Elektronické bankovnictví a bezpečnost

Na současnou nedobrou situaci v bezpečnosti finančního sektoru společně ukazují analytici světových konzultačních firem. Podíváme se proč. Nebyla to kryptologie a vynález digitálního podpisu, ale internet, který způsobil, že finanční trh se v posledních desetiletích od základu změnil.

Dále budeme hovořit jen o bankách, přestože změna nastala ve všech oblastech finančních institucí i produktů, jako jsou pojistky, hypotéky, elektronické platby, domácí i firemní platby. Kryptologie jen díky digitálnímu podpisu pomohla bankám v počátcích, aby se nebály vstoupit na neprobádanou půdu internetového bankovnictví v dobách, kdy mu ještě nikdo nevěřil. Jakmile internet a později mobilní telefony ovládly masový trh, zisk smazal všechny obavy a banky přijaly mizivé riziko podvodů oproti neskutečným výhodám, které bankovnictví on-line přineslo.

Bezpečnost šla stranou. Staré těžkopádné bankovní informační systémy nestačily a za chodu se vytvářely nové. Banky fúzovaly a problémy s informatikou narůstaly. Slepence se stávaly složitějšími. A tomu odpovídá stav v bezpečnosti. Těžko lze nalézt někoho, kdo by mohl v jakékoliv finanční instituci říci, že ví, jak funguje informační systém a jeho bezpečnost. Výjimkou je pouze několik nových, na zelené louce stavěných systémů tak, jako tomu kdysi bylo u nás u ebanky. Nicméně jednou snad bude vše integrováno a zabezpečeno.

Neříkáme to proto, abychom získali bankovní zakázky nebo si vylili srdíčko, ale proto, že tento stav začíná být problémem. Dosud byla rizika malá, ale banky nyní začíná znepokojovat prudký nárůst ztrát, internacionalizace útočníků a geografická rozprostřenost útoků. Nárůst ztrát bankovnictví on-line se v posledních čtyřech letech odhaduje na asi 100 % ročně.

Kuriózní je nedávný případ, kdy si parta lidí z jedné blízké země nekrytými výběry z bankomatů přišla na miliony v jiné evropské zemi. Použité platební karty byly pravé, takže policie zadržené lidi zase propustila. To, že přišli na trik, že z jistých bankomatů lze vybírat donekonečna hotovost na platné karty, byla bezpečnostní chyba banky. Šlo o vážené klienty, kteří bance nic zlého neprovedli! A další otázka je, zda to vůbec byla chyba banky, protože bankomaty pro ni může provozovat jiná společnost, která si zase najímá jinou společnost na doplňování peněz, jinou na přenos transakcí, údržbu a administraci. A to nehovoříme o tom, že někdo jiný bankomaty vyrábí, někde vznikají superdůležité klíče, s jejichž pomocí lze s bankomatem dělat na dálku cokoliv, a že informační systém banky může být outsourcovaný, atd. Také nehovoříme o tom, že existují administrátoři, kteří nechají v bankomatu přednastavené heslo 1234, jež je vytištěno v návodu (stalo se). Nehovoříme ani o tom, že někdo může připustit, aby v bankomatu byl operační systém Windows a s ním i tzv. trojští koně, zachytávající otevřeně PIN (stalo se).

Když vznikne škoda

Klienty taková situace sice nijak netěší, ale naproti tomu, toto jsou problémy bank. Jestliže dojde k nějakému neoprávněnému výběru nebo transakci, při nichž bychom měli přijít o své peníze, nemusíme se vzhledem k výše uvedenému stavu obávat trvat na náhradě. Velmi pravděpodobně taková škoda bude nahrazena. Dosud se tak postupuje, protože jde skutečně o podvody, a nikoliv ze strany klientů. Jestliže by však banka nechtěla škodu nahradit (za podmínky, že jste skutečně neudělali úmyslně chybu), můžete s klidným svědomím banku žalovat. Škoda, která bance vznikla, je mizivá ve srovnání s tím, že by musela zpřístupnit svůj „dokonalý informační systém“ soudnímu znalci, aby posoudil, že z tohoto „systému“" nemohlo nic uniknout.

Situaci řeší banky v tichosti. V září na ni ale důrazně upozornilo několik významných amerických a světových institucí, které se specializují na analýzu, odhalování a zamezování krádeží, podvodů a bankovní kriminality, např. Guardian Analytics, FDIC, Asociace elektronických plateb NACHA, Centrum analýzy finančních institucí FS-ISAC, Senátní výbor USA, Gartner aj. Tyto instituce říkají, že „kyberútočníci“ se stávají velmi pokročilými, a doporučují několik základních pravidel, z nichž některá vybíráme.

Doporučení expertů

- *Buďte si vědomi svých finančních práv:* Dožadujte se u své banky její politiky a opatření k ochraně vašeho účtu.
- *Žádejte svoji banku, aby zvýšila investice do bezpečnostní techniky:* Vaše peníze jsou chráněny pouze touto technikou. Mnoho institucí nemá v pořádku ani základní autentizační procedury. Požadujte, aby banka používala monitoring on-line a proaktivní ochranu proti podvodům a krádežím, aby jim mohla zabránit v reálném čase.
- *Kontrolujte svůj účet:* všímejte si čehokoliv neobvyklého a sledujte své platby. Mnoho bank nabízí klientům upozornění na podezřelé transakce. Využívejte je a požadujte taková varování.
- *Starejte se o bezpečnost svého počítače:* mnoho lidí přichází o peníze vlivem své neopatrnosti. Nestarají se o antivirové a antimalwarové prostředky a nechají počítač napospas škodlivému softwaru, který zachytí jejich přístupová hesla a odešle je útočníkům. Přestože je obrana složitá, a právě proto, že nikdo nemůže vyloučit zavirování, je naprosto nezbytné kombinovat přístupové heslo s autorizací pomocí zpráv SMS, autentizačních kalkulátorů apod.

Několik čísel

- O největší krádeži údajů k platebním kartám jsme se dozvěděli letos. Osmadvacetiletý Američan Albert Gonzalez se společně s několika anonymními ruskými komplici dostal do databází velkých obchodních řetězců (i do jiných systémů) a prodával ukradené informace po celém světě. Šlo o 130 milionů kreditních a debetních karet.
- Zloději se zaměřují již na krádeže zašifrovaných i nezašifrovaných bloků PIN k těmto kartám a spolupracují i s lidmi uvnitř bank. Nyní jsou běžné mezinárodní gangy na padělání karet pracující on-line po celém světě.
- Jeden koordinovaný útok byl zaznamenán v minulém roce, kdy bylo během několika hodin okolo půlnoci 8. listopadu vybráno v bankomatech 9 milionů dolarů. Do akce bylo zapojeno 100 karet a 130 bankomatů ve 49 městech od Moskvy po Atlantu.

V poslední době jde organizovanost útoků tak daleko, že např. klient si vybírá peníze z bankomatu, netuší, že probíhá krádež jak údajů z jeho karty, tak i PIN a že tyto údaje jsou posílány on-line na jiné místo ve světě, kde je za několik hodin vyroben duplikát jeho karty a na něj vybrána hotovost z jeho účtu v tamním bankomatu.

Za všemi uvedenými útoky je nedůsledné využití kryptografie jako jedné z metod ochrany dat. Jednou je to její ignorování, jindy slabé autentizační metody nebo ochrana komunikace, potřetí nereagování na nové útoky. Také bankomaty by mohly přestat používat staré moduly, navrhované před několika desítkami let, a napadnutelné komunikační protokoly. Experti na bezpečnost se shodují v tom, že tuto oblast je nutné brzy zcela změnit.

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

LITERATURA

[1] Archiv článků kryptologie pro praxi: http://cryptography.hyperlink.cz