

Odvětví platebních karet (PCI)

Standard bezpečnosti dat (DSS)  
  
Dotazník pro sebehodnocení B-IP  
a Osvědčení o shodě

Obchodníci se samostatným PTS POI terminálem připojeným pomocí IP – bez elektronického uchovávání dat držitelů karet

Pro užití s PCI DSS verze 3.2.1  
  
Revize 1.0.

Červen 2018

# Změny dokumentu

| **Datum** | **Verze** | **Revize SAQ** | **Popis** |
| --- | --- | --- | --- |
| N/A | 1.0 |  | Nepoužité |
| N/A | 2.0 |  | Nepoužité |
| únor 2014 | 3.0 |  | Nové SAQ pro požadavky aplikovatelné na obchodníky, kteří zpracovávají kartová data pomocí samostatného terminálu schváleného jako PTS POI zařízení s IP konektivitou na procesora.  Obsahuje sladění s požadavky PCI DSS verze 3.0 a testovacími procedurami. |
| 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. |
| 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 změn dokumentu, aby odrážel požadavky přidané v aktualizaci duben 2016 Aktualizace sekce „Než začnete“, aby vysvětlovala termín „SCR“ a záměr povolených systémů.  Přidán požadavek 8.3.1 v souladu se záměrem požadavku 2.3. Přidán požadavek 11.3.4 k ověření řízení segmentace, pokud je segmentace používána. |
| 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](#_Toc13755458)

[Obsah 2](#_Toc13755459)

[Než začnete 3](#_Toc13755460)

[PCI DSS – Postup vyplnění sebehodnotícího dotazníku 3](#_Toc13755461)

[Jak porozumět sebehodnotícímu dotazníku 4](#_Toc13755462)

[Očekávané testování 4](#_Toc13755463)

[Vyplnění sebehodnotícího dotazníku 5](#_Toc13755464)

[Postup v případech, kdy nelze aplikovat dané požadavky 5](#_Toc13755465)

[Výjimky ze zákona 5](#_Toc13755466)

[Oddíl 1: Informace o hodnocení 6](#_Toc13755467)

[Oddíl 2: Dotazník pro sebehodnocení B-IP 9](#_Toc13755468)

[Vybudování a udržování bezpečné sítě a systémů 9](#_Toc13755469)

[Požadavek 1: Instalovat a udržovat konfiguraci firewallů za účelem ochrany dat držitelů karet 9](#_Toc13755470)

[Požadavek 2: Nepoužívat výchozí nastavení od dodavatele pro systémová hesla a jiné bezpečnostní parametry 11](#_Toc13755471)

[Ochrana dat držitelů karet 13](#_Toc13755472)

[Požadavek 3: Chránit uchovávaná data držitelů karet 13](#_Toc13755473)

[Požadavek 4: Zašifrovat přenos dat držitelů karet po otevřených veřejných sítích 15](#_Toc13755474)

[Udržování programu kontroly zranitelnosti 16](#_Toc13755475)

[Požadavek 6: Vyvíjet a udržovat bezpečné systémy a aplikace 16](#_Toc13755476)

[Zavedení přísných opatření a kontrol přístupu 17](#_Toc13755477)

[Požadavek 7: Omezit přístup k datům držitelů karet jen podle oprávněné potřeby 17](#_Toc13755478)

[Požadavek 8: Identifikovat a autentizovat přístup k systémovým komponentám 18](#_Toc13755479)

[Požadavek 9: Omezit fyzický přístup k datům držitelů karet 19](#_Toc13755480)

[Pravidelné monitorování a testování sítí 22](#_Toc13755481)

[Požadavek 11: Pravidelně testovat bezpečnostní systémy a procesy 22](#_Toc13755482)

[Udržování politiky informační bezpečnosti 24](#_Toc13755483)

[Požadavek 12: Udržovat politiku zaměřenou na informační bezpečnost pro všechen personál 24](#_Toc13755484)

[Příloha A1: Dodatečné požadavky PCI DSS na poskytovatele sdíleného hostingu 26](#_Toc13755485)

[Příloha A2: Dodatečné požadavky na subjekty používající SSL/dříve TLS pro transakce za fyzické přítomnosti platební karty u POS POI terminálových připojení 26](#_Toc13755486)

[Příloha A3: Dodatečné hodnocení pro specifické subjekty DESV (Designated Entities Supplemental Validation) 26](#_Toc13755487)

[Příloha B: Pracovní list náhradního řešení 27](#_Toc13755488)

[Příloha C: Vysvětlení pro „Nevztahuje se” (N/A) 28](#_Toc13755489)

[Oddíl 3: Validace a podrobnosti o osvědčení 30](#_Toc13755490)

# Než začnete

SAQ B-IP byl vypracován tak, aby zohlednil požadavky vztahující se na obchodníky, kteří zpracovávají data držitelů karet pouze přes samostatné terminály schválené jako PTS POI zařízení připojené přes IP protokol na platebního procesora. Výjimkou jsou POI zařízení klasifikovaná jako SCR (Secure Card Reader); obchodníci používající SCR nejsou oprávněny použít tento dotazník SAQ.

SAQ B-IP obchodníci mohou být obchodníci působící buď v kamenném obchodě (karta přítomna), nebo přijímající písemné/telefonické objednávky (karta nepřítomna), kteří neuchovávají data držitelů karet v počítačovém systému.

SAQ B-IP obchodníci potvrzují, že pro tento platební kanál:

* Vaše společnost používá pouze samostatné terminály schválené jako PTS zařízení (vyjma SCR) připojené pomocí IP k poskytovateli platebních služeb ke zpracování kartových dat zákazníků;
* samostatná POI zařízení připojená pomocí IP jsou validována v rámci programu PTS POI vystaveném na webových stránkách PCI SSC;
* samostatná POI zařízení připojená pomocí IP nejsou připojená do žádného dalšího systému Obchodníka (toho lze dosáhnout síťovou segmentací pro izolování POI zařízení od zbytku sítě);
* jediný datový přenos z PTS POI zařízení je směrem k poskytovateli platebních služeb;
* POI zařízení nepoužívá pro komunikaci s poskytovatelem platebních služeb žádné další zařízení (tj. počítač, mobilní telefon, tablet, apod.);
* jakákoliv data držitelů karet, která Vaše společnost uchovává jsou v papírové podobě (např. papírové záznamy nebo papírové kopie účtenek) a tyto dokumenty nejsou přijímány elektronicky;
* Vaše společnost neuchovává kartová data v elektronickém formátu.

***Tento SAQ se nevztahuje na e-commerce kanály.***

Tato zkrácená verze SAQ obsahuje otázky vztahující se na specifický typ prostředí drobného obchodníka, jak je definováno ve výše uvedených kritériích způsobilosti. Pokud existují požadavky PCI DSS aplikovatelné na vaše prostředí, které nejsou pokryté tímto SAQ, může to být známkou toho, že tento SAQ není vhodný pro vaše prostředí. Navíc musíte stále být v souladu se všemi aplikovatelnými požadavky PCI DSS, abyste byli v souladu s PCI DSS.

## 

## 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 B-IP)
* 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 AOC (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 tabulka 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 tabulce 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. |

## Postup v případech, kdy nelze aplikovat dané požadavky

Zatímco mnohé organizace vyplňují v dotazníku SAQ B-IP každou položku, na subjekty se specifickými obchodními modely se některé položky nebudou vztahovat. Například od společnosti, která nevyužívá bezdrátové technologie ve své síti, se neočekává, že bude dokazovat shodu s požadavky, které se týkají právě bezdrátové technologie (například, Požadavek 1.2.3, 2.1.1 a 4.1.1).

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.

## 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: |  | | |
| 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 (např. prodejny, firemní kanceláře, datová centra, call centra atd.) a shrnutí všech lokací zahrnutých v PCI DSS posudku. | | |
| **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** | | |
| Využívá Vaše společnost kvalifikovaného integrátora či prodejce (QIR)? | | Ano  Ne |
| **V případě, že Ano:** | | |
| **Jméno QIR společnosti:** |  | |
| **Jméno zástupce QIR společnosti:** |  | |
| **Popis poskytovaných služeb:** |  | |

|  |  |  |
| --- | --- | --- |
| 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.* | | |

|  |  |
| --- | --- |
| **Část 2g. Způsobilost k vyplnění SAQ B-IP** | |
| Obchodník potvrzuje, že je způsobilý k vyplnění této zkrácené verze Dotazníku pro sebehodnocení, protože pro tento platební kanál: | |
|  | Obchodník používá pouze samostatné terminály schválené jako PTS zařízení (vyjma SCR) připojené pomocí IP protokolu k poskytovateli platebních služeb ke zpracování kartových dat zákazníků; |
|  | Samostatná POI zařízení připojená pomocí IP jsou validována v rámci programu PTS POI vystaveném na webových stránkách PCI SSC; |
|  | Samostatná POI zařízení připojená pomocí IP protokolu nejsou připojená do žádného dalšího systému obchodníka (toho lze dosáhnout síťovou segmentací pro izolování POI zařízení od zbytku sítě); |
|  | Jediný datový přenos z PTS POI zařízení je směrem k poskytovateli platebních služeb; |
|  | POI zařízení nepoužívá pro komunikaci s poskytovatelem platebních služeb žádné další zařízení typu počítač, mobilní telefon, tablet, apod.); |
|  | Obchodník neukládá kartová data v elektronickém formátu. |
|  | Obchodník uchovává pouze papírové záznamy nebo účtenky s jakýmikoliv daty držitelů karet a tyto dokumenty nejsou přijímány elektronicky. |

# Oddíl 2: Dotazník pro sebehodnocení B-IP

|  |
| --- |
| ***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:**

## Vybudování a udržování bezpečné sítě a systémů

### 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** |
| 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 |  |  |  |  |
| 1.1.4 | (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 |  |  |  |  |
| 1.1.6 | (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 |  |  |  |  |
| 1.2 | 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.* |  | | | | |
| **PCI DSS Otázka** | | **Očekávané Testování** | **Odpověď**  **(zaškrtněte jednu odpověď pro každou otázku)** | | | |
| **ANO** | **ANO s „CCW“** | **NE** | **N/A** |
| 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 |  |  |  |  |
| 1.2.3 | 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: |  | | | | |
| 1.3.3 | 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 |  |  |  |  |

### 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** |
| 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 |  |  |  |  |
| 2.3 | 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 |  |  |  |  |

## 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** |
| 3.2 | (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 |  |  |  |  |

### 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** |
| 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 | (b) Existují politiky, které určují, že nechráněná čísla karet (PAN) nesmí být zasílána technologiemi pro zasílání zpráv koncovým uživatelem? | * Zkontrolujte politiky a postupy |  |  |  |  | |

## Udržování programu kontroly zranitelnosti

### 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** |
| 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 |  |  |  |  |

## Zavedení přísných opatření a kontrol 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** |
| 7.1 | Je omezen přístup k systémovým komponentám a datům držitelů karet jen na ty osoby, jejichž práce takový přístup vyžaduje, dle následujícího? |  | | | | |
| 7.1.2 | Jsou přístupy k privilegovaným uživatelským účtům omezeny dle následujícího:   * přiřazen pouze k rolím, které specificky vyžadují privilegovaný přístup? * omezen pouze na minimální oprávnění nezbytná pro plnění pracovních povinností? | * Přezkoumejte psané politiky kontroly přístupu * Rozhovor s personálem * Rozhovor s managementem * Zkontrolujte privilegované uživatelské účty (ID) |  |  |  |  |
| 7.1.3 | Jsou přiřazeny přístupy podle klasifikace jednotlivých pracovních míst a funkcí? | * Přezkoumejte psané politiky kontroly přístupu * Rozhovor s managementem * Zkontrolujte privilegované uživatelské účty (ID) |  |  |  |  |

### 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** |
| 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 |  |  |  |  |
| 8.3 | 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 | |  |  |  |  |
| 8.5 | 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 | |  |  |  |  |

### 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** |
| 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 |  |  |  |  |
| 9.5 | 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 |  |  |  |  |
| 9.6 | | (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 |  |  |  |  |
| 9.8 | | (a) Jsou všechna média zničena, když jich již není zapotřebí z provozních ani právních důvodů? | * 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 |  |  |  |  |
| 9.9 | | 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 |  |  |  |  |

## Pravidelné monitorování a testování sítí

### 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** |
| 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 |  |  |  |  |
| 11.3.4 | 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 |  |  |  |  |

## 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 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** |
| 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 po každé změně prostředí? | * Zkontrolujte politiku informační bezpečnosti * 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 |  |  |  |  |
| 12.3.3 | Seznam všech takovýchto zařízení a personálu s přístupem? | * Zkontrolujte politiky používání * Rozhovor s odpovědným personálem |  |  |  |  |
| 12.3.5 | Přijatelné použití technologie? | * 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 |  |  |  |  |
| 12.4 | 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 |  |  |  |  |
| 12.5 | (b) Jsou následující odpovědnosti řízení informační bezpečnosti formálně přiděleny jedinci nebo týmu: |  | | | | |
| 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 |  |  |  |  |
| 12.6 | (a) Existuje a poskytuje formální program bezpečnostního povědomí celému personálu informace o politikách a postupech bezpečnosti dat držitelů karet? | * Zkontrolujte program povědomí o bezpečnosti |  |  |  |  |
| 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 |  |  |  |  |
| 12.10.1 | (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) |  |  |  |  |

## 

## 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** |
| 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 |  |  |  |  |

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 |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

## 

# Oddíl 3: Validace a podrobnosti o osvědčení

|  |  |
| --- | --- |
| **Část 3. Ověření podle standardu PCI DSS** | |
| **Toto AOC je založeno na výsledcích uvedených v SAQ B-IP (Část 2), datováno** *( datum dokončení SAQ),* Na základě výsledků zdokumentovaných v SAQ B-IP 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 na ne 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 B-IP 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 potřebné 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 společnosti🡩* | | *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 |  |  |  |
| 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 |  |  |  |
| 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 |  |  |  |

\* Zde uvedené požadavky PCI DSS se vztahují k otázkám v Oddílu 2 dotazníku SAQ



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)