PCI DSS

Co je PCI DSS?

Bezpečnostní standard PCI DSS (Payment Card Industry Data Security Standard) představuje mezinárodní pravidla, definující podmínky nakládání s údaji držitelů platebních karet, které jsou obsaženy na platebních kartách.
Tato mezinárodní pravidla, jejichž plnění je vyžadováno kartovými asociacemi a společnostmi, jsou určena pro organizace, které zpracovávají, přenášejí nebo uchovávají data držitelů platebních karet (z platebních karet a o kartových transakcích). Cílem těchto mezinárodních pravidel je omezit rizika úniků uvedených dat a tím jejich možnému zneužití.
PCI DSS jako modelový rámec pro zajištění bezpečnosti obsahuje nejvhodnější postupy k minimalizaci rizika odcizení dat.

Ochrana údajů držitelů platebních karet představuje skutečný problém po celém světě. Ochranou dat se musí zabývat nejen banky, které platební karty vydávají, ale také obchodníci, kteří je přijímají. Údaje o platební kartě musí samozřejmě chránit také samotní držitelé platebních karet.

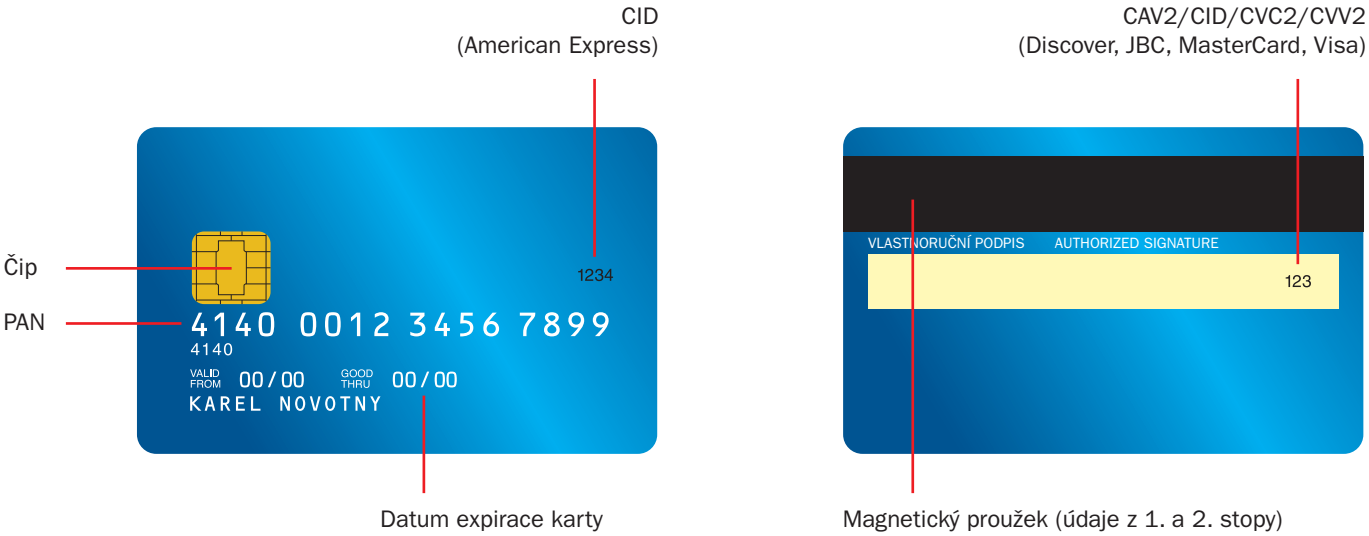
Ať jste velkou mezinárodní společností nebo majitelem jediného obchodu, ať provozujete kamennou prodejnu nebo internetový obchod, pokud přijímáte platební karty, je zcela zásadní, aby Vaše obchodní činnost byla v souladu s bezpečnostními standardy PCI DSS.

Soulad s mezinárodními pravidly PCI DSS je povinný pro všechny obchodníky, kteří přijímají platební karty a je striktně a bez rozdílu vyžadován všemi bankami po celém světě.

Jako obchodník nesete odpovědnost za ochranu dat držitelů karet zejména v místě prodeje a za jejich bezpečný přenos do platebního systému. Vaší odpovědností je nastavit a zabezpečit systémy, které používáte tak, aby nebyla ohrožena data Vašich klientů a to včetně systémů Vašich partnerů a subdodavatelů. Nejlepším postupem jak minimalizovat možnost odcizení dat je neukládat **žádná kartová data**.

Jaká kartová data chránit?

a) data držitelů platebních karet – číslo karty, datum její expirace, jméno držitele karty. Tato data lze, pokud je to nevyhnutelně nutné, ukládat v případě dodržení bezpečnostních požadavků vyplývajících ze standardu PCI DSS,
b) citlivá ověřovací data (kódy CAV2/CVC2/CVV2/CID, kompletní data z magnetického proužku, osobní identifikační číslo (PIN)). **Ukládání těchto dat není za žádných okolností povoleno!**



Citlivá data mohou být odcizena z mnoha míst:

– platebního terminálu,
– prostoru, kde jsou ukládány papírové účtenky v případě, že data obsahují,
– počítačového systému,
– nahrávky skryté kamery při ověřování dat,
– tajného záznamu z drátového i bezdrátového připojení Vaší firmy.

V současné době pachatelé zaměřují svou pozornost i na drobné obchodníky, jejichž systémy jsou mnohdy méně odolné proti napadení a jsou tedy snazším zdrojem kartových informací. I proto je dodržování standardů PCI DSS povinné pro všechny obchodníky přijímající platební karty.

Jaký je význam splňování standardů PCI DSS?

– Váš systém je bezpečný a držitelé platebních karet Vám mohou důvěřovat. Důvěra zákazníků zvyšuje pravděpodobnost, že se k Vám budou vracet, že budou Vaši společnost doporučovat dále.
– Zlepšení Vaší spolupráce se zpracovatelskou bankou a dalšími subjekty – partnery, které potřebujete pro své podnikání.
– Snížení rizika mimořádných finančních výdajů (například v důsledku zneužití kartových údajů k podvodům a jiné trestní činnosti).
– Snížení nákladů na případné vyšetřování a právní zastoupení.
– Snížení rizika negativního zájmu médií o Vaši společnost.

Jaké jsou důsledky nesplnění požadavků PCI DSS?

– Nekalé nakládání s daty platebních karet může mít negativní efekt na všechny zainteresované strany – na zákazníky, obchodníky i finanční instituce.
– Jediný incident může znamenat zničení Vaší pověsti a problémy ve Vašem podnikání.
– V konečném důsledku by Vaše společnost mohla být sankcionována a také by po Vás mohla být vyžadována úhrada nákladů spojených se šetřením zneužití dat a za související právní úkony.

Jak Vám můžeme pomoci?

Vaše zpracovatelská banka Vám na požádání sdělí, do jaké úrovně kategorizace se svým počtem transakcí řadíte a jaká jsou pro Vaši úroveň stanovena kriteria ověřování plnění mezinárodních pravidel PCI DSS.

Veškeré nezbytné informace týkající se bezpečnostních požadavků v oblasti přijímání platebních karet, včetně standardu PCI DSS, kategorizace subjektů a jim stanovených povinností, je Vám k dispozici na **www.pcisecuritystandard.org**.

Vážíme si Vaší spolupráce, a proto jsme pro Vás připravili portál, který obsahuje základní informace a dokumenty k mezinárodním pravidlům PCI DSS v českém jazyce. Oceníme Vaše náměty a připomínky k obsahu.

Portál www.pcistandard.cz nyní bude sloužit i Vám!

Děkujeme Vám, že se zabýváte ochranou dat z platebních karet.