WINCOR NIXDORF

Certifikovaný PCI DSS auditor - QSA

Wincor Nixdorf s.r.o.

Evropská 33a

160 00 Praha 6

Tel.: +420 233 034 129

Email: pci@wincor-nixdorf.cz

PCI DSS jako norma pro bezpečnost v odvětví platebních karet byla oficiálně akceptována dvěma největšími asociacemi – společnostmi VISA a MasterCard. Později ji přijaly i další společnosti v tomto odvětví jako American Express, Dinners Club nebo JCB. Pro řízení celého programu bezpečnosti v odvětví platebních karet byla také založena společnost PCICo., jejímiž zakladateli a zároveň vlastníky jsou právě jednotlivé asociace.

PCI vyžaduje, aby všichni obchodníci, poskytovatelé služeb a banky obchodníků, kteří uchovávají, zpracovávají nebo přenášejí data o transakcích uskutečněných prostřednictvím platebních karet, podstoupili akreditaci v rámci normy PCI DSS. Úrovní bezpečnostních auditů, které je potřeba absolvovat, je několik a záleží na velikosti organizace a počtu transakcí za rok. Kritéria pro akreditaci definovaná asociací VISA pro obchodníky jsou specifikována v Tabulce 1.

Společně s normou PCI DSS byly vytvořeny dva kontrolní nástroje ověřující, zda je tato norma dodržována - **audit** založený na testování na místě a **externí testování** zranitelností síťové infrastruktury a aplikací. Audit založený na testování na místě musí být realizován jednou ročně, externí testování zranitelností musí být prováděno čtvrtletně. Prověřovací činnosti požadované v rámci normy PCI DSS mohou vykonávat pouze auditoři, respektive auditorské firmy pověřené, otestované a akreditované asociacemi VISA a MasterCard.

AUDIT ZALOŽENÝ NA TESTOVÁNÍ NA MÍSTĚ

Audit je založen na principu testování souladu skutečného stavu informační bezpečnosti v dané organizaci s dvanácti bezpečnostními požadavky, které jsou publikovány v rámci normy PCI DSS a rozdělují se do šesti hlavních kategorií:

A: Vystavěj a udržuj bezpečnou síť

1. Instaluj a udržuj bezpečnou konfiguraci firewallu.
2. Nepoužívej implicitní systémová hesla a ostatní bezpečnostní parametry.

B: Ochraňuj data držitelů karet

3. Ochraňuj uložená data.
4. Šifruj přenos dat držitelů karet a citlivých informací přes veřejné sítě.

C: Udržuj program pro řízení zranitelností

5. Používej a pravidelně aktualizuj antivirový software.
6. Zajisti vývoj a údržbu bezpečných systémů a aplikací.

D: Zaveď silné přístupové kontroly

7. Povol přístup k datům pouze na základě zásady potřebných znalostí.
8. Přiřaď jednotný identifikátor každému uživateli informačního systému.
9. Omez fyzický přístup k datům držitelů karet.

E: Pravidelně sleduj a testuj síť

10. Sleduj a zaznamenávej veškerý přístup k síťovým zdrojům a datům držitelů karet.
11. Pravidelně testuj bezpečnostní systémy a procesy.

F: Udržuj informační bezpečnostní politiku

12. Udržuj politiku pokrývající informační bezpečnost.

V rámci každého z výše uvedených dvanácti bezpečnostních požadavků norma PCI DSS specifikuje řadu konkrétních detailních požadavků, k nimž je navíc vytvořena testovací procedura, kterou musí auditor realizovat a jejíž výsledky musí dokumentovat. Na základě provedených a dokumentovaných testů auditor rozhodne, zda je konkrétní bezpečnostní požadavek splněn, respektive zda daná technická nebo procedurální kontrola v auditované organizaci funguje správně. U organizací, jež nepodléhají povinnosti auditu prováděného na místě nezávislým akreditovaným auditorem, avšak zpracovávají určité množství platebních transakcí, je alternativou tohoto auditu vyplnění dotazníku (**Self-Assessment Questionnaire**) a jeho odeslání do asociací.

EXTERNÍ TESTOVÁNÍ ZRANITELNOSTÍ ANEB SIMULACE ÚTOKU HACKERA

Slabiny a bezpečnostní díry objevují hackeři (počítačově nadaní jedinci, kteří se snaží neoprávněně získat přístup k cizím informačním systémům prostřednictvím počítačové sítě) prakticky denně. Jedinou možnou obranou proti jejich útoku a kompromitaci informačních systémů je pravidelná instalace bezpečnostních záplat. Pro zajištění bezpečnosti systémů, které zpracovávají, uchovávají nebo přenášejí data o platebních transakcích, vyžaduje norma PCI DSS **čtvrtletní externí testování zranitelností**.

Testování zranitelností je založeno na principu simulace činnosti útočníka (hackera) z internetu. Testeři, kteří jsou pro tuto činnost akreditováni asociacemi platebních karet, se pokoušejí ze svých laboratoří připojených na internet „nabourat" do sítě klienta a získat z jeho informačních systémů citlivá data.

MasterCard provádí každoročně opakované testování všech PCI auditorů akreditovaných pro externí testování zranitelností. Na testovacím prostředí sestaveném asociací MasterCard se zjišťuje, zda je daný auditor schopen v rámci 24hodinového testu identifikovat všechny známé bezpečnostní slabiny, jež se v testovacím prostředí vyskytují.

GLOBÁLNÍ PŘÍSTUP K PROVÁDĚNÍ PCI AKREDITACÍ A ZKUŠENOSTI Z PROVEDENÝCH AUDITŮ

PCI DSS je globální norma, která je jednotná pro relevantní organizace v odvětví platebních karet na celém světě. Auditorské firmy se proto musí vypořádat s problémem, jak provádět audity v souladu s takovouto globální normou v různých zemích světa a zároveň zajistit konzistentní přístup a jednotnou kvalitu výstupů. Příkladem možného řešení tohoto problému je přístup mezinárodní společnosti Wincor Nixdorf. Jeho základem je vytvoření jednoho globálního týmu pro provádění PCI DSS auditů. Audit na místě je realizován týmy z jednotlivých lokálních poboček auditora, neboť vyžaduje místní jazykovou znalost. V rámci auditu je totiž potřeba prověřit dokumentované postupy a směrnice, které mohou být v lokálním jazyce. Závěrečné zprávy ze všech auditů jsou před odesláním do asociací prověřeny globálním týmem – tím je zajištěna jednotná úroveň kvality výstupů na celosvětové úrovni.

Kritickým místem pro správné provedení PCI DSS akreditace je úvodní nastavení rozsahu auditu. Jednak je potřeba určit, do jaké úrovně auditovaná organizace patří (Úroveň 1, 2, 3 nebo 4) a také přesně stanovit, které komponenty informačního a komunikačního systému organizace spadají do záběru PCI DSS. Zejména u organizací globálního charakteru, kam patří například obchodní řetězce, to není vždy triviální záležitost.

TYPICKÉ PROBLÉMY BRÁNÍCÍ DOSAŽENÍ SOULADU S PCI DSS

Typické problémy, se kterými jsme se setkali při provádění auditů, by se daly shrnout do tří základních oblastí - ukládání citlivých po autorizaci platební transakce, nezdokumentovaný informační systém a typické problémy z oblasti informační bezpečnosti.

Ukládání citlivých po autorizaci platební transakce

Citlivá data (například celé číslo karty) nesmí obchodníci po provedení autorizace platební transakce za žádných okolností ukládat. Nicméně u řady našich klientů jsem se setkali s tím, že tato data se ukládají na různých místech informačního systému, například v záznamech událostí (logy), zálohách nebo přímo v databázi.

Nezdokumentovaný informační systém

I druhá oblast souvisí s problémem ukládání citlivých dat. U řady našich klientů jsme se při provádění auditu setkali se stavem, kdy v důsledku toho, že různé části systému historicky vznikaly řadu let a jejich vývoj nebyl řádně dokumentován, nám klient často ani nebyl schopen vysvětlit, jaká konkrétní data různými částmi informačního systému vlastně procházejí.

Typické problémy z oblasti informační bezpečnosti

PCI DSS je norma z oblasti informační bezpečnosti a vyžaduje komplexní řešení této problematiky v rámci organizace. Nicméně u našich klientů se často setkáváme se stavem, kdy informační bezpečnost není dostatečně řešena. Typickými příklady mohou být chybějící nebo nedostatečné zaznamenávání událostí (logování a monitorování), neexistence procesu pro pravidelnou aktualizaci bezpečnostních záplat, nedostatečná kontrola nad řízením změn nebo nedostatečné povědomí o bezpečnosti mezi zaměstnanci společnosti.

NABÍDKA SPOLEČNOSTI WINCOR NIXDORF

1. **Úvod do problematiky PCI DSS**
    - **Popis:** Obecný úvod do problematiky PCI DSS.
    - **Výstup:** Popis hlavních bezpečnostních rizik, která souvisí s platebními kartami.
    - **Doba trvání:** 1 – 2 dny.

2. **Vymezení rozsahu PCI DSS**
    - **Popis**: Bude určen rozsah PCI DSS a budou vymezeny oblasti, které jsou součástí zákazníkovi systémové architektury a musí být v souladu s požadavky PCI DSS.
    - **Techniky**: Kontrola dostupné dokumentace, rozhovory s vybranými pracovníky, workshopy.
    - **Výstup**: Soupis systémů a oblastí, které budou dotčeny PCI DSS.
    - **Doba trvání**: 3 – 5 dní.

3. **Gap analýza podle standardu PCI DSS**
    - **Popis**: Bude provedena kontrola souladu zákaznických systémů s 12 požadavky standardu PCI DSS.
    - **Techniky**: Kontrola dostupné dokumentace, rozhovory s vybranými pracovníky, workshopy, kontrola konfigurovatelných parametrů systémů a zařízení.
    - **Výstup**: Souhrnná zpráva o zákazníkově souladu se standardem PCI DSS.
    - **Doba trvání**: Přibližně 2 až 3 týdny.

4. **PCI DSS preaudit – kontrola kvalifikace před formálním auditem**
    - **Popis:** Bude provedena rychlá kontrola zákaznických systémů a postupů a bude prověřena připravenost pro formální PCI DSS audit.
    - **Výstup:** Stručné shrnutí stavu zákazníkovi připravenosti na PCI DSS audit.
    - **Doba trvání**: 3 dny.

5. **Formální PCI DSS audit**
    - **Popis**: Bude proveden formální audit shody zákazníkovi systémové infrastruktury se standardy PCI DSS. Na rozdíl od předchozích služeb nemůže být při provádění formálního PCI DSS auditu dán prostor k rozboru a nápravě nalezených incidentů. Výstupem bude zpráva, kde bude konstatováno, jestli jsou všechny PCI DSS požadavky splněny, resp. nesplněny.
    - **Techniky**: Kontrola dostupné dokumentace, rozhovory s vybranými pracovníky, workshopy, kontrola konfigurovatelných parametrů systémů a zařízení.
    - **Výstup:** Formální PCI DSS report. V případě, že nedošlo k žádnému pozitivnímu nálezu, je vystaven certifikát o shodě systémů se standardy PCI DSS.
    - **Doba trvání:** Přibližně 1 až 2 týdny.

6. **Externí pre- scan zranitelnosti**

- **Popis**: Podle požadavků PCI DSS bude proveden pre-scan zranitelnosti všech systémů, které zpracovávají platební transakce a mají externí komunikační interface. Scan bude proveden ručně s možností konzultace k problematickým oblastem.
- **Techniky**: Externí scan zranitelnosti.
- **Výstup**: Report o postupu scanování, seznam nálezů a jejich klasifikace podle PCI DSS, konzultace k nálezům.
- **Doba trvání**: Přibližně 3 dny (maximální rozsah je 5 IP adres).

7. Finální formální PCI DSS scan

- **Popis:** Bude proveden finální formální scan, který bude automatizovaný a na rozdíl od pre-scanu nebude dán prostor k diskuzi k případným nálezům. Výsledkem bude pouze konstatování výsledku scanování - scan proběhl úspěšně nebo ne.
- **Techniky**:Automatizovaný scan provedený certifikovaným nástrojem.
- **Výstup:** Formální scan report vydaný certifikovaným ASV.
- **Doba trvání**: Přibližně 1 den.

8. Scanování webových aplikací

- **Popis:** Bude provedeno automatizované scanování webových aplikací za účelem identifikace jejich zranitelnosti a omezení rizik, např. nekorektní konfigurace webu, SQL injekce, cross-site scripting, resp. hrozby uvedené v OWASP Top 10.
- **Techniky**: Automatický scan provedený certifikovaným nástrojem.
- **Výstup**: Formální scan report vydaný certifikovaným ASV.
- **Doba trvání**: Přibližně 1 den.

9. Konzultace při zpracování PCI Self Assessment dotazníku

- **Popis**: Bude provedeno automatizované scanování webových aplikací za účelem identifikace jejich zranitelnosti a omezení rizik, např. nekorektní konfigurace webu, SQL injekce, cross-site scripting, resp. hrozby uvedené v OWASP Top 10.
- **Techniky**: Automatický scan provedený certifikovaným nástrojem.
- **Výstup**: Formální scan report vydaný certifikovaným ASV.
- **Doba trvání**: Přibližně 2 týdny.