

Lze důvěřovat bankomatům?

Skimming je krádež informací o platební kartě, které jsou použitelné pro platnou finanční transakci. Za rok 2009 činily v Evropě ztráty z tzv. bankomatové kriminality v přepočtu 20 miliard korun, což je asi 150 % oproti roku předchozímu.

Technická vyspělost podvodníků

Novou charakteristikou útoků na bankomaty je velmi vysoká profesionalita a mezinárodní rozměr. Najdou se i útoky méně technicky vyspělé, i hrubé násilí, ale alarmující je nárůst té nejprofesionálnější kriminality, kterou si lze představit. Běžný občan se proti ní téměř nemůže bránit. Zakrytí klávesnice rukou při vkládání PIN může částečně zabránit, ale ne všem. Skimmeři využívají dokonale překryvné nástavce na originální díly bankomatů, které nelze rozeznat ani barvou, ani povrchovou úpravou, ani technickým provedením od přirozených součástí bankomatu. Bankomaty nemají ve světě jednotný vzhled, ba naopak. Ani u domácích bankomatů, které dokonale známe, protože je mnoho let používáme, nelze zkontrolovat, zda bezpečnostní antiskimmovací hrdlo není dílem útočníka. Proti dokonalé napodobenině máme velmi málo šancí. Klienti, kteří rukou dokonale zakrývají klávesnici při vkládání PIN, jsou zase bezmocní proti tomu, když na originální klávesnici je nalepena klávesnice útočníka (obr. 1), nerozeznatelná od originálu. U útočnickovy klávesnice, která má stejný design, se nerozpozná miniaturní navýšení, nelze ji odlepit a dokonale splývá s povrchem. Útočník má dnes v ruce všechny trumfy. Dostupné jsou také minikamery, mikroténkové nalepovací fólie (obr. 2) apod.

Skimmující útočníci mají za cíl získat údaje o kartě, popř. její PIN. Kód PIN není to nejdůležitější, protože na uskutečnění obchodu s kartou stačí znát pouze pár čísel o kartě. U spousty nákupů (včetně internetu) jde pouze o jméno držitele, číslo karty, expirace, v nehorším případě o kódy CVV na zadní straně karty. To vše skimmovací zařízení v bankomatu nebo v platebním terminálu přečte (obr. 3 až 5).

Mezinárodní spolupráce skimmerů

Bankomatová kriminalita má mezinárodní rozměr a využívá dělbu práce. Skimmeři v jedné zemi nasbírají údaje a anonymně je prodají na internetu jiné skupině nebo komplicům. Druhá skupina v jiné zemi nakoupí od jiného dodavatele něco, čemu lze říkat zlatý pramen. Pramen není nic jiného než technická realizace možnosti určitého převodu peněz pomocí získaných údajů z platebních karet. Raději nerozvádějme možnosti těchto transferů, jen řekněme, že

jde o automatizované techniky. Nejde o to, koupit si ledničku nebo tisíc ledniček v internetovém obchodě. To druhé by bylo dosti podezřelé. Pramen musí umožnit zadat čísla a přeměnit je na peníze nebo velké dodávky zboží. Fáze proměny získaných údajů z platebních karet je ale nejsložitější, a často je příčinou dopadení pachatelů.

Jak se bránit?

Co máme dělat my, uživatelé výhod platebních karet a pohodlného nákupu čokoliv přes internet? Slovy klasika, „nedělejte nic jako dosud“. To, že bankomaty nebo jejich



Obr. 1 Nalepovací klávesnice



Obr. 2 Odhalený panel s kamerou, dole vpravo falešný vložený nástavec

v supermarketu, ale i bezpečnostní kamera, číšník nebo skimmovací zařízení na milionech platebních terminálů a bankomatů ve světě.

Technická řešení existují

Naštěstí technika je velmi schopná – a kryptografie také. Možná přijde nová obrana proti skimmingu, jistě je, že stará



Obr. 3 Bankomat se skimmovacím zařízením



Obr. 4 Detail falešného nástavce



Obr. 5 Falešný panel

části je možné padělat, není problém nás, ale problém bank a provozovatelů bankomatů. Technika pokročila a bankomaty jsou stále stejně jako před dvaceti lety. To je dlouhodobě neudržitelné. Situaci lze řešit také tím, že se celosvětově přejde na čipové platební karty. K tomu se již postupně přistupuje, a je to levnější než výměna bankomatů. Pro fungování uvedeného řešení je třeba, aby místo magnetického proužku nebo údajů vytištěných na kartě bylo k uskutečnění transakce nebo k výběru z bankomatu nutné, aby se „zúčastnil“ také čip na kartě. A navíc je třeba, aby to platilo na celém světě. V opačném případě bude vždy existovat onen zlatý pramen, kde dokonale kryptografie na čipu bude vyřazena. Co to znamená, je technologická revoluce v mezinárodním obchodě. Musí zmizet imprintéry, které využívají embosované platební karty, musí zmizet karty s magnetickými proužky, musí zmizet internetové platby využívající údaje na kartě, které si může přečíst každý, kdo na kartu chvíli vidí. Tím může být nejen pokladní

opatření jsou nyní neúčinná, že oddělení bank hlídající podezřelé platby nutně bují, a to banky donutí přemýšlet, jak to udělat jinak.

Jestliže se stanete předmětem podvodu, je pravděpodobné, že vzniklou škodu za nedokonalou bankovní techniku nebudete hradit vy. Jen v Evropě by tak bylo v roce 2008 nutné zaplatit škody za 10 302 ohlášených skimmovacích podvodů. Zdá se, že to není naše starost, ale koneckonců je, protože banky škody zaplatí sice méně viditelně, zato z našich peněz.

Nebudeme zde dávat rady, co dělat u bankomatu, ale doporučujeme si čas od času na internetu vyhledat ATM skimming. Úpravy na obrázcích v článku mohou být snadno překonány nápaditějšími zařízeními.

Vlastimil Klíma, nezávislý kryptolog,
v.klima@volny.cz