Bezpečnost při použití platebních karet na internetu

IVO ROSOL, OKSYSTEM

Platební karty nebyly původně určeny pro platby na internetu. Následující řádky popisují některá rizika a protiopatření, která souvisí s rostoucím použitím platebních karet pro internetové platby.

Čipové platební karty snížily riziko zneužití ztracených a odcizených karet použitých v terminálu obchodníka a u bankomatu. Taková transakce vyžaduje použití kryptografických klíčů, uložených bezpečně na čipu a povinné zadání PIN. V kontrastu s tím se významně zvyšuje četnost zneužití čipových platebních karet v transakcích, kdy karta a její držitel nejsou fyzicky přítomny u obchodníka – zejména při nákupu zboží a služeb na internetu. Zde se zatím bezpečnostního potenciálu čipu nevyužilo.

A jaké jsou rizikové faktory z pohledu držitele karty? Mezi nejčastěji zmiňovaná rizika v souvislosti s platební kartou patří použití ztracené nebo odcizené karty, neoprávněné použití údajů karty zaměstnancem obchodníka (*tzv. skimming*) nebo získání údajů karty pomocí útoků na sociální inteligenci držitele karty (*phishing*).

BEZPEČNOST ČIPOVÉ TECHNOLOGIE

Čipové platební karty snížily riziko zneužití ztracených a odcizených karet pro platby, kdy je karta použita v terminálu obchodníka nebo bankomatu. Taková transakce vyžaduje použití kryptografických klíčů, uložených bezpečně na čipu a povinné zadání PIN držitele karty.

V kontrastu s tím se významně zvyšuje četnost zneužití čipových platebních karet v transakcích, kdy karta a její držitel nejsou fyzicky přítomny u obchodníka – zejména při nákupu zboží a služeb na internetu. Zde se zatím bezpečnostního potenciálu čipu nevyužilo.

Jaká je bezpečnostní úloha platební karty při platbě po internetu? Z pohledu držitele karty a jeho bezpečnosti bohužel žádná, stejnou službu poskytne kus papíru, na kterém je opsáno několik údajů z karty – její číslo, platnost, označení držitele a CVV2 kód. Některé banky přímo vydávají virtuální internetovou „kartu“ v této podobě.

BEZPEČNOSTNÍ OPATŘENÍ NA KARTĚ

V minulosti byla aplikována relativně jednoduchá bezpečnostní opatření k omezení zneužití platební karty, jedním ze známých mechanismů je použití číselného kódu CVV2/CVC2 (*Card Verification Value/Card Verification Code*). Tento kód je vytištěn na rubové straně karty a je tvořen třemi číslicemi. Kód není součástí informace uložené na magnetickém proužku, nebo na čipu karty, takže není používán v běžných platebních transakcích, kdy je karta předložena obchodníkovi. Po skončení transakce navíc není povoleno CVV2/CVC2 uchovávat.

Dalším opatřením je uvádění pouze části čísla karty na účtenkách vydávaných obchodníkem. To sice snižuje pravděpodobnost zneužití karty obchodníkem, není to ale žádnou překážkou v případě použití ztracené nebo odcizené karty pro platby na internetu.

SW PRO DETEKCI PODVODŮ

Banky provozují software pro detekci podvodů, napomáhající odhalení podezřelých transakcí na základě různých příznaků nestandardního vzorce chování. Například vysoká platba v místě vzdáleném od „domovské“ lokality držitele karty, případně z počítače, jehož adresa je uvedena na „černé listině“ jsou důvodem pro kontrolu.

Účinné je též získání informací z hromadných dat transakcí, které mohou odhalit kompromitovaná zařízení

ODPOVĚDNOST ZA ZTRÁTU

Odpovědnost je rozprostřena mezi držitele karty, obchodníka a banky, konkrétní rozdělení je zakotvené ve smluvních podmínkách v závislosti na legislativě dané země.

Zodpovědnost držitele karty je zpravidla omezena do termínu ohlášení ztráty karty a maximální výškou částky (*v Evropské unii 150 EUR*). Pokud je ale při platební transakci použita EMV karta a PIN, případnou ztrátu nese držitel karty z důvodu hrubé nedbalosti při zacházení s PIN.

Obchodník je zodpovědný, pokud porušil závazná pravidla stanovená bankou. Strašákem internetových obchodníků je zpětné zúčtování (*chargeback*) v důsledku reklamované transakce, kdy může vydavatel požadovat od zpracovatelské banky vrácení celé částky transakce nebo její části. Tento postup se používá v případě, kdy je nějaká dříve realizovaná transakce napadena držitelem karty z důvodu opravňujícího k vrácení účtované částky. Podle aktuálního verdiktu Nejvyššího soudu v případě Českých aerolinií musí obchodník dokonce vrátit prostředky, zaplacené na základě podvodně získaných údajů z platební karty.

V ostatních případech nese ztrátu vydávající banka nebo banka obchodníka (*zpracovatelská banka*).

PLATBA NA INTERNETU

Platba po internetu je tradičně chápána jako nejrizikovější transakce s platební kartou, a to pro všechny zúčastněné strany.

Základním bezpečnostním měřítkem je použití bezpečné internetové komunikace, založené na protokolech TLS/SSL a důvěryhodném certifikátu web serveru internetového obchodu. Moderní internetové prohlížeče důrazně varují uživatele, pokud existuje problém s certifikátem zabezpečení webu.

Ještě větší úroveň jistoty o autenticitě webu lze získat, pokud je web server vybaven certifikátem EV SSL (*Extended Validation*). Browser v tomto případě zobrazuje adresní lištu zabarvenou zeleně, společně se jménem certifikační autority a názvem společnosti, které byl certifikát vydán.

INTERNETOVÉ PLATBY KARTOU S 3D SECURE

Významným krokem ke zvýšení bezpečnosti plateb po internetu je zavedení technologie 3D Secure a její podpora u internetových obchodů a bank vydavatelů platebních karet.

3D Secure na straně internetového obchodníka

Mechanismus 3D Secure začaly banky v České republice zavádět nejprve na straně internetových obchodníků. Praktickým důsledkem je sjednocení mechanismu akceptace karet prostřednictvím platebních bran bankovních institucí obchodníků. Na příslušných stránkách obchodníků i platebních bran jsou zobrazena loga Verified by Visa a MasterCard Secure Codea.

Použití platební brány

Platební brána je souhrn technického a programového vybavení provozovaný bankou, anebo jejím smluvním partnerem, umožňující internetovým obchodům akceptovat platební karty. Hlavní výhodou platební brány je relativně jednoduchá implementace jejího použití na straně systému web obchodu a dále skutečnost, že obchodník nemá přístup k údajům o platební kartě klienta.

Protokol 3D Secure

Zákazník nakupující v internetovém obchodě vybere platbu platební kartou. Web obchodníka přesměruje prohlížeč zákazníka na zabezpečenou stránku platební brány zpracovatelské banky, kde zákazník vyplní údaje o kartě. Platební brána vyšle dotaz na adresářový server kartové organizace, která vrátí informaci, zda je použitá karta zařazena do systému 3D Secure, a informaci, jak kontaktovat autentizační server vydavatele karty. V případě, kdy karta není zařazena do systému 3D Secure transakce, pokračuje bez autentizace klienta.

Prohlížeč zákazníka je přesměrován na autentizační stránku vydavatelské banky, kde zákazník vyplní autentizační informaci. Lze použít různé technologie autentizace, například jednorázové heslo, zaslané pomocí SMS zprávy na mobilní telefon zákazníka. Výsledek autentizace je digitálně podepsán a prostřednictvím prohlížeče zákazníka odeslán na stránku platební brány.

V případě, kdy autentizace proběhla úspěšně (*nebo pokud karta není zařazena do systému 3D Secure*), je internetová platba dále zpracována jako běžná platební transakce. Systém odešle požadavek na autorizaci platby, kterou zpracovatelská banka předá vydavatelské bance. Vydavatelská banka provede autorizaci a vrátí autorizační kód.

3D Secure na straně držitele karty

Využití možnosti autentizace držitele karty v průběhu transakce prostřednictvím mechanismu 3D Secure zavádějí tuzemské banky až v současné době, tuto službu jako první zavedla Citibank, následovaná ČSOB a Poštovní spořitelnou. Lze očekávat, že další banky se připojí k tomuto trendu.

Výhodou pro držitele karty je zejména skutečnost, že při nákupu ve webovém obchodě zapojeném do 3D Secure poskytuje údaje karty pouze jedinému subjektu – své vydávající bance, přesněji řečeno jejímu smluvnímu partnerovi provozujícímu platební bránu. Držitel karty ale nesmí podlehnout klamnému pocitu dokonalé bezpečnosti. Na vlastní kartě se zapojením do systému 3D Secure nic nezměnilo, pouze jedno z mnoha rizik při použití karty se zmenšilo.

Držitel karty za to ovšem platí tím, že nese zodpovědnost za transakce s autentizací, které nemůže popřít. Situace je zcela analogická jako u transakcí, které byly provedeny v přítomnosti karty s použitím PIN.

OTEVŘENÁ OTÁZKA NA ZÁVĚR

Zcela na místě je otázka, proč není použita EMV čipová karta k autentizaci svého držitele v rámci 3D Secure a na místo toho jsou využívány jiné mechanismy.

Lze si jistě představit důvody, související s pořízením čteček čipových karet a software a rozsáhlou podporou uživatelů; tyto procesy jsou ale zvládnuty pro internetové bankovnictví. Odpovědět mohou jedině banky a kartové organizace. ■

Ivo Rosol je ředitelem vývojové divize společnosti OKsystem.