat držitelů karet, jakmile nejsou zapotřebí z právních, regulačních a/nebo provozních důvodů? | * Zkontrolujte politiky a postupy * Rozhovor s personálem * Přezkoumejte mechanismus mazání |  |  |  |  |  |
| (c) Existují specifické požadavky na držení dat držitelů karet?  *Například data držitelů karet mají být uchovávána po X období z Y provozních důvodů* | * Zkontrolujte politiky a postupy * Rozhovor s personálem * Přezkoumejte požadavky na držení dat |  |  |  |  |  |
| (d) Je aplikován čtvrtletní proces na identifikování a bezpečné mazání uchovávaných dat držitelů karet, které přesahují definované požadavky na držení dat? | * Zkontrolujte politiky a postupy * Rozhovor s personálem * Sledujte procesy mazání |  |  |  |  |  |
| (e) Splňují všechna uložená data držitelů karet požadavky definované politikou držení dat?? | * Přezkoumejte soubory a systémové záznamy |  |  |  |  |  |
| 3.2 | (a) *Tento testovací postup je platný pouze pro Issuera (vydavatelská banka)* |  | | | | | |
| (b) *Tento testovací postup je platný pouze pro Issuera (vydavatelská banka)* |
| (c) Jsou citlivá autentizační data mazána nebo upravována tak, aby nebyla použitelná po dokončení autorizačního procesu? | * Zkontrolujte politiky a postupy * Přezkoumejte konfigurace systémů * Přezkoumejte procesy mazání |  |  |  |  |  |
|  | (d) Jsou dodržovány u všech systémů následující požadavky týkající se neuchovávání citlivých autentizací dat po autorizaci (i pokud jsou šifrovaná): |  | | | | | |
| 3.2.1 | Neuchovává se úplný obsah žádné stopy (magnetického proužku umístěného na zadní straně karty nebo ekvivalentní data obsažená v čipu nebo jinde) po autorizaci?  *Tato data jsou alternativně označována jako úplná stopa, stopa, stopa 1, stopa 2 a data magnetického proužku.*  ***Poznámka:*** *Za normálního průběhu provozu může být zapotřebí držet následující datové prvky z magnetického proužku:*   * *Jméno držitelů karet,* * *Číslo karty (PAN),* * *Datum ukončení platnosti,* * *Service code*   Za účelem minimalizace rizika uchovávejte pouze ty datové prvky potřebné pro provoz. | * Přezkoumejte zdroje dat včetně: * Příchozích transakčních dat * Všech záznamů * Historie souborů * Souborů trasování * Databázových schémat * Obsahů databází |  |  |  |  |  |
| 3.2.2 | Není po autorizaci uchováván ověřovací kód/hodnota (card verification code/value) (trojmístné nebo čtyřmístné číslo na líci nebo rubu platební karty) používané k verifikaci transakcí bez přítomnosti karty? | * Přezkoumejte zdroje dat včetně: * Příchozích transakčních dat * Všech záznamů * Historie souborů * Souborů trasování * Databázových schémat   Obsahů databází |  |  |  |  |  |
| 3.2.3 | Není uchováván po autorizaci osobní identifikační číslo (PIN) ani zašifrovaný PIN blok? | * Přezkoumejte zdroje dat včetně: * Příchozích transakčních dat * Všech záznamů * Historie souborů * Souborů trasování * Databázových schémat * Obsahů databází |  |  |  |  |  |
| 3.3 | Je PAN maskovaný tak, že pokud je zobrazován (maximálně lze se zobrazit prvních šest a poslední čtyři číslice), pouze personál s legitimním provozním důvodem mohou vidět více jak prvních šest nebo poslední čtyři číslice PAN?  ***Poznámka****: Tento požadavek nenahrazuje přísnější požadavky platné pro zobrazení dat držitelů karet — například právní požadavky nebo požadavky kartových společností pro stvrzenky na prodejních místech (POS).* | * Zkontrolujte politiky a postupy * Zkontrolujte role, které potřebují přístup k zobrazení celého PAN * Přezkoumejte konfigurace systémů * Sledujte zobrazení PAN |  |  |  |  |  |
| 3.4 | Je číslo karty (PAN) znečitelněno všude, kde se uchovává (včetně přenosných digitálních médií, záložních médií, přihlašovacích vstupů/logů), a to použitím kteréhokoliv z následujících přístupů?   * One-way hashes (jednosměrné hashování) vycházející z silné kryptografie (hash musí zahrnovat celé číslo karty) * Truncation - Zkrácení/odříznutí (hashování nelze použít k náhradě odříznuté části čísla karty) * Indexové tokeny a jednorázová hesla PAN (PANy musí být bezpečně uloženy) * Silná kryptografie s příslušnými procesy a postupy managementu klíčů   ***Poznámka****: Pro podvodníka je relativně jednoduché rekonstruovat původní číslo karty, pokud mají přístup jak k odříznutému číslu karty, tak k jeho hashované verzi. Pokud jsou v prostředí subjektu přítomny hashovaná i odříznutá verze stejného čísla karty, musí se zavést dodatečné kontroly, aby se zajistilo, že hashovaná i odříznutá verze nemohou být korelovány k rekonstrukci původního čísla karty.* | * Přezkoumejte dokumentace dodavatele * Přezkoumejte datová úložiště * Přezkoumejte vyjímatelná média * Přezkoumejte auditní záznamy |  |  |  |  |  |
| 3.4.1 | Pokud je použito šifrování disku (a ne databázové šifrování na úrovni sloupce nebo souboru), jsou přístupy řízeny následujícím: ***Poznámka****: Tento požadavek platí nad rámec dalších požadavků PCI DDS k šifrování správě klíčů* |  | | | | | |
| (a) Je logický přístup spravován odděleně a nezávisle na standartní autentizaci a přístupových mechanismech vlastního operačního systému (například nepoužívat lokální databáze uživatelských účtů nebo ověřovací údaje (credentials) pro login do sítě)? | * Přezkoumejte systémové konfigurace * Sledujte autentizační proces |  |  |  |  |  |
| (b) Jsou kryptografické klíče bezpečně uloženy (například na výměnných médiích, která jsou adekvátně chráněna silnou kontrolou přístupu)? | * Přezkoumejte procesy * Rozhovor s personálem |  |  |  |  |  |
|  | (c) Jsou data držitelů karet na přenositelných médiích šifrovaná, ať jsou uložena kdekoliv?  ***Poznámka****: Pokud není šifrování disku použito k zašifrování výměnných médií, pak data uložená na těchto médiích bude třeba učinit nečitelnými některou jinou metodou.* | * Přezkoumejte systémové konfigurace * Sledujte procesy |  |  |  |  |  |
| 3.5 | Jsou klíče používané k bezpečnému šifrování dat držitelů karet zabezpečené proti odhalení a zneužití?  ***Poznámka****: Tento požadavek se vztahuje na klíče používané k šifrování uložených dat držitelů karet a také se vztahují na klíče pro šifrování klíčů, používaných k ochraně klíče pro šifrování dat držitelů karet – takovéto klíče pro šifrování musí být přinejmenším tak silné, jako klíče pro šifrování dat.* |  | | | | | |
| 3.5.1 | *Tento požadavek je platný pouze pro poskytovatele služeb* |  | | | | | |
| 3.5.2 | Je přístup ke klíčům omezen na co nejmenší počet správců? | * Přezkoumejte seznamy uživatelů s přístupem |  |  |  |  |  |
| 3.5.3 | Jsou uchovávány soukromé šifrovací klíče používané k šifrování/dešifrování dat držitelů karet vždy v jedné (nebo více) z následujících možností?   * Zašifrované s klíčem pro šifrování klíčů, který je přinejmenším stejně silný jako klíč pro šifrování dat, a který je uložen odděleně od klíče pro šifrování dat. * V rámci bezpečného šifrovacího prostředku (např. jako je šifrovací modul Hardware (Host) Security Module (HSM), nebo zařízení point-of-interaction schválené PTS) * Jako minimálně dvě komponenty plné délky (full-length key components) nebo sdílené klíče (key shares), v souladu s metodou přijímanou v odvětví.   ***Poznámka****: Pro veřejné klíče (public keys) není vyžadováno jejich uchovávání* | * Zkontrolujte dokumentované postupy * Přezkoumejte konfigurace systémů a úložiště klíčů, včetně klíčů pro šifrovaní klíčů |  |  |  |  |  |
| 3.5.4 | Jsou šifrovací klíče uchovávány na co nejmenším počtu míst? | * Přezkoumejte umístění pro uchovávání klíčů * Sledujte procesy |  |  |  |  |  |
| 3.6 | (a) Jsou všechny procesy správy klíčů a postupy pro šifrovací klíče užívané k šifrování dat držitelů karet dokumentovány a implementovány? | * Zkontrolujte postupy správy klíčů |  |  |  |  |  |
|  | (b) *Tento testovací postup je platný pouze pro poskytovatele služeb* |  | | | | | |
|  | (c) Jsou nastaveny postupy a procesy pro správu klíčů podle následujících požadavků: |  | | | | | |
| 3.6.1 | Jsou nastaveny postupy správy klíčů tak, aby specifikovaly, jak generovat silné klíče? | * Zkontrolujte postupy správy klíčů * Sledujte postupy generování klíčů |  |  |  |  |  |
| 3.6.2 | Specifikují postupy správy klíčů, jak se mají klíče bezpečně distribuovat? | * Zkontrolujte postupy správy klíčů * Sledujte metody distribuce klíčů |  |  |  |  |  |
| 3.6.3 | Specifikují postupy správy klíčů, jak bezpečně uchovávat klíče? | * Zkontrolujte postupy správy klíčů * Sledujte metody pro bezpečné uchovávání klíčů |  |  |  |  |  |
| 3.6.4 | Definují postupy správy klíčů dobu platnosti každého používaného typu klíče (cryptoperiod) a definují proces pro změnu klíče na konci definované doby platnosti klíče (např. po uplynutí definovaného časového období a/nebo po vytvoření určitého objemu šifrovaného textu daným klíčem), jak bylo definováno odpovídajícím dodavatelem aplikace nebo vlastníkem klíče, a odpovídá osvědčeným postupům a doporučením v odvětví (např. NIST Special Publication 800-57)? | * Zkontrolujte postupy správy klíčů * Rozhovor s personálem |  |  |  |  |  |
| 3.6.5 | (a) Specifikují postupy správy klíčů stažení nebo náhradu (např. po archivaci, zničení a/nebo odvolání) klíčů, je-li to nutné, pokud integrita klíčů byla oslabena (např. odchod zaměstnanců znalých části otevřeného textu klíče), nebo je podezření na kompromitování klíčů? | * Zkontrolujte postupy správy klíčů * Rozhovor s personálem |  |  |  |  |  |
| (b) Specifikují postupy správy klíčů nahrazení klíčů, pokud byly kompromitovány, nebo je podezření na jejich kompromitování? | * Zkontrolujte postupy správy klíčů * Rozhovor s personálem |  |  |  |  |  |
| (c) Pokud jsou drženy prošlé nebo nahrazené šifrovací klíče, pak tyto klíče musí být bezpečně archivovány (např. použitím klíče k šifrování klíčů). Mohou být archivované šifrovací klíče použity pouze za účelem dešifrování/ověření a nikoliv na šifrování? | * Zkontrolujte postupy správy klíčů * Rozhovor s personálem |  |  |  |  |  |
| 3.6.6 | Je-li použito manuální správy šifrovacích klíčů v otevřené formě, takové operace musí být spravovány s využitím rozdělení znalostí a duální kontroly s využitím následujících:   * Je využito rozdělení znalostí o klíčích, takže části klíčů jsou pod kontrolou dvou nebo tří lidí, kdy každý zná jen svou část klíče a společně rekonstruují klíč celý?   A   * Provádí se duální kontrola klíčů, takže k provedení operace správy klíčů jsou vyžadováni nejméně dva pracovníci a jedna osoba nemá přístup k autentizačním materiálům (například hesla nebo klíče)?   ***Poznámka****: Příklady manuálních operací správy klíčů zahrnují mimo jiné např. generování klíčů, přenos, zavádění, ukládání a zničení.* | * Zkontrolujte postupy správy klíčů * Rozhovor s personálem a/nebo * Sledujte procesy |  |  |  |  |  |
| 3.6.7 | Specifikují postupy správy klíčů, zda je zabráněno neautorizované náhradě klíčů? | * Zkontrolujte postupy * Rozhovor s personálem * Sledujte procesy |  |  |  |  |  |
| 3.6.8 | Specifikují postupy správy klíčů procesy pro správce klíčů prohlášení (písemné nebo elektronické), že chápou svoji odpovědnost správce a akceptují ji? | * Zkontrolujte postupy * Zkontrolujte dokumentace nebo další evidence |  |  |  |  |  |
| 3.7 | Jsou bezpečnostní politiky a provozní postupy pro ochranu uložených dat držitelů karet:   * dokumentovány, * používají se * jsou známy všem dotčeným stranám? | * Zkontrolujte bezpečnostní politiky a provozní postupy * Rozhovor s personálem |  |  |  |  |  |

### Požadavek 4: Zašifrovat přenos dat držitelů karet po otevřených veřejných sítích

| **PCI DSS Otázka** | | **Očekávané Testování** | **Odpověď**  **(zaškrtněte jednu odpověď pro každou otázku)** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ANO** | **ANO s „CCW“** | | **NE** | **N/A** | **Netestováno** | |
| 4.1 | (a) Je používána silná kryptografie a bezpečnostní protokoly k ochraně citlivých dat držitelů karet během přenosu po otevřených veřejných sítích?  **Poznámka:** Příklady otevřených veřejných sítí, zahrnují, ale nejsou omezeny jen na: internet, bezdrátové technologie, včetně 802.11 a Bluetooth, mobilní technologie, například Globální Systém pro Mobilní komunikaci (GSM), Code division multiple access (CDMA), General Packet Radio Service (Mobilní datová rádiová služba, GPRS). | * Zkontrolujte dokumentované standardy * Zkontrolujte politiky a postupy * Zkontrolujte všechny lokace s přenosem nebo příjmem dat držitelů karet * Přezkoumejte konfigurace systémů |  |  |  | |  |  | |
| (b) Jsou přijímány pouze důvěryhodné klíče a/nebo certifikáty? | * Sledujte příchozí a odchozí přenosy * Přezkoumejte klíče a certifikáty |  |  |  | |  |  | |
| (c) Jsou implementovány bezpečnostní protokoly, používající pouze bezpečné konfigurace a nepodporující nezabezpečené verze nebo konfigurace? | * Přezkoumejte konfigurace systémů |  |  |  | |  |  | |
| (d) Je implementována správná síla šifrování pro používanou metodologii šifrování? (Zkontrolujte doporučení dodavatele / osvědčené postupy) | * Zkontrolujte dokumentace dodavatele * Přezkoumejte konfigurace systémů |  |  |  | |  |  | |
| (e) Je pro implementaci TLS povolen protokol TLS vždy, když jsou data držitelů karet vysílána nebo přijímána?  *Např. pro implementaci prostřednictvím webového prohlížeče:*   * *„HTTPS“ se zobrazuje jako protokol prohlížeče Universal Record Locator (URL), a* * *Data držitelů karet jsou vyžadována pouze tehdy, pokud se „HTTPS“ objeví jako součást URL.* | * Přezkoumejte konfigurace systémů |  |  |  | |  |  | |
| 4.1.1 | Používají se osvědčené postupy odvětví k implementaci silné kryptografie pro autentizaci a přenos u bezdrátových sítí přenášejících data držitelů karet nebo připojených do prostředí dat držitelů karet?  ***Poznámka****: Používání WEP jako bezpečnostní kontroly je zakázáno.* | * Zkontrolujte standardy * Zkontrolujte bezdrátové sítě * Přezkoumejte nastavení konfigurace systémů |  |  | |  |  | |  | |
| 4.2 | (a) Jsou nechráněná čísla karet (PAN) upraveny tak aby byla nečitelná nebo šifrovaná kdykoliv jsou zasílaná prostřednictvím technologie odesílání zpráv konečným uživatelem (například email, instant messaging, SMS, chat, apod.)? | * Sledujte procesy * Zkontrolujte odchozí přenosy. |  |  | |  |  | |  | |
| (b) Existují politiky, které určují, že nechráněná čísla karet (PAN) nesmí být zasílána technologiemi pro zasílání zpráv koncovým uživatelem? | * Zkontrolujte politiky a postupy |  |  | |  |  | |  | |
| 4.3 | Jsou bezpečnostní politiky a provozní postupy pro ochranu přenosu dat držitelů karet:   * dokumentovány * používají se * jsou známy všem dotčeným stranám? | * Zkontrolujte bezpečnostní politiky a provozní postupy * Rozhovor s personálem |  |  | |  |  | |  | |

## Udržování programu kontroly zranitelnosti

### Požadavek 5: Chránit všechny systémy proti malware a pravidelně aktualizovat antivirový software nebo programy

| **PCI DSS Otázka** | | **Očekávané Testování** | **Odpověď**  **(zaškrtněte jednu odpověď pro každou otázku)** | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ANO** | **ANO s „CCW“** | **NE** | **N/A** | **Netestováno** |
| 5.1 | Je nainstalovaný antivirový software na všechny systémy běžně postihované závadným softwarem? | * Přezkoumejte konfigurace systémů |  |  |  |  |  |
| 5.1.1 | Jsou antivirové programy schopné detekovat, odstranit a chránit před všemi známými typy závadného softwaru (*Například: viry, trojské koně, červy, spyware, adware a rootkits)*? | * Zkontrolujte dokumentace dodavatele * Přezkoumejte konfigurace systémů |  |  |  |  |  |
| 5.1.2 | Provádíte pravidelná vyhodnocení k identifikaci a zhodnocení vývoje malware hrozeb k ověření, že předmětné systémy nejsou běžně ovlivněny závadným softwarem, a že tomu tak bude i nadále? | * Rozhovor s personálem |  |  |  |  |  |
| 5.2 | Jsou všechny antivirové mechanismy udržovány následovně: |  |  |  |  |  |  |
| (a) Je veškerý antivirový software a definice udržován aktuální? | * Přezkoumejte politiky a postupy * Přezkoumejte antivirové konfigurace včetně hlavní instalace * Přezkoumejte komponenty systémů |  |  |  |  |  |
| (b) Jsou povoleny a prováděny automatické aktualizace a pravidelné skeny? | * Přezkoumejte antivirové konfigurace včetně hlavní instalace * Přezkoumejte komponenty systémů |  |  |  |  |  |
| (c) Jsou všechny antivirové mechanismy nastaveny tak, aby generovaly auditní záznamy (auditlogs), které jsou drženy podle Požadavku 10.7 PCI DSS? | * Přezkoumejte antivirové konfigurace včetně hlavní instalace * Zkontrolujte procesy uchovávání záznamů |  |  |  |  |  |
| 5.3 | Jsou všechny antivirové mechanismy:   * Aktivně spuštěné? * Není možnost je vypnout nebo změnit uživatelem?   ***Poznámka****: Antivirové řešení může být dočasně deaktivováno pouze v případě, že existuje legitimní technická potřeba, je schválena vedením a to případ od případu. Pokud má být ze specifického důvodu deaktivována antivirová ochrana, musí to být formálně schváleno. Během doby, po kterou není antivirová ochrana aktivní, může být také nutné implementovat další bezpečnostní opatření.* | * Přezkoumejte antivirové konfigurace včetně hlavní instalace * Přezkoumejte komponenty systémů * Sledujte procesy * Rozhovor s personálem |  |  |  |  |  |
| 5.4 | Jsou bezpečnostní politiky a provozní postupy pro ochranu systémů před malwarem:   * dokumentovány * používají se * jsou známy všem dotčeným stranám? | * Zkontrolujte bezpečnostní politiky a provozní postupy * Rozhovor s personálem |  |  |  |  |  |

### Požadavek 6: Vyvíjet a udržovat bezpečné systémy a aplikace

| **PCI DSS Otázka** | | **Očekávané Testování** | | | **Odpověď**  **(zaškrtněte jednu odpověď pro každou otázku)** | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ANO** | **ANO s „CCW“** | **NE** | **N/A** | **Netestováno** |
| 6.1 | Je zaveden proces identifikace bezpečnostních slabin, včetně následujícího:   * Používání spolehlivých externích zdrojů pro identifikace nových bezpečnostních zranitelností? * Přiřazení klasifikací rizik zranitelnostem, které zahrnují identifikaci všech zranitelností s „vysokým“ nebo „kritickým“ rizikem?   ***Poznámka:*** *Rizikové hodnocení má být založeno na osvědčených postupech, jakož i na posouzení případného dopadu. Například kritéria pro hodnocení zranitelnosti mohou zahrnovat zvážení základního skóre CVSS, a/nebo klasifikace ze strany dodavatele, a/nebo typu dotčených systémů.*  *Metody pro vyhodnocení zranitelnosti a přiřazení hodnocení rizika se bude lišit podle prostředí organizace a strategie posouzení rizika. Hodnocení rizika by mělo minimálně identifikovat všechny zranitelnosti považované v daném prostředí za "vysoké riziko". Vedle hodnocení rizika mohou být zranitelnosti považovány za "kritické" v případě, že představují bezprostřední ohrožení prostředí, mají dopad na kritické systémy a/nebo by mohly mít za následek potenciální kompromitaci, pokud by nebyly řešeny. Příklady kritických systémů mohou být bezpečnostní systémy, zařízení a systémy s přístupem veřejnosti, databáze a další systémy, které uchovávají, zpracovávají nebo přenášejí data držitelů karet* | * Zkontrolujte politiky a postupy * Rozhovor s personálem * Sledujte procesy | | |  |  |  |  |  |
| 6.2 | (a) Jsou všechny komponenty systémů a softwaru chráněny proti známým zranitelnostem instalováním vhodných bezpečnostních záplat dodaných dodavatelem? | * Zkontrolujte politiky a postupy | | |  |  |  |  |  |
|  | (b) Jsou kritické bezpečnostní záplaty instalovány v průběhu jednoho měsíce od zpřístupnění?  ***Poznámka****: Kritické bezpečnostní záplaty by měly být identifikovány podle procesu klasifikace rizik definovaného v Požadavku 6.1.* | * Zkontrolujte politiky a postupy * Přezkoumejte komponenty systémů * Porovnejte seznam instalovaných bezpečnostních záplat se seznamem záplat aktuálně vydaných dodavatelem | | |  |  |  |  |  |
| 6.3 | (a) Existují a jsou ověřeny procesy vývoje softwaru a vycházejí ze standardů v odvětví a/nebo osvědčených postupů? | * Zkontrolujte procesy vývoje softwaru * Přezkoumejte procesy * Rozhovor s personálem | | |  |  |  |  |  |
| (b) Jsou procesy informační bezpečnosti dodržovány po celou dobu životního cyklu vývoje aplikace? | * Zkontrolujte procesy vývoje softwaru * Přezkoumejte procesy * Rozhovor s personálem | | |  |  |  |  |  |
| (c) Jsou softwarové aplikace vyvíjeny dle standardu PCI DSS (např. bezpečná autentizace a logování)? | * Zkontrolujte procesy vývoje softwaru * Přezkoumejte procesy * Rozhovor s personálem | | |  |  |  |  |  |
| (d) Je proces vývoje softwaru zajištěn dle požadavků 6.3.1-6.3.2: |  | | | | | | | |
| 6.3.1 | Jsou odstraněny vývojové, testovací a/nebo účty aplikací na zakázku, uživatelská ID a hesla před uvedením aplikace do produkčního stavu nebo před předáním uživateli? | * Zkontrolujte procesy vývoje softwaru * Rozhovor s personálem | | |  |  |  |  |  |
| 6.3.2 | Je prověřen programový kód, připravený na zakázku, před jeho uvedením do produkce nebo předáním zákazníkům a identifikovány možné zranitelnosti programu (s použitím buď manuálních, nebo automatizovaných procesů) s využitím minimálně následujících kroků:   * Změny kódu jsou přezkoumány jinými osobami než autorem původního programu a osobami se znalostmi o technikách prověřování kódu a bezpečných programátorských postupů? * Prověrky kódu zajistí, že program je vyvinut v souladu s postupy bezpečného programování? * Příslušné opravy jsou implementovány před uvedením do provozu? * Výsledky prověrky kódu jsou přezkoumány a schváleny vedením před uvedením do provozu?   ***Poznámka:*** *Tento požadavek na prověření kódu se vztahuje na všechny upravené programy (interní i čelící veřejné doméně), jako součást životního cyklu vývoje systému. Prověření kódu programů může být provedeno poučeným interním personálem nebo třetí stranou. Veřejné webové aplikace také podléhají dodatečným kontrolám, pokud čelí veřejné doméně, k řešení trvalých hrozeb a zranitelnosti po implementaci, podle definice v Požadavku 6.6 PCI DSS.* | * Zkontrolujte politiky a postupy * Rozhovor s personálem * Přezkoumejte nedávné změny a záznamy o změnách | | |  |  |  |  |  |
| 6.4 | Jsou pro řízení změn procesů a postupů dodržovány pro všechny změny systémových komponent? Postupy musejí obsahovat následující: |  | | | | | | | |
| 6.4.1 | (a) Jsou odděleny vývojová/testovací prostředí od produkčního prostředí? | * Zkontrolujte procesy a postupy řízení změn * Přezkoumejte síťovou dokumentaci a konfigurace síťových zařízení | | |  |  |  |  |  |
|  | (b) Je zavedeno nastavení kontrol přístupu a jsou zavedeny kontroly přístupu k posílení oddělení mezi vývojovým/testovacím prostředím a produkčním prostředím? | * Zkontrolujte procesy a postupy řízení změn * Přezkoumejte nastavení řízení přístupu | | |  |  |  |  |  |
| 6.4.2 | Je zavedeno oddělení povinností mezi personálem přiděleným k vývojovému/testovacímu prostředí a personálem přiděleným k produkčnímu prostředí? | * Zkontrolujte procesy a postupy řízení změn * Sledujte procesy * Rozhovor s personálem | | |  |  |  |  |  |
| 6.4.3 | Nejsou produkční data („živá“ čísla karet) používána pro testování nebo vývoj? | * Zkontrolujte procesy a postupy řízení změn * Sledujte procesy * Rozhovor s personálem * Přezkoumejte testovací data | | |  |  |  |  |  |
| 6.4.4 | Jsou testovací data a účty odstraněny ze systémových komponent před aktivací systému / uvedením do produkčního provozu? | * Zkontrolujte procesy a postupy řízení změn * Sledujte procesy * Rozhovor s personálem * Přezkoumejte produkční systémy | | |  |  |  |  |  |
| 6.4.5 | (a) Jsou dokumentované postupy řízení dokumentovány a vyžadují následující?   * Dokumentace dopadu. * Dokumentované schválení změn pověřenými stranami. * Provedení funkčního testování a ověření, zda změny nemají nepříznivý účinek na bezpečnost systému. * Postupy návratu (roll back). | * Zkontrolujte procesy a postupy řízení změn | | |  |  |  |  |  |
| (b) Jsou následující požadavky uplatněny a dokumentovány pro všechny změny: |  | | | | | | | |
| 6.4.5.1 | Dokumentace dopadu? | * Přezkoumejte dokumentaci řízení změn * Sledujte změny v dokumentaci řízení změn | | |  |  |  |  |  |
| 6.4.5.2 | Dokumentované schválení změn pověřenými stranami? | * Sledujte změny v dokumentaci řízení změn * Přezkoumejte dokumentaci řízení změn | | |  |  |  |  |  |
| 6.4.5.3 | (a) Je provedeno funkční otestování a ověřeno, zda změny nemají nepříznivý dopad na bezpečnost systému? | * Sledujte změny v dokumentaci řízení změn * Přezkoumejte dokumentaci řízení změn | | |  |  |  |  |  |
|  | (b) Je při změnách vlastního kódu provedeno testování aktualizací na to, aby byly v souladu s Požadavkem 6 PCI DSS předtím, než jsou uvedeny do provozu? | * Sledujte změny v dokumentaci řízení změn * Přezkoumejte dokumentaci řízení změn | | |  |  |  |  |  |
| 6.4.5.4 | Postupy návratu (roll back)? | * Sledujte změny v dokumentaci řízení změn * Přezkoumejte dokumentaci řízení změn | | |  |  |  |  |  |
| 6.4.6 | Při dokončení významných změn, jsou všechny relevantní požadavky PCI DSS implementovány na všech nových nebo změněných systémech a sítích a je dokumentace náležitě aktualizována? | * Sledujte změny v dokumentaci řízení změn * Přezkoumejte dokumentaci řízení změn * Rozhovor s personálem * Sledujte dotčené systémy a sítě | | |  |  |  |  |  |
| 6.5 | (a) Zachycují procesy vývoje softwaru běžné zranitelnosti kódu? | * Přezkoumejte politiky a postupy vývoje softwaru | | |  |  |  |  |  |
|  | (b) Jsou vývojáři aspoň jednou ročně školeni v aktuálních technikách bezpečného programování včetně způsobů, jak se vyvarovat známým zranitelnostem kódování? | * Přezkoumejte záznamy školení. * Přezkoumejte politiky a postupy vývoje softwaru | | |  |  |  |  |  |
| (c) Jsou aplikace vyvíjeny podle návodů bezpečného programování k ochraně aplikací před minimálně následujícími zranitelnostmi:  ***Poznámka****: Zranitelná místa, jejichž seznam je uveden v bodech 6.5.1 až 6.5.10, byla v odvětví rozšířena a řešena osvědčenými postupy v době vydání této verze standardu PCI DSS. Vzhledem k aktualizaci osvědčených postupů pro řízení zranitelnosti (například Průvodce OWASP, SANS CWE Top 25, CERT Secure Coding, apod.), musí být pro tyto požadavky použity osvědčené postupy.* |  | | | | | | | |
| 6.5.1 | Obsahují techniky kódování informace o injection flaws (vsunutí chybového kódu), zejména SQL?  ***Poznámka****: Je třeba brát v potaz OS Command Injection, LDAP a XPath Injection flaws a další možnosti.* | | * Přezkoumejte politiky a postupy vývoje softwaru * Rozhovor s odpovědným personálem | |  |  |  |  |  |
| 6.5.2 | Obsahují techniky kódování informace o zranitelnosti spojené s buffer overflow (přetečení vyrovnávací paměti)? | | * Přezkoumejte politiky a postupy vývoje softwaru * Rozhovor s odpovědným personálem | |  |  |  |  |  |
| 6.5.3 | Obsahují techniky kódování informace o nezabezpečeném kryptografickém úložišti ? | | * Přezkoumejte politiky a postupy vývoje softwaru * Rozhovor s odpovědným personálem | |  |  |  |  |  |
| 6.5.4 | Obsahují techniky kódování informace o nezabezpečené komunikaci? | | * Přezkoumejte politiky a postupy vývoje softwaru * Rozhovor s odpovědným personálem | |  |  |  |  |  |
| 6.5.5 | Obsahují techniky kódování informace o nesprávném zpracování chyb? | | * Přezkoumejte politiky a postupy vývoje softwaru * Rozhovor s odpovědným personálem | |  |  |  |  |  |
| 6.5.6 | Obsahují techniky kódování všechny zranitelnosti s vysokým rizikem („high risk“) identifikované v procesu identifikace zranitelnosti (jak je definováno v Požadavku 6.1 PCI DSS)? | | * Přezkoumejte politiky a postupy vývoje softwaru * Rozhovor s odpovědným personálem | |  |  |  |  |  |
| Pro webové aplikace a aplikační rozhraní (interní a externí) jsou aplikace vyvíjeny na základě pokynů bezpečného kódování k ochraně aplikací před následujícími dalšími zranitelnostmi: | | | | | | | | | |
| 6.5.7 | Obsahují techniky kódování informace o zranitelnosti metody Cross-site Scripting (XSS)? | | * Přezkoumejte politiky a postupy vývoje softwaru * Rozhovor s personálem | |  |  |  |  |  |
| 6.5.8 | Obsahují techniky kódování informace o nesprávné kontrole přístupu, jako jsou nezabezpečené přímé odkazy na objekty, selhání v omezení přístupů na URL a převody adresářů a selhání v omezení přístupu uživatelů k funkcím? | | * Přezkoumejte politiky a postupy vývoje softwaru * Rozhovor s odpovědným personálem | |  |  |  |  |  |
| 6.5.9 | Obsahují techniky kódování informace o padělaném požadavku z prohlížeče (Cross-site Request Forgery, CSRF)? | | | * Přezkoumejte politiky a postupy vývoje softwaru * Rozhovor s odpovědným personálem |  |  |  |  |  |
| 6.5.10 | Obsahují techniky kódování informace o přerušovaném ověření identity (autentizace) a správu relace? | | | * Přezkoumejte politiky a postupy vývoje softwaru * Rozhovor s odpovědným personálem |  |  |  |  |  |
| 6.6 | U veřejně přístupných webových aplikací (čelících veřejnému přístupu, „public-facing“) je nutné průběžně reagovat na nové hrozby a zranitelná místa a zajištění, aby byly tyto aplikace chráněny před známými útoky pomocí kterékoli z těchto metod:   * Revizí veřejně přístupné webové aplikace (public-facing) prostřednictvím manuálních nebo automatizovaných nástrojů nebo metod pro bezpečnostní vyhodnocení zranitelnosti aplikací, a to následovně: * Nejméně jednou ročně * Po jakékoliv změně * Organizací, která se specializuje na bezpečnost aplikací * Nejméně všechny zranitelnosti popsané v Požadavku 6.5 jsou zahrnuty v posuzování * Všechny zranitelnosti jsou opraveny * Aplikace je po opravách znovu vyhodnocena   ***Poznámka:*** *Toto posouzení není totéž jako skenování zranitelnosti provedené podle Požadavku 11.2.*  ***-NEBO-***   * Instalací automatického technického řešení detekujícího a zabraňujícího internetovým útokům (například webové aplikační firewally) a to následovně: * Je umístěno před webovou veřejně přístupnou aplikací k detekci a prevenci internetových útoků. * Je aktivně spuštěno a aktuální. * Generuje auditní logy. * Je konfigurováno buď na blokování webových útoků, nebo na generování varování, které je okamžitě prověřeno. | | | * Zkontrolujte zdokumentované procesy * Rozhovor s personálem * Přezkoumejte záznamy posouzení bezpečnosti aplikací * Přezkoumejte nastavení konfigurace systémů |  |  |  |  |  |
| 6.7 | Jsou bezpečnostní politiky a provozní postupy pro vývoj a údržbu bezpečných systémů a aplikací:   * dokumentovány * používají se * jsou známy všem dotčeným stranám? | | | * Zkontrolujte bezpečnostní politiky a provozní postupy * Rozhovor s personálem |  |  |  |  |  |

## Zavedení silných opatření pro řízení přístupu

### Požadavek 7: Omezit přístup k datům držitelů karet jen podle oprávněné potřeby

| **PCI DSS Otázka** | | **Očekávané Testování** | **Odpověď**  **(zaškrtněte jednu odpověď pro každou otázku)** | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ANO** | **ANO s „CCW“** | **NE** | **N/A** | **Netestováno** |
| 7.1 | Je omezen přístup k systémovým komponentám a datům držitelů karet jen na ty osoby, jejichž práce takový přístup vyžaduje, dle následujícího? |  | | | | | |
|  | * Existují zde písemné politiky řízení přístupu, které zahrnují následující? * Definování potřeby přístupu a přiřazení oprávnění pro každou roli * Omezení přístupu podle oprávnění uživatelova ID na minimum oprávnění nezbytných pro plnění pracovních povinností * Přiřazení přístupu založeného na klasifikaci a pracovní funkci jednotlivého personálu * Dokumentované schválení (elektronické nebo písemné) oprávněnými osobami pro veškerý přístup, včetně seznamu schválených specifických oprávnění. | * Přezkoumejte písemné politiky řízení přístupu |  |  |  |  |  |
| 7.1.1 | Jsou definovány potřeby přístupu pro každou roli, včetně:   * Systémových komponent a zdrojových dat, ke kterým každá role musí mít přístup pro svou pracovní funkci? * Úrovně oprávnění požadovaných pro přístup ke zdrojům (například uživatel, administrátor, apod.)? | * Přezkoumejte role a potřeby přístupu |  |  |  |  |  |
| 7.1.2 | Jsou přístupy k privilegovaným uživatelským účtům omezeny dle následujícího:   * omezen pouze na minimální oprávnění nezbytná pro plnění pracovních povinností? * přiřazen pouze k rolím, které specificky vyžadují privilegovaný přístup? | * Rozhovor s personálem * Rozhovor s managementem * Zkontrolujte privilegované uživatelské účty (ID) |  |  |  |  |  |
| 7.1.3 | Jsou přiřazeny přístupy podle klasifikace jednotlivých míst a funkcí personálu? | * Rozhovor s managementem * Zkontrolujte uživatelské účty (ID) |  |  |  |  |  |
| 7.1.4 | Je vyžadován dokumentovaný souhlas autorizovanými stranami specifikujícími požadovaná oprávnění? | * Zkontrolujte uživatelské účty (ID) * Porovnejte s dokumentovanými souhlasy * Porovnejte přidělená práva s dokumentovanými souhlasy |  |  |  |  |  |
| 7.2 | Je zaveden systém kontroly přístupů pro systémové komponenty, které omezují přístupy, na základě provozní potřeby uživatelů, a pokud není vydáno zvláštní povolení, je nastaveno na „zakázat vše“ („deny all“), pokud to není výslovně povoleno, dle následujícího: |  | | | | | |
| 7.2.1 | Jsou zavedeny systémy kontroly přístupu pro všechny systémové komponenty? | * Zkontrolujte dokumentace dodavatele * Přezkoumejte nastavení konfigurace |  |  |  |  |  |
| 7.2.2 | Jsou systémy kontroly přístupu konfigurovány tak, aby vyžadovaly přidělení oprávnění jednotlivcům na základě klasifikace pracovní náplně a funkce? | * Zkontrolujte dokumentace dodavatele * Přezkoumejte nastavení konfigurace |  |  |  |  |  |
| 7.2.3 | Mají systémy kontroly přístupu výchozí nastavení „zakázat vše“? | * Zkontrolujte dokumentace dodavatele * Přezkoumejte nastavení konfigurace |  |  |  |  |  |
| 7.3 | Jsou bezpečnostní politiky a provozní postupy pro omezení přístupu k datům držitelů karet:   * dokumentovány * používají se * jsou známy všem dotčeným stranám? | * Přezkoumejte bezpečnostní politiky a provozní postupy * Rozhovor s personálem |  |  |  |  |  |

### Požadavek 8: Identifikovat a autentizovat přístup k systémovým komponentám

| **PCI DSS Otázka** | | **Očekávané Testování** | | | | **Odpověď**  **(zaškrtněte jednu odpověď pro každou otázku)** | | | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ANO** | **ANO s „CCW“** | | **NE** | | **N/A** | | **Netestováno** | |
| 8.1 | Jsou definovány politiky a postupy pro zajištění řádné správy identifikace uživatelů a uživatelů, kteří nejsou spotřebiteli, a správců všech systémových komponent, dle následujícího: |  | | | | | | | | | | | | |
| 8.1.1 | Jsou přiděleny všem uživatelům jedinečné uživatelské ID před umožněním jejich přístupu k systémovým komponentám nebo datům držitelů karet? | * Zkontrolujte postupy pro hesla * Rozhovor s personálem | | | |  |  | |  | |  | |  | |
| 8.1.2 | Je řízeno přidávání, mazání a změny uživatelských ID, ověřovacích údajů (credentials) a dalších objektů identifikace tak, aby uživatelské ID byly implementovány pouze tak, jak bylo schváleno (včetně specifických privilegií)? | * Zkontrolujte postupy pro hesla * Přezkoumejte ID privilegovaných a běžných uživatelů a související oprávnění * Sledujte systémová nastavení | | | |  |  | |  | |  | |  | |
| 8.1.3 | Jsou ihned rušeny nebo deaktivovány přístupy každému uživateli, jehož přístupové oprávnění bylo ukončeno? | * Zkontrolujte postupy pro hesla * Přezkoumejte účty zrušených uživatelů * Zkontrolujte aktuální seznamy přístupů * Sledujte navrácená fyzická autentizační zařízení | | | |  |  | |  | |  | |  | |
| 8.1.4 | Jsou odstraněny/deaktivovány neaktivní uživatelské účty do 90 dní? | * Zkontrolujte postupy pro hesla * Sledujte uživatelské účty | | | |  |  | |  | |  | |  | |
| 8.1.5 | (a) Jsou účty používané třetími stranami k přístupu, podpoře nebo údržbě systémových komponent prostřednictvím vzdáleného přístupu povoleny pouze během doby, kdy je potřeba, a zakázány, když se nepoužívají | * Zkontrolujte postupy pro hesla * Rozhovor s personálem * Sledujte procesy | | | |  |  | |  | |  | |  | |
|  | (b) Jsou účty vzdáleného přístupu třetích stran monitorovány v době, kdy jsou používány? | * Rozhovor s personálem * Sledujte procesy | | | |  |  | |  | |  | |  | |
| 8.1.6 | (a) Jsou omezeny opakované pokusy o přístup do systému uzamčením uživatelského jména (ID) po ne více než maximálně 6 pokusech? | * Zkontrolujte postupy pro hesla * Přezkoumejte nastavení konfigurace systémů | | | |  |  | |  | |  | |  | |
| (*b) Tento testovací postup je platný pouze pro poskytovatele služeb* |  | | | | | | | | | | | | |
| 8.1.7 | Jakmile je uživatelský účet uzamčen, je doba uzamčení nastavena na minimálně 30 minut nebo dokud, správce nepovolí ID uživatele? | * Zkontrolujte postupy pro hesla * Přezkoumejte nastavení konfigurace systémů | | | |  |  | |  | |  | |  | |
| 8.1.8 | Pokud byla relace nečinná déle než 15 minut, je požadována po uživateli opakovaná autentizace (například, znovu zadáním hesla) pro reaktivaci terminálu nebo relace? | * Zkontrolujte postupy pro hesla * Přezkoumejte nastavení konfigurace systémů | | | |  |  | |  | |  | |  | |
| 8.2 | Je kromě přidělení jedinečného uživatelského ID využívána jedna nebo více z následujících metod k ověření všech uživatelů?   * Něco, co znáte – jako je heslo nebo heslová fráze * Něco, co máte – jako je token nebo čipová karta * Něco, kým jste – například biometrika. | * Zkontrolujte postupy pro hesla * Sledujte autentizační procesy | | | |  |  | |  | |  | |  | |
| 8.2.1 | (a) Je použito silné kryptografie, které učiní všechny autentizační údaje (jako jsou hesla/heslové fráze) nečitelné během přenosu a ukládání na všechny systémové komponenty? | * Zkontrolujte postupy pro hesla * Zkontrolujte dokumentace dodavatele * Přezkoumejte nastavení konfigurace systémů * Sledujte soubory hesel * Sledujte přenosy dat | | | |  |  | |  | |  | |  | |
| (*b) Tento testovací postup je platný pouze pro poskytovatele služeb* |  | | | | | | | | | | | | |
| 8.2.2 | Je ověřena identita uživatele před změnou autentizačních údajů (například provádění resetu hesla, poskytování nového tokenu nebo generování nových klíčů)? | * Zkontrolujte autentizační postupy * Sledujte personál v místě | | | |  | |  | |  | |  | |  | |
| 8.2.3 | (a) Jsou parametry hesla / heslové fráze nastaveny tak, aby vyhovovaly následujícímu?   * minimální délka hesla je nejméně sedm znaků * obsahuje jak numerické, tak abecední znaky.   Alternativně musí mít hesla / heslové fráze složitost a sílu, která je alespoň rovnocenná parametrům uvedených výše. | * Přezkoumejte nastavení konfigurace systémů pro ověření parametrů hesel | | | |  | |  | |  | |  | |  | |
| (*b) Tento testovací postup je platný pouze pro poskytovatele služeb* |  | | | |  | |  | |  | |  | |  | |
| 8.2.4 | (a) Jsou měněna uživatelská hesla / heslové fráze nejméně každých 90 dní? | * Zkontrolujte postupy pro hesla * Přezkoumejte nastavení konfigurace systémů | | | |  | |  | |  | |  | |  | |
| (*b) Tento testovací postup je platný pouze pro poskytovatele služeb (* |  | | | | | | | | | | | | | |
| 8.2.5 | (a) Musí jednotlivec zadat nové heslo / heslovou frázi, které je odlišné od kteréhokoliv z posledních čtyř jeho nebo jejích používaných hesel / heslových frází? | * Zkontrolujte postupy pro hesla * Prozkoumejte vzorek systémových komponent * Přezkoumejte nastavení konfigurace systémů | | | |  | |  | |  | |  | |  | |
|  | (*b) Tento testovací postup je platný pouze pro poskytovatele služeb* |  | | | | | | | | | | | | | |
| 8.2.6 | (a) Je nastaveno heslo / heslová fráze pro první použití a při resetu na jedinečnou hodnotu pro každého uživatele, a je po prvním použití okamžitě změněno? | * Zkontrolujte postupy pro hesla * Přezkoumejte nastavení konfigurace systémů * Sledujte bezpečnostní personál | | | |  | |  | |  | |  | |  | |
| 8.3 | Je veškerý individuální nekonzolový administrativní přístup a veškerý vzdálený přístup k prostředí dat držitelů karet zabezpečen více-faktorovým ověřením identity dle následujícího:  ***Poznámka****: Více-faktorové ověření (autentizace) vyžaduje, aby pro ověření byly použity minimálně dvě ze tří autentizačních metod (viz PCI DSS Požadavek 8.2 ohledně popisu autentizačních metod). Použití jednoho faktoru dvakrát (např. použití dvou různých hesel) není považováno za více-faktorové ověření.* |  | | | | | | | | | | | | |
| 8.3.1 | Je více-faktorové ověření zavedeno pro veškerý nekonzolový přístup do prostředí dat držitelů karet pro osoby s administrativním přístupem? | * Přezkoumejte konfigurace systémů * Sledujte přihlašování administrátora k CDE | | | |  |  | |  | |  | |  | |
| 8.3.2 | Je více-faktorové ověřením identity zavedeno pro všechny vzdálené přístupy k síti (jak pro uživatele tak pro administrátora, a včetně přístupu třetích stran pro podporu anebo údržbu) jejichž původ je vně sítě subjektu? | * Přezkoumejte konfigurace systémů * Sledujte vzdáleně připojený personál | | | |  |  | |  | |  | |  | |
| 8.4 | (a) Jsou autentizačních politiky a postupy zdokumentovány a komunikovány všem uživatelům? | * Zkontrolujte politiky a postupy * Zkontrolujte distribuční metody * Rozhovor s personálem * Rozhovor s uživateli | | | |  |  | |  | |  | |  | |
| (b) Zahrnují autentizační postupy a politiky, následující?   * Návod k výběru silných autentizačních údajů * Návod, jak by uživatelé měli chránit své autentizační údaje * Pokyny pro uživatele, aby nepoužívali dříve použitá hesla * Pokyny ke změně hesel, pokud existuje podezření, že heslo by mohlo být „kompromitováno“ | * Zkontrolujte politiky a postupy * Zkontrolujte dokumentace poskytované uživatelům | | | |  |  | |  | |  | |  | |
| 8.5 | Jsou zakázány skupinové, sdílené či generické účty, hesla nebo jiné autentizační metody dle následujícího:   * Generická ID uživatele a účty jsou zakázány nebo odstraněny. * Neexistují sdílená ID uživatele pro činnosti zprávy systému a dalších kritických funkcí. * Sdílená a generická ID uživatele nejsou používána k správě jakýchkoli systémových komponent? | * Zkontrolujte politiky a postupy * Přezkoumejte seznamy ID uživatelů * Rozhovor s personálem | | | |  |  | |  | |  | |  | |
| 8.5.1 | *Tento požadavek je platný pouze pro poskytovatele služeb* |  | | | | | | | | | | | | |
| 8.6 | Pokud jsou použity jiné autentizační mechanismy (například fyzické nebo logické bezpečnostní tokeny, čipové karty, certifikáty, atd.), je použití těchto mechanismů přiřazeno následovně?   * Autentizační mechanismy musí být přiřazeny k jednotlivému účtu a nesmí být sdíleny mezi více účty. * Musí být zavedeny fyzické a/nebo logické kontroly, aby bylo zajištěno, že pouze určený účet může použít tento mechanismus k získání přístupu. | * Zkontrolujte politiky a postupy * Rozhovor s personálem * Přezkoumejte konfigurační nastavení systémů a/nebo fyzické kontroly | |  | | |  | |  | |  | |  | |
| 8.7 | Všechny přístupy ke každé databázi obsahující data držitelů karet (včetně přístupů přes aplikace, administrátory a všechny ostatní uživatele) jsou omezeny následovně: |  | | | | | | | | | | | | |
|  | (a) Jsou všechny uživatelské přístupy k databázím, uživatelské dotazy a uživatelské činnosti nad databázemi (například přesuny, kopírování, mazání) prováděny pouze prostřednictvím programových metod (například prostřednictvím uložených postupů)? | * Zkontrolujte politiky a postupy autentizace databáze * Přezkoumejte nastavení konfigurace databází a aplikací | |  | | |  | |  | |  | |  | |
|  | (b) Jsou přímé přístupy uživatelů k databázi nebo dotazy nad databází omezeny na administrátory databáze? | | * Zkontrolujte politiky a postupy autentizace databáze * Přezkoumejte nastavení řízení přístupu do databází * Přezkoumejte konfigurační nastavení databázových aplikací | |  | |  | |  | |  | |  | |
| (c) Jsou ID aplikací použity pouze aplikacemi (a nikoliv individuálními uživateli nebo jinými procesy)? | | * Zkontrolujte politiky a postupy autentizace databáze * Přezkoumejte nastavení řízení přístupu do databází * Přezkoumejte konfigurační nastavení databázových aplikací | |  | |  | |  | |  | |  | |
| 8.8 | Jsou bezpečnostní politiky a provozní postupy pro identifikaci a ověřování:   * dokumentovány * používají se * jsou známy všem dotčeným stranám? | | * Přezkoumejte bezpečnostní politiky a provozní postupy * Rozhovor s personálem | |  | |  | |  | |  | |  | |

### Požadavek 9: Omezit fyzický přístup k datům držitelů karet

| **PCI DSS Otázka** | | **Očekávané Testování** | **Odpověď**  **(zaškrtněte jednu odpověď pro každou otázku)** | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ANO** | **ANO s „CCW“** | **NE** | **N/A** | **Netestováno** |
| 9.1 | Jsou používané odpovídající kontroly vstupu do objektu za účelem omezení a monitorování fyzického přístupu k systémům v prostředí dat držitelů karet? | * Sledujte kontroly fyzického přístupu * Sledujte personál v místě |  |  |  |  |  |
| 9.1.1 | (a) Jsou zavedeny videokamery a/nebo jiné mechanismy kontroly přístupu k monitorování individuálního fyzického přístupu do citlivých oblastí?  ***Poznámka****: „Citlivá oblast“ odkazuje na jakékoliv datové centrum, serverová místnost nebo jakýkoliv prostor se systémy, které uchovávají, zpracovávají nebo přenášejí data držitelů karet. Vyloučeny jsou veřejné (public-facing) prostory, kde jsou přítomny pouze prodejní terminály, jako například prostory pokladních v maloobchodě.* | * Zkontrolujte politiky a postupy * Sledujte mechanismy fyzického monitorování * Sledujte bezpečnostní funkce |  |  |  |  |  |
| (b) Jsou chráněny buď videokamery nebo mechanismy kontroly přístupu (nebo oboje) před manipulací nebo deaktivací? | * Sledujte procesy * Rozhovor s personálem |  |  |  |  |  |
| (c) Jsou data shromážděná z videokamer a/nebo kontrolních mechanismů překontrolována a korelována s dalšími vstupy? | * Zkontrolujte politiky a postupy * Rozhovor s bezpečnostním personálem |  |  |  |  |  |
| (d) Jsou data shromážděná z videokamer a/nebo kontrolních mechanismů uložena nejméně tři měsíce, není-li to zákonem jinak omezeno? | * Zkontrolujte postupy pro držení dat * Sledujte uchovávání dat * Rozhovor s bezpečnostním personálem |  |  |  |  |  |
| 9.1.2 | Jsou implementovány fyzické a/nebo logické kontroly, které omezují přístup k veřejně přístupným síťovým konektorům?  *Například síťové konektory umístěné ve veřejných prostorách a prostorách přístupných pro návštěvníky by mohly být deaktivovány a aktivovány pouze tehdy, je-li přístup k síti výslovně autorizován. Alternativně by mohly být implementovány procesy, které zajistí, že návštěvníci v prostorách s aktivními síťovými konektory, budou vždy pouze s doprovodem.* | * Zkontrolujte politiky a postupy * Rozhovor s personálem * Sledujte umístění |  |  |  |  |  |
| 9.1.3 | Jsou omezeny fyzické přístupy k bodům bezdrátového přístupu, bránám (gateways), ručním zařízením (handheld devices), síťovému / komunikačnímu hardwaru a telekomunikačním linkám? | * Zkontrolujte politiky a postupy * Rozhovor s personálem * Sledujte zařízení |  |  |  |  |  |
| 9.2 | (a) Jsou definovány postupy pro identifikaci a rozlišení mezi personálem a návštěvníky, které zahrnují následující:   * Identifikaci personálu a návštěvníků (například přiřazením visaček) * Změny na požadavky přístupu * Zrušení nebo ukončení identifikace končícího personálu a návštěvníků s prošlou platností (jako jsou ID visačky)?   *Pro účely Požadavku 9 se slovem „personál“ rozumí zaměstnanci na plný či částečný úvazek, zaměstnanci na dobu určitou, kontraktoři a konzultanti, kteří jsou fyzicky přítomni v prostorách daného subjektu. Pojmem „návštěvník“ se rozumí prodejce, host někoho z personálu, servisní pracovníci či kdokoli, kdo se potřebuje dostat do zařízení na krátkou dobu, obvykle ne delší než jeden den.* | * Zkontrolujte politiky a postupy * Rozhovor s personálem * Sledujte metody identifikace (např. visačky) * Sledujte postupy pro návštěvy |  |  |  |  |  |
| (b) Jsou návštěvníci jasně označeni a je snadné rozlišit mezi personálem a návštěvníky? | * Sledujte metody identifikace |  |  |  |  |  |
| (c) Je přístup k identifikačnímu procesu (jako je systém visaček) omezen na autorizovaný personál? | * Sledujte fyzické kontroly a řízení přístupu pro systém visaček |  |  |  |  |  |
| 9.3 | Jsou fyzické přístupy personálu k citlivým oblastem kontrolovány podle následujícího:   * Je přístup autorizován a založen na funkci jednotlivých osob? * Je přístup zrušen ihned po ukončení? * Jsou všechny mechanismy fyzického přístupu, jako jsou klíče, přístupové karty, atd., jsou vráceny nebo deaktivovány? | * Rozhovor s personálem * Přezkoumejte seznamy řízení přístupu * Sledujte personál v místě * Porovnejte seznamy zaměstnanců s ukončeným pracovním vztahem se seznamy řízení přístupu |  |  |  |  |  |
| 9.4 | Jsou identifikace a přístupy návštěvníků definovány dle následujícího: |  | | | | | |
| 9.4.1 | Jsou návštěvníci před vstupem autorizováni, a jsou stále doprovázeni v prostorách, kde jsou zpracovávána nebo uchovávána data držitelů karet? | * Zkontrolujte politiky a postupy * Sledujte procesy návštěv, včetně toho jak je přístup řízen * Rozhovor s personálem * Sledujte návštěvy a používání visaček |  |  |  |  |  |
| 9.4.2 | (a) Jsou návštěvníci identifikováni a jsou jim vydány visačky nebo jiné označení, které má dobu platnosti a viditelně je odlišuje od místního personálu? | * Sledujte používání visaček u personálu a návštěv * Přezkoumejte identifikaci. |  |  |  |  |  |
| (b) Mají visačky návštěvníků nebo jiné prvky identifikace expirační dobu? | * Sledujte procesy * Přezkoumejte identifikaci. |  |  |  |  |  |
| 9.4.3 | Jsou návštěvníci požádáni, aby odevzdali visačky nebo identifikaci před opuštěním objektu nebo ke dni ukončení jejich platnosti? | * Sledujte procesy * Sledujte opouštění objektu návštěvami |  |  |  |  |  |
| 9.4.4 | (a) Jsou udržovány záznamy o vstupu (log) návštěvníků do objektu, místností s počítači a datových center, kde jsou zpracovávána nebo uchovávána data držitelů karet? | * Zkontrolujte politiky a postupy * Přezkoumejte záznamy o návštěvách * Sledujte procesy návštěv * Přezkoumejte držení záznamů |  |  |  |  |  |
| (b) Obsahují záznamy (návštěvnické logy) jméno návštěvníka, reprezentovanou firmu a personál autorizující fyzický přístup? | * Zkontrolujte politiky a postupy * Přezkoumejte záznamy o návštěvách |  |  |  |  |  |
| (c) Jsou záznamy drženy nejméně po tři měsíce? | * Zkontrolujte politiky a postupy * Přezkoumejte držení záznamů o návštěvách |  |  |  |  |  |
| 9.5 | Jsou všechna média fyzicky zabezpečena (kromě jiných i u počítačů, vyjímatelných elektronických médií, papírových stvrzenek, papírových sestav a faxů)?  *Pro účely požadavku č. 9 „média“ jsou všechna papírová a elektronická média obsahující data držitelů karet* | * Zkontrolujte politiky a postupy pro fyzického zabezpečení medií * Rozhovor s personálem |  |  |  |  |  |
| 9.5.1 | Je umístění (lokace), kde jsou uloženy zálohy médií, revidována nejméně jednou ročně, aby se potvrdilo, že je bezpečné? | * Zkontrolujte politiky a postupy pro kontrolu umístění médií mimo pracoviště * Rozhovor s bezpečnostním personálem |  |  |  |  |  |
| 9.6 | (a) Je zavedena a udržována pro jakékoli druhy médií přísná vnitřní i vnější kontrola distribuce? | * Zkontrolujte politiky a postupy pro distribuci médií |  |  |  |  |  |
|  | (b) Zahrnují kontroly následující: |  | | | | | |
| 9.6.1 | Jsou média klasifikována tak, aby mohla být identifikována citlivost dat? | * Zkontrolujte politiky a postupy pro klasifikaci médií * Rozhovor s bezpečnostním personálem |  |  |  |  |  |
| 9.6.2 | Jsou média zasílána bezpečným kurýrem nebo jinou zasílací metodou, která může být přesně sledována? | * Rozhovor s personálem * Přezkoumejte dokumentaci a záznamy sledování distribuce médií |  |  |  |  |  |
| 9.6.3 | Schválil management všechna média, která jsou přesouvána mimo bezpečnou oblast (včetně médií distribuovaných jednotlivcům)? | * Rozhovor s personálem * Přezkoumejte dokumentaci a záznamy sledování distribuce médií |  |  |  |  |  |
| 9.7 | Je udržována přísná kontrola nad ukládáním a dostupností médií? | * Zkontrolujte politiky a postupy |  |  |  |  |  |
| 9.7.1 | (a) Jsou inventární záznamy všech médií správně udržovány? | * Přezkoumejte inventární záznamy |  |  |  |  |  |
| (b) Je prováděna inventarizace médií nejméně jednou ročně? | * Přezkoumej inventární záznamy * Rozhovor s personálem |  |  |  |  |  |
| 9.8 | (a) Jsou všechna média zničena, když jich již není zapotřebí z provozních ani právních důvodů? | * Zkontrolujte politiky a postupy periodické likvidace médií |  |  |  |  |  |
|  | (b) Existuje politika periodické likvidace médií a pokrývá všechna média a definuje požadavky dle následujících kroků?   * Papírové kopie materiálů musí být rozřezány na kousky, spáleny nebo rozdrceny tak, že lze důvodně předpokládat, že kopie materiálů nelze rekonstruovat. * Skladovací kontejnery používané pro materiály, které mají být zničeny, musí být zabezpečeny. * Data držitelů karet na elektronických médiích musí být učiněna nezrekonstruovatelnými (např. prostřednictvím bezpečného mazacího programu v souladu se standardem uznávaným v odvětví pro bezpečné mazání), nebo fyzickým zničením média. | * Zkontrolujte politiky a postupy periodické likvidace médií |  |  |  |  |  |
| (c) Jsou média zničena dle následujícího: |  | | | | | |
| 9.8.1 | (a) Jsou materiály s fyzickými kopiemi rozřezány, spáleny nebo rozdrceny tak, aby data držitelů karet nemohla být zrekonstruována? | * Rozhovor s personálem * Přezkoumejte postupy * Sledujte procesy |  |  |  |  |  |
| (b) Jsou skladovací kontejnery používané pro materiály, které obsahují informace určené ke zničení, zabezpečeny proti přístupu k jejich obsahu? | * Přezkoumejte bezpečnost skladovacích kontejnerů |  |  |  |  |  |
| 9.8.2 | Jsou data držitelů karet na elektronických médiích učiněna neobnovitelnými (např. prostřednictvím bezpečného mazacího programu v souladu se standardem uznávaným v odvětví pro bezpečné mazání nebo jiným fyzickým zničením média) tak, aby nemohla být data zrekonstruována? | * Sledujte procesy * Rozhovor s personálem |  |  |  |  |  |
| 9.9 | Jsou chráněna zařízení, která získávají data platebních karet prostřednictvím přímé fyzické interakce s kartou, před nedovolenou manipulací a záměně dle následujícího?  ***Poznámka****: Tyto požadavky se vztahují na čtecí zařízení karet používaných při transakcích za přítomnosti karet (to znamená, že karta je protažena nebo vložena) v místě prodeje. Tento požadavek se nevztahuje na komponenty s ručním vstupem jako jsou počítačové klávesnice a POS klávesnice.* |  | | | | | |
| (a) Vyžadují politiky a postupy, aby byl seznam takových zařízení udržován? | * Zkontrolujte politiky a postupy |  |  |  |  |  |
| (b) Vyžadují politiky a postupy aby byla prováděna pravidelná kontrola zařízení za účelem zjištění, zda s ním nebylo manipulováno nebo nebylo nahrazeno? | * Zkontrolujte politiky a postupy |  |  |  |  |  |
| (c) Vyžadují politiky a postupy školení personálu, aby si byli vědomi podezřelého chování a hlásili manipulaci nebo náhradu zařízení? | * Zkontrolujte politiky a postupy |  |  |  |  |  |
| 9.9.1 | (a) Obsahuje seznam zařízení následující body?   * Značku a model zařízení * Umístění zařízení (např. adresa místa nebo objektu, kde se zařízení nachází) * Sériové číslo zařízení nebo jiný způsob unikátní identifikace | * Přezkoumejte seznam zařízení |  |  |  |  |  |
|  | (b) Je seznam přesný a aktuální? | * Sledujte zařízení a jejich umístění a porovnejte se seznamem |  |  |  |  |  |
|  | (c) Je seznam zařízení aktualizován když je zařízení přidáno, přemístěno, vyřazeno z provozu atd.? | * Rozhovor s personálem |  |  |  |  |  |
| 9.9.2 | (a) Jsou pravidelně kontrolovány povrchy zařízení, aby se zjistila neoprávněná manipulace (např. přidání Skimmeru -nelegální čtečky karet do zařízen) nebo výměně (např. kontrolou sériového čísla nebo jiné charakteristiky zařízení pro ověření, zda zařízení nebylo vyměněno za podvodné) podle následujícího?  ***Poznámka****: Příklady příznaků, které naznačují, že se zařízením mohlo být manipulováno nebo bylo nahrazeno, jsou neočekávané přílepky nebo kabely zapojené do zařízení, chybějící nebo změněné bezpečnostní štítky, rozbité nebo jinak barevné kryty nebo změny sériového čísla nebo jiné vnější znaky.* | * Rozhovor s personálem * Sledujte procesy inspekce a porovnejte s definovanými procesy |  |  |  |  |  |
| (b) Je si personál vědom postupů pro prohlídky zařízení? | * Rozhovor s personálem |  |  |  |  |  |
| 9.9.3 | Je personál školen, aby si byl vědom pokusů o manipulaci se zařízením nebo jejich výměně, dle následujícího? |  | | | | | |
|  | (a) Obsahují školící materiály pro personál v místě prodeje následující?   * Ověřit identitu jakýchkoli osob třetí strany, které tvrdí, že je personál opravy nebo údržby, před udělením přístupu k provedení opravy nebo údržby zařízení. * Neinstalovat, nevyměňovat ani nevracet zařízení bez ověření. * Být si vědom podezřelého chování kolem zařízení (např. pokusy neznámých osob o odpojení nebo otevření zařízení). * Hlásit podezřelé chování a známky manipulace se zařízením nebo jeho výměnu (substituci) příslušnému personálu (například manažerovi nebo bezpečnostnímu pracovníkovi). | * Zkontrolujte školící materiály |  |  |  |  |  |
|  | (b) Je personál v místě prodeje školen a je si vědom postupů pro detekci a hlášení pokusů o manipulaci nebo výměnu zařízení? | * Rozhovor s personálem v umístění POS zařízení |  |  |  |  |  |
| 9.10 | Jsou bezpečnostní politiky a provozní postupy pro omezení fyzického přístupu k datům držitelů karet:   * dokumentovány * používají se * jsou známy všem dotčeným stranám? | * Přezkoumejte bezpečnostní politiky a provozní postupy * Rozhovor s personálem |  |  |  |  |  |

## Pravidelné monitorování a testování sítí

### Požadavek 10: Sledovat a monitorovat všechny přístupy k síťovým zdrojům a datům držitelů karet

| **PCI DSS Otázka** | | **Očekávané Testování** | | **Odpověď**  **(zaškrtněte jednu odpověď pro každou otázku)** | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ANO** | | **ANO s „CCW“** | **NE** | **N/A** | **Netestováno** | | |
| 10.1 | (a) Jsou auditní stopy spuštěny a aktivovány pro systémové komponenty? | * Sledujte procesy * Rozhovor s administrátory systémů | |  | |  |  |  |  | | |
| (b) Jsou přístupy k systémovým komponentám spojeny s jednotlivými uživateli? | * Sledujte procesy * Rozhovor s administrátory systémů | |  | |  |  |  |  | | |
| 10.2 | Jsou implementovány automatizované auditní stopy pro všechny systémové komponenty pro rekonstrukci následujících událostí: |  | | | | | | | | | |
| 10.2.1 | Všechny individuální přístupy uživatele k datům držitelů karet? | * Rozhovor s personálem * Sledujte auditní záznamy * Přezkoumejte nastavení auditních záznamů | |  | |  |  |  |  | | |
| 10.2.2 | Všechny akce jednotlivců provedené s root (nejvyšším) nebo administrativním oprávněním? | * Rozhovor s personálem * Sledujte auditní záznamy * Přezkoumejte nastavení auditních záznamů | |  | |  |  |  |  | | |
| 10.2.3 | Přístup ke všem auditním stopám? | * Rozhovor s personálem * Sledujte auditní záznamy * Přezkoumejte nastavení auditních záznamů | |  | |  |  |  |  | | |
| 10.2.4 | Neplatné pokusy o logický přístup? | * Rozhovor s personálem * Sledujte auditní záznamy * Přezkoumejte nastavení auditních záznamů | |  | |  |  |  |  | | |
| 10.2.5 | Použití a změny identifikačních a autentizačních mechanismů – mimo jiné vytváření nových účtů a zvyšování oprávnění - a všechny změny, doplnění nebo vymazání účtů s root nebo administrativními oprávněními? | * Rozhovor s personálem * Sledujte auditní záznamy * Přezkoumejte nastavení auditních záznamů | |  | |  |  |  |  | | |
| 10.2.6 | Inicializace, vypnutí nebo pozastavení auditních záznamů? | * Rozhovor s personálem * Sledujte auditní záznamy * Přezkoumejte nastavení auditních záznamů | |  | |  |  |  |  | | |
| 10.2.7 | Vytvoření a mazání objektů na systémové úrovni? | * Rozhovor s personálem * Sledujte auditní záznamy * Přezkoumejte nastavení auditních záznamů | |  | |  |  |  |  | | |
| 10.3 | Jsou zaznamenány následující položky auditních stop pro všechny systémové komponenty pro každou událost: |  | | | | | | | | | |
| 10.3.1 | Identifikace uživatele? | * Rozhovor s personálem * Sledujte auditní záznamy * Přezkoumejte nastavení auditních záznamů | |  | |  |  |  |  | | |
| 10.3.2 | Typ události? | * Rozhovor s personálem * Sledujte auditní záznamy * Přezkoumejte nastavení auditních záznamů | |  | |  |  |  |  | | |
| 10.3.3 | Datum a čas? | * Rozhovor s personálem * Sledujte auditní záznamy * Přezkoumejte nastavení auditních záznamů | |  | |  |  |  |  | | |
| 10.3.4. | Indikace úspěchu nebo selhání? | * Rozhovor s personálem * Sledujte auditní záznamy * Přezkoumejte nastavení auditních záznamů | |  | |  |  |  |  | | |
| 10.3.5 | Původ události? | * Rozhovor s personálem * Sledujte auditní záznamy * Přezkoumejte nastavení auditních záznamů | |  | |  |  |  |  | | |
| 10.3.6 | Identita nebo název dotčených dat, systémové komponenty nebo zdroje? | * Rozhovor s personálem * Sledujte auditní záznamy * Přezkoumejte nastavení auditních záznamů | |  | |  |  |  |  | | |
| 10.4 | Jsou všechny časy kritických systémů synchronizovány prostřednictvím použití technologie synchronizace a je tato technologie udržována aktuální?  ***Poznámka:*** *Jedním z příkladů technologie časové synchronizace je Protokol síťového času (Network Time Protocol, NTP).* | * Zkontrolujte standardy a procesy časové konfigurace | |  | |  |  |  |  | | |
| 10.4.1 | Jsou následující procesy implementovány pro kritické systémy tak, aby měly správný a shodný čas? |  | | | | | | | | | |
|  | (a) Získává časové signály z vnějších zdrojů pouze určený časový server a jsou časové signály z vnějších zdrojů založeny na mezinárodním atomovém čase nebo na UTC? | * Zkontrolujte standardy a procesy časové konfigurace * Přezkoumejte časové parametry systémů | |  | |  |  |  |  | | |
|  | (b) Pokud se vyskytuje více než jeden určený časový server, spolupracuje určený centrální časový server s druhým, aby zachovaly přesný čas? | * Zkontrolujte standardy a procesy časové konfigurace * Přezkoumejte časové parametry systémů | |  | |  |  |  |  | | |
|  | (c) Přijímají systémy časové informace pouze z určených centrálních časových serverů? | * Zkontrolujte standardy a procesy časové konfigurace * Přezkoumejte časové parametry systémů | |  | |  |  |  |  | | |
| 10.4.2 | Jsou časové údaje chráněny dle následujícího:  (a) Jsou přístupy k časovým údajům omezeny pouze na personál s provozní potřebou přístupu k časovým údajům? | * Přezkoumejte konfigurace systémů a nastavení synchronizace času a záznamů. | |  | |  |  |  |  | | |
| (b) Jsou jakékoli změny nastavení času na kritických systémech logovány, monitorovány a revidovány? | * Přezkoumejte konfigurace systémů a nastavení synchronizace času a záznamů. | |  | |  |  |  |  | | |
| 10.4.3 | Jsou nastavení času přijímána z časových zdrojů akceptovatelných v odvětví (z důvodu zabránění změny hodin zlomyslným jedincem)?  *Tyto změny mohou být volitelně šifrovány symetrickým klíčem a mohou být vytvořeny kontrolní seznamy specifikující IP adresy klientských počítačů pro kontrolu při aktualizaci času (pro zabránění neautorizovaného použití interních časových serverů).* | * Přezkoumejte systémové konfigurace | |  | |  |  |  |  | | |
| 10.5 | Jsou zabezpečeny auditní stopy tak, aby nemohly být měněny? |  | | | | | | | | | |
| 10.5.1 | Je omezeno prohlížení auditních stop na ty, kteří to potřebují ke své práci? | * Rozhovor se systémovými administrátory * Přezkoumejte konfigurace a oprávnění systémů | |  | |  |  |  |  | | |
| 10.5.2 | Jsou chráněny soubory auditních stop před neautorizovanými modifikacemi? | * Rozhovor se systémovými administrátory * Přezkoumejte konfigurace a oprávnění systémů | |  | |  |  |  |  | | |
| 10.5.3 | Jsou pohotově zálohovány soubory auditních stop na centralizovaný záznamový server nebo médium, které se obtížně pozměňuje? | * Rozhovor se systémovými administrátory * Přezkoumejte konfigurace a oprávnění systémů | |  | |  |  |  |  | | |
| 10.5.4 | Jsou záznamy týkající se technologií „externí“ komunikace (například bezdrátové technologie, firewally, DNS, maily) zapisovány na bezpečný, centralizovaný interní záznamový server nebo médium? | * Rozhovor se systémovými administrátory * Přezkoumejte konfigurace a oprávnění systémů | |  | |  |  |  |  | | |
| 10.5.5 | Je použit software pro sledování integrity souborů nebo software zjišťující změny v záznamech, aby bylo zajištěno, že existující data záznamů nemohou být změněna bez vygenerování varování (ačkoliv přidání nových dat by varování spustit nemělo)? | | * Přezkoumejte nastavení, monitorované soubory a výsledky z monitorovaných aktivit |  |  | |  |  | | |  | | |
| 10.6 | Jsou záznamy a bezpečnostní události pro všechny systémové komponenty zkontrolovány tak, aby bylo možné identifikovat anomálie nebo podezřelé aktivity dle následujícího?  ***Poznámka****: Pro dosažení souladu s požadavkem 10.6. mohou být využity nástroje pro sběr záznamů, analýzy a varování.* | |  | | | | | | | | | | |
| 10.6.1 | (a) Jsou písemné postupy a politiky definované pro přezkoumání následujícího nejméně jednou denně, a to buď manuálně, nebo pomocí „logovacích“ nástrojů?   * Všechny bezpečnostní události * Záznamy o všech systémových komponentách, které uchovávají, zpracovávají nebo přenášejí data držitelů karet a/nebo citlivá autentizační data (SAD) * Záznamy všech kritických systémových komponent * Záznamy všech serverů a systémových komponent, které vykonávají funkce zabezpečení (například firewally, systémy detekce narušení / prevence proti narušení systémů (IDS/IPS), autentizace serverů, přesměrující servery pro e-commerce, atd.). | | * Zkontrolujte bezpečnostní politiky a postupy |  | |  |  |  | |  | | | |
| (b) Jsou výše zmíněné záznamy a bezpečnostní události revidovány nejméně jednou denně? | | * Sledujte procesy * Rozhovor s personálem |  | |  |  |  | |  | | | |
| 10.6.2 | (a) Jsou definovány bezpečnostní politiky a postupy pro pravidelné kontroly záznamů všech ostatních systémových komponent, a to buď ručně, nebo pomocí logovacích nástrojů, založené na politikách organizace a strategie řízení rizik? | | * Zkontrolujte bezpečnostní politiky a postupy |  | |  |  |  | |  | | | |
|  | (b) Jsou kontroly všech ostatních systémových komponent prováděny v souladu s politikou organizace a strategií řízení rizik? | | * Zkontrolujte dokumentace posouzení rizik * Rozhovor s personálem |  | |  |  |  | |  | | | |
| 10.6.3 | (a) Jsou definovány bezpečnostní politiky a postupy pro posuzování výjimek a anomálií, identifikovaných během prověřování? | | * Zkontrolujte bezpečnostní politiky a postupy |  | |  |  |  |  | | |
| (b) Je během přezkumného procesu prováděno sledování výjimek a anomálií? | | * Sledujte procesy * Rozhovor s personálem |  | |  |  |  |  | | |
| 10.7 | (a) Existují politiky a postupy pro držení auditních záznamů a vyžadují, že jsou záznamy drženy nejméně jeden rok, přičemž minimálně tři měsíce musí být bezprostředně k dispozici pro analýzu (například online, archivovaná nebo obnovitelná ze záloh)? | | * Zkontrolujte bezpečnostní politiky a postupy |  | |  |  |  |  | | |
| (b) Jsou auditní záznamy drženy nejméně po dobu jednoho roku? | | * Rozhovor s personálem * Přezkoumejte auditní záznamy |  | |  |  |  |  | | |
| (c) Mohou být záznamy za minimálně tři poslední měsíce bezprostředně k dispozici pro analýzu? | | * Rozhovor s personálem * Sledujte postupy |  | |  |  |  |  | | |
| 10.8 | *Tento požadavek je platný pouze pro poskytovatele služeb* | |  |  | |  |  |  |  | | |
| 10.9 | Jsou bezpečnostní politiky a provozní postupy pro monitorování veškerého přístupu k síťovým zdrojům a datům držitelů karet?   * dokumentované * používají se * jsou známy všem dotčeným stranám? | | * Zkontrolujte bezpečnostní politiky a provozní postupy * Rozhovor s personálem |  | |  |  |  |  | | |

### Požadavek 11: Pravidelně testovat bezpečnostní systémy a procesy

| **PCI DSS Otázka** | | **Očekávané Testování** | **Odpověď**  **(zaškrtněte jednu odpověď pro každou otázku)** | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ANO** | **ANO s „CCW“** | **NE** | **N/A** | **Netestováno** |
| 11.1 | (a) Jsou zavedeny procesy k detekci a identifikaci obou autorizovaných i neautorizovaných bodů bezdrátového přístupu na čtvrtletní bázi?  ***Poznámka****: Metody, které mohou být použity, zahrnují mimo jiné skeny bezdrátových sítí, fyzické/logické kontroly systémových komponent a infrastruktury, kontrolu přístupu do sítě (Network Access control, NAC), nebo bezdrátové IDS/IPS.*  *Metody, které budou použity, musí dostatečně detekovat a identifikovat neautorizovaná zařízení.* | * Zkontrolujte politiky a postupy |  |  |  |  |  |
| (b) Detekuje a identifikuje metodologie všechny neautorizované body bezdrátového přístupu, včetně alespoň těch následujících?   * Karty WLAN vložené do systémových komponent * Přenosná nebo mobilní bezdrátová zařízení připojená na systémové komponenty k vytvoření bodu bezdrátového přístupu (například prostřednictvím USB, apod.); a * Bezdrátová zařízení připojená na síťový port nebo síťové zařízení. | * Vyhodnoťte metodologii |  |  |  |  |  |
| (c) Je-li pro identifikaci autorizovaných i neautorizovaných bezdrátových přístupových bodů využito bezdrátového skenování, je skenování prováděno nejméně čtvrtletně pro všechny systémové komponenty a zařízení? | * Přezkoumejte vystup z aktuálního skenu bezdrátové sítě |  |  |  |  |  |
| (d) Je-li využíváno automatické monitorování (například bezdrátové IDS/IPS, NAC, apod.), je monitorování nakonfigurováno tak, aby generovalo varování („alerty“) pro informování personálu? | * Přezkoumejte konfigurační nastavení |  |  |  |  |  |
| 11.1.1 | Je udržován inventární seznam autorizovaných bodů bezdrátového přístupu a dokumentováno obchodní zdůvodnění pro všechny autorizované body bezdrátového přístupu? | * Přezkoumejte inventární záznamy |  |  |  |  |  |
| 11.1.2 | (a) Definuje a vyžaduje reakci Plán Reakce na Incident (IRP) v případě, že je detekován neautorizovaný bod bezdrátového přístupu? | * Prozkoumejte plán reakce na incident (IRP) (viz. požadavek 12.10.) |  |  |  |  |  |
|  | (b) Jsou podniknuty kroky v případě odhalení neautorizovaného bodu bezdrátového přístupu? | * Rozhovor s odpovědným personálem * Zkontrolujte poslední skeny bezdrátových sítí a související odezvy |  |  |  |  |  |
| 11.2 | Jsou nejméně čtvrtletně spouštěny externí a interní skeny zranitelnosti a též po jakékoliv významné změně v síti (jako je instalace nových systémových komponent, změny v topologii sítě, úprava firewallových pravidel, upgrade produktu), dle následujícího:  ***Poznámka****: V procesu čtvrtletních skenů se mohou kombinovat reporty z více skenů, aby se prokázalo, že všechny systémy byly skenovány a všechny příslušné zranitelnosti byly řešeny. Může být vyžadována další dokumentace k ověření, že neopravené zranitelnosti jsou v řešení.*  *Pro první shodu s PCI DSS není vyžadováno, aby byly úspěšně dokončeny skeny za čtyři čtvrtletí, pokud hodnotitel ověří, že1) poslední výsledek skenu byl úspěšný, 2) subjekt má zdokumentované politiky a postupy vyžadující čtvrtletní skenování, a 3) zranitelnosti zjištěné ve výsledku skenu byly opraveny, jak je prokázáno v opakovaném skenu. V letech následujících po prvním přezkumu PCI DSS musí být absolvovány čtyři úspěšné čtvrtletní skeny.* |  | | | | | |
| 11.2.1 | (a) Jsou prováděny interní skeny zranitelnosti čtvrtletně? | * Zkontrolujte reporty skenování |  |  |  |  |  |
|  | (b) Řeší proces interního skenování zranitelností s vysokým rizikem "high risk" a zahrnuje opětovné skeny k ověření zranitelností s vysokým rizikem (jak je definováno v PCI DSS požadavku 6.1.) dokud nejsou dořešeny? | * Zkontrolujte reporty skenování |  |  |  |  |  |
|  | (c) Jsou čtvrtletní interní skeny provedeny kvalifikovaným interním zdrojem (zdroji) nebo kvalifikovanou třetí stranou, a pokud ano, existuje organizační nezávislost hodnotitele (není požadován QSA nebo ASV)? | * Rozhovor s personálem |  |  |  |  |  |
| 11.2.2 | (a) Jsou prováděny čtvrtletně externí skeny zranitelnosti?  ***Poznámka:*** *Čtvrtletní externí skeny zranitelnosti musí být prováděno Schváleným dodavatelem skenování (ASV) schváleným radou Payment Card Industry Security Standards Council (PCI SSC).*  *Odkazujeme na ASV Program Guide uveřejněný na internetových stránkách PCI SSC ohledně odpovědnosti zákazníka za skenování, přípravu skenování atd.* | * Zkontrolujte výsledky externích skenů zranitelnosti za poslední čtyři čtvrtletí |  |  |  |  |  |
| (b) Splňují výsledky externího čtvrtletního skenu a opětovného skenu požadavky průvodce programu ASV (ASV Program Guide) pro schválený sken (například nejsou zranitelnosti s dosaženým skóre 4 a výše podle CVSS a žádné automatické chyby)? | * Zkontrolujte výsledky každého externího čtvrtletního skenu a opětovného skenu |  |  |  |  |  |
| (c) Jsou čtvrtletní skeny externí zranitelnosti prováděny prostřednictvím PCI SSC Schváleného dodavatele skenování (ASV)? | * Zkontrolujte výsledky každého externího čtvrtletního skenu a opětovného skenu |  |  |  |  |  |
| 11.2.3 | (a) Jsou prováděny interní a externí skeny, a podle potřeby opětovné skeny, po každé významné změně?  ***Poznámka****: Skeny musí být prováděny kvalifikovanou osobou* | * Přezkoumejte a korelujte dokumentaci řízení změn a reporty skenů. |  |  |  |  |  |
| (b) Zahrnuje proces skenování opakované skeny, dokud:   * Pro externí skeny neexistují zranitelnosti, které by dosáhly skóre 4.0 či více podle CVSS? * Pro interní skeny byl získán schvalující výsledek nebo jsou všechny „High-risk“ zranitelnosti definované v PCI DSS Požadavku 6.1. vyřešeny? | * Zkontrolujte reporty skenování |  |  |  |  |  |
| (c) Jsou skeny provedeny kvalifikovaným interním zdrojem (zdroji) nebo kvalifikovanou externí třetí stranou, a pokud ano, existuje organizační nezávislost hodnotitele (není požadován QSA nebo ASV)? | * Rozhovor s personálem |  |  |  |  |  |
| 11.3 | Zahrnuje metodologie pro penetrační testování následující body?   * Testování je založeno na přístupech penetračního testování přijatém v IT oboru (např. normě NIST SP800-115) * Zahrnuje pokrytí pro celé ohraničené prostředí dat držitelů karet a kritických systémů * Zahrnuje interní i externí testování sítě * Obsahuje testy pro ověření segmentace a kontroly pro snižování rozsahu * Definuje penetrační testy aplikační vrstvy, které zahrnují minimálně zranitelnosti uvedené v Požadavku 6.5 * Definuje penetrační testy síťové vrstvy, které zahrnují komponenty podporující síťové funkce a také operační systémy * Zahrnuje přezkoumání a posouzení hrozeb a zranitelností během posledních 12 měsíců * Určuje držení výsledků testování penetrace a výsledků nápravných akcí. | * Přezkoumejte metodologii penetračního testování * Rozhovor s odpovědným personálem |  |  |  |  |  |
| 11.3.1 | (a) Je externí penetrační test provedennejméně jednou ročně, podle definované metodologie, po všech významných změnách v prostředí (infrastruktura nebo aplikace), jako například upgrade operačního systému, rozšíření části sítě do prostředí nebo přidání webového serveru? | * Přezkoumejte rozsah činností * Přezkoumejte výsledky z posledního externího penetračního testu. |  |  |  |  |  |
| (b) Byl proveden test kvalifikovaným interním zdrojem nebo kvalifikovanou externí třetí stranou, a je-li to případné, existuje organizační nezávislost testera (nemusí být QSA nebo ASV)? | * Rozhovor s odpovědným personálem |  |  |  |  |  |
| 11.3.2 | (a) Jsou prováděny interní testy penetrace nejméně jednou ročně a po jakékoliv významné změně infrastruktury nebo aktualizace či modifikace aplikace (jako například upgrade operačního systému, podsíť přidaná k prostředí nebo webový server přidaný k prostředí)? | * Přezkoumejte rozsah činností * Přezkoumejte výsledky z posledního interního penetračního testu. |  |  |  |  |  |
|  | (b) Jsou testy prováděny kvalifikovaným interním zdrojem nebo kvalifikovanou externí třetí stranou, a je-li to případné, existuje organizační nezávislost testera (nemusí být QSA nebo ASV)? | * Rozhovor s odpovědným personálem |  |  |  |  |  |
| 11.3.3 | Jsou zjištěné zneužitelné zranitelnosti opraveny a opakované testování potvrdilo, že zranitelnost byla opravena? | * Přezkoumejte výsledky penetračního testování |  |  |  |  |  |
| 11.3.4 | Pokud se segmentace používá k oddělení prostředí dat držitelů karet (CDE) od jiných sítí: |  | | | | | |
| (a) Jsou pro testování všech metod segmentace definovány postupy penetračního testování, k potvrzení, že jsou funkční a efektivní a izolují všechny systémy mimo rozsah od systémů v prostředí dat držitelů karet (CDE)? | * Přezkoumejte řízení segmentace * Zkontrolujte metodologii penetračního testování |  |  |  |  |  |
| (b) Splňuje penetrační testování k ověření řízení segmentace následující?   * Je provedeno nejméně jednou ročně a po každé změně kontroly / metody segmentace. * Pokrývá všechny používané kontroly / metody segmentace. * Ověřuje, že metody segmentace jsou funkční a efektivní, a izolují všechny systémy mimo rozsah od systémů v prostředí dat držitelů karet (CDE). | * Přezkoumejte výsledky z posledního penetračního testu |  |  |  |  |  |
|  | (c) Jsou testy prováděny kvalifikovanými interními zdroji nebo kvalifikovanou třetí stranou a pokud ano, existuje zde organizační nezávislost testujícího (není třeba aby byl QSA nebo ASV)? | * Rozhovor s odpovědným personálem |  |  |  |  |  |
| 11.3.4.1 | *Pouze pro poskytovatele služeb:* Pokud je použitá segmentace: |  |  |  |  |  |  |
| 11.4 | (a) Jsou nasazeny techniky (jako je detekce narušení systémů a/nebo systémy prevence proti narušení) k monitorování veškeré komunikace:   * Na hranici prostředí dat držitelů karet * V kritických bodech v prostředí dat držitelů karet | * Přezkoumejte konfigurace systémů * Přezkoumejte síťové diagramy |  |  |  |  |  |
| (b) Jsou techniky detekce narušení a/ nebo prevence narušení konfigurovány tak, aby varovali personál před podezřelými průniky? | * Přezkoumejte konfigurace systémů * Rozhovor se vzorkem odpovědného personálu |  |  |  |  |  |
| (c) Jsou všechna zařízení provádějící detekce narušení a/ nebo prevence narušení udržovány a aktualizovány podle pokynů dodavatele k zajištění optimální ochrany? | * Přezkoumejte konfigurace IDS / IPS * Přezkoumejte dokumentace dodavatelů |  |  |  |  |  |
| 11.5 | (a) Je nasazen mechanismus detekce změn (například nástroje monitorování integrity souborů) pro detekování neautorizovaných modifikací (včetně změn, doplnění a odstranění) kritických systémových souborů, konfigurační soubory nebo obsah souboru?  *Příklady souborů, které by měly být monitorovány:*   * *Systémové spustitelné soubory (k interpretování programů, executables).* * *Spustitelné soubory aplikace (executables)* * *Konfigurace a soubory parametrů* * *Centrálně uložené, historické nebo archivované, trasovací (log) a auditní soubory* * *Další kritické soubory určené subjektem (například pomocí vyhodnocení rizika nebo jinými způsoby).* | * Sledujte nastavení systému a monitorované soubory * Přezkoumejte nastavení konfigurace systémů |  |  |  |  |  |
|  | (b) Je mechanismus konfigurován tak, aby varoval personál při neautorizovaných modifikacích (včetně změn, doplnění a odstranění) kritických systémových souborů, konfiguračních souborů nebo souborů obsahu a je minimálně jednou týdně prováděno porovnání kritických souborů?  ***Poznámka****: Pro účely detekce změn jsou kritické soubory obvykle ty, které se pravidelně nemění, ale jejich modifikace může signalizovat narušení nebo riziko narušení systému. Mechanismy detekce změn, jako jsou produkty monitorování integrity souborů, jsou obvykle dodávány s předkonfigurovanými kritickými soubory pro příslušný operační systém. Další kritické soubory, jako například ty pro aplikace na zakázku, musí být vyhodnoceny a definovány subjektem (tj. obchodníkem nebo poskytovatelem služeb).* | * Sledujte nastavení systému a monitorované soubory * Zkontrolujte výsledky z monitorovaných činností |  |  |  |  |  |
| 11.5.1 | Je implementován proces k reakci na každé upozornění generované mechanismem detekce změn? | * Přezkoumejte nastavení konfigurace systémů |  |  |  |  |  |
| 11.6 | Jsou bezpečnostní politiky a provozní postupy pro monitorování bezpečnosti a testování:   * dokumentovány * používají se * jsou známy všem dotčeným stranám? | * Přezkoumejte bezpečnostní politiky a provozní postupy * Rozhovor s personálem |  |  |  |  |  |

## Udržování politiky informační bezpečnosti

### Požadavek 12: Udržovat politiku zaměřenou na informační bezpečnost pro všechen personál

***Poznámka:*** *Pro účely požadavku 12 se „personálem“ rozumí zaměstnanci pracující na plný i zkrácený úvazek, na dobu určitou, i kontraktoři a konzultanti, kteří jsou rezidenty v místě subjektu anebo mají přístup do systémů a prostředí obsahujících data držitelů karet (CDE).*

| **PCI DSS Otázka** | | **Očekávané Testování** | **Odpověď**  **(zaškrtněte jednu odpověď pro každou otázku)** | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ANO** | **ANO s „CCW“** | **NE** | **N/A** | **Netestováno** |
| 12.1 | Je bezpečnostní politika zavedena, zveřejněna, udržována a rozšířena veškerému příslušnému personálu? | * Zkontrolujte politiku informační bezpečnosti |  |  |  |  |  |
| 12.1.1 | Je bezpečnostní politika zkontrolována nejméně jednou ročně a aktualizována pokaždé změně prostředí? | * Zkontrolujte politiku informační bezpečnosti * Rozhovor s odpovědným personálem |  |  |  |  |  |
| 12.2 | (a) Je proces vyhodnocování rizik, který identifikuje aktiva, hrozby a zranitelnosti, implementován tak, že:   * identifikuje kritická aktiva, hrozby a zranitelnosti * vyúsťuje ve formální dokumentovanou analýzu rizik?   *Příklady metodologie vyhodnocení rizik zahrnují, kromě jiného, OCTAVE, ISO 27005 and NIST SP 800-30.* | * Zkontrolujte proces ročního posouzení rizik * Rozhovor s personálem |  |  |  |  |  |
| (b) Je proces vyhodnocování rizik prováděn nejméně jednou ročně a po významné změně prostředí (např. nabytí, fúze, přemístění, atd.)? | * Zkontrolujte dokumentace posouzení rizik * Rozhovor s odpovědným personálem |  |  |  |  |  |
| 12.3 | Jsou používané politiky pro kritické technologie vyvíjeny tak, aby definovaly správné užívání těchto technologií a vyžadovaly následující  ***Poznámka****: Příklady kritických technologií zahrnují, kromě jiného, vzdálený přístup a bezdrátové technologie, notebooky, tablety, vyjímatelná média, používání emailu a používání internetu.* |  | | | | | |
| 12.3.1 | Výslovné schválení autorizovanými stranami k použití technologií? | * Zkontrolujte politiky používání * Rozhovor s odpovědným personálem |  |  |  |  |  |
| 12.3.2 | Autentizace pro užívání technologie? | * Zkontrolujte politiky používání * Rozhovor s odpovědným personálem |  |  |  |  |  |
| 12.3.3 | Seznam všech takovýchto zařízení a personálu s přístupem? | * Zkontrolujte politiky používání * Rozhovor s odpovědným personálem |  |  |  |  |  |
| 12.3.4 | Metoda, jak přesně a snadno určit vlastníka, kontaktní informace a účel (např. označování, kódování a/nebo inventarizace zařízení)? | * Zkontrolujte politiky používání * Rozhovor s odpovědným personálem |  |  |  |  |  |
| 12.3.5 | Přijatelné použití technologie? | * Zkontrolujte politiky používání * Rozhovor s odpovědným personálem |  |  |  |  |  |
| 12.3.6 | Akceptovatelné umístění v síti pro technologie? | * Zkontrolujte politiky používání * Rozhovor s odpovědným personálem |  |  |  |  |  |
| 12.3.7 | Seznam společností schválených produktů? | * Zkontrolujte politiky používání * Rozhovor s odpovědným personálem |  |  |  |  |  |
| 12.3.8 | Automatické odpojení relace u technologií s dálkovým přístupem po stanovené době nečinnosti? | * Zkontrolujte politiky používání * Rozhovor s odpovědným personálem |  |  |  |  |  |
| 12.3.9 | Aktivace technologií s dálkovým přístupem pro dodavatele a obchodní partnery pouze tehdy, pokud to dodavatelé a obchodní partneři potřebují, s okamžitou deaktivací po použití? | * Zkontrolujte politiky používání * Rozhovor s odpovědným personálem |  |  |  |  |  |
| 12.3.10 | (a) Je při přístupu personálu k datům držitelů karet prostřednictvím technologií s dálkovým přístupem zakázáno kopírování, přesuny a uchovávání dat držitelů karet na lokálních pevných discích a výměnných elektronických médiích, pokud to není výslovně povoleno pro definovaný provozní účel?  *Kde je provozní potřeba oprávněna, musí politiky použití vyžadovat ochranu dat v souladu s platnými požadavky PCI DSS.* | * Zkontrolujte politiky používání * Rozhovor s odpovědným personálem |  |  |  |  |  |
|  | (b) Vyžadují používané politiky pro personál s oprávněným pověřením pro přístup k datům držitelů karet ochranu těchto dat v souladu s požadavky PCI DSS? | * Zkontrolujte politiky používání * Rozhovor s odpovědným personálem |  |  |  |  |  |
| 12.4 | Definuje jasně bezpečnostní politika a postupy odpovědnost v oblasti informační bezpečnosti pro všechen personál? | * Zkontrolujte politiku a postupy informační bezpečnosti * Rozhovor se vzorkem odpovědného personálu |  |  |  |  |  |
| 12.4.1 | *Tento požadavek je platný pouze pro poskytovatele služeb.* |  | | | | | |
| 12.5 | (a) Je odpovědnost pro informační bezpečnost formálně svěřena hlavnímu bezpečnostnímu pracovníkovi (Chief Security Officer) nebo jinému členovi vedení obeznámenému s problematikou bezpečnosti? | * Zkontrolujte politiky a postupy informační bezpečnosti |  |  |  |  |  |
|  | (b) Jsou následující odpovědnosti řízení informační bezpečnosti formálně přiděleny jedinci nebo týmu: |  | | | | | |
| 12.5.1 | Jsou zavedeny, dokumentovány a distribuovány bezpečnostní politiky a postupy? | * Zkontrolujte politiky a postupy informační bezpečnosti |  |  |  |  |  |
| 12.5.2 | Je monitorováno a analyzováno bezpečnostní varování a informace a distribuováno k příslušnému personálu? | * Zkontrolujte politiky a postupy informační bezpečnosti |  |  |  |  |  |
| 12.5.3 | Vytváření, dokumentování a distribuce reakcí na bezpečnostní incidenty a eskalačních postupů k zajištění včasného a efektivního nakládání s nimi za všech situací? | * Zkontrolujte politiky a postupy informační bezpečnosti |  |  |  |  |  |
| 12.5.4 | Jsou spravovány uživatelské účty, včetně přidávání, mazání a modifikací? | * Zkontrolujte politiky a postupy informační bezpečnosti |  |  |  |  |  |
| 12.5.5 | Jsou monitorovány a kontrolovány všechny přístupy ke karetním datům? | * Zkontrolujte politiky a postupy informační bezpečnosti |  |  |  |  |  |
| 12.6 | (a) Existuje a poskytuje formální program bezpečnostního povědomí celému personálu informace o politikách a postupech bezpečnosti dat držitelů karet? | * Zkontrolujte program povědomí o bezpečnosti |  |  |  |  |  |
| (b) Zahrnují postupy bezpečnostního programu informovanosti následující? |  | | | | | |
| 12.6.1 | (a) Poskytuje program bezpečnostního povědomí četné metody komunikace povědomí a vzdělávání personálu (například plakáty, dopisy, vzkazy, webový trénink, porady a propagace)?  ***Poznámka****: Metody se mohou měnit v závislosti na roli personálu a jejich úrovně přístupu k datům držitele karet.* | * Zkontrolujte program povědomí o bezpečnosti * Zkontrolujte postupy programu povědomí o bezpečnosti. * Zkontrolujte záznamy návštěvnosti programu povědomí o bezpečnosti |  |  |  |  |  |
| (b) Účastní se personál školení o bezpečnosti po nástupu a nejméně jednou ročně? | * Přezkoumejte postupy a dokumentaci programu povědomí o bezpečnosti |  |  |  |  |  |
| (c) Dokončili zaměstnanci školení týkající se bezpečnostní informovanosti a jsou si vědomi důležitosti zabezpečení dat držitelů karet? | * Rozhovor s personálem |  |  |  |  |  |
| 12.6.2 | Je od personálu nejméně jednou ročně vyžadováno potvrzení, že četli a pochopili bezpečnostní politiku a postupy? | * Přezkoumejte postupy a dokumentaci programu povědomí o bezpečnosti |  |  |  |  |  |
| 12.7 | Je potenciální personál (viz. definice personálu výše) před přijetím prověřován, aby se minimalizovala rizika útoků z interních zdrojů?  *(Například posuzování zázemí zahrnuje historii předchozích zaměstnání, trestní rejstřík, úvěrovou historii a prověření referencí.)*  ***Poznámka****: Pro potencionální personál, jako jsou například pokladní v obchodech, kteří mají přístup vždy jen k jedné kartě při provádění transakce, je tento požadavek pouhým doporučením.* | * Rozhovor s vedením personálního oddělení |  |  |  |  |  |
| 12.8 | Jsou udržovány a implementovány politiky a postupy pro řízení poskytovatelů služeb, s nimiž jsou data držitelů karet sdílena, nebo kteří by mohli mít vliv na bezpečnost dat držitelů karet, dle následujícího: |  | | | | | |
| 12.8.1 | Je udržován seznam poskytovatelů služeb včetně popisu poskytovaných služeb? | * Zkontrolujte politiky a postupy * Sledujte procesy * Zkontrolujte seznam poskytovatelů služeb. |  |  |  |  |  |
| 12.8.2 | Je udržována písemná smlouva, která zahrnuje ujednání, že poskytovatelé služeb jsou zodpovědní za bezpečnost dat držitelů karet, kterými poskytovatelé služeb disponují nebo jinak uchovávají, zpracovávají nebo přenášejí jménem zákazníka, nebo v rozsahu, v jakém mohou mít vliv na bezpečnost prostředí dat držitelů karet zákazníka?  ***Poznámka****: Přesné znění ujednání bude záviset na dohodě mezi oběma stranami, s uvedením podrobností o poskytované službě a odpovědnostmi každé strany. Ujednání nemusí obsahovat přesné znění uvedené v tomto požadavku.* | * Sledujte písemné smlouvy * Zkontrolujte politiky a postupy |  |  |  |  |  |
| 12.8.3 | Je zajištěno zavedení procesu zapojení poskytovatelů služeb, včetně „due diligence“ před uzavřením závazku? | * Sledujte procesy * Zkontrolujte politiky a postupy a podpůrné dokumentace |  |  |  |  |  |
| 12.8.4 | Je udržován program k monitorování stavu shody poskytovatele služeb se standardem PCI DSS nejméně jedenkrát ročně? | * Sledujte procesy * Zkontrolujte politiky a postupy a podpůrné dokumentace |  |  |  |  |  |
| 12.8.5 | Jsou udržovány informace o tom, které požadavky PCI DSS jsou spravované každým poskytovatelem služeb, a které jsou řízeny subjektem? | * Sledujte procesy * Zkontrolujte politiky a postupy a podpůrné dokumentace |  |  |  |  |  |
| 12.9 | *Tento požadavek je platný pouze pro poskytovatele služeb* |  | | | | | |
| 12.10 | Byl implementován plán reakce na incident (IRP) tak, aby neprodleně reagoval na narušení systému, dle následujícího: |  | | | | | |
| 12.10.1 | (a) Byl vytvořen plán reakce na incident (IRP) tak, aby mohl být implementován v případě události narušení systému? | * Zkontrolujte plán reakce na incident (IRP) * Zkontrolujte postupy plánu reakce na incident (IRP) |  |  |  |  |  |
| (b) Řeší plán minimálně: |  | | | | | |
| * Role, odpovědnosti, komunikační a kontaktní strategie v případě narušení včetně vyrozumění kartových společností? | * Zkontrolujte postupy plánu reakce na incident (IRP) |  |  |  |  |  |
| * Specifické postupy reakce na incidenty? | * Zkontrolujte postupy plánu reakce na incident (IRP) |  |  |  |  |  |
| * Postupy obnovení a zachování kontinuity provozu? | * Zkontrolujte postupy plánu reakce na incident (IRP) |  |  |  |  |  |
| * Procesy zálohování dat? | * Zkontrolujte postupy plánu reakce na incident (IRP) |  |  |  |  |  |
| * Analýza zákonných požadavků pro reporting narušení? | * Zkontrolujte postupy plánu reakce na incident (IRP) |  |  |  |  |  |
| * Pokrytí a reakce všech kritických systémových komponent? | * Zkontrolujte postupy plánu reakce na incident (IRP) |  |  |  |  |  |
| * Odkazy nebo zahrnutí postupů odezvy na incident od kartových společností? | * Zkontrolujte postupy plánu reakce na incident (IRP) |  |  |  |  |  |
| 12.10.2 | Je plán testován nejméně jednou ročně, včetně požadavků vyjmenovaných v 12.10.1? | * Zkontrolujte postupy Plánu reakce na incident (IRP) * Rozhovor s odpovědným personálem |  |  |  |  |  |
| 12.10.3 | Je určen konkrétní personál, který budou k dispozici 24 hodin 7 dní v týdnu (24/7), aby reagovali na varování? | * Sledujte postupy * Zkontrolujte politiky * Rozhovor s odpovědným personálem |  |  |  |  |  |
| 12.10.4 | Je poskytováno personálu, který má odpovědnost za případné narušení bezpečnosti, odpovídající školení? | * Sledujte procesy * Zkontrolujte postupy Plánu reakce na incident (IRP) * Rozhovor s odpovědným personálem |  |  |  |  |  |
| 12.10.5 | Jsou zahrnuta varování z bezpečnostních monitorovacích systémů, která se týkají kromě jiného detekce narušení, prevence narušení, firewallů a sledování integrity souborů? | * Sledujte procesy * Zkontrolujte postupy Plánu reakce na incident (IRP) |  |  |  |  |  |
| 12.10.6 | Jsou vyvinuty postupy modifikace a zdokonalení plánu odezvy podle získaných ponaučení s přihlédnutím k vývoji v oboru? | * Sledujte procesy * Zkontrolujte postupy Plánu reakce na incident (IRP) * Rozhovor s odpovědným personálem |  |  |  |  |  |
| 12.11 | *Tento požadavek je platný pouze pro poskytovatele služeb* |  |  |  |  |  |  |

## Příloha A1: Dodatečné požadavky PCI DSS na poskytovatele sdíleného hostingu

Tato příloha není určena pro obchodníka.

## Příloha A2: Dodatečné požadavky na subjekty používající SSL/dříve TLS pro transakce za fyzické přítomnosti platební karty u POS POI terminálových připojení

| **PCI DSS Otázka** | | **Očekávané Testování** | **Odpověď**  **(zaškrtněte jednu odpověď pro každou otázku)** | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **ANO** | **ANO s „CCW“** | **NE** | **N/A** | **Netestováno** |
| A2.1 | *Pro POS POI terminály (****u obchodníka nebo v místě akceptace plateb****) používající SSL a/nebo dříve TLS:* Jsou zařízení potvrzena, že nejsou náchylná k žádným známým zneužitím pro SSL dříve TLS?  ***Poznámka:*** *Tento požadavek je zamýšlen tak, aby se vztahoval na subjekty, s POS POI terminálem, jako je obchodník. Tento požadavek není zamýšlen pro poskytovatele služeb, kteří slouží jako konečný nebo připojovací bod pro tyto POS POI terminály, požadavky A2.2 a A2.3 se vztahují k POS POI poskytovatelům služeb.* | * Zkontrolujte dokumentaci (například dokumentaci dodavatele, detaily konfigurace systému/sítě, které ověřují, že POS POI zařízení nejsou náchylná na žádná známá zneužití pro SSl/dříve TLS |  |  |  |  |  |
| A2.2 | *Tento požadavek je platný pouze pro poskytovatele služeb.* |  |  |  |  |  |  |
| A2.3 | *Tento požadavek je platný pouze pro poskytovatele služeb.* |  |  |  |  |  |  |

Příloha A3: Dodatečné hodnocení pro specifické subjekty DESV (Designated Entities Supplemental Validation)  
  
Tato příloha se týká pouze subjektů určených kartovou společností nebo acquirerem, po kterých je vyžadována další validace stávajících PCI DSS požadavků. Subjekty, od kterých se vyžaduje validace této přílohy, by měly k hlášení využít DESV Supplemental Reporting Template a Supplemental Attestation of Compliance a konzultovat postup jejich podání s příslušnou kartovou společností a/nebo acquirerem.

## Příloha B: Pracovní list náhradního řešení

*Použijte tuto pracovní list k definování náhradních řešení pro každý požadavek, u kterého bylo zaškrtnuto „ANO s CCW“.*

***Poznámka:*** *Pouze společnosti, které podstoupily analýzu rizik a mají legitimní technologické nebo zdokumentované provozní obtíže, mohou při plnění shody uvažovat o náhradních řešeních.*

*Pro více informací o náhradním řešení a pokynech, jak vyplnit tuto pracovní list, se podívejte na přílohy B, C a D standardu PCI DSS.*

**Číslo a definice Požadavku:**

|  |  |  |
| --- | --- | --- |
|  | **Požadovaná informace** | **Vysvětlení** |
| 1. **Omezení** | Seznam omezení znemožňující shodu s původním požadavkem. |  |
| 1. **Cíl** | Definovat cíl původní kontroly, identifikovat cíl splněný kompenzační kontrolou. |  |
| 1. **Identifikované riziko** | Identifikovat jakékoli další riziko způsobené absencí původní kontroly. |  |
| 1. **Definice kompenzační kontroly** | Definovat kompenzační kontroly a vysvětlit, jak jsou řešeny cíle původní kontroly a zvýšená rizika, pokud jsou nějaká. |  |
| 1. **Validace kompenzační kontroly** | Definovat, jak byly kompenzační kontroly ověřeny a testovány. |  |
| 1. **Udržování** | Definovat uplatňované procesy a kontroly k udržování kompenzačních kontrol. |  |

## Příloha C: Vysvětlení pro „Nevztahuje se”(N/A)

*Pokud byl v dotazníku zaškrtnut sloupec “N/A” (Not Applicable), použijte tento pracovní list k vysvětlení, proč související požadavek nelze ve vaší organizaci uplatnit.*

|  |  |
| --- | --- |
| **Požadavek** | **Důvod proč požadavek nelze uplatnit** |
| Příklad:3.4 | Data držitelů karet nejsou nikdy ukládána elektronicky |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

## Příloha D: Vysvětlení Požadavku „Netestováno”

*Pokud je ve sloupci zaškrtnuto „Netestováno“, použijte tuto pracovní list k vysvětlení, proč související požadavek nebyl zahrnut do části hodnocení.*

|  |  |  |
| --- | --- | --- |
| **Požadavek** | **Popis, která část/části požadavku nebyla testována** | **Popis, proč požadavek nebyl testován** |
| *Příklady:* | | |
| *Požadavek 12* | *Požadavek 12.2 byl jediným požadavkem, který byl testován. Všechny další požadavky Požadavku 12 byly vyloučeny.* | *Toto hodnocení zahrnuje pouze požadavky patřící do Milestone 1 „Prioritního Přístupu“ (Prioritized Approach).* |
| *Požadavek 1-8, 10-12* | *Pouze Požadavek 9 byl zahrnut do tohoto hodnocení. Všechny další požadavky byly vyloučeny.* | *Společnost je poskytovatelem fyzického hostingu (CO-LO) a pouze fyzická bezpečnost byla zahrnuta v tomto hodnocení.* |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# 

# Oddíl 3: Validace a podrobnosti o osvědčení

|  |  |
| --- | --- |
| **Část 3. Ověření podle standardu PCI DSS** | |
| **Toto AOC je založeno na výsledcích uvedených v SAQ D (Část 2), datováno** *( datum dokončení SAQ),* Na základě výsledků zdokumentovaných v SAQ D poznamenáno výše, podepsané osoby identifikované v části 3b-3d, podle potřeby, potvrzují následující stav shody pro subjekt identifikovaný v části 2 tohoto dokumentu (**zaškrtněte jedno**): | |
|  | **Shoda**: Všechny oddíly dotazníku PCI DSS SAQ jsou vyplněné, na všechny otázky je dána kladná odpověď, takže výsledkem je celkový rating SHODA. Tímto (Název společnosti) prokázal plnou shodu s  PCI DSS. |
|  | **Není shoda:** Nejsou vyplněny všechny oddíly dotazníku PCI DSS SAQ nebo ne na všechny otázky je odpověď kladná, takže výsledkem je celkový rating **NENÍ SHODA.** Tímto (Název společnosti)neprokázal plnou shodu s PCI DSS.  **Cílové datum** pro dosažení shody:  Subjekt předkládající tento formulář se statutem „**Není shoda“** může být požádán, aby vyplnil Akční plán v Části 4 tohoto dokumentu. *Před vyplňováním Části 4 postup ověřte u své zpracovatelské banky nebo platební společnosti (platebních společností).* |
|  | **Shoda, ale s právními výjimkami**: U jednoho nebo více požadavků bylo zaškrtnuto „NE“ kvůli právnímu omezení, které znemožňuje splnění konkrétního požadavku. Tato možnost vyžaduje další revizi od zpracovatele (acquirera) nebo platebních asociací.  *Je-li zaškrtnuto, vyplňte následující:*   |  |  | | --- | --- | | **Nesplněný požadavek** | **Detaily, jakým způsobem právní omezení zabraňuje splnění požadavku** | |  |  | |  |  | |

| **Část 3a. Potvrzení stavu** | |
| --- | --- |
| **Podepisující potvrzuje:** *(zaškrtněte vše, co se hodí)* | |
|  | Dotazník pro sebehodnocení D PCI DSS, verze *číslo verze,* byl vyplněn podle pokynů zde uvedených. |
|  | Všechny informace ve výše uvedeném SAQ a v tomto osvědčení věrně zobrazují výsledky mého hodnocení ve všech významných ohledech. |
|  | Potvrdil jsem společně se svým dodavatelem platební aplikace, že platební systém neuchovává citlivá autentizační data po autorizaci |
|  | Přečetl jsem PCI DSS a uznávám, že musím vždy zachovávat udržovat plnou shodu s PCI DSS, příslušnou mému prostředí. |
|  | V případě změny mého prostředí, uznávám, že musím přehodnotit své prostředí a implementovat všechny další příslušné PCI DSS požadavky |
|  | V ŽÁDNÝCH systémech přezkoumaných během tohoto hodnocení nebyl nalezen žádný důkaz uchovávání  dat obsažených na magnetickém proužku (tj. stopě)[[1]](#footnote-1), dat CAV2, CVC2, CID nebo CVV2[[2]](#footnote-2) ani dat PIN[[3]](#footnote-3) po autorizaci transakce |
|  | ASV skeny jsou vyhotoveny PCI SSC schváleným dodavatelem skenováníASV(PCI SSC Approved Scanning Vendor) (ASV název) |

|  |  |
| --- | --- |
| **Část 3b. Osvědčení obchodníka** | |
|  | |
| *Podpis výkonného ředitele obchodníka* 🡩 | *Datum:* |
| *Jméno výkonného ředitele obchodníka:* | *Funkce:* |

|  |  |  |
| --- | --- | --- |
| **Část 3c. Qualified Security Assessor (QSA) Potvrzení (v případě potřeby)** | | |
| Pokud byl QSA zapojen nebo pomáhal u tohoto hodnocení popište jeho roli: |  | |
|  | | |
| *Podpis řádně pověřeného úředníka QSA🡩* | | *Datum:* |
| *Jméno řádně pověřeného úředníka:* | | *Společnost QSA:* |
|  | | |
| **Část 3d. Internal Security Assessor (ISA) Potvrzení (v případě potřeby)** | | |
| Pokud byl ISA zapojen nebo pomáhal u tohoto hodnocení, identifikujte ISA osobu a popište jeho roli: |  | |
|  | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Část 4. Akční plán pro požadavky se stavem Není shoda | | | | |
| Vyberte u každého požadavku vhodný „stav shody s požadavky PCI DSS“. Jestliže na kterýkoli z těchto požadavků odpovíte „NE“, může od Vás být požadováno poskytnutí data, kdy Vaše společnost očekává dosažení shody s požadavkem a stručný popis akcí, které se provádějí ke splnění požadavku.  *Před vyplňováním Části 4 postup ověřte u své zpracovatelské banky nebo platební společnosti (platebních společností).* | | | | |
| **Požadavek PCI DSS** | **Popis požadavku** | **Statut shody** (vyberte jedno) | | **Datum a akce nápravy** (je-li statut shody  „NENÍ SHODA“) |
| **ANO** | **NE** |
| 1 | Instalovat a udržovat konfiguraci firewallu na ochranu dat držitelů karet |  |  |  |
| 2 | Nepoužívat výchozí nastavení od dodavatele pro systémová hesla a jiné bezpečnostní parametry |  |  |  |
| 3 | Chránit uchovávaná data držitelů karet |  |  |  |
| 4 | Zašifrovat přenos dat držitelů karet po otevřených veřejných sítích |  |  |  |
| 5 | Chránit všechny systémy proti malware a pravidelně aktualizovat antivirový software nebo programy |  |  |  |
| 6 | Vyvíjet a udržovat bezpečné systémy a aplikace |  |  |  |
| 7 | Omezit přístup k datům držitelů karet jen podle oprávněné potřeby |  |  |  |
| 8 | Identifikovat a autentizovat přístup k systémovým komponentám |  |  |  |
| 9 | Omezit fyzický přístup k datům držitelů karet |  |  |  |
| 10 | Sledovat a monitorovat všechny přístupy k síťovým zdrojům a datům držitelů karet |  |  |  |
| 11 | Pravidelně testovat bezpečnostní systémy a procesy |  |  |  |
| 12 | Udržovat politiku zaměřenou na informační bezpečnost pro všechen personál |  |  |  |
| Příloha A2 | Dodatečné požadavky na subjekty používající SSL/dříve TLS pro transakce za fyzické přítomnosti platební karty u POS POI terminálových připojení |  |  |  |



1. Data zašifrovaná na magnetickém proužku používaná k autorizaci během transakce s přítomností karty. Subjekty si nesmějí ponechat úplná data z magnetického proužku po autorizaci transakce. Jediné prvky dat na stopě, které smějí být zachovány, jsou číslo karty (PAN), datum expirace a jméno držitele karty. [↑](#footnote-ref-1)
2. Trojciferná nebo čtyřciferná hodnota sloužící k ověření transakcí bez přítomnosti karty a vytištěná na podpisovém proužku nebo napravo od něj nebo na lícové straně platební karty. [↑](#footnote-ref-2)
3. Osobní identifikační číslo zadané držitelem karty během transakce s přítomností karty a/nebo zašifrovaný PIN blok uvedený ve zprávě o transakci. [↑](#footnote-ref-3)