

STANDARDSY A PRAVIDLA PRO BEZPEČNOU AKCEPTACI PLATEBNÍCH KARET

Standard PCI DSS

PCI DSS je norma pro fyzickou a informační bezpečnost v odvětví platebních karet, která vyžaduje, aby všichni obchodníci, poskytovatelé služeb a banky obchodníků, kteří uchovávají, zpracovávají nebo přenášejí data o transakcích uskutečněných prostřednictvím platebních karet, postupovali v souladu s bezpečnostními standardy PCI DSS. Cílem PCI DSS 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.

Obchodník nese odpovědnost za ochranu dat držitelů platebních karet zejména v místě prodeje a za jejich případný přenos do pokladního či jiného počítačového systému. Nastavení a zabezpečení systémů musí být ošetřeno tak, aby nebyla ohrožena data držitelů platebních karet, a to včetně systémů vašich dodavatelů. Nejlepším postupem, jak minimalizovat možnost odcizení citlivých dat, je neukládat žádná karetní data.

JAKÁ KARETNÍ DATA CHRÁNIT?

- data držitelů platebních karet – číslo karty, datum její expirace, jméno držitele karty
- citlivá ověřovací data (kódy CAV2 / CVC2 / CVV2 / CID, kompletní data z magnetického proužku, osobní identifikační číslo (PIN))

CITLIVÁ DATA CHRAŇTE ZEJMÉNA V

- prostoru, kde jsou ukládány papírové stvrzenky z terminálu, v případě, že data obsahují
- pokladním či počítačovým systémem, pokud jsou přenášena
- nahrávkách z bezpečnostních kamer (nesmí být snímána klávesnice terminálu / PIN Padu pro zadávání PINu)
- záznamech z drátového i bezdrátového připojení obchodníka

Dodržování standardů PCI DSS je povinné pro všechny obchodníky přijímající Platební karty. Obchodník je povinen se s uvedenými PCI-DSS podrobně seznámit a zavazuje se je dodržovat.

Veškeré nezbytné informace týkající se bezpečnostních požadavků v oblasti přijímání platebních karet, včetně standardu PCI DSS, kategorizace subjektů a jim stanovených povinností, jsou vám k dispozici na www.pcisecuritystandards.org, případně na internetových stránkách Sdružení pro bankovní karty – www.pcistandard.cz.

REGISTRACE POSKYTOVATELŮ SLUŽEB AKCEPTACE PLATEBNÍCH KARET

Na základě nařízení VISA musí být všichni dodavatelé služeb (dále jen „Agenti“), kteří přicházejí do styku s daty z platebních karet VISA, registrováni na stránkách. www.visaeurope.com/receivingpayments/security/third-party-agents

Je nutné ověřit, že vaši Agenti jsou na výše uvedených stránkách zaregistrováni. V případě, že váš Agent není na těchto stránkách registrován, je třeba toto bezpodmínečně zajistit. V opačném případě může banka požadovat zastavení zpracování dat VISA karet a jejich držitelů.

KDO JE TO AGENT?

Každý, kdo pro obchodníka poskytuje službu, která zahrnuje zpracování, skladování nebo přenášení dat držitelů karet (přímo nebo nepřímo).

Registrace Agentů je důležitá především pro všechny Online rezervační agentury, např. pro hotely, cestovní kanceláře a agentury, letecké společnosti nebo půjčovny.

Dalšími typickými příklady Agentů jsou:

- call Centra
- řešení zpracování plateb obchodníka
- poskytovatelé platebních služeb
- poskytovatelé Web-hostingu
- služby detekce podvodů (monitoring) atp

Seznam registrovaných Agentů včetně doplňujících informací naleznete na stránkách.

www.visaeurope.com/receivingpayments/security/downloads-and-resources Obchodníci mají také povinnost nahlásit každého svého Agentu útvaru Akceptace karet ČSOB prostřednictvím e-mailu akceptacekaret@csob.cz. Do předmětu mailu uveďte heslo: AGENTI.

PRAVIDLA BEZPEČNÉ AKCEPTACE PATEBNÍCH KARET U PATEB BEZ PŘÍTOMNOSTI PATEBNÍ KARTY

Vzhledem k riziku finanční ztráty, kterou může obchodník utrpět při nedodržení bezpečnostních pravidel pro zpracování karetních transakcí, si vás dovoluujeme upozornit na nejčastěji používané scénáře podvodů s platebními kartami a připomenout postupy, které je nutné dodržet, abyste se nestali obětí těchto podvodů.

PRAVIDLA BEZPEČNÉ AKCEPTACE

1. Transakci bez přítomnosti platební karty (CNP – Card Not Present) lze provést pouze u:
 - předautorizace
 - dokončení předautorizace a to pouze u Půjčoven za předpokladu, že byla provedena Předautorizace karetní platby s přítomností platební karty
 - Advance Deposit (nevratná záloha)
 - No Show (N.S.)
 - Priority / Express Check-Out Service v případě, že byla provedena Předautorizace karetní platby s přítomností platební karty
2. Mail Order (M.O.) / Telephone Order (T.O.) transakci:
 - lze provést pouze na základě písemné či telefonické objednávky zboží či služeb a souhlasu držitele karty (formulář „Zmocnění obchodníka“)
 - nerozdělujte na menší částky
 - nikdy nerozdělujte mezi více karet – mějte se na pozoru, pokud vám klient nabízí další čísla platebních karet z důvodu jejich nefunkčnosti nebo nedostatečného krytí
3. Veškerou korespondenci a další doklady k platbě kartou vždy uchovávejte pro případ reklamace.
4. Při zrušení rezervace provádějte refundaci (Návrat / Storno ve prospěch účtu držitele platební karty) vždy a pouze na platební kartu, kterou jste použili k provedení původní transakce. Nikdy nevracejte peníze jiným způsobem a nepřístupujte na možnost vrácení peněz prostřednictvím:
 - hotovosti
 - společností zprostředkávajících převod peněz, refundaci na jinou kartu, než kterou bylo placeno
 - převodem peněz na bankovní účet, atd
5. Nikdy nevyužívejte kartu klienta k uhrazení jiných služeb, než je platba za vámi standardně poskytované služby (ubytování, půjčení dané věci) či služby s tím přímo souvisejícími (parkování, mini bar, No Show, apod.). Pokud klient bude chtít kartou uhradit platby za zboží nebo služby, které standardně nenabízíte (nákup elektroniky, alkoholu, letenek, luxusních předmětů, nebo zaplatit tlumočnicka, průvodce, kurýra apod.), provedení platby odmítněte.
6. Nikdy neprovádějte platbu typu Dokončení předautorizace, pokud jste předtím na stejnou kartu neprovedli Předautorizaci karetní platby. Dokončení předautorizace proveďte včas a bez zbytečného odkladu. Alespoň jedna z těchto transakcí musí proběhnout za přítomnosti platební karty, přičemž transakce musí být ověřena PINem nebo stvrzenka podepsaná držitelem karty. 7. Dbejte vždy na to, aby klient, který si objednává ubytování osobně v hotelu, provedl platbu na platebním terminálu za přítomnosti karty. Zkontrolujete si tak, že jméno na platební kartě souhlasí se jménem klienta (a jeho občanským průkazem / pasem použitým při rezervaci) a klient je oprávněným držitelem karty.

PŘÍKLADY PODVODŮ

První kontakt s klientem.

Průběh podvodu:

- Klient zašle objednávku na dlouhodobý pobyt pro větší skupinu lidí (rodinná dovolená, firemní akce, svatba apod.) za lákavě vysokou cenu. V tomto stadiu je komunikace s klientem velmi pružná a zcela bezproblémová. Aby podtrhl svou důvěryhodnost, zašle v průběhu komunikace i kopii pasu, který bývá ve většině případů padělaný. Požaduje, aby platba byla provedena předem v plné výši (např. z důvodu nutnosti předložení faktury svému zaměstnavateli). V případě, že je jeho platební karta odmítnuta, okamžitě vám poskytne další čísla karet až do okamžiku, kdy je platba na některou z nich schválena. Varovný signál – klient zkouší více karet a ty jsou odmítány.
- Zahraniční cestovní agentura, kterou neznáte a standardně s ní nespolupracujete, pošle objednávku na rezervaci pobytu větší skupiny svých klientů, kteří přijedou s tlumočnickem a objednávají další nestandardní služby, např. zajištění transportu na větší vzdálenosti, nákup elektroniky apod. Požadují provedení platby předem v plné výši a zaslání provize za zprostředkování obchodu. Varovný signál – neznámý obchodní partner, nestandardní služby.
- Do hotelu či půjčovny dorazí klient, často se vydává za cizince nebo majitele karty vydané v zahraničí, chce zaplatit pobyt kartou, kterou sice nemá u sebe, ale má její kopii nebo pouze číslo karty, datum platnosti a CVV / CVC uložené v telefonu. Přesvědčí pracovníka, aby provedl

Dokončení předautorizace, aniž by předtím byla provedena Předautorizace platby. Varovný signál – klient vás nabádá k provedení nestandardního typu platby.

Průběh podvodu:

V okamžiku, kdy máte peníze za rezervaci připsány na účtu, přichází klient s dramatickým příběhem člověka v nouzi nebo s požadavkem na vyplacení provize a odměny za službu:

- „V mé rodině se objevila velmi těžká nemoc / úmrtí. Navíc mi dnes ukradli peněženku, ve které jsem měl všechny karty, proto není možné, abyste mi na ně vrátili peníze. Za vaši vstřícnost nabízím storno poplatků ve výši XX %, pokud mi zbytek peněz pošlete zpět jiným způsobem (převodem na účet apod.).“
- „Cestuji a okradli mě! Kupte mi, prosím, na mou kartu telefon / notebook a zašlete mi jej na mou současnou adresu.“
- „Okradli mě / Nemám možnost si sám koupit letenky! Kupte mi je prosím s použitím mnou poskytnutých údajů o kartě.“
- „Jsme cestovní agentura, pošlete nám za ubytování našich klientů provizi a platbu za tlumočnicka ve výši XXX EUR.“ Pokud nemáte s danou společností uzavřenou platnou smlouvu o provizi, a peníze přesto pošlete, riskujete přímou finanční ztrátu.

V některých případech dorazí host tzv. z ulice, většinou působí jako seriózní cizinec. Po ubytování přichází s následujícím příběhem:

- Zahraniční cestovní agentura, kterou neznáte a standardně s ní nespolupracujete, pošle objednávku na rezervaci pobytu větší skupiny svých klientů, kteří přijedou s tlumočnickem a objednávají další nestandardní služby, např. zajištění transportu na větší vzdálenosti, nákup elektroniky apod. Požadují provedení platby předem v plné výši a zaslání provize za zprostředkování obchodu. Varovný signál – neznámý obchodní partner, nestandardní služby.
- „Okradli mě, ale mám číslo jiné své karty (můj přítel vám zašle souhlas s platbou a údaje o své platební kartě faxem / e-mailem), které použijte k provedení platby za ubytování, případně na vyplacení hotovosti, kterou použiji do té doby, než mi banka zašle novou kartu.“

Nepřipusťte žádnou jinou možnost platby kartou než předložení reálné platební karty na místě!

Pokud dojde k podvodným transakcím, dříve či později oprávněný držitel platební karty zjistí, že došlo ke zneužití jeho platební karty, a podá reklamaci u své banky. Na základě této reklamace banka zašle žádost o vrácení peněz na reklamované platby. Veškeré platby bez přítomnosti karty, které držitel karty označí za podvodné, jste povinni refundovat, a to v plné výši. Pokud tedy provedete na žádost domnělého držitele karty jakékoli převody peněz, nákupy atd., nebude možné požadovat uhrazení těchto nákladů po pravém držiteli platební karty!

V případě, že jste provedli Dokončení předautorizace platby bez předchozí Předautorizace, případně provedete Dokončení předautorizaci v částce vyšší, než byla výše Předautorizace, a účet držitele karty je díky těmto transakcím v záporném zůstatku, zahájí banka klienta reklamační řízení, které prohrajete v důsledku nedodržení postupů při provádění karetních transakcí, a reklamovanou částku budete muset bance vrátit.

Mějte vždy na paměti, že za nesprávně provedenou refundaci, případně za zpracování podvodné objednávky nesete v reklamačním řízení finanční odpovědnost.

V případě jakýchkoliv pochybností o důvěryhodnosti klienta nebo jeho nestandardních požadavcích se obraťte na HELPDESK PK ČSOB.

E-mail: akceptacekaret@csob.cz

Telefon: [+420 495 800 116](tel:+420495800116)