MASARYKOVA UNIVERZITA
Ekonomicko - správní fakulta

Krizový management elektronického bankovnictví

Rizika elektronického bankovnictví

seminární práce

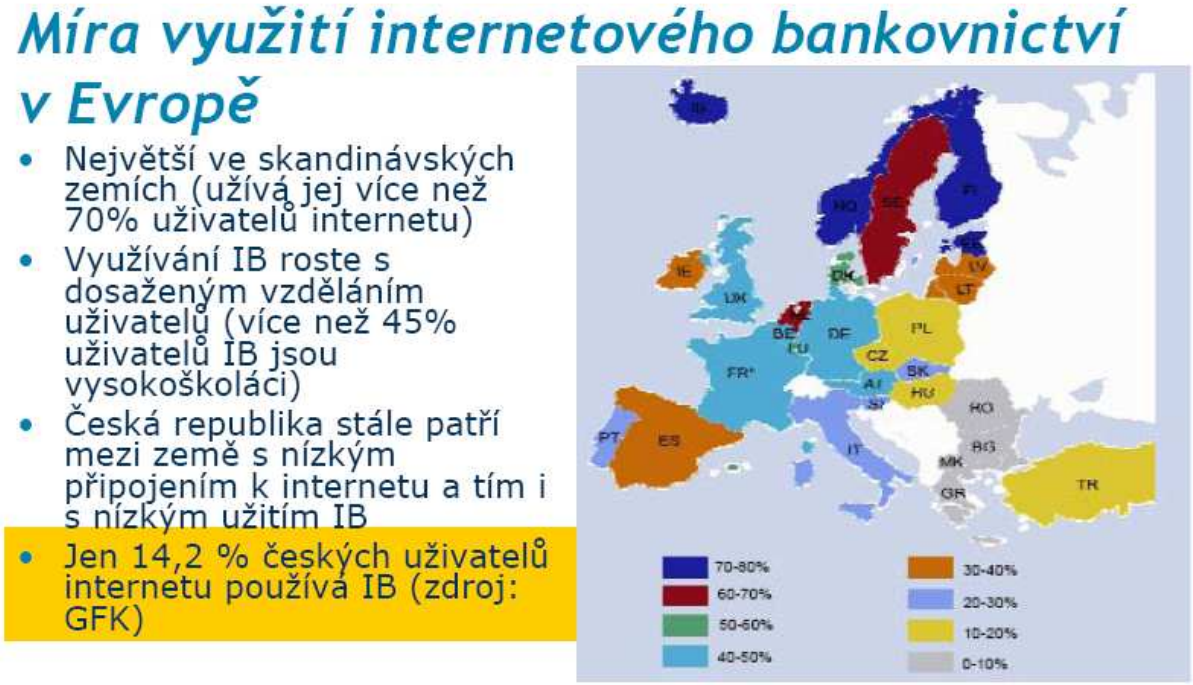
Vypracovali: Tomáš Komínek, 136548
Jiří Rousek, 136870
Seminární skupina: PFKMEB/4
Datum: 19.10.2007

Obsah

Úvod

Zavádění nových komunikačních technologií do bankovnictví má velký přínos jak pro zákazníka, tak i pro banku v roli poskytovatele služeb. Tím se ale také otevírá prostor např. pro neoprávněné přístupy k cizím účtům a další rizikové situace spojené s tímto typem moderního bankovnictví. Tato kapitola je rozdělena do dvou částí tak, že v první se zaměříme na výhody a nevýhody jak z pohledu banky, tak z pohledu klienta. Druhá část je věnována rizikům a otázce bezpečnosti elektronického bankovnictví. Na uváděném obrázku vidíme využití internetového bankovnictví v Evropě.

Obrázek 1:



Zdroj: www.csob.cz/WebCsob/Csob/Servis-pro-media/PB_CSOB_ELB_seminar_bezpecnost.pdf

1. Výhody a nevýhody elektronického bankovnictví

Z pohledu klienta jako zákazníka je jisté, že se stává, prostřednictvím mnoha nabízených způsobů komunikace se svým účtem, jako jsou například mobilní telefony, internet nebo PDA, pánem svého času. Komunikační kanály elektronického bankovnictví může využít kdykoli a kdekoli, 24 hodin denně, 7 dní v týdnu, po celý rok. Už nemusí chodit na pobočku s platebním příkazem, kvůli zjištění stavu na účtu, nemusí vystát dlouhou frontu, případně se stresovat, zda bude jeho podpis shodný s tím na podpisovém vzoru při výběru hotovosti na přepážce. Současně se otevírají zcela nové perspektivy, jako například možnost objednávat a platit služby a zboží právě prostřednictvím internetu.

Zavádění elektronických forem bankovních služeb vyžaduje nemalé náklady na pořízení technologií a zavádění služeb, což lze řadit mezi nevýhody pro banky. Na druhé straně však skýtá velký prostor pro úspory běžných provozních nákladů bankovních ústavů, tak nákladů na transakci na straně zákazníka. Banky tím významně ušetří pracovní sílu a zákazníkům slibují pohodlnější obsluhu, a to prakticky odkudkoli po čtyřiadvacet hodin denně za nižší poplatky.

Proto se vesměs všechny banky na trhu snaží vystrnadit klienty ze svých kamenných poboček a svojí cenovou politikou je motivovat k vyžívání těchto moderních způsobů spravování svého účtu.

1.1. Výhody

Výhodou pro klienta je tedy ušetřený čas (nemusí navštívit banku, nepřetržitý pracovní provoz) a možnost komunikovat s bankou z různých míst. Banka rovněž ušetří, a sice na transakčních nákladech.

1.2. Nevýhody

Mezi nevýhody elektronického bankovnictví z hlediska klienta banky patří především nutnost přístupu k příslušnému elektronickému komunikačnímu kanálu a někdy též vlastnictví speciálního elektronického zařízení. Samozřejmostí také musí být znalost zacházení s tímto komunikačním kanálem, případně zařízením. Pro banku pak nemusí být zřízení a udržování elektronického bankovnictví nikterak levnou záležitostí. Investice do technologií (zvláště ty počáteční) jsou nemalé a ani údržba systému není zadarmo.

Nevýhodou pro klienta je tedy nutnost mít a umět ovládat patřičné technické vybavení. Pro banku jsou nevýhodou v prvních fázích při zavádění patřičných systémů vysoké finanční náklady, problémem je rovněž nutnost jednoznačné identifikace klienta bez osobního kontaktu a vysoké nároky na bezpečnost komunikace. Nevýhodou pro banku je i odtažitost od klienta a horší pozice při získávání informací a nabídkách klientům.

Tabulka 1: Výhody a nevýhody jednotlivých forem elektronického bankovnictví

Typ elektronického bankovnictví	Výhody	Nevýhody
Telefonní bankovnictví		
- telefonní bankéř	- Komunikace s živým člověkem, který v případě nesnází snadno poradí – při získávání informací se tak klient může zeptat na vše co potřebuje a při zadávání trvalého příkazu se nemusí bát, že si nebude moci poradit s některou položkou	- Omezení časové dostupnosti bankéře - v některých bankách je poradce přístupný jen v určitých hodinách
- IVR (Interaktivní hlasová odezva)	- Nepřetržitý provoz – dostupnost 24 hodin denně, 7 dní v týdnu.	- Nutnost telefonu s tónovou volbou - IVR systém není a nikdy vzhledem ke své povaze pro klienta nebude uživatelsky příjemný. - Vůbec se nehodí k nasazení tam, kde komunikace s bankou je poměrně živá a častá.
GSM bankovnictví		

- SMS bankovnictví	- Služba není závislá na tom, kterého mobilního operátora používáte. - Pokud službu banka nabízí, není k jejímu používání nutná speciální SIM karta	- Služba není nijak zabezpečená požadavek se odesílá jako běžná SMS zpráva. - Komponování speciálních SMS zpráv je poněkud těžkopádné.
- GSM SIM Toolkit	- Služba je uživatelsky mnohem příjemnější a navíc lépe zabezpečená. - Bezpečným způsobem Využívání informačních (zjištění zůstatku, transakční historie) i transakčních (zadání platebního příkazu) služeb	- Nutnost mít speciální bankovní SIM kartu a mobilní telefon podporující technologii SIM Toolkit.
WAP bankovnictví	- Přístupnost odkudkoli a kdykoli	- Ve srovnání s ostatními technologiemi je WAP pomalý, nákladný a komplikovaný (nutná také podpora WAP v telefonu)
Homebanking	- Přehlednost – na monitoru si klient může nechat zobrazit právě ta data, která potřebuje, vidí je přehledně uspořádána na obrazovce. - Přístup z pohodlí domova - Možnost propojení homebankingu na účetní software (avšak pouze v případě, že homebanking i účetní software podporují stejný datový formát) - Možnost zadávat hromadné platební příkazy – ostatní způsoby elektronického bankovnictví většinou tuto funkci nenabízejí. - Vysoká úroveň zabezpečení – vytáčí se speciální číslo (data tedy nejdou přes internet), data jsou digitálně podepisována a šifrována (konkrétní způsob se u jednotlivých bank liší). Po několika neautorizovaných pokusech o spojení s bankou dojde k zablokování klienta.	- Omezená přístupnost (pouze z počítače, na kterém je nainstalován příslušný bankovní software) - Poplatky za homebanking patří ve srovnání s ostatními formami přímého bankovnictví spíše k těm vyšším (instalace, aktivace, paušál, výměna klíčů, zaškolení obsluhy atd.) - Časové omezení - některé banky zpracovávají informace (pohyby na účtu apod.) jen v pracovní době
Internetové bankovnictví	- Není nutná instalace speciálních programů	- Na rozdíl od Homebankingu jej nelze propojit s účetním

		softwarem
	- Spojení s bankou je možné z kteréhokoli počítače připojeného k síti internet	- Není tak operativní, jako například GSM Banking (internet není mobilní)
	- Relativně snadná obsluha	
	- Další výhody stejné jako u *HomeBankingu (viz výše)* – přehlednost, hromadné příkazy atd.	

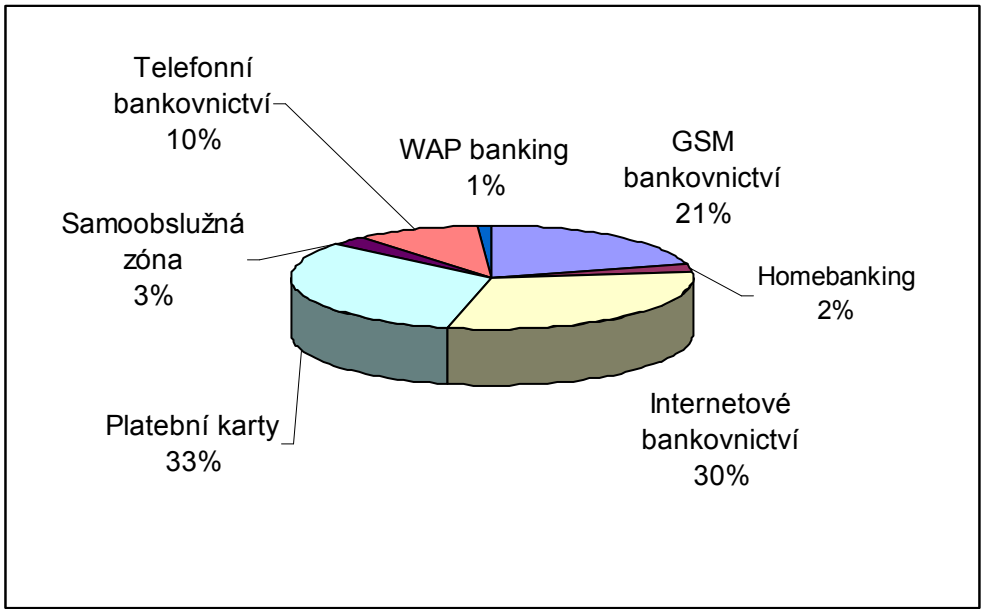
Zdroj: PEKÁRKOVÁ, L. (2006): *Elektronické bankovnictví, jeho možnosti a další vývoj*, bakalářská práce, Masarykova Univerzita, Příloha 1: Výhody a nevýhody jednotlivých forem elektronického bankovnictví

Protože v případě elektronického bankovnictví nemá banka s klientem osobní kontakt, je potřebné nějakým jiným způsobem zjistit a bezpečným způsobem ověřit identitu klienta. Bezpečnosti celkově je třeba věnovat velkou péči, což může být náročné jak finančně, tak na znalosti příslušných pracovníků bank i klientů samotných.

2. Bezpečnost internetového bankovnictví

Bezpečnost elektronického bankovnictví je široké téma. Proto se zaměříme pouze na jedno jeho odvětví, v současnosti nejprogresivnější – internetové bankovnictví.

Graf 1: Využití jednotlivých forem elektronického bankovnictví v ČR



Pramen: převzato z http://www.mobilmania.cz
(průzkum z roku 2004 ve spolupráci se serverem www.mesec.cz[1])

[1] LUTONSKÝ, M.: *Banka v mobilu i jinde: výsledky průzkumu.* Mobilmania.cz [on-line]. 2004. Dostupný na < http://www.mobilmania.cz/Operatori/AR.asp?ARI=106954 > [cit. 2006-05-14]

Otázka bezpečnosti je ožehavá snad u každého nového způsobu elektronického bankovnictví. Pokud se zaměříme na bankovnictví internetové, souvisí jeho bezpečnost velmi úzce s bezpečností samotného internetu. Řešení zabezpečení lze rozdělit na dva základní úkoly. Prvním je zajištění bezpečné datové cesty po sítích internetu mezi systémem internetového bankovnictví na straně banky a komunikačním nástrojem (většinou webovým prohlížečem) na straně klienta. Druhým úkolem je zajistit bezpečnou identifikaci klienta.

Pro zabezpečení komunikace klienta s bankou je k prohlížeči běžně používanému protokolu HTTP[2] ještě potřeba využít nadstavbu SSL[3], protože samotné HTTP umí provést pouze autentizaci uživatele na základě hesla (neumí tedy např. šifrovat data). HTTP kombinovaný s SSL tvoří dohromady protokol HTTPS. Všechny běžné prohlížeče umí tento protokol používat a navíc používají bezpečné 128-bitové symetrické šifrování. Pro případného útočníka sice není podle expertů velký problém získat kompletní komunikaci mezi bankou a klientem, ale obdrží ji v dobře šifrované podobě a není v jeho silách data rozluštit. Úroveň zabezpečení poskytovaná touto technologií je ze strany bank považována za dostatečnou. Navíc za celou dobu existence internetových aplikací všech českých bank nevznikl zatím žádný skandál, který by odkryl nedostatky a díry v zabezpečení těchto internetových bran.

Míra bezpečnosti závisí tedy především na způsobu identifikace klienta. V zásadě existuje 5 bezpečnostních nástrojů vstupní identifikace klienta:

- ***uživatelské jméno a heslo*** - Uživatelské jméno má podobu čísla účtu nebo čísla platební karty. Přístup je pro klienta v obou případech snadný - může být ale stejně snadný i pro neoprávněnou osobu, která získá potřebná čísla a kódy.
- ***PIN kalkulátor*** – Jedná se o přístroj velikosti kalkulačky, který při přihlašování do aplikace internetového bankovnictví nebo při autorizaci transakcí generuje náhodnou kombinaci PIN čísel. Kalkulátor poskytuje vyšší úroveň zabezpečení než bezpečnostní heslo. Klient má navíc možnost nastavit denní limit tak, aby transakce od určité výše musely být autorizovány pomocí kalkulátoru. Přístroj není jinak využitelný.
- ***mobilní telefon*** – Po zadání uživatelského jména a hesla klient obdrží přístupový kód od banky přímo na displej mobilního telefonu. Ochrana tohoto klíče je zajištěna omezenou dobou použitelnosti (zpravidla 30 minut) a platností na jedno přihlášení. Zajištění lze využít u všech tří mobilních operátorů (T-Mobile, O_2 i Vodafone). Výhodou je, že uživatel s sebou nemusí nosit žádný přístroj navíc a ve svém telefonu může využívat i GSM bankovnictví.
- ***čipová karta*** – Autorizace probíhá kontrolou identifikačních údajů na čipové kartě uživatele. Klient tedy musí disponovat čtečkou čipových karet a tak se do jisté míry stírá výhoda internetového bankovnictví, že je dostupné kdekoliv a z každého počítače. V současné době není čtečka standardní výbavou počítačů a širší uplatnění si toto zabezpečení zřejmě najde během několika následujících let.
- ***digitální certifikát –*** Certifikát je množina elektronických dat, která kompletně popisuje danou osobu, vydaná certifikační autoritou teprve po ověření, že daná osoba je skutečně tím, za koho se vydává. Klient od banky obdrží zpravidla 2 certifikáty. SSL certifikát[4] a

[2] Hyper Text Transfer Protocol – protokol pro přenos souborů na internetu

[3] Secure Sockets Layer – protokol pro přenos soukromých dat přes internet vyvinutý firmou Netscape. Používá kryptografický systém založený na dvou klíčích – veřejném, kterým se zpráva pro příjemce zašifruje a soukromém, kterým si zprávu příjemce rozšifruje. Tento způsob šifrování se nazývá symetrický.

[4] SSL certifikát je možné přirovnat k elektronickému průkazu totožnosti. Je uložen v internetovém prohlížeči. Certifikát může získat, rušit a obnovovat pouze uživatel oprávněný používat systém internetového bankovnictví. Správu certifikátů provádí registrační autorita

podpisový certifikát. SSL certifikát je instalován do internetového prohlížeče, a klient může začít využívat online pasivní přístup ke svým účtům. Pokud ale chce využívat služeb internetového bankovnictví z jiného počítače, je třeba certifikát exportovat nejlépe na disketu (export byť na lokální síť se nedoporučuje a export na internet se rovná hazardování s účtem) a importovat do příslušného počítače. Při vstupu do systému aplikace ověří, zda je uživatel majitelem disponibilních práv k ovládání účtu. Při využívání aktivních operací se aplikace dotáže na podpisový certifikát ověřeným navíc heslem klienta a plní tak de facto funkci elektronického podpisu. Certifikáty jsou omezeny platností zpravidla na dobu jednoho roku, poté je nutné z bezpečnostních důvodů vygenerovat nový kód.

Způsoby zabezpečení lze rozdělit i podle jejich úrovně. Např. méně bezpečné způsoby přístupu do systému jsou využívány pouze pro pasivní operace, jako je sdělení zůstatku na účtu a výpis účetních operací. Společným atributem je však využití špičkové úrovně zabezpečení pro aktivní operace, např. zadávání příkazů k úhradě a podobně.

Certifikáty nebo elektronický podpis jsou generovány s platností až jednoho roku, což sice přináší klientům jistý komfort (nemusí se stále starat o častou obnovu certifikátů), ale klade vyšší požadavky na bezpečné uložení a používání těchto klíčů. Pokud uživatel bedlivě opatruje svoje přístupové kódy, hesla a certifikáty, možnost zneužití přístupu k účtu přes internet je mizivá. Ostatně dokládá to i skutečnost, že za celou dobu existence internetového bankovnictví nedošlo k žádnému vážnějšímu incidentu. Mnohem větší riziko spočívá v používání klasických platebních karet, což mimo jiné dosvědčují zprávy o zneužívání a krádežích s databázemi čísel platebních karet.

2.1. Internetové bankovnictví a bezpečnost v České republice

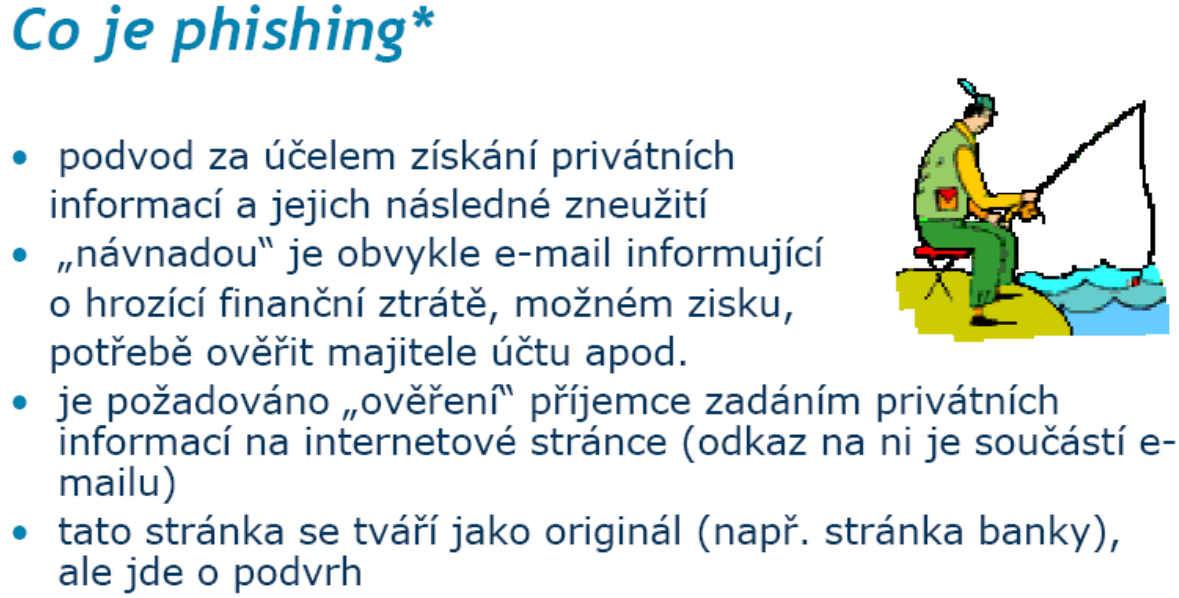
Podle odborníků je v současné době největším limitujícím faktorem bezpečnosti internetbankingu chování klienta. Banky obyčejně nedoporučují používat k přihlášení na svůj účet počítače, o nichž klient nic neví – typicky v internetových kavárnách.

"Neznámý počítač" je pro klienta potenciálně nebezpečný, neboť může bez jeho vědomí "zcizit" certifikát / soukromý klíč (uložený společně v souboru) a heslo, příp. uživatelské jméno a heslo. Dalším nebezpečím je tzv. phishing, kdy jsou klienti prostřednictvím e-mailové zprávy vyzváni k vyplnění a odeslání citlivých údajů[5]. Záměrem těchto zpráv jé získání osobních a nebo finančních informací o klientovi, které se dají většinou jednoduše zneužít. Naštěstí ale o tomto riziku ví čím dál více klientů a i banky na tento jev upozorňují na svých stránkách. Sofistikovanější metodou získání osobních údajů je pharming[6]. Tento způsob se prozatím ale objevuje pouze u klientů amerických a velkých evropských bank.

[5] Klient dostane mail, který působí dojmem, že jej zaslala jeho banka, s žádostí o vyplnění citlivých údajů na stránce uvedené v odkazu. Stránky, na které je přesměrován, však samozřejmě nepatří bance, a klient tak útočníkovi svěří svá data. Ta pak bývají obratem zneužita pro přístup na jeho účet

[6] Typická oběť pharmingu má na svém počítači trojského koně, příp. červa, který pokusy o přístup na internetové stránky banky přesměrují klienta na podvodné stránky, které jsou téměř dokonalou kopií originálních stránek banky. Zde se klient chová jako na stránkách banky, kde se cítí bezpečně, a zadává své údaje bez obav. Útočník se tak lehce dostane k údajům internetového bankovnictví, číslu karty apod.

Obrázek 2: Phishing



Zdroj: www.csob.cz/WebCsob/Csob/Servis-pro-media/PB_CSOB_ELB_seminar_bezpecnost.pdf

Úrovní zabezpečení se mohou banky zásadně lišit. U dvou (Česká spořitelna a Citibank) stačí k přihlášení do služby internetbanking přihlašovací jméno (číslo) a heslo. Tento způsob je sice pohodlný, nicméně z uvedených způsobů nejméně bezpečný[7]. Česká spořitelna umožňuje těm klientům, kterým tento způsob zabezpečení nestačí, možnost používat PIN kalkulátor, tedy zařízení, které po zadání PINu (případně údajů vztahujících se k transakci) vygeneruje jedinečný kód pro danou transakci. Jeho vydání stojí 300 korun.

Další banky standardně používají k zabezpečení certifikáty či specifické předměty (PIN kalkulátory, mobilní telefony). ČSOB a Raiffeisenbank tak činí pouze pro aktivní transakce. V ČSOB se klient přihlásí do internetbankingu pomocí identifikačního čísla a PINu, aktivní operace jsou pak zabezpečeny pomocí „SMS klíče" – klient si nechá zaslat na svůj mobilní telefon kód, který je vygenerován právě pro tuto transakci. Jeho zadáním poté operaci potvrzuje. Zpráva ovšem není chráněna bankovním PINem (tzv. BPIN využívaný bankovními aplikacemi, viz níže). Klientům s vyššími požadavky na bezpečnost nabízí banka bezpečnostní certifikát uložený společně se soukromým klíčem na čipové kartě (viz níže). U Raiffeisenbank stačí klientům pro pasivní transakce rovněž pouze přihlašovací jméno a heslo. Pro provedení aktivních operací ovšem již potřebují certifikát. Po zadání hesla, které si při jeho generování zvolili, je transakce provedena. Mezi operace, které lze provést bez použití certifikátu, však patří například i změna hesla.

Tři banky zabezpečily pomocí certifikátu přístup na účet i potvrzování aktivních operací – Komerční banka, GE Capital Bank a Živnostenská banka. U Komerční banky si klient vygeneruje jeden certifikát, který použije pro přihlášení i potvrzení transakce. U GE Capital

[7] Existují dokonce volně prodejné miniaturní sondy, které dokáží „odposlouchávat" klávesnici, jsou velmi nenápadné a nevyžadují žádný zásah do programového vybavení počítače – potenciální útočník pak při použití tohoto zařízení zná všechny údaje, které potřebuje.

Bank a Živnostenské banky je třeba vygenerovat certifikáty dva – SSL certifikát a podpisový certifikát. SSL certifikát je třeba importovat do prohlížeče (slouží k přihlášení), podpisový je poté zapotřebí pro autorizaci transakcí. Živnobanka chystá pro své klienty možnost ukládat certifikáty na zařízení USB token[8].

Klientům vyžadujícím vyšší zabezpečení nabízí Komerční banka a ČSOB bezpečnostní certifikát na čipové kartě. Nejde ovšem o zcela standardní a jednoduchou věc – čtečka čipových karet není obvyklou součástí vybavení počítače a také její cena není zrovna nízká[9].

Klienti HVB Bank používají pro přístup ke službám internetového bankovnictví i jejich provádění vždy PIN kalkulátor. Jednorázový poplatek za jeho získání a inicializaci elektronického bezpečnostního klíče činí 490 korun.

eBanka nabízí svým klientům tři druhy zabezpečení – mobilním, internetovým či osobním elektronickým klíčem. Nejběžnějším je mobilní – na mobilní telefon je klientovi po identifikaci klientským číslem zaslán autentizační kód[10]. Pro potvrzení údajů k případné aktivní operaci je pak stejným kanálem zaslán ještě certifikační kód. Osobní elektronický klíč (OEK) není nic jiného než PIN kalkulátor – stojí ovšem klienta 89 Kč/měsíc. Internetový elektronický klíč (IEK) je založený na standardních certifikátech. Jádro klíče představuje soubor, ve kterém je bezpečně uložen certifikát a soukromý klíč. Tento soubor si klient vygeneruje a nainstaluje na svůj počítač a využívá jej k přístupu k účtu nebo zadávání aktivních operací. Vlastní přístup k IEK je chráněn heslem, které si uživatel sám zvolí.

Obrázek 3: Způsoby autentizace při internetbankingu v jednotlivých bankách

	Uživ. jméno a heslo	Certifikát	Čipová karta	SMS kód	PIN kalkulátor
BAWAG Bank	ano				
Citibank	ano				
Česká spořitelna	ano		ano		ano
ČSOB	ano		ano		
eBanka		ano		ano	ano
GE Money Bank	ano	ano			
HVB Bank					ano
Komerční banka		ano	ano		
Poštovní spořitelna	ano				
Raiffeisenbank	ano				
Volksbank	ano				
WSPK	ano				
Živnostenská banka	ano	ano			

[8] USB token je zařízení, které slouží k ukládání a správě důvěrných dat jako jsou digitální certifikáty a páry privátních a veřejných klíčů v chráněných úložištích. Je u nich zajištěno, že privátní klíč neopouští dané zařízení a nemůže být zneužit. Vzhledem k použité technologii poskytuje velmi bezpečné úložiště certifikátů.

[9] V ČSOB ji lze získat v rámci balíčku Aktivní konto, za něž klient zaplatí 170 korun za měsíc (součástí je dále kromě běžného účtu kreditní a debetní (embosovaná) karta, kontokorent, tři kanály přímého bankovnictví, 10 elektronických operací měsíčně a několik SMS zpráv o stavu účtu zdarma). Jinak stojí vydání čipové karty s bezpečnostním certifikátem 100 Kč, vydání čtečky čipových karet potom dle druhu 500 až 1950 korun). Komerční banka zpoplatňuje vydání čipové karty 390 korunami

[10] K jeho přečtení je nutno zadat BPIN, speciální osobní identifikační číslo, které chrání přístup k mobilnímu elektronickému klíči (MEK); k využívání MEK je nutné mít SIM kartu s bankovní aplikací

Pramen: studie ze serveru Měšec.cz[11]

Jak již bylo řečeno, mají tyto různé způsoby zabezpečení své výhody i nevýhody. U první metody (přihlašovací jméno a heslo) již byly zmíněny. U certifikátu je nevýhodou nepohodlí spojené s generováním certifikátu a nutností nosit certifikát včetně soukromého klíče s sebou. Navíc v internetové kavárně hrozí zneužití certifikátu (resp. soukromého klíče), což se týká i případů, kdy klient v tomto prostředí používá čipovou kartu. U některých bank je navíc jeden z certifikátů nutno importovat do prohlížeče a poté mazat. Z tohoto hlediska jsou ostatní způsoby zabezpečení bezpečnější a pohodlnější. Nejpohodlnější je pak mobilní telefon, neboť ten má jeho uživatel u sebe stále a nemusí přenášet nic navíc.

Samozřejmostí internetbankingu je šifrovaná komunikace mezi bankou a klientem. Dalšími bezpečnostními opatřeními mohou být tyto prvky: automatické odhlášení při nečinnosti, limity operací, zablokování při několika špatných zadáních hesla či možnost zasílání informačních zpráv. Banky navíc radí "fixní" hesla často měnit. Jednorázová hesla (generovaná PIN kalkulátory či rozesílaná pomocí mobilu) mívají potom omezenou platnost (obyčejně v řádech minut).

Některé banky ovšem mohou ale překvapit při používání internetového bankovnictví negativně. Pokud se totiž klient z účtu neodhlásí a přejde rovnou na jiné stránky, dostane se tlačítkem „Zpět“ zpátky na svůj účet. U Komerční banky a ČSOB alespoň nemůže případný útočník bez dalších prvků provádět aktivní operace, u České spořitelny by ale klienti měli dát pozor – pokud nepoužívají autentizační kalkulátor, mohli by o své peníze snadno přijít.[12]

3. Rizika elektronického bankovnictví z pohledu banky

V bance probíhá řada procesů, v nichž banka vstupuje do rizika. Toto riziko v mnoha případech není možné či není efektivní zcela eliminovat (neboť by toto opatření vedlo k podstatnému snížení výnosů banky), je tedy nutné je řídit.[13] Bankovní rizika se dělí na:

- externí: politická, měnová, kursová, úroková; tedy ta, která nejsou ovlivněna druhem použitého komunikačního kanálu.
- interní: podvody, technická a technologická rizika; tedy ta, která přímo souvisejí s činností banky a použitý komunikační kanál je přímo ovlivňuje.

Rizika lze charakterizovat vedle pravděpodobnosti výskytu bezpečnostního incidentu i velikostí potenciálně způsobené škody.

Inovace v oblasti technologií a zvyšující se konkurence mezi bankami přinesla rozšíření nabídky bankovních služeb. Imperativem doby se stává poskytování služeb prostřednictvím elektronických distribučních kanálů jak podnikové, tak i retailové klientele. S rychlým rozvojem elektronického bankovnictví jsou však spojená i určitá rizika.

---

[11] ZÁMEČNÍK, P., KRČMÁŘ, P.: *Analýza zabezpečení internetového bankovnictví v České republice.* Měšec.cz[on-line],2005.Dostupný na adrese < http://i.iinfo.cz/urs-att/Mesec.cz-studie_int.bankovnictvi-112002647608700.pdf> [cit. 2006-05-14]

[12] ŽALOUDNÍKOVÁ, V.: *Bezpečnost internetového bankovnictví: skutečnost, nebo mýtus?* iDnes.cz [on-line]. 2004. Dostupný na adrese <http://fincentrum.idnes.cz/fi_blind.asp?r=fi_blind&c=A040618_130902_fi_blind_vra> [cit. 2006-05-14]

[13] PETRJÁNOŠOVÁ, B., PEČÍNKOVÁ, M.: Bankovnictví I, 1. vyd. Brno: ESF MU, 1998, 178 s. ISBN 80-210-1357-5.

Pro zajištění bezpečných služeb elektronického bankovnictví je důležité, aby každý článek v řetězci poskytovatelů elektronického bankovnictví tato rizika identifikoval a přijal adekvátní opatření vedoucí k jejich eliminaci, resp. ke snížení možných následků. Zjednodušeně lze rizika pojící se s oblastí elektronického bankovnictví rozdělit na obecná, která se vyskytují i v oblasti klasického bankovnictví, a na rizika pro elektronické bankovnictví specifická. Specifická rizika jsou představována jednak novými druhy rizik a jednak zvýšenou mírou rizik existujících v klasickém bankovnictví. Pro vedoucí pracovníky bank tak vyplývá nový úkol zajistit revizi stávajících postupů řízení rizik v oblasti poskytování bankovních služeb a tyto postupy eventuálně upravit a přizpůsobit novým podmínkám.

Charakteristické vlastnosti elektronického bankovnictví přinášejí následující skupiny rizik. Rychlost změny vyvolaná inovacemi v technologiích i potřebou rozšířené nabídky služeb poskytovaných klientům je mnohem větší než u klasických bankovních produktů. Systémy podporující produkty klasického bankovnictví byly tradičně implementovány v průběhu relativně dlouhého implementačního cyklu po důkladných detailních testech. Naproti tomu v případě elektronického bankovnictví jsou banky mnohdy tlačeny konkurenčním bojem k co nejrychlejší implementaci nových řešení - často v době čítající pouze několik měsíců od okamžiku zrodu konceptu řešení do okamžiku jeho masivního nasazení. Tato skutečnost klade mimořádné nároky na kvalitu strategického zhodnocení záměru a provedení analýzy rizik a kvalitu bezpečnostních posudků před samotným zahájením implementace nové služby.

Transakční webové aplikace jsou úzce svázány s tradičními bankovními systémy tak, aby bylo umožněno tzv. straight-through processing[14] (STP) elektronických transakcí. Automatizované STP na jedné straně eliminuje možnost vzniku chyby způsobené lidským faktorem, na druhé straně dramaticky zvyšuje závislost na bezchybně navržené systémové architektuře a provozní spolehlivosti jednotlivých částí komplexních informačních systémů.

Elektronické bankovnictví zvyšuje závislost banky na informačních technologiích, a tím i komplexnost technických a bezpečnostních aspektů řešení, komplexnost partnerských vztahů, aliancí, dodavatelských vztahů, outsourcingu a jiných vztahů banky se třetími stranami.

Internet má globální povahu. Jde o otevřenou síť přístupnou téměř odevšud anonymními uživateli, s posíláním zpráv přes neznámá místa, někdy i přes bezdrátová pojítka. Tento fakt zvyšuje potřebu důrazu kladeného na bezpečnostní opatření, techniky autentizace uživatele a ochrany dat, standardy ochrany osobních údajů a procedury sběru a vyhodnocování auditních záznamů.

Mezi nezbytná bezpečnostní opatření patří:

- autentizace klientů přistupujících prostřednictvím elektronického bankovnictví do informačního systému banky. Toto opatření pravděpodobně nepotřebuje bližší vysvětlení. Jde o jednoznačné a bezpečné určení identity klienta přistupujícího prostřednictvím elektronického distribučního kanálu a stanovení jeho oprávnění.
- zajištění nezpochybnitelnosti autorství a zajištění odpovědnosti v případě transakcí elektronického bankovnictví s cílem dosažení právní odpovědnosti.
- zajištění vhodného oddělení povinností s cílem zamezit přílišnému nebo nevhodnému kumulování oprávnění jednotlivých zaměstnanců.

[14] V současné době přistupují mnohé zahraniční i české banky k provádění zahraničních plateb systémem Straight Through Processing (STP), tj. plně automatickému zpracování došlých plateb bez ručních oprav. Pokud platební příkaz obsahuje správné údaje, je systémem banky příjemce zpracován automaticky.

- systémy elektronického bankovnictví musejí mít implementovány vhodné a dostatečné mechanismy pro kontrolu autorizačního procesu a procesu přidělování přístupových práv.
- zajištění integrity transakcí elektronického bankovnictví, záznamů a informací. Je potřeba si uvědomit, že STP v mnoha případech znesnadňuje proces detekce a nápravy programátorských chyb a podvodného jednání. Je proto důležité věnovat dostatečnou pozornost zabezpečení a monitorování systémů, které pracují na bázi STP.
- vytváření jednoznačných auditních záznamů o každé jednotlivé transakci a jejich vyhodnocování.
- důvěrnost klíčových informací. Toto opatření je potřeba zajistit jak při zpracování dat v bance, tak zejména při zpracování dat třetími stranami.[15]

[15] FIALKA, M.:*Řízení rizik v elektronickém bankovnictví* KPMG [on-line]. 2001. Dostupný na adrese <http://www.kpmg.cz/index.thtml/cz/library/press/2001/index.html?cid=52616e646f6d4956712ac5e9699aea1af96eacbd3076926a> [cit. 2006-05-14]

Závěr

Co mají dělat lidé, kteří používají přímé bankovnictví a chtějí riziko vykradení účtu minimalizovat? Základem je vybrat banku, která nabízí vysoký stupeň zabezpečení přenášených dat. Existuje několik úrovní ochrany. K nejlépe hodnoceným finančním ústavům patří ty, které jsou zabezpečeny prostřednictvím elektronického klíče a elektronického podpisu. Na opačném konci pomyslného žebříčku stojí systémy, do kterých se uživatel hlásí jen pomocí zvoleného hesla. I tak se jedná o velice problematické téma, nejen vzhledem k možnostem dnešní doby, ale i k vývoji technologií, počítačových sítí a internetu. Je tedy nezbytně nutné, aby každý účastník internetového bankovnictví řádně promyslel možné dopady těchto systémů a své jednotlivé kroky v nich.

Seznam použité literatury

PEKÁRKOVÁ, L. (2006): *Elektronické bankovnictví, jeho možnosti a další vývoj*, bakalářská práce, Masarykova Univerzita

PETRŽELOVÁ, J. (2005): *Bezpečnost v elektronickém bankovnictví v ČR*, diplomová práce, Masarykova Univerzita

ROSECKÝ, M. (2005): *Bezpečnosť elektronického bankovníctva*, diplomová práce, Masarykova Univerzita

PETR, A. (2005): *Možnosti elektronického bankovnictví pro e-commerce*, diplomová práce, Masarykova Univerzita

PETRJÁNOŠOVÁ, B., PEČÍNKOVÁ, M.: *Bankovnictví I*, 1. vyd. Brno: ESF MU, 1998, 178 s. ISBN 80-210-1357-5

FIALKA, M.:*Řízení rizik v elektronickém bankovnictví* KPMG [on-line]. 2001. Dostupný na <http://www.kpmg.cz/index.thtml/cz/library/press/2001/index.html?cid=52616e646f6d4956712ac5e9699aea1af96eacbd3076926a> [cit. 2006-05-14]

LUTONSKÝ, M.: *Banka v mobilu i jinde: výsledky průzkumu.* Mobilmania.cz [on-line]. 2004. Dostupný na < http://www.mobilmania.cz/Operatori/AR.asp?ARI=106954 > [cit. 2006-05-14]

ZÁMEČNÍK, P., KRČMÁŘ, P.: *Analýza zabezpečení internetového bankovnictví v České republice* Měšec.cz [on-line], 2005. Dostupný na adrese < http://i.iinfo.cz/urs-att/Mesec.cz-studie_int.bankovnictvi-112002647608700.pdf> [cit. 2006-05-14]

ŽALOUDNÍKOVÁ, V.: *Bezpečnost internetového bankovnictví: skutečnost, nebo mýtus?* iDnes.cz [on-line]. 2004. Dostupný na adrese <http://fincentrum.idnes.cz/fi_blind.asp?r=fi_blind&c=A040618_130902_fi_blind_vra> [cit. 2006-05-14]

INTERNETOVÉ ZDROJE:
server banky Komerční banka: http://www.kb.cz
server banky ČSOB: http://www.csob.cz
server banky Citibank: http://www.citibank.cz
server banky eBanka: http://www.ebanka.cz
server banky Živnobanka: http://www.zivnobanka.cz