Praha 27.10.2009

Sdružení pro bankovní karty - SBK vydává tiskovou zprávu s cílem představit českému trhu celosvětové bezpečnostní standardy PCIDSS. Pro bližší a detailnější seznámení s oblastí PCIDSS připravilo SBK oficiální české webové stránky **www.pcisecuritystandards.cz**.

## PCIDSS

PCIDSS (Payment Card Industry Data Security Standard) představuje bezpečnostní normu pro platební karty vydanou karetními asociacemi a společnostmi. Norma je určena pro organizace, které zpracovávají, přenášejí nebo uchovávají data o držitelích platebních karet a kartových transakcích. Jejím cílem je zamezit únikům citlivých dat o držitelích platebních karet a karetním podvodům. Originální znění standardů je k dispozici na **www.pcisecuritystandards.org**

PCIDSS je rozdělen do 12 kategorií, kdy každá z nich obsahuje zcela konkrétní bezpečnostní doporučení, jak chránit údaje o platebních kartách. Soulad s PCIDSS je pravidelně prověřován u všech subjektů zpracovávajících karetní data. Úroveň prověření závisí na počtu a typu karetních transakcí za rok.

## Proč SBK

Implementace mezinárodních bezpečnostních standardů PCIDSS do národního prostředí si žádá koordinovaný a komplexní postup kroků. SBK se profiluje jako subjekt, který svým charakterem činnosti napomáhá implementovat standardy PCIDSS na domácím trhu. Za tímto účelem byly vytvořeny oficiální české webové stránky, které za obecné shody všech zúčastněných subjektů, systémově a přehledně informují o krocích potřebných k naplnění povinností uplatnění standardů PCIDSS.

Sdružení pro bankovní karty - SBK je zájmovým sdružením právnických osob - bank příp. i jiných organizací, jejichž zájmem je rozvoj platebních karet v České republice a koordinace prací, souvisejících s tímto rozvojem. V zájmu svých členů jedná s tuzemskými i mezinárodními organizacemi z oblasti platebních karet. SBK rozvíjí a koordinuje činnost v oblastech nekonkurenčního charakteru, zejména v oblasti prevence, bezpečnosti, edukace, provozních a technických charakteristik, legislativního rámce apod. Více informací o SBK naleznete na **www.bankovnikarty.cz**

## Spolupráce s partnery

SBK spolupracuje v oblasti implementace standardů PCIDSS na českém trhu s několika vybranými partnery. Hlavními partnery jsou společnost Wincor-Nixdorf a IBM ČR, kteří jsou zároveň jedinými držiteli QSA na domácím trhu. Mezi odborné partnery patří společnosti Diners Club Czech, MasterCard Europe pro ČR a Visa EU pro ČR. Mezi odborné konzultanty patří společnost Bellpro. Významným a zásadním nástrojem pro implementaci standardů PCIDSS je a bude oficiální webová stránka **www.pcisecuritystandards.cz**, na které jsou umístěné veškeré důležité informace o PCIDSS v českém jazyce.

## Obecné informace pro obchodníky

PCIDSS (Payment Card Industry Data Security Standards) je bezpečnostní normou, jejímž cílem je zamezit únikům citlivých dat o držitelích platebních karet a karetním podvodům. Tato norma vyžaduje, aby všichni obchodníci (ale stejně tak i poskytovatelé služeb a banky obchodníků), kteří zpracovávají, přenášejí nebo uchovávají data o držitelích platebních karet a kartových transakcích, podstoupili akreditaci v rámci normy PCIDSS.

Norma definuje 4 úrovně, to kterých jsou obchodníci zařazeni a kritéria k jednotlivým úrovním, které obchodník musí k získání certifikace splnit. Určení úrovně u obchodníka záleží na typu a počtu transakcí za rok. Jednotlivé úrovně a kritéria pro akreditaci definovaná asociacemi pro obchodníky jsou specifikována následovně:

| Úroveň | Obchodníci | Kritéria pro certifikaci |
|---|---|---|
| Úroveň 1 | • všichni obchodníci, kteří zpracovávají více než šest miliónů transakcí za rok (bez ohledu na typ platebního kanálu)<br>• všichni obchodníci, na které byl proveden úspěšný útok, který vyústil v kompromitaci dat držitelů karet<br>• všichni obchodníci, o kterých VISA/MC na základě svého vyjádření rozhodne, že jsou obchodníky úrovně 1 za účelem minimalizovat rizika kompromitace celého platebního VISA systému | • Pravidelný roční audit přímo u obchodníka (provedený nezávislým "Security Assessor" nebo interním auditem podepsaným zástupcem společnosti)<br>• Pravidelný čtvrtletní externí testování zranitelností (provedené certifikovaným nezávislým „Scan Vendor") |
| Úroveň 2/3 | Úroveň 2<br>• všichni obchodníci, kteří zpracovávají jeden milión až šest miliónů transakcí za rok | • vyplnění SAQ dotazníku (vyplňuje Obchodník)<br>• Pravidelný čtvrtletní externí testování zranitelností (provedené certifikovaným nezávislým „Scan Vendor") |
| | Úroveň 3<br>• všichni internetoví obchodníci, kteří zpracovávají 20 tisíc až 150 tisíc e-commerce transakcí za rok | |
| Úroveň 4 | • všichni ostatní obchodníci (tj. pod jeden milión transakcí) bez ohledu na typ platebního kanálu | • vyplnění SAQ dotazníku – doporučeno (vyplňuje Obchodník)<br>• čtvrtletní externí testování zranitelností – doporučeno (provedené certifikovaným nezávislým „Scan Vendor") |

Audit v rámci normy PCIDSS mohou vykonávat pouze akreditovaní auditoři (seznam akreditovaných společností je uveden v sekci Auditoři). Čtvrtletní Externí testování zranitelnosti mohou provádět pouze certifikovaní Scan vendors (Seznam akreditovaných společností je uveden v sekci Auditoři) Více informací vztahujících se k dotazníkům úrovně 2 a 3 naleznete v sekci Dotazníky, více informací k auditu požadovaném pro úroveň 1 naleznete v sekci Navigace a Auditoři. Další informace poskytne zúčtovací banka, tedy banka přes kterou máte uzavřenou smlouvu o akceptaci platebních karet.

**Dotazník vlastního hodnocení** (Self-Assessment Questionnaire - SAQ)

Dotazník vlastního hodnocení (SAQ - Self-Assessment Questionnaire) je nástroj, jehož smyslem je pomáhat obchodníkům a poskytovatelům služeb v sebehodnocení souladu s pravidly PCIDSS. Dotazník je určen obchodníkům a poskytovatelům služeb úrovně 2 a 3 (viz PCIDSS - obecné informace pro obchodníky), kteří nemusí podstoupit pravidelný roční audit přímo u obchodníka. SAQ slouží k ověření shody obchodníka s pravidly PCIDSS. Obchodník odešle dotazník po jeho vyplnění zpracovatelské bance (acquirerovi), která je tento dotazník povinna předložit na vyžádání kartové asociaci (Visa, MasterCard,...)

Pravidla PCIDSS definují 5 kategorií obchodníků (viz následující tabulka). Pro jednotlivé kategorie jsou přiřazeny určené typy dotazníků SAQ.

**SAQ A (Self-Assessment Questionnaire - SAQ A)**

Dotazník SAQ A se vztahuje na obchodníky, kteří uchovávají pouze papírové sestavy o stvrzenkách s daty držitelů karet, neukládají data o držitelích karet v elektronickém formátu a nezpracovávají nebo nepřenášejí žádná data držitelů karet ve svých prostorech. Tito obchodníci vyplněním SAQ A a odpovídající Atestaci shody (Attestation of Compliance), potvrdí, že:

- společnost zpracovává pouze transakce bez přítomnosti karty (card-not-present), tj. e-commerce nebo písemné/telefonní objednávky;
- společnost neukládá, nezpracovává ani nepřenáší data držitelů karet na svých pracovištích, ale zcela využívá služeb poskytovatelů třetích stran;
- společnost potvrdila, že poskytovatelé třetích stran zajišťují ukládání, zpracování a/nebo přenos dat držitelů karet v shodě s PCI DSS;
- společnost uchovává pouze papírové sestavy o stvrzenkách s daty držitelů karet a tyto dokumenty nejsou přijímány elektronicky; a
- společnost neukládá žádná data o držitelích karet v elektronickém formátu.

Tato kategorie se nikdy nevztahuje na obchodníky, kteří zároveň mají POS terminály/imprintery, které používají při fyzickém kontaktu s klienty

**SAQ B (Self-Assessment Questionnaire - SAQ B)**

Dotazník SAQ B se vztahuje na obchodníky, kteří zpracovávají data držitelů karet jen přes imprintery („žehličky") – kategorie 2 nebo samostatné POS terminály – kategorie 3.

Oba tyto typy obchodníků mohou buď pracovat v „kamenných obchodech" (s přítomností karty) nebo v rámci elektronického obchodování nebo mohou přijímat písemné/telefonické objednávky (bez přítomnosti karty).
Tito obchodníci vyplněním SAQ B a příslušného Osvědčení o shodě, potvrdí, že:

**u kategorie 2**:

- společnost používá jen imprintery
- společnost nepřenáší data držitelů karet telefonní linkou ani internetem;
- společnost uchovává jen papírové výkazy nebo papírové kopie stvrzenek; a
- společnost neuchovává data držitelů karet v elektronickém formátu;

**u kategorie 3**:

- společnost používá jen samostatné POS terminály (připojené telefonní linkou k vašemu procesoru);
- samostatné POS terminály nejsou připojeny k jakýmkoli jiným systémům ani k internetu;
- společnost uchovává jen papírové výkazy nebo papírové kopie stvrzenek; a
- společnost neuchovává data držitelů karet v elektronickém formátu.

Každá část tohoto dotazníku se zaměřuje na specifickou oblast bezpečnosti na základě požadavků ve Standardu bezpečnosti dat PCI.

**SAQ C (Self-Assessment Questionnaire - SAQ C)**

Dotazník SAQ C se vztahuje na obchodníky, kteří zpracovávají data držitelů karet přes platební Aplikace (například POS systémy) připojené k internetu (přes vysokorychlostní připojení, DSL, kabelový modem apod.), ale kteří neuchovávají data držitelů karet v žádném počítačovém systému. Tyto platební Aplikace jsou připojeny k internetu buď proto, že:

1. platební Aplikace je na osobním počítači připojeném k internetu nebo
2. platební Aplikace je připojena k internetu, aby přenášela data držitelů karet.

Mohou to být obchodníci působící buď v „kamenných obchodech" (s přítomností karty) nebo v rámci elektronického obchodování nebo mohou přijímat písemné/telefonické objednávky (bez přítomnosti karty). Tito obchodníci vyplněním SAQ C a příslušného Osvědčení o shodě, potvrdí, že:

- společnost má systém platební Aplikace a připojení k internetu na stejném zařízení;
- platební Aplikace/internetová zařízení nejsou připojena k žádným jiným systémům ve vašem prostředí;
- společnost zachovává jen papírové výkazy nebo papírové kopie stvrzenek;
- společnost neuchovává data držitelů karet v elektronickém formátu; a
- dodavatel platební Aplikace vaší společnosti používá pro vzdálenou podporu vašeho platebního systému bezpečnou techniku.

Na základě požadavků ve PCI Standardu bezpečnosti dat se každý oddíl tohoto dotazníku zaměřuje na specifickou oblast bezpečnosti.

**SAQ D (Self-Assessment Questionnaire - SAQ D)**

Dotazník SAQ D se vztahuje na všechny ostatní obchodníky, kteří nesplňují popisy v dotaznících A-C a všechny poskytovatele služeb, kteří byli kartovou asociací určeni jako způsobilí pro vyplnění dotazníku SAQ. Zatímco mnohé organizace, které vyplňují SAQ D, budou potřebovat provést ověření shody u každého požadavku PCI DSS, některé organizace s velmi specifickými obchodními modely mohou zjistit, že některé požadavky se na ně nevztahují. Například od společnosti, která nepoužívá při své činnosti vůbec bezdrátovou technologii, se neočekává, že bude provádět ověření shody s kapitolami PCI DSS, které jsou specificky určeny pro bezdrátovou technologii. Informace o vyloučení bezdrátové technologie a některých jiných specifických požadavků najdete v níže uvedeném návodu.

**kontakt**

Roman Kotlán
výkonný ředitel SBK - Sdružení pro bankovní karty
m : 604 727 501
e : roman.kotlan@bankovnikarty.cz

Petr Sládek
předseda skupiny PCIDSS SBK
m : 605 236 836
e : petr.sladek@bts-cee.cz


www.bankovnikarty.cz
JET SET
lounge bar & restaurant
Co je PCI DSS


www.bankovnikarty.cz
JET SET
lounge bar & restaurant


www.bankovnikarty.cz
lounge bar &
Co je PCI DSS


JET SET
lounge bar & restaurant
Co je PCI DSS


www.bankovnikarty.cz
JET SET
lounge bar & restaurant