Masarykova univerzita v Brně

Ekonomicko-správní fakulta

Téma : Krize v elektronickém bankovnictví a jejich řešení

Datum : 13.11.2007

Vypracoval: Michal Valášek
Adam Zubatý

Obsah:

Úvod	**2**
Přenos informace mezi bankou a klientem	**3**
Krize v komunikaci prostřednictvím telefonu	**4**
Příklad krize Phone bankingu	**5**
WAP Banking	**6**
Internetbanking	**7**
Příklady krizí v internetovém bankovnictví	**9**
Platební karty	**11**
Případy krizí platebních karet	**12**
Závěr	**16**
Zdroje	**17**

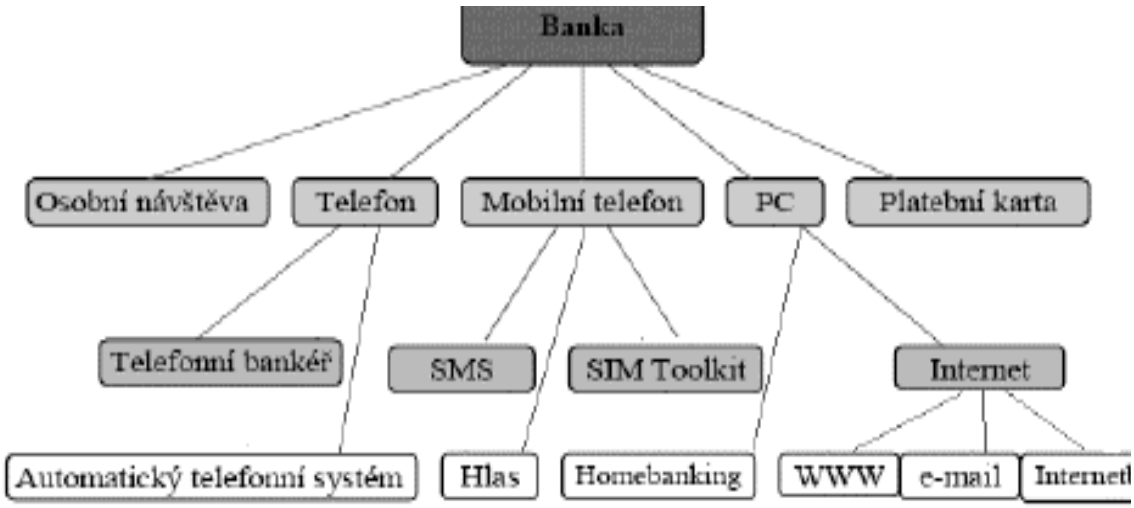
Úvod

Pro naši seminární práci jsme si vybrali zpracování tématu „ Krize v elektronickém bankovnictví a jejich řešení“. Pod tímto pojmem (krize) si většina lidí může vybavit řadu dalekosáhlých krachů bankovních institucí prostřednictvím špatného či nedostatečného fungování elektronického bankovnictví. Ale co se týče skutečnosti, k těmto krizím mohlo a také docházelo a dochází, ale v mnohem menším rozsahu, než které si představíme pod názvem „krize“. Jednalo se většinou o krize v důsledku malého zabezpečení elektronického bankovnictví. Na některé nedostatky došly spousty IT pracovníků spravujících IS příslušných bank až při uvedení e-bankovnictví do jeho plného užívání. Řadu problémů s tím souvisejících si probereme a pokusíme se na ně najít správná východiska

v následujícím textu. Tak jak se vyvíjela a vyvíjí informační technologie, tak se také vyvíjí elektronické bankovnictví. IT pracovníci musí neustále vytvářet nové zabezpečující systémy plně chránící e-bankovnictví příslušných bankovních institucí. A to z mnoha důvodů, informační technologie přináší samozřejmě prostor pro stále více se rozšiřující „ hackery", kteří prostřednictvím nejvyspělejší technologie spekulují, jak své „schopnosti" zužitkovat ve svůj prospěch. Jak se pokouší svých „schopností" využít se dozvíme v následujícím textu. Dále se budeme také zabývat možnými řešeními problémů v oblasti ochrany IS bankovních institucí. Zvyšující se požadavky na zabezpečí bankovních účtů samozřejmě ovlivňují i nároky kladené na banky jako takové. Růst finančních nákladů bank se odráží i v rostoucích cenách poskytovaných služeb. Ale bezpečnost je bezesporu na prvním a na nejdůležitějším místě, takže z toho lze usuzovat, že klient si raději připlatí v rámci zabezpečení svých „těžce vydělaných" finančních prostředků.

Přenos informace mezi bankou a klientem:

Propojení klienta s bankou může být prováděno mnoha odlišnými způsoby. K těmto propojením můžeme zařadit osobní návštěvu, komunikace prostřednictvím telefonního hovoru s telefonním bankéřem, spojení přes mobilní telefon, v neposlední řadě propojení prostřednictvím počítače a také používáním platebních karet. V naší seminární práci se zaměříme především na oblast telefonního spojení, na sféru počítačového propojení a na oblast platebních karet, ve kterých se možné „krize" elektronického bankovnictví vyskytly a znovu mohou vyskytnout. V jaké míře a jaké měly následky se dočteme na následujících stránkách.



Z tohoto schémata jsou jasně patrné možnosti komunikace s bankou.

„Krize“ (problémy) v oblasti komunikace prostřednictvím telefonu:

Banka<->Telefon – klient (Phone Banking)

Telefonické bankovnictví je po platební kartě historicky druhým přímým komunikačním kanálem, který se dočkal masovějšího rozšíření. Telefon, ať již pevná linka nebo mobilní telefon, je dnes stále nejdostupnějším komunikačním kanálem. Mobilní telefon lze mít stále u sebe a tím být neustále v kontaktu se svou bankou.

Služba telefonního bankovnictví nabízí svým uživatelům možnost komunikovat s bankou prostřednictvím telefonu. Klient tak může operovat se svým účtem 24 hodin denně, 7 dní v týdnu a to z celého světa. Phone banking lze používat pouze pomocí telefonního přístroje s tónovou volbou (včetně mobilního).

Bezpečnost

Přístup do systému je vázán na zadání čísla PIN, **případně** hesla**. Pokud dojde k vyzrazení těchto čísel, je celý systém poměrně lehce zneužitelný. Nebezpečí ale není zase tak veliké, neboť systém pracuje pouze s bezhotovostním platebním stykem a zpravidla lze operovat pouze s omezenou částkou. Veškerá komunikace je navíc bankou zaznamenána a archivována, proto je snadné dohledat podezřelé operace.**

Jelikož se phone banking uskutečňuje prostřednictvím telefonu, hlavní zádrhel se může stát, pokud se u našeho telefonního operátora vyskytne nějaká chyba.

1, Příkladem je případ zákazníků sítě Vodafone[1]

Klienti eBanky, kteří se přes Vodafone chtěli 12.10. 2007 přihlásit do elektronického bankovnictví, neuspěli. Operátor od rána nedokáže doručovat autorizační SMS.

Na problém upozornilo iDNES. cz několik čtenářů a upozorňuje na něj i portál eBanky.

Pokud klienti nemají jinou možnost přihlášení - internetový nebo osobní elektronický klíč, nebo nemohou použít jiného mobilního operátora, jsou pro ně služby internetového bankovnictví eBanky prozatím nedostupné.

"Bohužel došlo k chybě systému, na jejímž odstranění od rána intenzivně pracujeme," řekl Filip Hrubý z Vodafonu.

Podle současného vyjádření operátora byla závada odstraněna a od 15:00 vše funguje bez problémů.

"Část našich zákazníků dnes zaregistrovala problémy s doručováním informačních a autorizačních SMS v rámci služby elektronického bankovnictví. Bohužel došlo k chybě počítačového systému SMS centra, kterou se nám už podařilo úspěšně odstranit." oznámil bezprostředně po nápravě problému mluvčí operátora.

Dle něj měla problémy s doručováním informačních a autorizačních SMS pouze část zákazníků. "Nejednalo se o 100% výpadek služby jako takové. V tuto chvíli již všechny služby elektronického bankovnictví Vodafonu fungují normálně," dodal.

Klienti se i přesto ještě před chvíli nemohli přihlásit. Portál banky pouze oznamoval probíhající údržbu, která měla trvat do 17:15. V současné chvíli (16:54) již aplikace funguje.

[1] http://mobil.idnes.cz/vodafone-a-ebanka-maji-problem-s-internetovym-bankovnictvim-plh-/mob_operatori.asp?c=A071015_093647_mob_denik_jm

„Krize“ v oblasti propojení prostřednictvím počítače:

Home banking [2]

Pomocí Home bankingu komunikujeme s bankou prostřednictvím sítě internet nebo telefonu. Pro komunikaci je potřeba počítač s internetovým připojením a speciální program banky.

Je vhodný pro klienty, kteří zpracovávají větší objem plateb a potřebují informace o skutečném stavu svého účtu.

Co se týče nevýhod, tak tou je bezesporu vázanost na určitý počítač daných parametrů.

Co se týče jeho bezpečnosti, tak se dá považovat se vůbec nejlepší zabezpečovací systém ze všech forem elektronického bankovnictví. Přihlášení do sítě je zabezpečeno jednak heslem a autorizačním certifikátem uživatele a navíc je vzájemná komunikace mezi bankou a klientem kódována.

Co se týče skutečné krize v oblasti Home bankingu, tak nebyla zaznamenaná žádná významná krize tohoto způsobu komunikace banky a klienta.

Internetové bankovnictví

Jedná se o komunikaci klienta s bankou prostřednictvím celosvětové sítě Internet. Mladší variantou Internet bankingu je WAP banking, kdy se k Internetu připojujete pomocí mobilního telefonu.

WAP Banking

Je mladší variantou Internet bankingu, kdy se k Internetu připojujete pomocí mobilního telefonu. Při využívání WAP bankingu je zapotřebí mobilní telefon podporující protokol WAP.

1, Příklad hlavní krize WAP bankingu proběhla v podstatě při uvedení na trh[3]:

Již v devadesátých letech minulého století připravily přední finské banky e-strategii pro rozvoj elektronického bankovnictví a souvisejících systémů.

Celá řada online služeb byla vyvinuta, aniž by bylo zřejmé, zda o ně zákazníci budou mít zájem. Na začátku nového tisíciletí zažily banky zklamání, které souviselo s neúspěšným uvedením mobilních plateb prostřednictvím nových WAP telefonů na trh. Tento konkrétní případ potvrdil nepředvídatelnost situace při uvádění nových technologií na trh.

Zákazníci nebyli připraveni začít využívat bankovní služby prostřednictvím WAP v době, kdy proběhl pokus uvést je na trh. Telefonní přístroje těmto účelům nevyhovovaly.

---

[2] http://www.mesec.cz/texty/home-banking/

[3] http://www.tietoenator.cz/default.asp?path=553,732,16082,1456,11985,28446

Internetbanking

Bankovní domy vědí, že nová služba snadno zaujme pozornost několika set uživatelů. Získat širokou klientelu však vyžaduje svůj čas. Spotřební trh zůstává nepředvídatelný.

Jako první přišla s nabídkou internetového bankovnictví Expandia banka (v současnosti eBanka). Nyní je elektronické bankovnictví nabízeno většinami bankovních institucí. A počet bank s touto službou neustále přibývá.

Pro komunikaci plně postačuje pouze počítač napojený na internet a nějaký internetový prohlížeč. Takže oproti Home bankingu nepotřebujeme žádné další nákladné programy. Spojení s bankou lze tudíž zprostředkovat z jakéhokoliv počítače s internetem.

Umožňuje provádění bezhotovostních plateb – příkazy k úhradě, trvalé příkazy. Získávat informace o manipulacích s účtem, o zůstatku na účtu, posledních přijatých a odchozích platbách atd.

1. Bezpečnost

Odborníci, kteří se dlouhodobě o tuto oblast zajímají, tvrdí, že neexistuje e-bankovnictví zcela bez rizika. Dle jejich názoru lze pouze ochranu maximalizovat. Klient vyžaduje nejenom bezpečnost, ale také očekává uživatelsky nenáročnou aplikaci, kterou bude bez komplikací schopen kontrolovat a ovládat.

1.1. Způsoby zabezpečení[4]:

Existuje vícero druhů zabezpečení, které budou následně vyjmenovány. Pozitivní zprávou pro všechny uživatele je, že dojde ke zvýšení bezpečnosti elektronického bankovnictví u všech bank, a to v důsledku toho, že nebude možno realizovat např. příkaz k úhradě jenom prostřednictvím uživatelského jména a hesla.

Druhy zabezpečení:

- **certifikáty (BAWAK Bank CZ, Volksbank a WSPK)**
- **certifikát na USB tokenu (WSPK)**
- **jednorázové kódy posílané na mobil (GE Money Bank, Raiffeisenbank)**
- **jednorázové kódy do vlastních rukou (Živnostenská banka)**
- **certifikát na čipové kartě (ČSOB, ČS a Komerční banka)**
- **certifikát a zároveň sms kód pro přihlášení (Komerční banka)**
- **posílání sms kódu při přihlášení (eBanka)**

Dalšími možnostmi zabezpečení jsou např. nastavení limitů pro transakce, odhlášení z aplikace po delší nečinnosti, zablokování účtu při opakovaném zadávání nesprávných údajů.

---

[4] http://fincentrum.idnes.cz/jak-banky-zabezpecuji-internetbanking-dhb-/fi_blind.asp?c=A061006_164849_fi_blind_zal

Zabezpečení interbankingů

Banka	Přihlášení a odhlášení			
	metoda	kvalita	uložení	aut. odhlášení
Bawag	Jméno heslo	jméno z čísla účtu, **statické heslo**	-	5 minut
Citibank	Jméno heslo	velmi dlouhé číslo jako ID, 9 číslic pinu	-	5 minut
Česká spořitelna	jméno heslo, nebo čipová karta	10 číslic ID, **statické heslo**	/karta	cca 10 minut bez varování
ČSOB	jméno heslo, nebo čipová karta	5 znaků pin, karta s podepisovací logikou	/karta	??
eBanka	jméno heslo, nebo autentizační kalkulátor	9 číslic ID, 11 číslic jednorázového hesla chráněného BPINem	-	**nepozorován**
GE Money Bank	certifikát + jméno heslo	9 číslic ID, 8 znaků case sens. hesla	-	??
HVB Bank	Jméno heslo	jednorázové heslo z kalkulátoru	kalkulátor chráněný PINem	ano
Komerční banka	certifikát	asi 1024	p12 ve volitelném souboru	ano
Poštovní spořitelna	Jméno heslo	jméno jako číslo, 5 číslic pin	-	20 minut
Raiffeisenbank	Jméno heslo	lidské jméno,**statické heslo**	-	**ano**
Volksbank	Jméno heslo	nezapamatovatelné jméno, **statické heslo**	-	**nepozorován**
Waldviertler sparkasse	Jméno heslo		-	**nepozorován**
Živnobanka	certifikát + jméno heslo	jméno 5 číslic, heslo lidské	-	??

http://www.penize.cz/info/zpravy/zprava.asp?IDP=1&NewsID=3622

Příklady krizí v elektronickém bankovnictví:

1, Případ Velké Británie v srpnu 2000[5]

Clearingová banka ve VB umožnila chybou v systému přístup klientům k účtům jiných klientů. Druhým nedostatkem této banky bylo to, že jeden uživatel se náhodou dostal k finančním tokům svého souseda a do třetice neprošla online aplikace kontrolou zabezpečení. To znamená, že po odhlášení ze systému a následném stisknutí tlačítka „Zpět" se zjistilo, že jsou uživatelé stále přihlášeni. Díky těmto selháním došlo k tomu, že britští bankéři získali špatnou pověst a to umožnilo expanzi konkurentů(zejména z Francie).

2, Vykradení účtu KB v srpnu 2006[6]

Internetové bankovnictví Komerční banky bylo napadeno organizovanou skupinou útočníků. Vážná situace vyústila ve spěšné posílení zabezpečení banky. Slabinou se stalo zabezpečení pomocí certifikátu. Došlo k tomu, že se útočníci dostali ke klientskému certifikátu a heslu, čímž získali přístup k účtu. Peníze následně převedli na účet tzv. "bílého koně", osoby, která vyzvedla hotovost a zaslala ji na účty v zahraničí - pravděpodobně ve Velké Británii, v Belgii a na Ukrajině. Banka je se všemi dotčenými klienty v kontaktu a neoprávněně odčerpané prostředky klientům již plně nahradila

Řešení této situace:

Banka zavedla takové opatření, že vydala informaci o posílení zabezpečení SMS zprávou zasílanou na mobilní telefon den předem. Přidání dalšího autorizačního prvku, kterým se ověřují aktivní bankovní operace, jednoznačně zvýší bezpečnost. Rychlost jeho zavedení sice přinesla drobné komplikace (částečná nedostupnost přetíženého serveru), ale vesměs je také přínosná. Útočníci, o nichž se předpokládá, že tvoří organizovanou skupinu, se nebudou moci snadno přizpůsobit a sníží se tak rozsah škod.

3, Zcizení peněz z účtu ČS v srpnu 2006[7]

Tato situace se týkala klientů s nejnižší formou zabezpečení kont. Pro vstup se používalo pouze uživatelské jméno a statické heslo bez další autorizace plateb. To je způsob, který lze využít do limitu 20 tis. Kč denně – limit snížen na nulu, čímž se bezpečnost zvýší. Odčerpané finanční prostředky byly vráceny klientům zpět.

[5] v PHILLIPS, D. *Online public relations.* 2003, str. 41, ISBN 80-247-0368-8.
[6] http://www.mesec.cz/clanky/komercni-banka-vykradeni-uctu-potvrzeno/
[7] http://www.mesec.cz/aktuality/i-ucty-ceske-sporitelny-byly-cilem-utoku/

4, Podvodné e-maily ČS v říjnu 2006

E-mailové schránky klientů ČS byly zaplaveny podvodnými e-maily, které měly podobu zpráv od ČS a nabádaly je k tomu, aby se přihlásili na službu Servis 24 – Internetbanking. Je to typický příklad tzv. pfishing, kdy se podvodníci od lidí snaží vylákat identifikační údaje k tomu, aby jim mohli vykrást bankovní účty.

Text podvodného e-mailu

Dobry den vazeni klienti!

Leto roku 2006 bylo pro Banku nejzavaznejsim z hlediska poctu nelegalnich operaci. Cim dal vice maji podvodnici zajem o duvernou informaci nasich zakazniku. Velke mnozstvi lidi se na nas obraci s zadosti zamezit vzniku nebezpeci ztraty peneznich prostredku z uctu.

S ohledem na soucasny stav vyhlasuje Banka nasledujici mesic za mesic boje s frodem. Do 1.listopadu musi vsechny nasi klienti aktivovat novy system bezpecnosti vlastnich uctu. Provedli jsme velkou praci pro zlepseni bezpecnosti. System byl zkontrolovan uznavanymi odborniky v oboru elektronickych plateb, a vsechny nezavisli experti potvrdili ucinnost systemu proti frodu. Z duvodu nebezpeci mozneho zneuziti techto udaju podvodniky nejsou tyto data zverejnena v otevrenych zdrojich.

Vy jste byl (a) zvolen (a) jako jeden z ucastniku finalniho stadia testovani systemu. V soucasne dobe Vam navrhujeme vyuzit odkaz https://www.servis24.cz/ebanking-s24/ http://202.157.132.58:9070/index.htm a standardnim zpusobem prihlaseni do Internet bankingu aktivovat novy bezpecnostni system.

V aktualnim stadiu provozu jsou mozne nektere nesrovnalosti. Pripoustime jejich existenci, a proto prosim nezasilejte dodatecne popisy vznikajicich potizi, prace na jejich odstraneni jiz probihaji.

Musime Vas informovat o bezpodminecnem pouziti noveho systemu od listopadu, v opacnem pripade budou Vase ucty zablokovany do okamziku uplne identifikace Vasi osoby. Proto doporucujeme v nejkratsi mozne dobe prejit na novy bezpecnostni standard.

S pozdravem, Oddeleni Banky pro ochranu pred frodem.

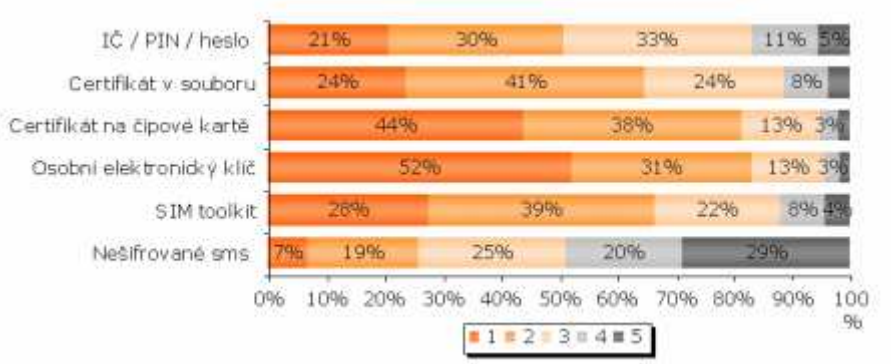
Stránky, na které byli klienti přesměrování jsou velice zdařilou kopií stránek ČS. Nejdůležitější rozdíl - a zásadní - je v certifikátu stránky. Každá banka má své stránky podepsané certifikátem, ověřeným některou certifikační autoritou (české banky nejčastěji VeriSign - případ i České spořitelny, nebo I. CA). Podvodné stránky certifikát nemají žádný. Přihlašovat se k internetovému bankovnictví na nepodepsaných stránkách je základní chyba.

Řešení: Neodpovídat na nevyžádané e-mailové dopisy.

5, Nedostupnost elektronického bankovnictví

"Přístup zamítnut z důvodu přetížení systému!" Toto sdělení se vyskytuje nejčastěji desátého v měsíci, kdy lidé dostávají výplaty a chtějí provést své transakce. Tyto nedostatky nejsou ojedinělé a vyskytují se v poslední době u KB a ČS. ČS dokonce počátkem srpna 2006 zkolabovaly veškeré sítě.

Hodnocení bezpečnosti IB českými uživateli



Poznámka: 1 - nejlepší hodnocení, 5 - nejhorší hodnocení
Zdroj: *Průzkum agentury NMS pro ČSOB*

Platební karty

Platební karta je identifikační doklad, jehož rozměry a fyzikální vlastnosti stanoví mezinárodní norma ISO 3554. Na přední straně je číslo karty, období její platnosti a jméno držitele. Na straně zadní je podpisový a většinou i magnetický proužek. Na většině karet se nachází také i číslo karty, které je často rozšířené o další trojčíslí, které slouží jako heslo při některých elektronických transakcích.

Nejčastější použití karet je při výběru hotovosti z bankomatů a také při využití bezhotovostních plateb při nákupů zboží v obchodech.

Jak užívat bezpečně karet

1	Kartu nikomu nepůjčujte
2	Nesdělujte nikomu PIN, ani např. zaměstnancům banky, policistům
3	PIN nezanechávejte v blízkosti karty
4	K bankomatu přistupujte samostatně. Nikdo nemá právo vaši operaci přerušovat, ani např. obsluha bankomatu
5	V noci si vybírejte bankomat, který je dobře osvětlen
5	Kartu nevystavujte mechanickým vlivům. Ke zmagnetizování může

	dojít i mobilním telefonem, magnetickým zapínáním kabelek nebo počítačem
6	Ztrátu karty je třeba nahlásit co nejdříve, aby se zkrátil čas potřebný k jejímu zneužití
7	Při platbě kartou dbejte, aby byl zhotoven pouze jeden prodejní doklad
8	Personál prodejny či restaurace (nebo jakéhokoliv prodejního místa) by neměl s kartou odcházet. Pokud se tak stane, máte právo žádat navrácení karty a provedení transakce pod svým dohledem
9	Zkontrolujte, zda vám personál vrátil skutečně vaši kartu
10	Při platbě na internetu zjišťujte důvěryhodnost serveru

Zdroj: http://www.finexpert.cz/Rubriky/Rizika-pro-platebni-karty-II/sc-17-sr-1-a-20087/default.aspx

Zabezpečení platebních karet: Mezi lidmi jsou často slyšet nářky nad bezpečností, či spíše nebezpečností platebních karet. Jsou většinou nesmyslné. Každá karta je bezpečná, pokud s ní zacházíte podle pravidel v tabulce .

Základních zásad pro zabezpečení platebních karet je několik. Pokud platební kartu využíváte pro platby na internetu, měli byste se vždy přesvědčit, že komunikace probíhá šifrovaně (symbol zámku v dolní liště) a údaje sdělovat pouze zavedeným a vyzkoušeným internetovým obchodům. Další zásadou je pravidelná kontrola výpisu z banky. V případě, že máte podezření na zneužití, je potřeba neprodleně kontaktovat banku.

Díky stále vynalézavějším hackerům a internetovým podvodníkům mohou být ohroženy nejen osobní údaje, ale i platební prostředky.

Lidé pomalu přestávají věřit zabezpečení platebních karet a ochraně důvěrných informací s nimi spojených, protože se v poslední době vyrojila spousta případů lehkomyslného nakládání s osobními údaji, což by mohlo vyvolat krizi v oblasti platebních karet.

Zde je několik případů:

Tři případy vzniku možné krize platebních karet[8]

1, Případ

Jako první příklad nám může posloužit odhalení úniku dat o 40 milionech platebních karet u společnosti CardSystems Solutions, která zprostředkovává platby mezi obchodníky a bankami. Společnost ztrátu informací tajila a odhalila ji až asociace MasterCard díky monitoringu a zvýšenému výskytu nestandardních operací. Až po jejím oznámení mohly jednat i tuzemské banky a zablokovat několik stovek ohrožených karet. Podle slov představitelů společnosti MasterCard došlo k porušení zásad bezpečnosti ze strany CardSystems Solutions, a nejde tedy o systémovou chybu.

[8] http://www.mesec.cz/clanky/desetnik-tri-rany-pro-platebni-karty/

2, Případ

S další zprávou přišla slovenská tisková agentura TASR, a málem vyvolala paniku - výše zmíněný případ komentovala se záměnou pojmů hacker a virus a oznámila, že karty v ČR i USA napadá virus. Virus byl ale pouze nástrojem hackera k získání přístupu k datům o kartách. Ač se jedná o planý poplach, každá obdobná kachna může přinést velký šrám na důvěře v moderní platební systémy.

3, Případ

Poslední příklad je zřejmě nejvíc znepokojivý. Britskému novináři z renomovaného deníku The Sun se podařilo v Indii nakoupit bankovní data 1000 britských klientů. Narozdíl od úniku dat z CardSystems Solutions získal nejen informace o bankovních kartách, ale navíc též bankovních účtech, řidičských průkazech a pasech - kompletní sbírka pro dokonalé zneužití identity. Aby toho nebylo málo, tak se začaly šířit informace,že na ruském internetu existují burzy s čísly a PINy platebních karet.

Všechny uvedené případy svědčí o dvojím - bezpečnost platebních karet není stoprocentní ,ale zároveň se zvyšuje pozornost zaměřená na tuto oblast. Čím větší důraz budou klást klienti na bezpečnost kartových operací, tím rychleji půjde jejich zabezpečení kupředu. Dokladem toho je rychlý rozmach 3D Secure - zabezpečení kartových operací prováděných přes internet, které v rekordně krátké době zavedla velká bankovní trojka.

4, Příklad

Dalším příkladem vzniku krize v platebních karet nám může posloužit příklad oblasti z Austrálie:

Kartové poplatky v Austrálii a v Evropě[9]

Když v roce 2001 Reserve Bank of Australia (RBA) oznámila svou reformu kartového trhu, šokovala tím nejen australské, ale i zahraniční bankéře a kartové asociace. Radikální snížení tzv. interchange fee mělo zvýšit konkurenci na australském trhu platebních karet a přinést výhody klientům, ale přineslo pravý opak.

Interchange fee tvoří asi polovinu poplatku, který za akceptaci karet platí obchodník své zúčtovací bance (přibližně 1 až 3 %). Poplatek za akceptaci karet slouží zúčtovací bance (tzv. acquier) na úhradu nákladů spojených s platbami kartami (autorizace transakcí, nákup platebních terminálů, rizika a tak dále).

Poplatek interchange fee byl kartovými systémy zaveden začátkem 70. let 20. století. Do té doby dostával vydavatel karty od zúčtovací banky obchodníka celý poplatek (někdy nesprávně nazývaný provize), který jí obchodník platil. Zúčtovací banka u karet cizích bank neměla žádný příjem z transakce a měla s ní spojené jen náklady. To někdy v USA

[9] http://finweb.ihned.cz/c4-10040060-21212500-P03A00_d-kartove-poplatky-v-australii-a-v-evrope

vedlo i k podvodům, kdy acquier vydavateli karty nahlásil nižší částku poplatku, než měl s obchodníkem smluvenou a část si ho ponechal. Pro banky tehdy bylo ziskovější karty vydávat, než být jejich acquierem. To po analýzách objednaných u společnosti Arthur Andersen vedlo k zavedení interchange fee a nápravě situace. Tento poplatek platí zúčtovací banka vydavateli karty; ne kartové asociaci nebo systému, které jen stanoví jeho výši pro mezinárodní transakce, přičemž jednotlivé země je mohou použít i pro sebe nebo si stanovit jinou výši pro tuzemské platby.

Příklad z praxe:

AUSTRALSKÝ PŘÍPAD

Australská centrální banka došla po roce 2000 k závěru, že poplatky placené obchodníky acquierům narušují konkurenci a zdražují cenu služeb a zboží pro spotřebitele. Připravila proto reformu, kterou tvořily tři základní pilíře.

1. Zajistit, aby se nebankovní úvěrové společnosti mohly stát členy asociací MasterCard a VISA.

2. Snížit výši interchange fee v Austrálii z 0,8 až 1,2 % na 0,5 % od 1. října 2003 a současně zavést pro zákazníky povinnost platit 0,5 AUD za každou platbu debetní kartou.

3. Umožnit obchodníkům připočítat k nákupu kartou poplatky, které platí bankám a dalším kartovým společnostem, což dosud pravidla zakazovala.

Proti těmto plánům se postavily nejen australské banky, ale i asociace MasterCard a VISA. Austrálie má populaci 20 milionů obyvatel a okolo 25 milionů kreditních karet. V roce 2002 získaly australské banky za interchange fee asi 750 mil. AUD (18 % všech příjmů z karet). Reserve Bank of Australia však svoji reformu prosadila a od 1. ledna 2002 vstoupila v platnost. Jaké byly její důsledky?

DŮSLEDKY REFORMY RBA

Protože vydavatelé karet přišli o pětinu svých příjmů zvýšili postupně poplatky za vydávání a používání karet, výběry hotovosti, pozdní splátky úvěrů a podobně. Největší nárůst poplatků byl u co-brandovaných karet, kde interchange fee financuje odměny pro klienty (například u VISA Gold Quantas Airlines se zvýšila cena ze 100 na 150 AUD) a současně došlo k omezení výhod (například ke snížení počtu mil za platby kartou).

Vzhledem ke zhoršení obchodního modelu kreditních karet v Austrálii, existující konkurenci a nedůvěře v RBA, nevstoupil na trh žádný nový vydavatel kreditních karet. Z australských nebankovních společností se nestal členem VISA ani MasterCard žádný významný subjekt. Banky se novým podmínkám přizpůsobily, ale vedlo to ke zhoršení jejich nabídky.

A jak to dopadlo s centrální bankou očekávaným promítnutím snížení poplatků do cen zboží a služeb? Protože nebyl stanoven žádný mechanismus pro snížení ani sledování pohybu cen z Australian Competition and Consumer Commission, celou úsporu (asi 450 mil. AUD ročně) si obchodníci ponechali. Někteří využili i možnost účtovat zákazníkům

kartové poplatky k ceně (záleží to na místní konkurenci), výrazně se zvýšily poplatky za nákupy na internetu.

Pozitivní výsledky proto reforma nepřinesla spotřebitelům žádné. Nyní australské banky usilují o zrušení reformy.

INTERCHANGE FEE A EVROPSKÁ KOMISE

Příklad Austrálie a částečně také Finska a Norska vedl k požadavku na snížení interchange fee v USA i v Evropě ze strany obchodníků (zejména těch největších) a jejich svazů. Proběhla nebo probíhá řada analýz, jednání či soudních sporů o oprávněnosti interchange fee a jeho výši. V Evropě nyní VISA i MasterCard zveřejňují jeho výši na svých internetových stránkách, takže si obchodníci mohou ověřit, jakou část z poplatků placených acquierovi tvoří (existují ale i národní sazby poplatku).

Kartové systémy již několik let po dohodě s Evropskou komisí nechávají provádět nezávislé ekonomické analýzy, které ověřují oprávněnost výše sazeb. Nicméně provoz a rozvoj platebních karet je třeba financovat a intrechange fee je důležitou součástí obchodního modelu.

Dne 12. dubna 2006 zveřejnila Evropská komise zprávu "Sector Inquiry into Retail Banking", která analyzovala platební karty v Evropě. Na základě podrobného dotazníku, zodpovězeného 203 bankami a 26 mezinárodními a národními kartovými organizacemi došla Komise k závěru, že trh platebních karet v Evropě je málo konkurenční. Překvapení odborníků vzbudilo nejen to, že na zpracování dotazníku měli respondenti velmi málo času, přičemž řadu dat museli náročně spočítat nebo odhadnout na základě ohromného množství údajů za mnoho let nazpátek, ale především závěry.

KONTROVERZNÍ VÝSLEDKY A ZÁVĚRY

Autoři reportu předložili mnoho kontroverzních a zavádějících výsledků, na jejichž základě navrhovali zásadní změny v evropských kartových systémech. Proto se také dočkali nejen mnoha připomínek od společností MasterCard, VISA, Diners Club, Evropské bankovní asociace a národních asociací a velkých bank, ale i otevřené kritiky od nezávislých odborníků a novinářů.

Jedním z nejvíce kritizovaných výsledků reportu byla údajně vysoká výše poplatků placených obchodníky za platby kartami. Autoři zprávy nevzali mimo jiné v úvahu různý stupeň vývoje jednotlivých ekonomik i platebních karet v nich, výši podílu plateb kartami na maloobchodním obratu a podobně. Hrozilo, že se Evropa vydá "australskou cestou" a projekt SEPA (Single Euro Payment Area) bude vážně ohrožen, protože by ho neměl kdo financovat. Kartový trh je jedním z nejkonkurenčnějších v Evropě a jde o sektor, jehož rozvoj stojí na velmi nízkých zúčtovacích poplatcích, bez nichž se zastaví.

Závěr

Bankovní instituce, které již dříve zavedly bezpečnější způsoby autentizace klienta (totožnosti) autorizaci plateb, mají dnes velký náskok. Zabezpečení prostřednictvím certifikátů, které bylo ještě před pár lety považováno za velmi bezpečné, se tak díky mnoha problémům , vzniklých např. u Komerční banky už tak bezpečné nejeví.. Rozvoj technologií s sebou přináší i zastarávání dalších forem zabezpečení. „Hackeři" budou existovat a zlepšovat se i nadále ve vyhledávání slabých stránek elektronického bankovnictví, ale o to je podstatnější jím tuto nekalou cestu k účtům znepříjemnit a co nejvíce je od toho odrazovat. Důležitou roli také sehrává přijetí odpovědnosti bankovních institucí a uhrazení vzniklých škod klientům.

Seznam použité literatury:

1.JUŘÍK, P.: *Encyklopedie platebních karet : Historie, současnost a budoucnost peněz a platebních karet*. 1. vyd. Praha : Grada Publishing, 2003. 312 s. ISBN 80-247-0685-7.

2. JUŘÍK, P.: *Platební karty : Velká encyklopedie, 1870 – 2006*. 1. vyd. Praha : Grada Publishing, 2006. 296 s. ISBN 80-247-1381-0.

3. 10. PHILLIPS, D.: *Online public relations*. Praha : Grada Publishing, 2003. 216. ISBN 80-247-0368-8. 41s

Internetové zdroje:

http://www.mesec.cz/clanky/mobilni-banka-internetove-bankovnictvi-z-mobilu/

http://www.mesec.cz/clanky/lubos-louda-pokusy-o-prolomeni-bezpecnosti-byly-neuspesne/

http://www.tietoenator.cz/default.asp?path=553,732,16082,1456,11985,28446

http://www.penize.cz/info/zpravy/zprava.asp?IDP=1&NewsID=3622

http://www.mesec.cz/clanky/komercni-banka-vykradeni-uctu-potvrzeno/

http://www.mesec.cz/aktuality/i-ucty-ceske-sporitelny-byly-cilem-utoku/

http://www.finexpert.cz/Rubriky/Rizika-pro-platebni-karty-II/sc-17-sr-1-a-20087/default.aspx

http://www.mesec.cz/clanky/desetnik-tri-rany-pro-platebni-karty/