Vysoká škola ekonomická v Praze

Fakulta managementu v Jindřichově Hradci

Bakalářská práce

Pavlína Vápeníková

2007

Vysoká škola ekonomická v Praze

Fakulta managementu v Jindřichově Hradci

Historie, současnost a budoucnost elektronického bankovnictví

Vypracovala:

Pavlína Vápeníková

Vedoucí bakalářské práce:

Ing. Pavel Pokorný

J.Hradec, prosinec 2007

VŠE

FAKULTA MANAGEMENTU

Vysoká škola ekonomická v Praze
Jarošovská 1117/II, 377 01 Jindřichův Hradec

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

pro akademický rok 2006/2007

Název práce:	**Historie, současnost a budoucnost elektronického bankovnictví**
Zadání práce:	Práce shrne historii a zanalyzuje současný stav a možnosti elektronického bankovnictví. Bude charakterizovat systém elektronického bankovnictví z hlediska používaného hardware a stavu zabezpečení včetně rizik z hlediska nákladu ze strany klienta a banky. Dále konkrétně popíše služby elektronického bankovnictví v některých našich peněžních ústavech a vazbu na některé účetní programy. V závěru se nastíní další možný vývoj elektronického bankovnictví.
Jméno studenta:	Pavlína Vápeníková
Ročník:	2.
Obor:	MANAGEMENT
Vedoucí práce:	Ing. Pavel Pokorný
Katedra:	Katedra managementu informací
Termín zadání:	23.6.2006
Termín odevzdání:	Dle vyhlášky o průběhu státních závěrečných zkoušek v ak. roce 2006/2007

V Jindřichově Hradci 23.6.2006

Ing. Vladimír Přibyl
proděkan pro pedagogickou činnost

Prohlášení

Prohlašuji, že bakalářskou práci na téma

»Historie, současnost a budoucnost elektronického bankovnictví«

jsem vypracovala samostatně.

Použitou literaturu a podkladové materiály

uvádím v přiloženém seznamu literatury.

J.Hradec, prosinec 2007

podpis studenta

Anotace

Historie, současnost a budoucnost elektronického bankovnictví

Práce shrnuje historii a analyzuje současný stav a možnosti elektronického bankovnictví. Charakterizuje systém elektronického bankovnictví z hlediska používaného hardware a stavu zabezpečení včetně rizik a z hlediska nákladů ze strany klienta a banky. Dále konkrétně popisuje služby elektronického bankovnictví v některých našich peněžních ústavech a vazbu na některé účetní programy. V závěru je nastíněn další možný vývoj přímého bankovnictví.

prosinec 2007

Poděkování

Děkuji všem, kteří mi při tvorbě této práce pomáhali a konzultovali, zvláště pak vedoucímu práce panu **Ing. Pavlu Pokornému** za jeho cenné rady a připomínky.

Obsah:

Úvod

Nezbytnou podmínkou komerčního úspěchu firmy je včasné zavedení a také praktické využití nových moderních technologií. Přesvědčila jsem se o tom během svého několikaletého působení v ČSOB, kde jsem viděla, jaké prostředky a úsilí jsou bankou v tomto směru vynakládány.

Za typický příklad využití moderních technologií v praxi může být považováno elektronické bankovnictví. Jeho vývoj a rozšíření jde ruku v ruce s technologickým pokrokem, který se projevuje ve stále se zlepšujících parametrech počítačů, mobilních telefonů a nabídkou společností, které zajišťují přístup k internetu. Tento pokrok vede také k neustálému snižování cen, což ve svém důsledku umožňuje masové šíření těchto technologií a na nich založených služeb. To je důvodem, proč se elektronické bankovnictví tak dynamicky rozvijí, a proč jsem si toto téma vybrala.

V této práci nastíním důvody vzniku elektronického bankovnictví, shrnu jeho historii a popíši současný stav včetně technologických zařízení, které jednotlivé kanály elektronického bankovnictví využívají. Stručně zmíním služby přímého bankovnictví, které v současné době nabízí GE Money Bank a ČSOB a také některé účetní systémy, které podporují datové formáty pro komunikaci s bankami.

Velkou pozornost budu věnovat problematice bezpečnosti. Detailně popíši rizika spojená s využitím jednotlivých kanálů elektronického bankovnictví a způsoby zabezpečení těchto kanálů (včetně porovnání některých bezpečnostních aspektů mezi jednotlivými bankami). Domnívám se, že další vývoj a šíření těchto služeb nebude bez zajištění bezpečnosti možný.

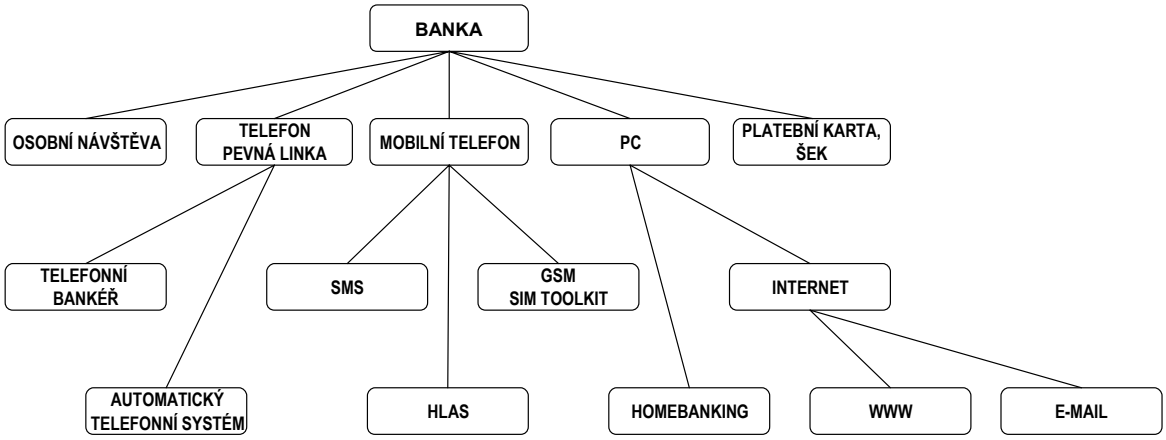
Ovšem jenom bezpečnost nestačí. Aby banky uspěly v ostrém konkurenčním boji, musí potencionálního klienta zaujmout kvalitou svých služeb a také jejich příznivou cenou. Proto uvedu konkrétní nabídku produktů EB vybraných bank působících na našem trhu s porovnáním ceny těchto produktů.

V rámci hodnocení současného stavu EB provedu SWOT analýzu nejvíce využívaného kanálu, a to internetového bankovnictví. Popíši silné a slabé stránky, příležitosti a hrozby pro tuto službu. Provedu zhodnocení jednotlivých rizik a na základě toho formuluji předpoklady pro jeho další úspěšný vývoj.

V hranatých závorkách u názvů odstavců je vždy uveden odkaz na literaturu (seznam literatury je uveden na konci této práce), která byla při zpracování dané kapitoly použita.

1 Historie elektronického bankovnictví

Pod pojmem elektronické bankovnictví si můžeme představit způsob komunikace mezi bankovním informačním systémem a jejím klientem, který je založen na elektronické formě. Tato forma je podmíněna stupněm vývoje a rozšíření informačních technologií. Dostatečný rozvoj informačních technologií a jejich přístupnost v každodenním životě vlastně umožnily vznik elektronického bankovnictví. Tak jak se postupně informační technologie vyvíjejí a rozšiřují, rozšiřuje se i množství a kvalita informačních kanálů mezi bankou a jejími klienty. Na obrázku 1 [2] jsou zobrazeny jednotlivé používané kanály komunikace klienta s bankou.



Obrázek 1: Možnosti komunikace klienta s bankou

1.1 Důvody vzniku elektronického bankovnictví

Tyto důvody můžeme nalézt jak na straně klienta, tak na straně banky. Klasické banky byly nuceny zavést elektronické bankovnictví pod tlakem konkurenčních firem, které nabízejí finanční produkty při využití moderní technologie. Jedná se například o co-branded karty, které spojují platební funkci bankovní karty s věrnostní kartou partnera z nebankovního sektoru. Tato karta slouží jako klasická kreditní či debetní karta dané banky, a zároveň umožňuje svému držiteli získat slevu u partnerské společnosti (např. BAWAG Bank nebo Raiffeisenbank nabízejí věrnostní platební karty Sphere[1], které umožňují klientovi využívat všech výhod, jež poskytují obchodní partneři banky, např. Kenvelo, Barum, Avis, Arcada , Orea Hotels aj. Celkem se jedná přibližně o 5000 obchodních míst v České i Slovenské republice, přičemž nabízené obchodní slevy se pohybují v rozpětí 5 - 50 %.).

[1] http://www.sphere.cz/?sec=2&what=3&lang=cz

Dalším důvodem byly úspory na investicích do budování a udržování pobočkové sítě a také na výdajích spojených se zaměstnanci. Ve srovnání s klasickou pobočkovou obsluhou snižuje elektronické bankovnictví náklady na přímou distribuci bankovních produktů. Tabulka 1 (zdroj[2]) ukazuje srovnání nákladů banky na jednu transakci přes různé kanály. Tato tabulka byla sestavena pro banky v USA v roce 1997. Zde je třeba poznamenat, že elektronické bankovnictví vyžaduje poměrně značné počáteční náklady, takže úspora finančních prostředků se jeví spíše v dlouhodobém horizontu.

Kompletní služby na pobočce	$1.07
Průměr po telefonu	$0.54
Kompletní služby prostřednictvím bankomatu	$0.27
Bankovní operace přes osobní počítač (třetí strana)	$0.015
Internetbanking	$0.010

Tabulka 1: Srovnání nákladů banky

Pro klienty bank znamená zavedení elektronického bankovnictví možnost využití nových bankovních produktů, které jsou pro ně atraktivní. Klient může komunikovat s bankou rychle a komfortně a bez omezení úřední doby. Nemusí absolvovat cestu do banky a z banky, nemusí stát frontu u přepážky a může místo toho lépe využívat svůj čas. To jsou důvody, proč klientela začíná vyžadovat zavedení elektronického bankovnictví, a tedy další pádný důvod pro banky tuto službu zavádět a dále rozšiřovat.

1.2 Vývoj informačních kanálů mezi klientem a bankou

Z hlediska použité technologie existují tři základní typy informačních kanálů mezi klientem a bankou :

- platební karty
- telefonní bankovnictví
- homebanking a internetbanking

1.2.1 Platební karty [1]

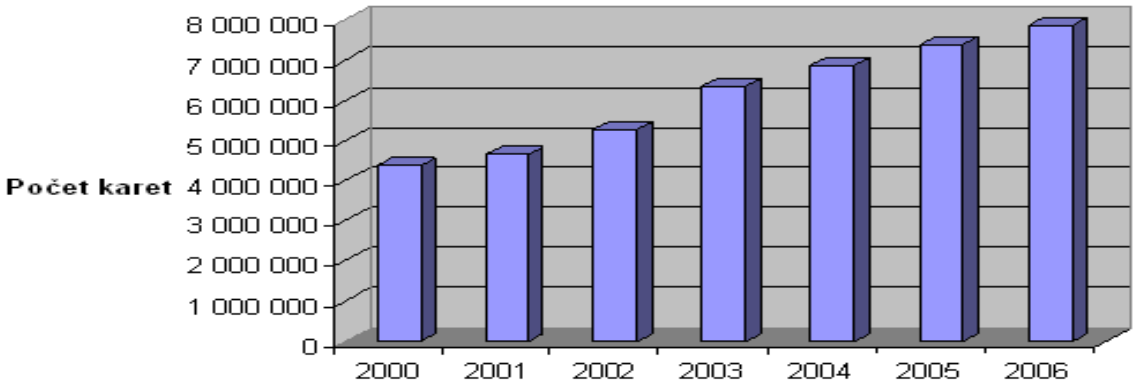
Podle obecně přijímané definice je platební karta identifikačním dokladem, jejíž rozměry a fyzikální vlastnosti stanoví mezinárodní norma ISO 3554. Platební karta umožňuje svému

[2] http://www.park.cz/uvod_do_elektronickeho_bankovnictvi

držiteli (majitelem je vždy banka, která ji vydala) provádět bezhotovostní platby a výběry v hotovosti – v bankomatech, na pobočkách bank, nebo v obchodech.

Historie platebních karet je podrobně popsána např. v [1]. V České republice (resp. v Československu) byly platební karty oficiálně akceptovány od roku 1965. Touto akceptací byl pověřen Čedok. První transakce byla provedena o 3 roky později, v roce 1968.

První platební karta, která byla vydána na našem území, byla dispoziční karta k tuzexovému účtu. Vydala ji Živnobanka v roce 1988. Stejná banka vydala v roce 1991 první VISA kartu u nás. Ve stejném roce vzniklo Mezibankovní sdružení pro platební karty (mezi zakladatele patřily ČSOB, Komerční banka, Investiční banka, Agrobanka a dvě slovenské banky). Tyto banky se staly vydavateli produktů společnosti EuroCard/MasterCard. V současné době jsou platební karty nejrozšířenějším produktem, jenž umožňuje vzdálený přístup k účtu elektronickou cestou. Na obrázku 2 (zdroj[3]) je vidět vývoj počtu platebních karet (součet kreditních, debetních i charge karet) v ČR od roku 2000.



Obrázek 2: Vývoj počtu platebních karet v ČR

1.2.2 Telefonní a GSM bankovnictví [3]

Za počátek této formy bankovnictví je považován rok 1989, kdy došlo ke vzniku First Direct Bank v Leedsu [22]. Tato banka obsluhovala klienty pouze na „dálku“ prostřednictvím telefonu. Příchod digitálních telefonních ústředen a telefonních přístrojů s tónovou volbou umožnil nasazení automatického telefonního systému. Další rozšíření elektronické

[3] http://www.bankovnikarty.cz

komunikace umožnil nástup mobilních telefonů digitálního standardu GSM. To umožnilo komunikovat jednak prostřednictvím SMS – tato komunikace však není uživatelsky příjemná, a proto došlo k vývoji tzv. GSM SIM Toolkit, což je softwarové rozhraní, které umožňuje libovolně obměňovat menu mobilního telefonu. Velkou zásluhu na rozvoji GSM u ČR má GE Capital Bank a její rozsáhlá reklamní akce „Mobil zdarma“ (při založení účtu dostal zákazník mobilní telefon a SIM kartu s instalovaným rozhraním Sim Toolkit zdarma). V současné době je GE Money Bank banka s největším počtem klientů, kteří mají službu GSM bankovnictví aktivovanou, a také ji aktivně využívají.

V roce 2000 zprovoznila eBanka další informační kanál založený na WAP (Wireless Aplication Protokol), což je technologie, která umožňuje přístup k internetu pomocí různých bezdrátových zařízení jako jsou mobilní telefony, osobní digitální organizéry (PDA), pagery nebo palubní počítače automobilů. Navzdory očekávání se tato služba příliš nerozšířila (v současnosti ji poskytují pouze eBanka a Živnostenská banka), a to z důvodu malého zájmu zákazníků. Dalším vývojem mobilních telefonů přinesl Java bankovnictví (v roce 2005 tuto službu začala poskytovat Komerční banka a následně i Živnobanka). Jedná se v podstatě o kombinaci GSM a internetového bankovnictví. Připojení k bance se uskutečňuje pomocí mobilního telefonu, který podporuje programovací jazyk JAVA, a který má dostatečnou paměť a požadované grafické rozhraní.

1.2.3 Homebanking a Internetbanking [21]

Homebanking (někdy nazývaný též PC banking) je založen na propojení osobního počítače klienta, na kterém je nainstalován speciální program, s počítačem banky prostřednictvím datové sítě. Toto spojení je možno realizovat buď přes telefonní spojení pomocí modemu, nebo připojením k internetu pomocí síťového adaptéru. Výhodou této služby je, že tyto produkty bývají kompatibilní s účetními a ekonomickými programy, což je zajímavé především pro střední a velké podniky, které potřebují provádět mnoho desítek transakcí denně. Nevýhodou je to, že je vázána na konkrétní počítač a je poměrně nákladná z důvodu instalace aplikace u klienta.

Internetbanking (internetové bankovnictví) je služba, která umožňuje komunikaci banky pomocí internetu, a to z jakéhokoliv místa na světě a počítače, na kterém je nainstalován internetový prohlížeč, a který splňuje určité minimální technické parametry. Za prvopočátek této služby lze považovat rok 1999, kdy ji zavedla tehdejší Expandia Banka [20]. V roce 2000 už nabízely internetové bankovnictví čtyři banky (Živnostenská banka, Union Banka,

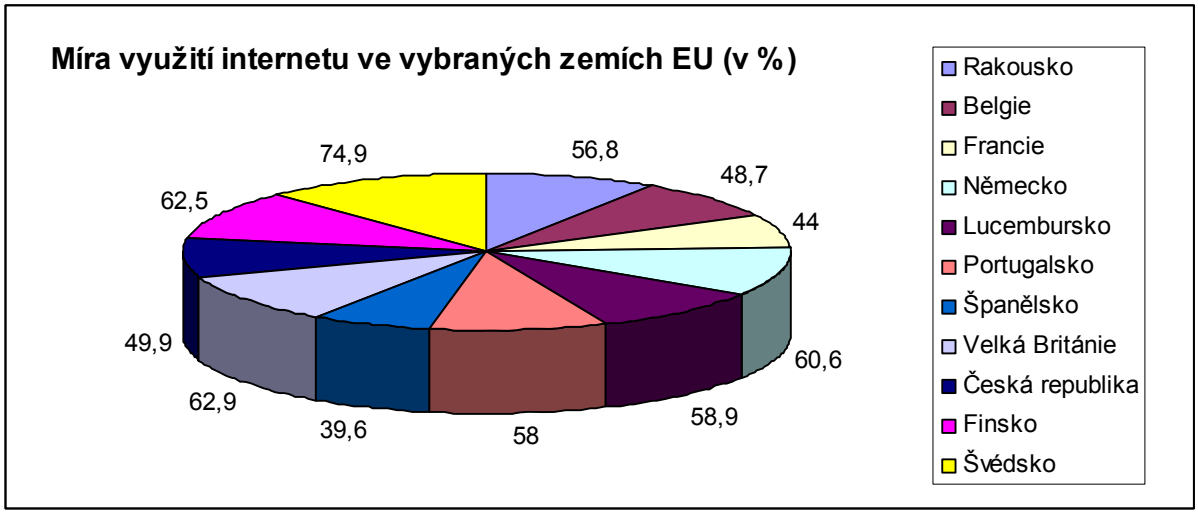
Raifeisenbank a GE Money Bank). V roce 2003 začala eBanka nabízet tzv. PDA bankovnictví – což je vlastně zjednodušená verze internetového bankovnictví pro využití tzv. PDA (Personal Digital Asistent). PDA bankovnictví je plně funkční také na kapesním počítači s mobilním telefonem tzv. MDA (Mobile Digital Asistent).

V současné době se stále více smazává rozdíl mezi Homebankingem a Internetbankingem. Například ČSOB přestala nabízet službu Homebanking 24 a místo toho nabízí službu BussinesBanking 24 Online, ve která je schopná provázat internetové bankovnictví a účetní systém dané firmy plně v on-line režimu.

Ještě většímu využívání internetového bankovnictví brání tři základní faktory. Prvním takovým faktorem je ještě stále nedostatečná nabídka přístupu k internetu. Druhým faktorem je často velmi nízká úroveň znalostí o možnostech využití internetu a o počítačích všeobecně mezi příslušníky starší generace a z ní pramenící nedůvěra v tuto technologii a v její bezpečnost. Třetím faktorem mohou být vyšší zřizovací náklady, především v domácnostech, kde není k dispozici osobní počítač. Tabulka 2 a obrázek 3 (zdroj [4]) ukazuje porovnání stavu využití internetového bankovnictví v České republice a v Evropě.

Země	Připojení k internetu (%)	Využití on-line bankovnictví (%)
Rakousko	56,8	40-50
Belgie	48,7	40-50
Francie	44	40-50
Německo	60,6	40-50
Lucembursko	58,9	50-60
Portugalsko	58	20-30
Španělsko	39,6	30-40
Velká Británie	62,9	40-50
Česká republika	49,9	10-20
Finsko	62,5	70-80
Švédsko	74,9	60-70

Tabulka 2: Porovnání využití internetu a on-line bankovnictví v ČR a v Evropě



Obrázek 3: Porovnání využití internetu v ČR a v Evropě

2 Používané zařízení

2.1 Bankomaty a platební karty

2.1.1 Bankomaty [1]

Bankomat se skládá ze tří základních částí :

1. trezoru s kazetami bankovek a bezpečnostním a spojovacím modulem
2. operátorské části sloužící k řízení bankomatu (PC, operátorská klávesnice a tiskárna)
3. provozní části skládající se z transportního a počítacího systému, tiskárny, obrazovky, klávesnice, snímače platebních karet, případně i dalších modulů (vkládání hotovosti apod.)

Bankomaty se dělí na dvě skupiny :

- peněžní automaty sloužící k výplatě hotovosti
- vícefunkční zařízení, která umožňují hotovost také ukládat

Cena bankomatu se liší podle toho, co všechno bankomat umí. Nejlevnější bankomaty, které slouží jen pro výběr peněz, stojí okolo 300 000 korun, ale u víceúčelových bankomatů se cena může vyšplhat i na několik milionů korun. Životnost se pohybuje okolo osmi až deseti let.

2.1.2 Platební karty [11]

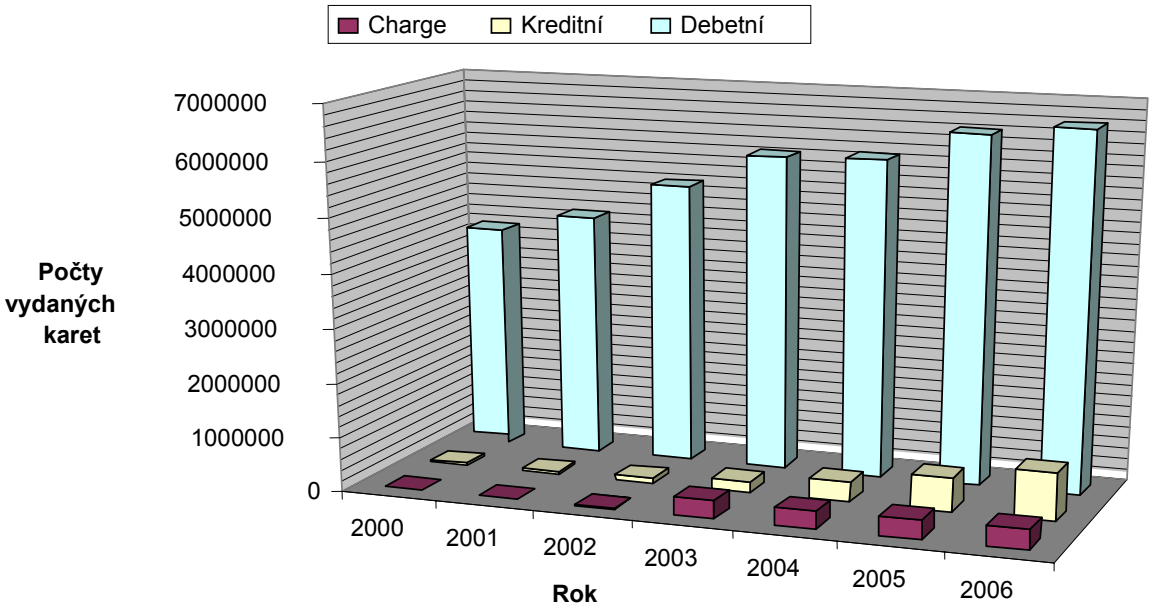
Platební karta je plastiková karta, odpovídající (z hlediska materiálu, rozměrů,…) mezinárodním normám, pomocí které může její majitel provádět bezhotovostní platby (v obchodech) a výběry hotovosti z běžného účtu, k němuž je karta vystavena.

Platební karta musí obsahovat tyto náležitosti:

- označení vydavatele karty. Nejvýznamnější vydavatele platebních karet lze v současnosti rozdělit do tří skupin:
    1. banky a bankovní asociace (VISA, Europany/Master Card, JCB)
    2. finanční společnosti (American Expres, Diners Club)
    3. obchodní domy, letecké, telekomunikační, olejářské společnosti apod.
- jméno držitele platební karty, popř. jinou formu identifikace (rodné číslo, podpis….)
- číslo platební karty
- platnost karty
- záznam dat (ve formě magnetického proužku, mikročipu, laserového záznamu)

Platební karty můžeme rozdělit podle

- Způsobu zúčtování (na obrázku 4 je uvedeny počty vydaných karet v ČR zdroj[4])
  - **Debetní karty** jsou pevně svázány s běžným účtem. Jejich použitím, ať jde o platbu u obchodníka anebo výběr z bankomatu, klient čerpá své peníze uložené na bankovním kontu. Poté, co provede kartou nějakou transakci, odečte banka příslušnou sumu z jeho účtu.
  - **Kreditní karty** znamenají nákup na úvěr. Karta není napojena na běžný účet, ale na účet úvěrový. Každá transakce s kartou znamená čerpání úvěru od banky. Ten pak musí klient v dohodnutém termínu splatit. Na rozdíl od debetních karet je při vydání kreditní karty zjišťována způsobilost klienta splatit budoucí úvěr (tzv. credit scoring).
  - **Charge karty** fungují obdobně jako karty kreditní s tím rozdílem, že banka na konci měsíce sestaví klientovi vyúčtování všech transakcí kartou. Ten pak musí celý dluh jednorázově splatit v dohodnutém termínu, zpravidla do konce následujícího měsíce. Z čerpané částky není účtován žádný úrok.
  - **Nákupní úvěrové karty** jsou vlastně kreditními kartami vydávanými nebankovními institucemi. Od svých bankovních sester se liší hlavně v ceně karty, výši úročení a omezené použitelnosti. Patří sem OK nebo YES karta.



Obrázek 4: Počty vydaných platebních karet v ČR

[4] http://www.bankovnikarty.cz

- Způsobu provedení
    - **Embosované karty** mají veškeré údaje (číslo karty, majitel, platnost apod.) plasticky vyraženy (v souladu se standardem ISO 7811). To umožňuje jejich použití i u obchodníků, kteří nemají elektronický terminál, ale pouze tzv. žehličku (imprinter). Platba probíhá tak, že obchodník vloží kartu do imprinteru a otiskne veškeré údaje z karty na účet, který pak zákazník podepíše. Každý obchod má nastaven tzv. floor limit, neboli výši útraty, kterou mohou jeho zákazníci provést kartou bez nutnosti platbu ověřit telefonem. Platby nad tento limit musí obchodník telefonicky ověřit. Embosované karty lze použít na více místech než karty elektronické. Daní za tuto výhodu je ale vyšší cena za vydání, vedení či blokaci (resp. stoplistaci) karty a jistá možnost zneužití karty i po nahlášení její ztráty či odcizení.
    - **Elektronické karty** jsou nejrozšířenějším typem karet u nás. Banky je většinou vydávají k účtu zdarma. Jsou určeny především k výběrům z bankomatu a pro platby u obchodníků, kteří mají elektronický platební terminál. Nevýhodou je jejich zatím omezená použitelnost u plateb v prodejnách.
- Vydávající asociace a třídy - naprostá většina karet vydaných v České republice nese logo mezinárodní asociace VISA Int. nebo MasterCard Int. Pro použití na našem území na značce (tzv. brandu) karty nezáleží - obě mají téměř stejný počet bankomatů i obchodních míst.
    - Karty **MasterCard** patří elektronické karty Cirrus a Maestro, v embosované verzi se setkáte s kartami MC Standard, velmi bonitním klientům jsou nabízeny karty MC Gold. Vrcholem řady je karta World Signium, která zatím v České republice nebyla vydána.
    - Karty **VISA** zahrnují elektronické karty VISA Electron, embosované VISA Classic, pro vyšší třídu klientů pak VISA Silver a VISA Gold. Nejvyšší kartou je VISA Platinum.
    - Ostatní platební karty např. **Diners Club**, **JBC** (Japan Credit Bureau) a **AMEX** (American Express). Ty jsou obecně určeny bonitnějším klientům a představují do jisté míry exklusivní platební nástroj.
- Použitelnosti
    - **Domácí karty** můžete využít k výběrům z bankomatů a placení v obchodech jen na území České republiky. Jsou označeny nápisem "valid only in the Czech

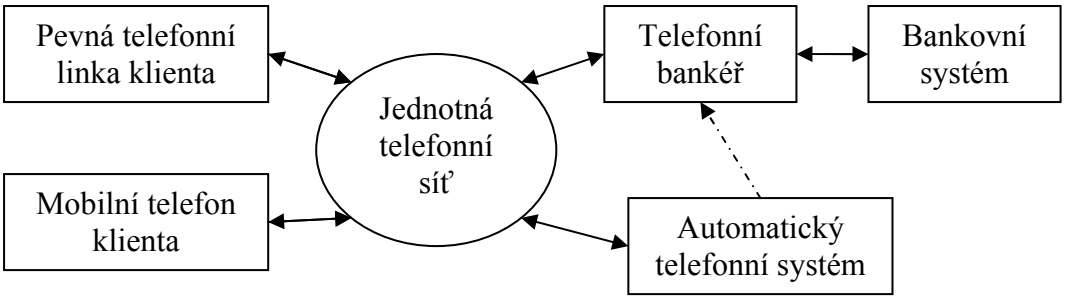
Republic". Banky od jejich vydávání z důvodu rozmachu placení v zahraničí upouštějí.

- **Mezinárodní karty** můžete používat jak na našem území, tak i v zahraničí. Dnes jsou téměř všechny karty vydávány jako mezinárodní.

- Technologie - pro elektronické transakce jsou platební karty vybaveny jednou z těchto technologií:
  - **Magnetický proužek** - je umístěn na zadní straně karty. Jsou na něm uloženy údaje o kartě a jejím držiteli, které jsou nutné pro provedení dané platby či výběru z bankomatu. Magnetický proužek neumožňuje tak vysoké zabezpečení uložených dat jako čip, proto na něm není uložen PIN.
  - **Čipová technologie** je například ve Francii úspěšně využívána už od devadesátých let. Celosvětová migrace na čip probíhá v těchto letech. Čip umožňuje díky vyššímu zabezpečení (využívajícímu dynamické šifrovací algoritmy) uložení PINu a nasazení karet pro elektronické transakce bez nutnosti ověření v centru (tzv. offline transakce).
  - **Hybridní karty** obsahují jak magnetický proužek, tak i čip. Toto řešení se používá hlavně v době přechodu z jedné technologie na druhou. V následujících letech bude většina karet vydávána jako hybridní.

2.2 Telefonní a GSM bankovnictví [2]

V případě „klasického“ telefonního bankovnictví, kdy klient komunikuje s telefonním bankéřem, postačí jakýkoli telefon (pevná linka nebo mobil). Pro případ komunikace s automatickým telefonním systémem však musí klientův telefon zvládat tónovou volbu popř. být vybaven přídavným adaptérem „tone dialer“. (telefonní přístroj s tónovou volbou při volbě telefonního čísla používá pro každou číslici – tlačítko- jiný tón o určité frekvenci, přístroj s pulzní volbou používá impulsy, pro každou číslici jiný počet impulsů). Automatický telefonní systém pracuje na základě menu, po kterém se lze pohybovat prostřednictvím tlačítek telefonu. Některé banky používají kombinaci automatického telefonního systému a živého telefonního bankéře. Schéma komunikace mezi bankou a jejím klientem je na obrázku 5 [zdroj 2].

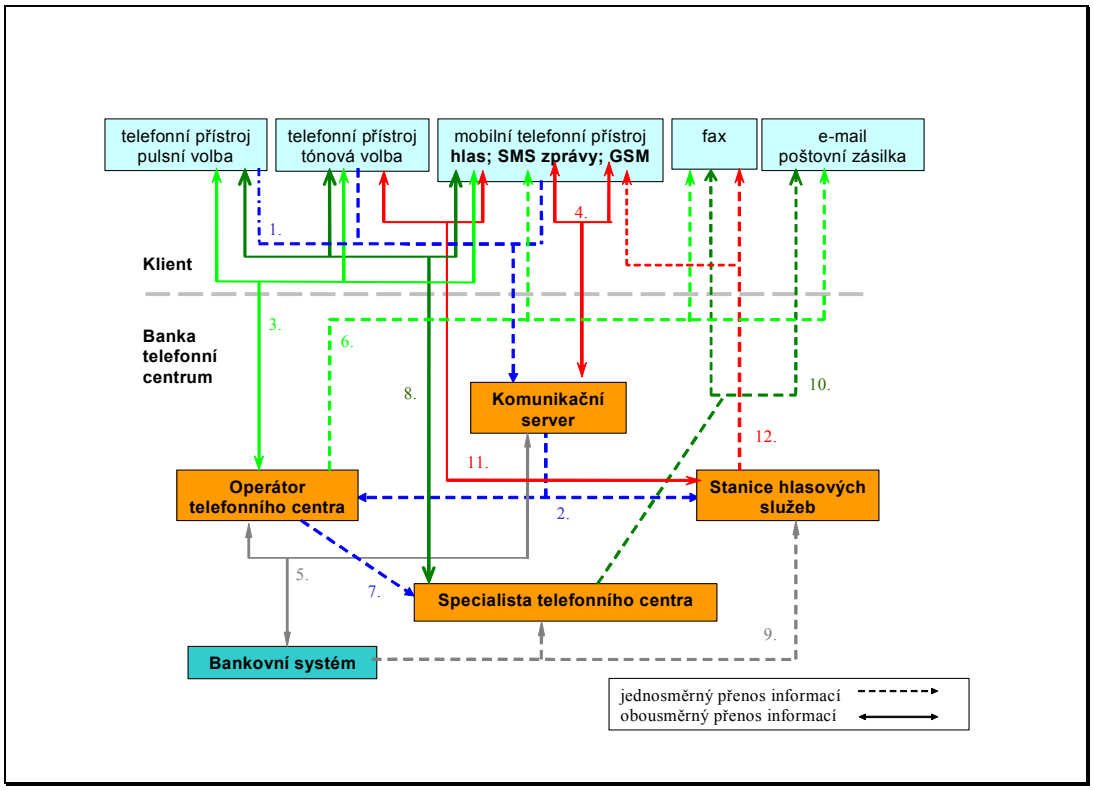


Obrázek 5: Komunikace mezi bankou a jejím klientem

V případě GSM bankovnictví (GSM je globální standard pro mobilní telefony určené k vysílání a příjmu; podle vlnové délky existují pásma: 900 MHz, 1800 MHz a 1900 MHz) komunikuje klient s bankou prostřednictvím mobilního telefonu. Tato komunikace může být formou :

- Šifrovaných SMS zpráv – v tomto případě klientovi postačí jakýkoliv mobilní telefon.
- Prostřednictvím SIM Toolkit – v tomto případě musí klient banky vlastnit mobilní telefon podporující technologii GSM SIM Toolkit s kartou, která obsahuje bankovní GSM SIM Toolkit, což je softwarové rozhraní, které umožňuje libovolně obměňovat menu mobilního telefonu.
- Využitím WAP technologie – v tomto případě musí klient vlastnit mobilní telefon, který podporuje WAP technologii (WAP je zkratka názvu Wireless Application Protocol - protokol pro bezdrátové aplikace. Jedná se o technologii, která umožňuje komunikaci mobilních zařízení - mobilních telefonů, kapesních počítačů - PDA, apod.) s internetovými servery a zobrazování obsahu speciálně upraveného pro tento účel. Aby mobilní telefon mohl zobrazovat wapové stránky, musí mít nainstalovaného wapového klienta (program). Jedná se o jakýsi mini internetový prohlížeč pro mobilní telefon.

Tok informací v rámci možností telefonního a GSM bankovnictví je zobrazen na obrázku 6 [zdroj 3].



Obrázek 6: Toky informací v rámci možností telefonního bankovnictví

1. klient volá z telefonních přístrojů komunikační server
2. klient si vybere operátora nebo hlasový automat
3. komunikace klient – operátor
4. komunikace zprávou SMS nebo GSM
5. výměna informací mezi bankovním systémem, operátorem a komunikačním serverem
6. operátor může odeslat nějaké informace formou SMS zprávy, faxem nebo e-mailem
7. v případě potřeby specifičtější informace přepne operátor hovor na specialistu
8. klient komunikuje se specialistou
9. specialista a hlasový automat získávají informace z bankovního systému
10. specialista odesílá specifické informace faxem, e-mailem nebo poštou
11. klient komunikuje s hlasovým automatem
12. hlasový automat odesílá SMS zprávu nebo fax

2.3 Homebanking a Internetbanking

V případě obou těchto služeb komunikuje klient s bankou prostřednictvím počítače, na kterém je instalován požadovaný aplikační software, a který má možnost spojení s komunikačním serverem příslušné banky.

2.3.1 Počítač klienta

Počítač klienta musí splňovat minimální systémové požadavky (hardware, operační systém...), které konkrétní banka požaduje. Rozdíl v případě homebankingu a internetbankingu je pouze v požadavku na určitou volnou kapacitu pevného disku (zpravidla v rozsahu desítek MB) – pro instalaci a provoz bankovní aplikace. Tyto minimální systémové požadavky se u jednotlivých bank v podstatě neliší (např. GE Money Bank požaduje : Procesor: Pentium 166 MHz, Operační paměť: 32 MB, Monitor: 15" (optimalizováno pro rozlišení 800 x 600 bodu), Operační systém: Windows (95, 98, ME, 2000, NT 4.0, XP)). V případě autorizace klienta elektronickým podpisem umístěným na čipové kartě je nutno, aby byl k dispozici volný port pro připojení čtečky čipových karet a také vlastní čtečka čipových karet.

2.3.2 Instalovaný aplikační software

V případě homebankingu musí mít klient na počítači nainstalován bankovní aplikaci, pomocí které bude komunikovat s bankou. Tu může klient nainstalovat buď z CD (které obdrží v bance) nebo si ho může stáhnout z internetových stránek dané banky. V případě internetbankingu musí být nainstalován prohlížeč www stránek. Některé banky požadují konkrétní prohlížeč (např. GE-Money bank požaduje Microsoft Internet Explorer 5 a vyšší), jiné banky např. ČSOB umožňují použití více druhů prohlížečů (MS Internet Explorer v. 5.5 SP 2 a vyšší, Mozilla 1.7.5, Mozilla Firefox 1.0, Netscape 7.2). V případě autorizace klienta pomocí elektronického podpisu uloženého na čipové kartě (je to jedna z možností autorizace klienta např. do systému ČSOB Internetbanking 24) je nutno nainstalovat sadu ovladačů čtečky a šifrovací program pro správu čipové karty – k tomu je však nutné mít na daném počítači právo administrátora systému, což v praxi omezuje počet počítačů, ze kterých se klient může přihlásit do internetbanky.

2.3.3 Spojení počítače s komunikačním serverem

V případě homebankingu může být počítač klienta propojen s komunikačním serverem příslušné banky buď pomocí internetu nebo pomocí vytáčeného spojení s bankou. Při využívání internetového bankovnictví je toto spojení uskutečněno přes internet (dle nastaveného přístupu klienta – např. přes lokální modem, pevné připojení, Wi-fi …).

3 Bezpečnost

Elektronické bankovnictví přináší zúčastněným stranám, tedy bance i jejímu klientovi značné výhody. Klient banky má on-line přístup ke svému účtu a peněžním prostředkům na něm (popřípadě i k dalším službám). Je to rychlé, pohodlné, diskrétní. Pro banku to znamená například úsporu nákladů. Vedle těchto nesporných kladů má elektronické bankovnictví i jeden významný zápor. Bohužel ne vždy je bezpečné. Podle [4] lze způsoby podvodů v elektronickém bankovnictví dělit na :

- „dobrovolné“ zaslání přihlašovacích údajů – pod tuto metodu spadá phishing a pharming
- „odchycení“ přihlašovacích údajů od uživatelů – užití trojských koňů, spyware, spamu
- „od třetích stran“ – získání hesel, PINů a dalších dat např. o platební kartě od subjektů, kde byly použity k úhradě
- „nabourání“ do systémů, tzv. hacking
- „rafinované útoky“ – pod tuto metodu spadají odposlechy, násilné donucení …

Aby se elektronické bankovnictví dále úspěšně rozvíjelo, je nutné minimalizovat pravděpodobnost těchto podvodů a zajistit maximální bezpečnost elektronické komunikace mezi klientem a bankou a z ní plynoucí důvěru klienta v tuto formu komunikace.

3.1 Bezpečnost platebních karet

3.1.1 Rizika spojená s používáním platebních karet [1]

Tato rizika lze rozdělit na tři základní kategorie – riziko zneužití karty cizí osobou, riziko zneužití nedoručené karty a riziko padělání karet. Největší ztráty vydavatelů tvoří zneužití ztracených nebo odcizených platebních karet (např. v roce 1996 se tento druh rizika podílel na celkových ztrátách asi 56 %). Jednou z metod zneužití platební karty je tzv. libanonská smyčka. Princip tohoto podvodu spočívá v tom, že na zdířce bankomatu je nalepen obdélníček s páskou z videokazety, která je ukryta uvnitř. Karta klienta ji následně našponuje a uvízne v načítacím zařízení. Zákazník natypuje PIN, který je blízko stojícím podvodníkem nebo dálkově pomocí dalekohledu odpozorován. Zákazník si vybere svoje peníze, ale bankomat mu jeho kartu nevrátí. Po odchodu zákazníka (ten zpravidla odchází do banky, aby si vyžádal

vrácení karty) odstraní pásku, vyjme kartu a použije ji k dalšímu výběru v hotovosti. Další používanou metodou je padělání platební karty pomocí skimovacího zařízení [8]. Toto zařízení je umístěno na vstupní zdířku bankomatu a kopíruje magnetický proužek. Druhou částí je kamera, většinou skrytá v připravené liště nad prostorem, kde se zadává PIN. Díky tomu si následně podvodník vyrobí padělek bankovní karty a provádí výběry peněz, aniž by o tom její majitel třeba i delší dobu věděl.

3.1.2 Zabezpečení platebních karet [1,10]

Je velmi důležité, aby majitel platební karty pravidelně kontroloval, zda ji stále ještě vlastní. Pokud zjistí, že ji buď ztratil nebo mu byla odcizena, je nutné okamžitě informovat svoji banku a ta provede tzv. stoplistaci karty.

Pro snížení rizika zneužití karty cizí osobou provádějí banky kontrolu totožnosti jejího držitele. Ta může být uskutečněna nutností zadat PIN (např. u bankomatu) nebo povinností podepsat stvrzenku v souladu s podpisovým vzorem uvedeným na kartě – tato metoda nemusí být vždy spolehlivá. Jednak se podpis lidí s léty mění (resp. může měnit) a jednak může případný zloděj „natrénovat“ správný podpis dle podpisového vzoru na ukradené kartě. Další způsob ověření totožnosti může být založen na biometrických metodách – kontrola fotografie, otisku prstu, rozboru hlasu apod. Např. First National Bank v JAR používá ve svých bankomatech identifikaci na základě rozboru hlasu.

Každá transakce pomocí bankomatu je on-line ověřena v autorizačním centru. Bankomat odešle na hostitelský počítač informace o kartě a PINu a následně obdrží zprávu, v níž je transakce buď autorizována, nebo zamítnuta. Tato komunikace je šifrována, takže pokud by ji někdo odposlouchával, nemůže zjistit PIN karty. Šifrování je uskutečněno pomocí metod symetrického šifrování DES (Data Encryption Standard) popřípadě 3DES (což znamená 3x po sobě zašifrování pomocí DES třemi různými klíči).

Aby bylo eliminováno riziko zneužití nedoručené karty, doručují banky platební karty svým klientům odděleně od PIN. Pokud se karta posílá poštou, je zpravidla neaktivní a klient ji musí následně telefonicky aktivovat.

Pro snížení rizika padělání platebních karet používají banky celou řadu ochranných prvků – hologramy, laserovou gravituru, mikrotext, ceninový tisk apod. Další zvýšení ochrany proti padělání znamená použití čipových karet. Citlivé informace, které tyto karty obsahují, jsou kódovány. Navíc karta obsahuje speciální chemickou vrstvu, která jí chrání proti analýze obsahu paměti. Např. dle [9] na konci roku 2006 vlastnili klienti skupiny ČSOB 1.3 miliónu aktivních čipových platebních karet a dle údajů ČSOB se doposud nevyskytl jediný padělek

takové karty. Čipové karty vydané většinou bank ČR stále nesou i magnetický proužek. Je to proto, že na světě zatím neexistuje jednotný přístup k čipové a magnetické technologii – jsou státy, které stále upřednostňují magnetický proužek, jiné naopak preferují čip. Magnetický proužek a zároveň čip umožní klientům použití těchto karet kdekoliv na světě. Bezpečnost využití čipové karty v ČR je v tomto směru ochráněna skutečností, že použití čipu je prioritní a zadání PIN je přitom povinné.

3.2 Bezpečnost telefonního a GSM bankovnictví

3.2.1 Rizika spojená s telefonním a GSM bankovnictvím [12]

V případě použití klasického telefonního přístroje není komunikace mezi klientem a bankou prakticky nijak zabezpečena. Bez ohledu na to, zda jednotliví operátoři šifrují data přenášená mezi ústřednami, minimálně hovory od zdrojového telefonu k nejbližší ústředně a od poslední ústředny k cílovému telefonu jsou nešifrovaná a tedy nechráněná. Pokud se komukoliv podaří napojit na tuto část přenosové linky, má možnost tuto komunikaci odposlouchávat.

V případě použití mobilního telefonu pracujícího v síti GSM je komunikace (hovory, SMS zprávy, GPRS) šifrována. Toto šifrování se děje pomocí šifry A5/1 a její slabší verze A5/2. Avšak tato šifra není považována za kryptograficky bezpečnou a bylo publikováno hned několik útoků na ni. Čas nutný pro určení klíče není nijak dlouhý. Pohybuje se v řádu stovek milisekund až do několika sekund, v závislosti na verzi algoritmu A5.

3.2.2 Zabezpečení telefonního a GSM bankovnictví [14,15]

Klasické telefonní bankovnictví je zabezpečeno identifikací a autentizací klienta.Ve většině případů se ověřuje uživatelské jméno a heslo či PIN, který je klientovi přidělen při zřízení služby. Vzhledem k odposlouchatelnosti spojení však některé banky využívají k autorizaci klienta více robustní řešení, jakým je například použití mobilního či elektronického klíče. Pokud komunikace probíhá s telefonním bankéřem, může být součástí autentizace i ověření znalosti identifikačních údajů vlastníka účtu, čísel smluv atp. Dialog může být veden selektivně, tj. ověřují se jen náhodně vybrané údaje nebo jejich části.

V případě GSM bankovnictví je přístup k bankovním operacím v mobilním telefonu chráněn bankovním PINem (BPIN). Veškerá komunikace mezi klientem a bankou je šifrována. Jednak šifrováním pomocí SIM Toolkit (šifra 3DES) a jednak šifrováním GSM sítě (šifra A5/1 je sice prolomena a program na její dešifrování je možno volně stáhnout z internetu, avšak je stále technicky velmi obtížné hovor odposlechnout; navíc by se postupně mělo přejít na šifru A5/3,

která je odolnější[5]). Přínosem pro bezpečnost může být i fakt, že GSM bankovnictví k jednomu účtu lze provozovat pouze z jedné SIM karty [14].
V případě použití WAP bankovnictví je komunikace rovněž šifrována. Mezi klientem a WAP bránou je použit šifrovací protokol WTLS. Mezi WAPovou bránou a webovým serverem je komunikace zajištěna SSL šifrovacím protokolem [15].

3.3 Bezpečnost internetového bankovnictví

3.3.1 Rizika spojená s využíváním internetového bankovnictví

Mezi formy elektronické kriminality, které v posledních letech nejvíce ohrožují internetové bankovnictví patří tzv. „phishing“ a „pharming“.

3.3.1.1 Phishing a pharming [5]

Slovo „phishing“ je složenina z anglických slov „fishing“ (rybaření nebo rybařit) a phreaking, což je slangový výraz označující krádež pomocí telefonní služby. Znamená podvod za účelem získání privátních informací a jejich následné zneužití. „Návnadou“ je obvykle e-mail informující o hrozící finanční ztrátě, možném zisku, potřebě ověřit majitele účtu apod. Tento mail požaduje „ověření“ příjemce zadáním privátních informací na internetové stránce (odkaz na ni je součástí mailu). Tato internetová stránka se vytváří jako originál (např. stránka banky), ve skutečnosti jde o podvrh. Pokud klient uvěří textu e-mailu a zadá požadované údaje, jsou tyto k dispozici útočníkovi. Ten pomocí předaných údajů převede peníze z účtu či platební karty podvedeného důvěřivce. Tyto podvodné stránky jsou často provozovány v exotických zemích (východní Asie, jižní Amerika), a proto je velmi těžké dohledat pachatele.
Techniky „phishingu“ jsou však stále více známé, a tak se autoři podvodných nabídek uchylují ke skrytější, ale efektivnější metodě útoku. Ta se nazývá tzv. „pharming“. Za základ tohoto slova bylo použito anglické slovo „farming“ (farmařit, pěstovat). Pharming je založen na modifikaci systému DNS, a to buď v počítači uživatele nebo serveru poskytovatele služeb internetu. Systém DNS (Domain Name Server) překládá zadaný název domény na skutečnou adresu webového serveru v síti (jeho adresu IP) – například www.vasebanka.cz přeloží na 146.04.04.04. Tento překlad probíhá prostřednictvím sítě. Pro urychlení procesu si počítač klienta nebo server poskytovatele internetu obvykle uchovává vlastní kopie výsledků překladu

[5] Dle Ondřej Málek : Generování pseudonáhodných dat, za použití metody LFSR, Bakalářská práce, Masarykova Universita, Fakulta informatiky, 2007

DNS, které získal pro dříve navštívené weby. Místo, kde je uchovává, se nazývá "mezipaměť DNS". Tím, že před položením vlastního dotazu v síti hledá nejprve ve své mezipaměti, počítač šetří čas a nezatěžuje Internet dotazy, na které již zná odpověď.

A právě tuto místní mezipaměť DNS útočníci zneužívají. Pomocí kódu trojského koně upraví tuto mezipaměť tak, že když uživatel zadá název své banky online, bude převeden na falešný web, který bude vypadat úplně stejně jako skutečný web banky. Při přihlašování pak klient neúmyslně vyzradí své identifikační údaje.

3.3.1.2 Případy kriminality v elektronickém bankovnictví

Pro ilustraci zde uvedu dva kriminální případy, které se skutečně staly v ČR během posledních dvou let.

3.3.1.2.1 První phishing v Česku [6]

S největší pravděpodobností historicky první phishingový útok v českém jazyce byl namířen proti klientům české pobočky CitiBank. Těmto klientům přišel počátkem března 2006 následující mail [6]:

Od: Citibank Online [alerts@citibank.cz]
Komu: Petr Nadenicek
Kopie:
Předmět: Important notice: Confirm Payment

citibank

Serial EM202-16

Vážený kliente Citibank Online®,

03/02/2006 na Váš běžný účet byl přijat převod v cizí měně na částku ve výši 2000 . Se shodou s *spotřebitelským souhlasem CitiBank® online*, je potřeba potvrdit tento převod pro jeho úspěšné zařazení na Váš běžný účet.

Pro potvrzení platby Vás prosím o návštěvu programu ovládání Vaším účtem CitiBank® online a dále postupujte podle předloženého návodu. V případě nepřijetí potvrzení v průběhu 48 hodin, bude částka vracena odesílateli.

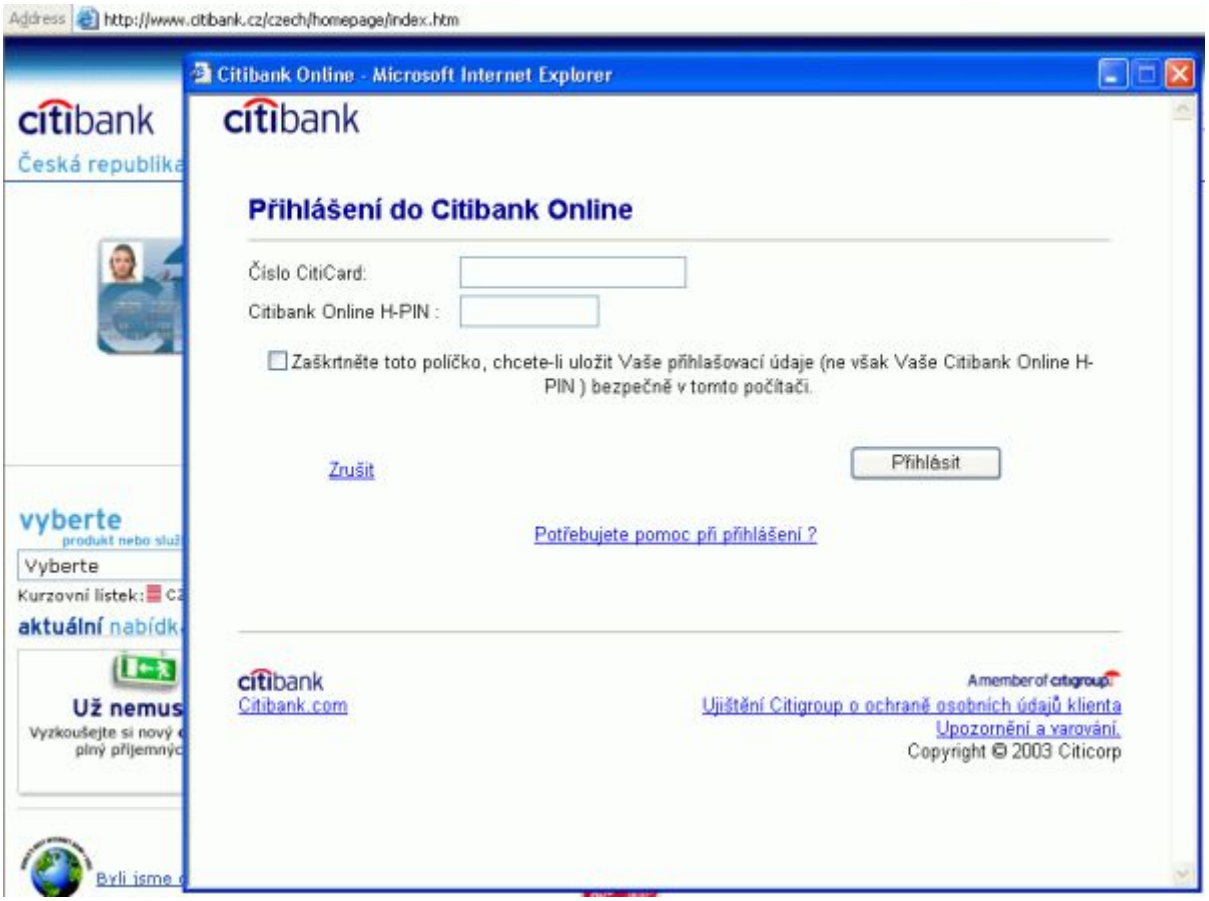
Pro vstup do programu CitiBank® online, **klikněte sem** >>>

S pozdravem
Služba CitiBank® Alerting Service

Obrázek 7: Ukázka podvodného mailu

Odkaz ("klikněte sem") uvedený v e-mailu směřuje na http://citi-online.czechrepublic-online.com/

Z databáze registrátora bylo možno zjistit, že majitelem domény czechrepublic-online.com byl jakýsi Travis Godfrey. Pokud uživatel odkaz použil, dostal se na regulérní stránky české CitiBank, před nimiž je ale otevřeno druhé okno s kolonkami pro přihlášení do on-line bankovního systému. Adresa, ze které okno pochází, ale není viditelná – tato stránka patřila útočníkovi(!) - viz obrázek 8 [6]. Cokoliv se do zde uvedených kolonek zadalo, získal útočník a mohl později zneužít k poškození klienta.



Obrázek 8: Stránky CitiBank jsou překryty podvodným oknem

V tomto konkrétním případě se naštěstí nic závažného nestalo. CitiBank se podařilo vyřadit stránku z provozu pár hodin po té, co se objevily první falešné emaily. Bezprostředně po zjištění podezření na phishing byli klienti banky informováni o této situaci prostřednictvím SMS zpráv a emailu. Žádný z klientů banky neutrpěl finanční ztrátu.

3.3.1.2.2 Napadení internetového bankovnictví Komerční banky [7]

24. 8. 2006 Komerční banka oficiálně potvrdila, že prostřednictvím jejího internetového bankovnictví Mojebanka došlo k odčerpání peněz neoprávněnou osobou. Banka zaznamenala 10 případů klientů, u kterých se objevily pokusy o zneužití jejich osobních počítačů. Vnitřní systémy banky nebyly v žádném případě narušeny. Jako reakci na tento incident zvýšila KB bezpečnost svého internetového bankovnictví tím, že zavedla nový způsob autorizace aktivních transakcí. Všichni uživatelé internetového bankovnictví Mojebanka, kteří používali k podepisování transakcí osobní certifikát v souboru, budou nyní při provádění aktivních operací zadávat i autorizační SMS kód.

Předpokládaný způsob zneužití účtu (policie odmítla komentovat jednotlivé vyšetřovací verze) byl ten, že pomocí phishingu 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.

3.3.2 Zabezpečení internetového a domácího bankovnictví [17]

Mezi základní požadavky na bezpečnost internetového a domácího bankovnictví patří :

- Důvěrnost – cílem tohoto požadavku je to, aby přenášená data zůstala důvěrná a nedostala se do nepovolaných rukou. Toho lze dosáhnout jejich zašifrováním, které způsobí, že když se tato data přece jen dostanou do rukou někoho nepovolaného, nebudou mu k ničemu, protože je nebude schopen dešifrovat.

- Integrita - tento požadavek souvisí s potenciálním nebezpečím modifikace dat, přenášených nezabezpečeným kanálem. Ať již v důsledku nějaké technické chyby či závady nebo v důsledku něčích nekalých aktivit by totiž mohlo dojít k pozměnění přenášených dat, což by právě u bankovních transakcí mohlo mít nedozírné následky (například pouhé připsání jedné nuly by mohlo opravdu zásadně změnit výši požadované transakce). Požadavek na "nezměnitelnost" dat bývá často poněkud slabší - ne takový, aby se vyloučila jakákoli, byť i sebemenší možnost změny. Místo toho se požaduje alespoň to, aby jakákoli eventuelní změna byla okamžitě a spolehlivě rozpoznatelná. Důvody jsou ryze praktické, protože zajištění bezpečné rozpoznatelnosti jakékoli změny je výrazně snazší a lacinější než zajištění absolutní "nezměnitelnosti", které snad ani nejde dosáhnout.

- Neodmítnutelnost - tento požadavek spočívá v tom, že každá z komunikujících stran potřebuje mít jistotu, že druhá strana nebude moci někdy později popřít cokoli z toho, co vyslala. Například když banka přijme elektronickou cestou nějaký požadavek svého klienta a provede jej, potřebuje mít jistotu, že klient si později vše nerozmyslí, nezačne tvrdit, že žádný požadavek nevznesl, a nezačne se domáhat navrácení původního stavu před provedením transakce. Princip zajištění potřebné "neodmítnutelnosti" je vcelku jednoduchý - je nutné zajistit aby příslušný požadavek musel být v takovém tvaru, aby jej nemohl vygenerovat nikdo jiný než příslušný klient.

- Identifikace a autentizace - tento požadavek je velmi důležitý – pokud banka komunikuje na dálku se svým klientem, musí spolehlivě určit, o kterého klienta se jedná (identifikace), a také se nade vší pochybnost ujistit, že se skutečně jedná o něj a ne o někoho, kdo se za příslušného klienta pouze vydává (autentizace). Způsobů jak zajistit identifikaci a autentizaci je celá řada a jsou vesměs založeny na něčem, co je pro oprávněného klienta charakteristické a unikátní - může jít například o znalost nějaké informace (hesla), vlastnictví nějakého předmětu (např. elektronického klíče), či o určitou fyziologickou charakteristiku (například otisk prstů).

- Certifikace - tento požadavek znamená potvrzení platnosti předávaných údajů, charakterizujících požadovanou finanční transakci. Jde například o číslo účtu klienta, číslo cílového účtu, převáděnou částky, variabilní symbol, specifický symbol atd. Certifikaci lze chápat jako zvláštní případ požadavku na integritu dat, specifický pro bankovní aplikace - banka se zde potřebuje ujistit o tom, že všechny údaje specifikující požadovanou transakci jsou skutečně takové, jaké jejich klient požaduje. Rozdíl mezi identifikací a autentizací na straně jedné a certifikací na straně druhé lze dokumentovat na průběhu práce klienta s jeho účtem - poprvé, než jej banka vůbec pustí do svého klientského systému, si musí zjistit jeho identitu (provést identifikaci klienta) a také ujistit se o tom, že jde skutečně o příslušného klienta (provést autentizaci). Poté již může klientovi zobrazit například stav jeho účtu, a nabídnout mu možnost zadávání jednotlivých transakcí. Ovšem pokaždé, když si pak klient nějakou transakci vyžádá, musí banka jeho požadavek ověřit, tj. vyžádat si certifikaci vznášeného požadavku.

3.3.2.1 Ověření identity banky [19]

Aby měl klient jistotu, že předává citlivá osobní data správnému subjektu, je potřeba zajistit nejen identifikaci zákazníka, ale také ověření totožnosti bankovního ústavu. V tomto případě je u všech českých bank shodně použit protokol SSL, kdy se banka prokáže webovému prohlížeči oficiálním SSL certifikátem, který obsahuje identifikační údaje potřebné k ověření totožnosti banky. SSL certifikát je vydán některou z takzvaných certifikačních autorit, která zajišťuje důvěryhodnost certifikátu. Seznam těchto autorit je vložen v prohlížeči a ten jim implicitně důvěřuje. Samotné stažení certifikátu a jeho ověření má na starosti webový prohlížeč na klientském počítači. Ten se postará o všechny potřebné kroky a zajistí vše automaticky. V případě, že je ověření úspěšné a prohlížeč rozhodne, že certifikát je platný, a klient komunikuje se správnou bankou, spojení se bez jakéhokoliv upozornění naváže.

3.3.2.2 Identifikace a autentizace klienta [14]

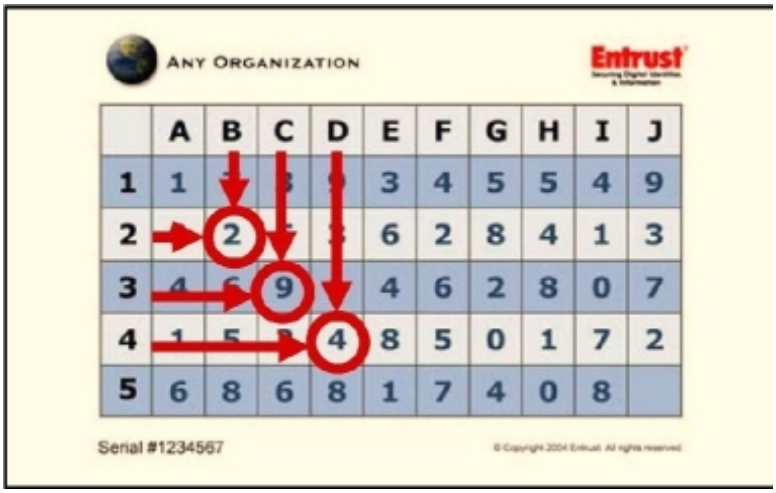
Při ověření identity klienta komunikujícího prostřednictvím počítače se můžeme setkat s autentizačními systémy, které využívají: uživatelského jména a hesla; certifikátu; čipové karty; SMS kódu; či autentizačního (PIN) kalkulátoru. V tabulce 3 jsou uvedeny způsoby autentizace klienta využívajícího internetové bankovnictví ve vybraných českých bankách (zdroj:internetové stránky jednotlivých bank).

Uživatelské jméno a heslo lze považovat za základní způsob ověření identity uživatele, který je však vhodný kombinovat s některým dalším. U některých bank je to však jediný možný způsob ověření identity (např. Poštovní spořitelna). Důležitými bezpečnostními aspekty u hesel jsou požadavky kladené na nově volená hesla (minimální délka; zda musí obsahovat číslice, velká písmena, speciální znaky) či počet chybných ověření, po kterých dojde k dočasnému zablokování účtu. Pro odblokování je typicky vyžadována návštěva pobočky, u některých bank je možné účet odblokovat i telefonicky. Obvykle za poplatek vydávají některé banky svým klientům časově omezený certifikát, který je použit pro ověření žádostí o autentizaci (podepsané příslušným soukromým klíčem). Tento certifikát by měl být uložen na externím paměťovém médiu (disketa, flash disk) a nahráván pouze v okamžiku, kdy je potřeba. Opět většinou za příplatek lze zvolit umístění těchto citlivých dat na kryptografickou čipovou kartu, kterou tato data neopustí, protože čipová karta provádí požadované kryptografické operace s citlivými klíči sama. Dále je možné pro autentizaci využít jednorázová hesla generovaná uživatelovým PIN kalkulátorem nebo jednorázová hesla bankou odesílaná přes jiný komunikační kanál, např. formou SMS zprávy.

Banka	Identifikační číslo a heslo	Osobní certifikát	SMS	Autentizační kalkulátor
Česká spořitelna	Ano	Ano	Ne	Ano
ČSOB	Ano	Ano	Ano	Ne
Poštovní spořitelna	Ano	Ne	Ne	Ne
Komerční banka	Ne	Ano	Ne	Ne
GE Money Bank	Ano	Ano	Ano	Ne
UniCredit Bank	Ne	Ne	Ne	Ano

Tabulka 3: Způsoby autentizace klienta

S dalším možným řešením přišla firma Entrust. Nazývá se Identity Gard a umožňuje oboustrannou tzv. *souřadnicovou autentizaci*. Každý uživatel je vybaven kartou (která se čas od času mění). Karta je potištěna tabulkou (viz. obrázek 9 [14]). Při autentizaci je pak uživatel kromě jména a hesla dotázán na několik znaků vytištěných na konkrétních políčkách v tabulce (např. B2, C3 a D4). Tento dodatečný autentizační mechanizmus poskytuje dobrou ochranu také proti podvrženým stránkám či různým druhům malwaru - několik útoků, které by odhalily login a heslo, dokáže totiž odhalit jen poměrně malou část znaků na autentizační kartě. Jednodušší formou tohoto mechanismu je volba sekundárního hesla, ze kterého musí uživatel při autentizaci zadat několik znaků z náhodně vybraných pozic.



Obrázek 9: Uživatelská karta

3.3.2.3 Šifrování dat [19]

Pokud jsou bezpečně ověřeny obě komunikující strany, může klient vstoupit do systému internetového bankovnictví a začít s ním pracovat. Dalším slabým místem je v tomto případě cesta, po které putují data oběma směry. Kdokoliv má totiž možnost komunikaci zachytit, pozdržet, případně přečíst a pozměnit. To je pochopitelně naprosto nepřípustné. Proto je nutno data proudící oběma směry šifrovat. Součástí SSL certifikátu je také veřejný šifrovací klíč,

který je během úvodního představování předán klientovi. Ten na oplátku předá zpět svůj veřejný klíč. Od této chvíle je pak veškerá komunikace na straně odesílatele šifrována veřejným klíčem druhé strany. Po přijetí jsou pak data opět dešifrována a následně normálně použita. O šifrování se opět stará transparentně webový prohlížeč a tuto činnost oznamuje obvykle ve stavové liště ikonou žlutého visacího zámku. Tím je uživateli oznamováno, že je vše v pořádku, SSL certifikát je platný a probíhá šifrování. Při kliknutí na tuto ikonu si pak můžeme přečíst informace z certifikátu a další údaje o komunikaci. V tabulce 4 (zdroj:internetové stránky jednotlivých bank) jsou uvedeny velikosti klíčů SSL šifry a používané certifikační autority u našich nejvýznamnějších bank.

Banka	Délka šifrovacího klíče	Certifikační autorita
Česká spořitelna	128 bitů	VeriSign
ČSOB	128 bitů	První Certifikační autorita
Poštovní spořitelna	128 bitů	První Certifikační autorita
Komerční banka	128 bitů	VeriSign
GE Money Bank	128 bitů	VeriSign
UniCredit Bank	128 bitů	VeriSign
eBanka+Raiffeisenbank	128 bitů	VeriSign

Tabulka 4: Délky klíčů SSL šifry a používané certifikační autority

3.3.2.4 Bezpečnost počítače klienta [18]

Sebelepší zabezpečení je neúčinné, pokud klient není dostatečně opatrný a při internetové komunikaci s bankou nedodržuje základní bezpečnostní pravidla. Tato pravidla lze shrnout do desatera bezpečného používání internetového bankovnictví [18,19]:

- Ochrana zabezpečovacích prvků (klientské číslo, PIN, Heslo..) - zabezpečovací prvky nikomu nesdělujte, ani rodinným příslušníkům, nezaznamenávejte si je na papírky, do diářů, do telefonu apod. a uchovávejte je odděleně na bezpečném místě.
- Nepoužívání jednoduchého hesla - jednoduché heslo se dá snadněji rozluštit a zneužít. Nepoužívejte proto slova, která mají souvislost s Vaším jménem, se jmény rodinných příslušníků, jejich datem narození, jejich telefonním číslem apod. Doporučuje se zvolit kombinaci velkých i malých písmen a číslic. Heslo by mělo mít minimálně osm znaků.
- Ochrana hesla - v žádném nastavení počítače nepovolujte zapamatování hesla. Heslo si pravidelně měňte a neopakujte je. Důležité je také vymazání historie prohlížeče.

- Ochrana PC a pravidelná aktualizace operačního systému - pravidelně instalujte aktualizační soubory, které odstraňují některé chyby či bezpečnostní rizika.
- Používání bezpečného počítače - pro práci s aplikací Internetové bankovnictví používejte pouze bezpečné počítače, které máte plně pod kontrolou a máte možnost ovlivnit jejich bezpečnostní nastavení.
- Ochrana počítače proti virům a spyware - mějte na svém počítači nainstalovaný antivirový program, který zvyšuje ochranu před škodlivými programy – viry. Stejně tak je vhodné používat anti-spyware program, který zvyšuje ochranu před sledováním Vaší činnosti na PC pomocí parazitních programů. Antivirové a anti-spyware programy pravidelně aktualizujte. Nestahujte z internetu neznámé soubory. Tyto soubory mohou společně se svým původním účelem nainstalovat na Váš počítač i nebezpečné programy.
- Připojení k internetu přes firewall - firewall je ochranný program nebo technické zařízení, které minimalizuje rizika neoprávněného přístupu k Vašemu počítači při připojení z internetu. Firewall zpracovává pouze Vámi zadané dotazy do sítě internet a všechna ostatní potencionálně nebezpečná data odfiltruje.
- Pozor na nedůvěryhodné emaily - neotvírejte e-mailové zprávy od neznámých adresátů nebo zprávy s podezřelým názvem či obsahem. V žádném případě nespouštějte přílohy takovýchto zpráv a zprávy bez otevření smažte. Nikdy nereagujte na e-mail, který po Vás bude požadovat sdělení osobních údajů, Hesla nebo PINu.
- Ověření certifikátu – ověřte si certifikát stránky, na které se k účtu přihlašujete. Pokud se vám přihlášení k účtu nepodaří, přestože vkládáte správné uživatelské jméno a heslo, neprodleně kontaktujte banku- mohli jste být přesměrováni na jiné stránky.
- Po ukončení práce s internetovým bankovnictvím se vždy odhlaste a zavřete okno prohlížeče.

4 Ekonomie banky, klienta, jeho náklady

Z pohledu banky znamená zavedení elektronického oproti klasickému bankovnictví jednak snížení nákladů banky a jednak změnu jejich struktury. Sníží se náklady na jednotlivé transakce, náklady na zpracování dat, náklady spojené s manipulací s hotovostními penězi, fixní náklady[6]. Větší budou naopak náklady na zavedení a obsluhu systému elektronického bankovnictví, náklady na udržení dostatečné úrovně zabezpečení systému EB (zabezpečení jednak vlastního systému banky, jednak komunikačního kanálu mezi klientem a bankou), náklady na zavádění nových technologií při zdokonalování komunikačních kanálů a rozšiřování služeb EB. S větším počtem nabízených produktů se mění i skladba příjmů banky. Dochází ke zvyšování objemu příjmů z poplatků za služby (je to součást tzv. neúrokových příjmů) na úkor úrokových příjmů.

Aby banky přiměly své klienty využívat kanály přímého bankovnictví, tyto služby cenově zvýhodňují. V tabulce 5 (zdroj:internetové stránky jednotlivých bank) je porovnání cen (v Kč), které klient banky zaplatí za vnitrobankovní platební příkaz zadaný na pobočce oproti platebnímu příkazu zadanému pomocí jednotlivých kanálů přímého bankovnictví.

Banka	Vnitrobankovní platební příkaz			
	Pobočka	Internet	Telefon	GSM
Česká spořitelna	45,-	2,-	2,-	2,-
ČSOB	30,-	3,-	9,-	3,-
Poštovní spořitelna	12/20/30[7]	Zdarma	Zdarma	Zdarma
Komerční banka	30,-	3,-	6,-	3,-
Ge Money Bank	39,-	3,-	3,-	3,-
UniCredit Bank	20,-	2,-	8,-	2,-
Bawag Bank	20,-	5,-	----	----

Tabulka 5: Porovnání poplatků za vnitrobankovní platební příkaz

Jedním z důležitých faktorů, který často ovlivňuje volbu přímého bankovnictví jsou poplatky za vedení přímého bankovnictví, které musí klient zaplatit. V tabulce 6 (zdroj:internetové stránky jednotlivých bank) je porovnání těchto poplatků (v Kč) mezi vybranými bankami. Údaje jsou platné pro rok 2007.

[6] údržba budov, nájemné, platy zaměstnanců
[7] v závislosti na výši platby

Banka	Internetové bankovnictví		Telefonické bankovnictví		GSM bankovnictví	
	Zřízení	Vedení	Zřízení	Vedení	Zřízení	Vedení
Česká spořitelna	Zdarma	100,-[8]	Zdarma	100,-	Zdarma	100,-
ČSOB	Zdarma[9]	Zdarma[9]	Zdarma	40,- / 20,-[10]	Zdarma	Zdarma
Poštovní spořitelna	Zdarma	Zdarma	Zdarma	Zdarma	Zdarma	30,-
Komerční banka	Zdarma	44,-	Zdarma	Zdarma	Zdarma	15,-
Ge Money Bank	Zdarma	39,-	Zdarma	39,-	Zdarma	39,-
UniCredit Bank	Zdarma	50,-	Zdarma	50,-	Zdarma	50,-
Bawag Bank	Zdarma	30,-	----------	----------	----------	----------

Tabulka 6: Porovnání poplatků za vedení přímého bankovnictví

[8] Cena je stanovena pro internetové, telefonní a GSM bankovnictví dohromady.
[9] Služba se poskytuje pouze v kombinaci se službou ČSOB Linka 24.
[10] Cena 40 Kč platí při užívání služeb ČSOB Linka 24, cena 20 Kč platí v kombinaci s jinou službou elektronického bankovnictví (cena za každou zmocněnou osob).

5 Současný stav elektronického bankovnictví

5.1 Nabídka českých bank

Každá banka má svou strategii, v rámci které se zaměřuje na příslušný segment trhu. Této strategii je podřízeno technické vybavení i rozsah poskytovaných služeb. V tabulce 7 je uveden souhrn služeb, které nabízejí naše nejvýznamnější banky a odhad procenta klientů dané banky využívajících služeb EB ([23,25]. Údaje platí pro počátek roku 2007.

Banka	Podíl klientů užívající EB	Telefonní a GSM bankovnictví	Internetbanking	Homebanking
Česká spořitelna	cca 20%	Servis 24 Telebanking GSM banking	Servis 24 Interbanking	Business 24 Interbanking
ČSOB	cca 26%	Linka 24 Mobil 24	ČSOB InternetBanking 24	ČSOB BusinessBanking 24
Poštovní spořitelna	cca 43%	Max Phone PS Max Mobil PS	Max Internetbanking PS	Max Homebanking PS
Komerční banka	cca 56%	Expresní linka Mobilní banka	Mojebanka	Profibanka Přímý kanál
GE Money Bank	cca 37%	Telefon Banka Mobil Banka	Internet Banka	BankKlient
eBanka a Raiffeisenbank	Údaje nejsou k dispozici	Telefonní bankéř Mobilní telefon	Internet	ekomunikátor
UniCredit Bank	cca 30%	Telebanking GSM banking	Online Banking	BusinessNet
Volksbank CZ	cca 30%	Phone banking	Internet Banking	Homebanking

Tabulka 7: Souhrn služeb přímého bankovnictví

5.2 Popis služeb elektronického bankovnictví GE Money Bank [24]

GE Money bank nepatří se svými cca 800 tisíci klienty mezi naše největší banky. Významný je však podíl počtu klientů, kteří využívají služby internetového bankovnictví. Banka udává, že tyto služby využívá okolo 300 000 klientů [23]. Banka nabízí tyto služby přímého bankovnictví :

5.2.1 Služby na bankomatech

Bankomaty slouží nejen pro výběr hotovosti, ale umožňují také zjišťování zůstatku na běžném účtu klienta, informace o blížícím se konci platnosti platební karty nebo informace o velikosti půjčky, o kterou může klient požádat.

5.2.2 Telefon Banka

Tato služba umožňuje provádět operace jako zjišťování zůstatků na účtech, zadávání platebních příkazů běžných korunových účtů, získávání aktuálních informací např. o kurzovních lístcích nebo úrokových sazbách prostřednictvím telefonu s tónovou volbou. Při získávání informací tímto způsobem komunikuje klient s automatickým hlasovým systémem. Mezi výhody této služby patří dostupnost informací 24 hodin denně a také výrazně nižší poplatek za uskutečněné transakce ve srovnání s transakcí na pobočce (3 Kč oproti 39 Kč).

5.2.3 Mobil Banka (GSM Banking)

Mobil Banka je bankovní aplikace nahraná ve mobilním telefonu klienta, která mu umožňuje zjišťování zůstatků na účtech, zadávat jednorázové platební příkazy, zadávat nebo rušit trvalé platební příkazy, zjistit si aktuální směnné kurzy a úrokové sazby, dobít předplacenou Go, Vodafone Kartu nebo Twist kartu sobě či komukoliv jinému. Díky službě infolimit může klient zjistit, jak hluboko do minusu ho pustí jeho Flexikredit nebo jak velkou půjčku Expres mu GE Money Bank nabízí. Mezi výhody této služby patří dostupnost informací 24 hodin denně a také výrazně nižší poplatek za uskutečněné transakce ve srovnání s transakcí na pobočce (3 Kč oproti 39 Kč).

5.2.4 Internet Banka

Tato služba umožňuje klientovi (mimo jiné) on-line získávání informací o zůstatcích na všech typech jeho účtů (běžný, spořící, úvěrový ..), zadávání domácích platebních příkazů v CZK, detailní přehled o pohybech na účtech a o platebních příkazech s informací, zda již byly zrealizovány, zadávat, měnit a rušit trvalý příkaz a povolení platby SIPO a inkasa, založení nebo zrušení spořícího účtu či revolvingového termínovaného účtu a převádět peníze z vašeho běžného účtu nebo na váš běžný účet dle vašich potřeb bez nutnosti návštěvy pobočky.

Podle způsobu zabezpečení si klient může zvolit jednu ze dvou variant :

- Internet banka s mobilním klíčem – tato služba je zpřístupněna po zadání identifikačního čísla, hesla a mobilního klíče, všechny aktivní operace je nutné

podepsat mobilním klíčem doručeným na registrovaný mobilní telefon. Přenos dat přes internet je zajištěn šifrováním (SSL, 128 bitů).

- Internet banka s certifikáty - tato služba je zpřístupněna po zadání identifikačního čísla a hesla na počítači s naimportovaným digitálním certifikátem (SSL certifikát). Všechny aktivní operace musí být podepsány digitálním podpisem a přenos dat přes internet je zajištěn šifrováním (SSL, 128 bitů).

5.2.5 BankKlient (Homebanking)

BankKlient je speciální aplikace, která umožňuje propojení účetního programu klienta s bankovním systémem. Je určena pro klienty provádějící vysoký počet bankovních transakcí (podnikatelé, organizace, státní orgány..). Instalace se provádí z CD, které klient obdrží na pobočce banky. Po instalaci systému si klient vygeneruje klíč k elektronickému podpisu a předá ho bance. Poté je služba aktivována a klient ji může využívat.

Komunikace s bankou prostřednictvím BankKlientu je možná buď pomocí internetu nebo pomocí vytáčeného spojení, popřípadě náhradním způsobem na disketách. První dva způsoby komunikace jsou funkčně rovnocenné a je na rozhodnutí klienta, který z nich použije. Při přenosu dat pomocí internetu je použito šifrování SSL s délkou klíče 128 bitů. Každá dávka je autorizována elektronickým podpisem.

Další zvýšení ochrany představuje šifrování dat, která procházejí mezi programem BankKlient a účetním systémem. Data jsou zašifrována volně šířitelným programem GnuPG a opatřena elektronickým podpisem. Návod a podrobný popis této služby je možno stáhnout z internetových stránek GE Money Bank [24].

Alternativou pro použití aplikace BankKlient, je některý z účetních systémů, který podporuje datový formát pro komunikaci s GE Money Bank.

5.3 Popis elektronického bankovnictví ČSOB [4]

5.3.1 ČSOB BusinesBanking 24 Online

Služba určená podnikatelům a firmám k obsluze podnikových financí prostřednictvím osobního počítače s připojením k internetu. Kromě provádění bankovních operací nabízí možnost získávat informace o stavu a pohybech na účtu a podporuje i výměnu dat s účetními systémy. Pro přístup k této službě se zákazník musí zaregistrovat na pobočce, která vede jeho účet. Přihlášení do systému se děje pomocí čipové karty a čtecího zařízení (to musí být připojeno k danému PC, na kterém také musí být nainstalován příslušný ovladač). Při přenosu

dat mezi klientem a bankou je použito šifrování SSL s délkou klíče 128 bitů. ČSOB BusinessBanking umožňuje (mimo jiné) zadávat tuzemské i zahraniční platební příkazy, vytvářet hromadná zadání příkazů k úhradě, exportovat data pro účetní programy, zobrazovat, tisknout a zasílat elektronické výpisy ve formátu PDF, TXT, HTML, XML, získávat informace o zůstatku (aktuálním i disponibilním) a pohybech na účtu.

5.3.2 ČSOB Internetbanking 24

Služba určená občanům, podnikatelům i firmám, která nabízí:

- Informace o účtu – zůstatek, historie, výpisy, podrobné informace.
- Platební operace – příkazy k úhradě, převody mezi účty klienta, trvalé příkazy, svolení k inkasu, dobíjení předplacených SIM karet.
- ČSOB Info 24 – informace o kurzovních lístkách, aktualitách, transakcích platebních karet, doplňkové informace.

Klient si může vybrat ze dvou způsobů autorizace

- Elektronickým podpisem – klient musí mít k počítači připojenou čtečku čipových karet, instalovaný certifikát certifikační autority I.CA v prohlížeči, platný certifikát na čipové kartě pro přihlašování a podepisování příkazů zasílaných ČSOB .
- SMS klíčem – klient navíc potřebuje mobilní telefon podporující technologii SIM Toolkit s aktivovanou službou ČSOB Mobil 24 pro příjem šifrovaných SMS zpráv.

Přihlášení je možné

- Identifikačním číslem a PINem
- Identifikačním číslem, PINem a SMS klíčem
- Certifikátem k elektronickému podpisu (na čipové kartě)

5.3.3 ČSOB Mobil 24

Služba určená občanům, podnikatelům i firmám, která umožňuje přistupovat k účtu prostřednictvím mobilního telefonu. Zabezpečení dat je provedeno šifrováním datového přenosu. Každá SIM karta má své šifrovací klíče.

Pro úspěšnou komunikace s bankou musí klient vlastnit

- mobilní telefon podporující technologii SIM Toolkit
- bankovní SIM kartu některého mobilního operátora - T-Mobile, Telefónica O2 nebo Vodafone

Tato služba nabízí :

- získání informace – o aktuálním zůstatku na vybraném účtu, o historii zaúčtovaných položek, o kurzech vybraných měn, o úrokových sazbách ČSOB
- provedení transakcí – příkazy k úhradě v rámci tuzemského platebního styku, převody prostředků mezi účty jednoho klienta ve stejné měně, možnost zřízení trvalého příkazu
- dobíjení předplacené SIM karty daného operátora
- přijímat šifrované SMS z ČSOB

5.3.4 Kvalifikované certifikáty

Služba určená občanům, podnikatelům i firmám, které potřebují elektronický podpis vydaný v souladu se zákonem o elektronickém podpisu. Kvalifikovaný certifikát tohoto podpisu umožní komunikaci s úřady státní správy a s dalšími komerčními subjekty, které ho akceptují.

5.4 Účetní systémy podporující elektronické bankovnictví

Firmy využívající služeb elektronického bankovnictví mohou buď využít softwarové aplikace, které nabízí přímo daná banka (např. již zmiňovaný program BankKlient), nebo mohou použít některý z účetních systémů, který podporuje vstupní a výstupní formát dat dané banky.

5.4.1 Money S3 [26]

Je to ekonomický systém určený pro malé a střední firmy. Pracuje s univerzálními formáty ABO (využívaný např. v GE Money Bank), GEMINY a MULTICASH. Dále podporuje konkrétní formáty bankovních domů jako jsou KB, ČSOB, ČS a další. Mezi možnostmi, které nabízí (např. podvojné účetnictví,a daňová evidence..) je i homebanking.

5.4.1.1 Homebanking

Tato služba umožňuje realizovat :

1) Příkazy k úhradě – program za pomoci průvodce připraví data ve formátu vhodném pro konkrétní komunikační program banky a zabezpečí i jeho spuštění. Postačí, když si jednorázově nastavíte u konkrétního bankovních účtu jeho propojení na zvolený homebanking.

2) Výpis z účtů, kurzy devizového trhu – díky obousměrné komunikace s bankou program zajistí funkce výpis z účtu. Klientovi umožní importovat a spravovat výpisy z bankovního

účtu a ulehčí mu tak od procházení stovek položek bankovních výpisů. Průvodce výpisem z účtu umí výpis nejenom vytisknout, ale na přání i automaticky spárovat s příslušnými pohledávkami nebo závazky a zaúčtovat. Navíc je možnost načítat kurzovní lístky některých bank.

5.4.2 Ekonomický systém POHODA [28]

Je to komplexní účetní, ekonomický a informační systém pro malé až střední firmy. Podporuje formáty dat pro komunikaci s bankovními domy, jako jsou: Komerční banka, Citibank, ČSOB, eBanka, GE Money bank, Živnostenská banka a HVB Bank. Dále podporuje formát Gemini používaný pobočkami německých bank, formát MultiCash. Podporuje také formát pro automatizované bankovní operace ABO a Office Line, který používá Česká spořitelna, Erste bank, Raiffeisenbank a další bankovní domy.

5.4.2.1 Homebanking

Je to sada funkcí, která umožňuje:

1) Výpisy z účtů – všechny zvolené výpisy, třeba i z různých bank, načte a postupně provede spárování, likvidaci a zaúčtování všech položek. Nakonec o provedené akci vytvoří přehledný zápis pro snadnou kontrolu ze strany klienta.

2) ***Příkazy k úhradě*** - všechny zvolené příkazy k úhradě uloží do souborů ve formátu dané banky, které poté stačí načíst do příslušného komunikačního programu a odeslat do banky elektronickou cestou. Podporovány jsou i příkazy k úhradě v cizí měně

3) ***Kurzové lístky*** - umožňuje načíst kurzy cizích měn z internetových stránek ČNB, nebo denní kursový lístek KB.

5.4.3 Systém KASKÁDA [27]

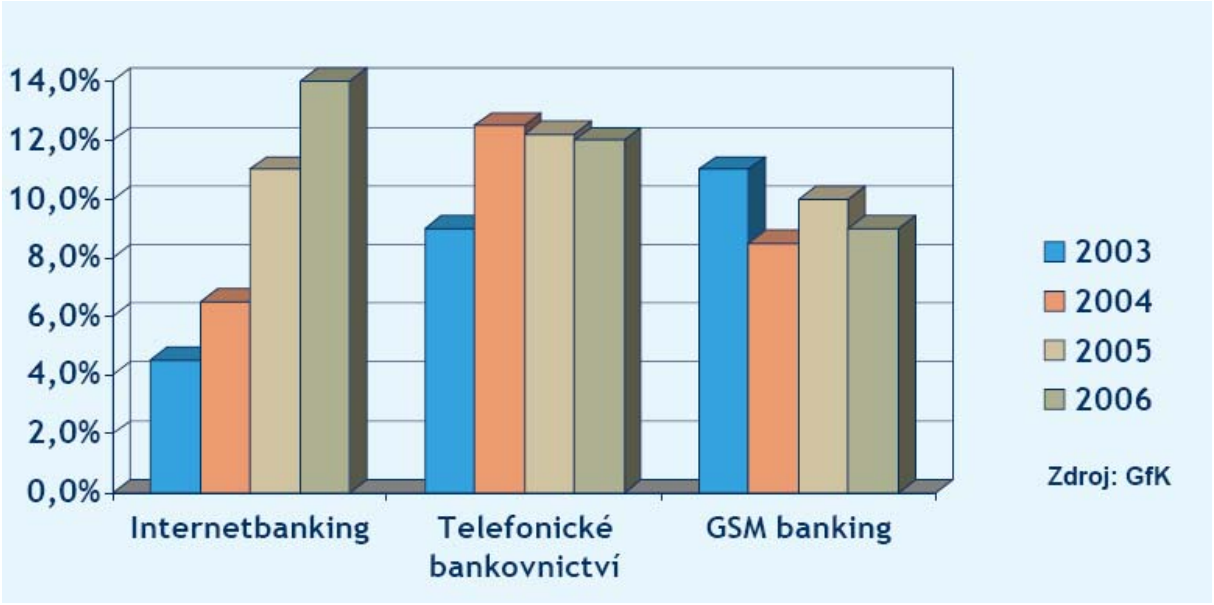
Je to informační systém, který mimo jiné umožňuje ekonomickou agendu, v rámci které nabízí:

- Platby faktur v libovolných měnách s automatickými přepočty kurzů, řešení kurzovních rozdílů.
- Veškeré operace provázané s příslušnými doklady, s obchodními partnery a s jejich evidovanými bankovními účty, samozřejmostí je průmět všech operací do účetnictví.
- Elektronická komunikace s bankou v obou směrech, tedy tvorba platebních příkazů i zpracování výpisů, automatické párování plateb s možnosti ručních zásahů

Podporuje formáty (jak importní, tak exportní) ABO (Komerční banka, Česká spořitelna, GE Money Bank, ČSOB), BEST formát KB (Komerční banka), MultiCash tuzemský (Česká spořitelna, RaiffeisenBank).

5.5 SWOT analýza současného stavu internetového bankovnictví

Z široké škály služeb elektronického bankovnictví se v současnosti nejvýznamněji prosazuje Internetbanking – jak je vidět např. na obrázku 10, kde je zobrazen časový vývoj využívání jednotlivých komunikačních kanálů mezi bankou a klientem (zdroj[11]). Domnívám se, že tento vývoj je způsoben širší dostupností internetu mezi klienty bank. Ti pak začínají využívat možnosti internetového bankovnictví na úkor bankovnictví telefonického a GSM bankovnictví.



Obrázek 10: Využití jednotlivých kanálů přímého bankovnictví

Z tohoto důvodu jsem se rozhodla provést SWOT analýzu současného stavu nikoliv celého elektronického bankovnictví, což je široký pojem s mnoha specifikami, ale pouze internetového bankovnictví.

[11] analýza mezi uživateli internetu, kterou vypracovala společnost Network Media Service (NMS). Publikováno www stránkách ČSOB

SWOT[12] [16] analýza je komplexní metoda kvalitativního vyhodnocení veškerých relevantních stránek fungování firmy (popř. problémů řešení, projektů atd.) a její současné pozice. Je silným nástrojem pro celkovou analýzu vnitřních i vnějších činitelů a v podstatě zahrnuje postupy technik strategické analýzy.

SWOT je zkratkou anglických slov

- Strengths (přednosti=silné stránky)
- Weaknesses (nedostatky=slabé stránky)
- Opportunities (příležitosti)
- Threats (hrozby)

SWOT analýza představuje kombinaci dvou analýz, S - W a O - T. Jádro této metody spočívá v klasifikaci a ohodnocení jednotlivých faktorů, které jsou rozděleny do čtyř základních skupin:

- Faktory vyjadřující silné nebo slabé vnitřní stránky organizace (tzv. SW analýza)
- Faktory vyjadřující příležitosti a nebezpečí jako vlastnosti vnějšího prostředí (tzv. OT analýza)

SWOT analýza vychází z předpokladu, že podnik dosáhne strategického úspěchu maximalizací předností a příležitostí a minimalizací nedostatků a hrozeb.

Schéma SWOT analýzy :

	S - silné stránky	W - slabé stránky
O – příležitosti	Strategie SO (využít silné stránky na získání výhody)	Strategie WO (překonat slabiny využitím příležitostí)
T- hrozby	Strategie ST (využít silné stránky na čelení hrozbám)	Strategie WT (minimalizovat náklady a čelit hrozbám)

Tabulka 8: Schéma SWOT analýzy

S-W analýza umožňuje identifikaci a hodnocení vnitřních silných a slabých stránek. Jsou identifikovány ty důležité silné stránky, ze kterých lze vycházet při stanovení další strategie vývoje. Slabé stránky identifikují ty faktory, které by měly být v rámci dalšího vývoje řešeny. Je ovšem důležité řešit pouze ty faktory, které mají zásadní význam, a odstranění kterých přinese očekávaný efekt.

O-T analýza umožňuje rozlišit atraktivní příležitosti, které mohou firmě (projektu) přinést výhody. Současně též nabádá k zamyšlení nad problémy, se kterými bude firma (projekt)

[12] Tato analýza byla vyvinuta Albertem Humphreym, který vedl v 60. a 70. letech výzkumný projekt na Stanfordově univerzitě, při němž byla využita data od 500 nejvýznamnějších amerických společností.

zápasit. Příležitosti by měly být posuzovány z hlediska jejich atraktivnosti a pravděpodobnosti úspěchu. Naopak rizika z hlediska vážnosti a pravděpodobnosti nastání rizikové události.

5.5.1 Silné stránky

- Při vykonávání bankovních operací nemusí klient navštívit banku
- Klient není vázán na otevírací dobu banky
- Klient nemusí komunikovat s bankou jen z jednoho místa
- Banka realizuje příslušné transakce s nižšími náklady
- Pro klienta je tato služba pohodlná a komfortní
- Klientovi se zobrazí (např. na monitoru nebo displeji telefonu) jen ty data, která ho zajímají)
- Cenová výhodnost pro klienta – příkazy zadávané elektronickou formou jsou levnější než příkazy zadávané osobně u přepážky banky
- Automatizací procesu se na straně banky snižuje riziko chybného zpracování transakce klienta
- Možnost snadného získání zpětných výpisů z účtů klienta
- Možnost zavedení doplňkových služeb (např. dobíjení předplacených karet mobilních operátorů, nebo tzv. e-messages, které mohou klienta informovat o různých událostech na jeho účtu pomocí e-mailu či SMS)
- Možnost lepší kontroly nad účtem

5.5.2 Slabé stránky

- Klient musí mít k dispozici dané technické vybavení
- Klient toto zařízení musí umět ovládat
- Vyšší náklady pro banku na zřízení a provoz systému elektronického bankovnictví
- Nutnost zajištění jednoznačné identifikace klienta (bez osobního kontaktu)
- Nutnost zajištění vysokého stupně bezpečnosti na straně banky
- Nutnost zajištění vysokého stupně bezpečnosti na straně klienta
- Nutnost zajištění vysokého stupně zabezpečení komunikace mezi klientem a bankou
- Složitější pozice banky při nabídce dalších služeb (není osobní kontakt)
- Podvědomé podceňování základních bezpečnostních pravidel ze strany některých klientů

5.5.3 Příležitosti

- Možnost neustálého rozšiřování poskytovaných služeb
- Možnost vylepšení a zatraktivnění již zavedených služeb
- Možnost zaujmout a získat novou (zpravidla bonitní klientelu)
- Oblíbenost EB u studentů (obecně u mladé generace), kteří pak zprostředkují kontakt s EB i ostatním členům rodiny, kteří buď EB nedůvěřují nebo nemají patřičně znalosti o používané technologii
- Další ušetření pracovní síly v bance
- Rozvoj internetu a jeho lepší přístupnost a vyšší rychlost umožňuje i lepší přístupnost a větší atraktivitu EB
- Informační kampaň, která přesvědčí další klienty, že EB je bezpečné, a která jim představí výhody EB

5.5.4 Hrozby

- Výpadek bankovních serverů, které způsobí nefunkčnost služby pro zákazníky
- Napadení bankovních serverů (např. hackery)
- Možnost odposlechu komunikace mezi klientem a bankou
- Možnost napadení klientova počítače a následné zneužití odcizených dat

5.5.5 Zhodnocení rizik internetového bankovnictví

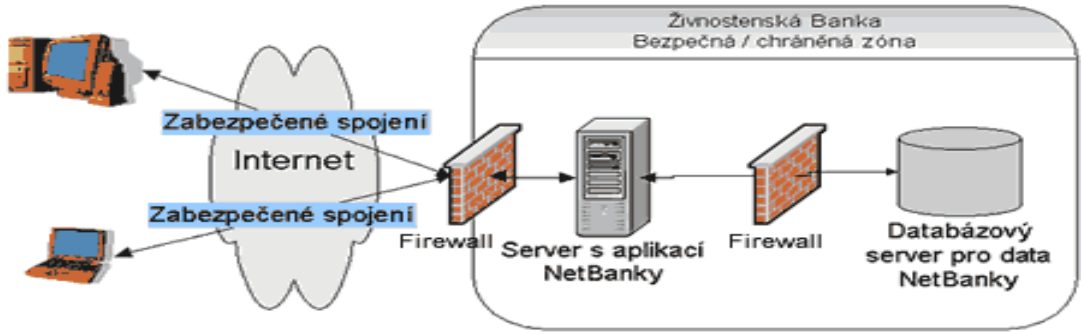
1. **Výpadek bankovních serverů, které způsobí nefunkčnost služby pro všechny zákazníky**: vždy existuje nenulová pravděpodobnost, že nastane událost tohoto typu. Ovšem toto riziko lze snížit na minimum zavedením vhodných opatření (například zálohováním dat na bankovních serverech, zálohováním jejich napájení, připojením k internetu prostřednictvím několika různých poskytovatelů internetových služeb, ochrana systému banky proti útoku typu přehlcení[13] ….).

2. **Napadení bankovních serverů (např. hackery)**: banky investují velké finanční prostředky pro zajištění a neustálou kontrolu bezpečnosti svého bankovního systému. Příkladem takových opatření může být například to, že systém elektronického bankovnictví běží na jiném serveru (počítači) než na kterém jsou uložena data klientů. Proto se domnívám, že pravděpodobnost události tohoto typu je velmi nízká. Na obrázku 11 (zdroj [14])je vidět

[13] Jedná se o zahlcení serveru neustále se opakujícími požadavky, které jsou účelně generovány ve velkém množství v co možná nejkratším časovém úseku.
[14] http://www2.ziba.cz/cs/netbanka/informace.html

schéma ochranných prvků internetového bankovnictví v Živnostenské bance (dnes už UniCredit Bank Czech Republic).

3. Možnost odposlechu komunikace mezi klientem a bankou: veškerá komunikace mezi klientem a jeho bankou probíhá v šifrované podobě. Všechny naše banky používají k šifrování SSL protokol (viz. tabulka 4 v kapitole 4.3.2.4). Potenciální útočník tedy zachytí pouze šifrované zprávy. Vzhledem k délkám šifrovacích klíčů, které všechny naše banky používají, je prolomení šifry natolik výpočetně a časově náročné, že se běžně pokládá za prakticky vyloučené. Domnívám se, že událost tohoto typu neznamená pro internetové bankovnictví zásadní nebezpečí.



Obrázek 11: Schéma ochranných prvků v Živnostenské bance

4. **Možnost napadení klientova počítače a následné zneužití odcizených dat**: pro laického uživatele může být problém udržovat zabezpečení svého počítače na dostatečné úrovni tak, aby na něj nikdo nemohl nainstalovat programy umožňující dálkovou správu včetně odečítání klávesnice (získání hesla), kopírování souborů (certifikátu), případně podvržení zobrazované informace. Velmi rizikové může být využívání služeb internetového bankovnictví na počítačích např. v elektronických kavárnách, kde uživatel nemá kontrolu nad tím, jaké programy (ať už škodlivé, či nikoliv) jsou nainstalovány. Problémem může být i podcenění bezpečnosti ze strany klienta např. zadáním cesty ke svému digitálnímu certifikátu a jeho hesla - příkladem pokusu o vylákání těchto citlivých údajů je případ ze 6. 3. 2007, kdy byl jeden se zákazníků internetového bankovnictví Raiffeisenbank přesměrován na falešné stránky této banky a vyzván – naštěstí pro něj ne příliš obvyklým způsobem, k zadání hesla a cesty k podpisovému certifikátu – viz. obrázek 12 (zdroj [13]). V tomto konkrétním případě, i díky zkomolené češtině na falešné stránce, klient žádné citlivé údaje neuvedl a kontaktoval banku. Podle mého názoru představují události tohoto typu největší ohrožení bezpečnosti internetového bankovnictví.

Obrázek 12: Podvodná stránka internetového bankovnictví Raiffeisenbank

6 Předpoklad dalšího vývoje EB

Domnívám se, že počet klientů využívajících služby elektronického bankovnictví v budoucnu poroste. Jedním z důvodů tohoto růstu je neustále se zlepšující přístup uživatelů k internetu (také i pokles ceny připojení a jeho zvyšující se rychlost). Druhým důvodem je vývoj a vylepšování služeb elektronického bankovnictví tak, aby více vyhovovaly požadavkům klientů. Hybnou silou pro tento vývoj a rozšiřování nabídky služeb je snaha jednotlivých bank uspět v ostrém konkurenčním boji o klienta.

Klientům z řad velkých firem, pro které je nutností automatická výměna dat s co nejmenším podílem lidské obsluhy, budou banky umožňovat větší provázanost mezi účetním programem a bankovním systémem. Pokračovat bude snaha o zjednodušení komunikace. Již dnes nabízejí některé banky možnost provozování homebankingu bez nutnosti instalace speciální bankovní aplikace – s bankovním systémem komunikuje přímo účetní program.

Pro drobnou klientelu, která využívá širokou nabídku jednotlivých produktů elektronického bankovnictví, budou banky svoji nabídku zdokonalovat. Očekávám, že banky nabídnou ještě více přátelštější design a intuitivní ovládání internetového bankovnictví, minimalizaci časových nároků – např. prodlev při získávání informací pomocí telefonního bankovnictví. Očekávám dále doplnění funkcí, které souvisí s prodejem bankovních produktů, např. prodej akcií, a také minimalizaci papírových výpisů ve prospěch elektronických, které budou finančně zvýhodněny (dnes tuto možnost nabízí GE Money Bank, ale bez finančního zvýhodnění).

Značnou pozornost budou banky i v budoucnu vynakládat na zabezpečení přímého bankovnictví. Při výběru jednotlivých bezpečnostních prvků však budou zohledňovat i jiné faktory (například cena, rychlost, jednoduchost, ovladatelnost, uživatelský komfort…) a budou se snažit mezi nimi vytvořit rovnováhu. Domnívám se, že se banky budou soustředit na nejslabší článek elektronického bankovnictví, a to na zabezpečení na straně klienta. Například formou různých reklamních nebo informačních kampaní mohou zvyšovat povědomí klientů o této problematice a přispívat tak k tomu, že klienti budou brát nutnost zabezpečení jako svoji prioritu.

Informační kampaně mohou být přínosné i z dalšího důvodu - pro získávání nových klientů, například seniorů, kteří zatím mají k těmto službám určitou nedůvěru, často pramenící z nízkých znalostí používané technologie. Největší pozornost však banky budou i nadále věnovat jiné skupině potencionálních klientů, a to studentům, především VŠ. Banky

předpokládají, že pokud je student spokojen s bankou už během studií, bude jejím klientem i do budoucna.

Díky očekávanému vstupu zahraničních bank na český bankovní trh se elektronické bankovnictví ještě více rozšíří. S tím souvisí případné snížení nákladů, neboť banky budou moci snížit počet zaměstnanců. S tímto rozšiřováním, vzhledem k nižší počítačové gramotnosti některých klientů, bude pravděpodobně souviset nárůst neoprávněných manipulací s účty klientů, na což budou muset banky reagovat, například zablokováním převodu do ciziny, zablokováním netypického příkazu s následným dotazem u klienta, či nutností dalších potvrzujících operací.

Závěr

Elektronické bankovnictví je dynamicky se rozvíjející obor, ve kterém se velmi rychle smazává hranice mezi minulostí, současností a budoucím vývojem. To co je dneska současnost se velmi rychle stává minulostí a budoucnost rychle přechází v současný stav. Proto je velmi důležité mít přehled nejen o současném stavu, ale i sledovat nové trendy. O to jsem se snažila ve své práci.

Určila jsem možné příčiny vzniku, stručně shrnula jeho historii a popsala současný stav, včetně konkrétních služeb dvou našich bank – ČSOB a GE Money bank. Při charakteristice elektronického bankovnictví z hlediska nákladů klienta jsem zjistila, že ve srovnání s operacemi prováděnými na pobočkách jednotlivých bank je využívání elektronických kanálů pro klienta jednoznačně výhodnější. Při porovnání nákladů jsem neshledala významné rozdíly mezi vybranými bankami.

Podrobně jsem se věnovala problematice bezpečnosti. Pro každý kanál existují konkrétní rizika, která klient, nebo banka při využití služeb přímého bankovnictví podstupují. Tyto rizika jsem se snažila objasnit, i na základě příkladů z praktického života, a zároveň jsem určila optimální způsoby zabezpečení, které je, alespoň částečně, eliminují. Absolutně zaručit bezpečnost však nebude možné ani v budoucnu, například proto, jak zmiňuji v kapitole 7, že se nedá od všech klientů využívajících služeb elektronického bankovnictví předpokládat dostatečná počítačová gramotnost.

V závěru své práce jsem provedla analýzu v současnosti nejpoužívanějšího kanálu elektronického bankovnictví – internetbankingu a na jejím základě jsem se pokusila nastínit budoucí vývoj přímého bankovnictví. Ten spočívá dle mého názoru v neustálém zkvalitňování služeb jednotlivých bank tak, aby zaujaly a přitáhly co nejvíce nových zákazníků. Domnívám se, že z pohledu klientů je tento vývoj jenom ku prospěchu.

Seznam použité literatury

[1] Pavel Juřík: Encyklopedie platebních karet , Grada Publishing, a.s., 2003, ISBN 80247-0685-7

[2] Michal Přádka, Jan Kala: Elektronické bankovnictví, Computer press, 2000, ISBN 8072263285

[3] Miroslav Máče: Elektronický platební styk, Grada Publishing, a.s., 2006, ISBN 8024717255

[4] Webové stránky ČSOB http://www.csob.cz/bankcz/cz/Csob/Servis-pro-media/Elektronicka-reseni-pro-komfort-klientu.htm (elektronický zdroj) [cit. září 2006]

[5] Webové stránky společnosti Symantec http://www.symantec.com/cs/cz/norton/library/article.jsp?aid=article1_08_06 (elektronický zdroj) [cit. Srpen 2006]

[6] Webový server Finance.cz http://www.finance.cz/zpravy/finance/63677/ (elektronický zdroj) [cit. březen 2006]

[7] Webový server Měšec.cz http://www.mesec.cz/clanky/komercni-banka-vykradeni-uctu-potvrzeno/ (elektronický zdroj) [cit. srpen 2006]

[8] Webové stránky Ministerstva Vnitra CŘ http://www.mvcr.cz/prevence/obcanum/publik/ts/2004/prosinec.doc (elektronický zdroj) [cit. prosinec 2004]

[9] Webové stránky Marketingových novin http://www.marketingovenoviny.cz/index.php3?Action=View&ARTICLE_ID=4607 (elektronický zdroj) [cit. říjen 2006]

[10] Fred Piper, Sean Murény: Kryptografie - průvodce pro každého, nakladatelství Dokořán, 2006, ISBN 80-7363-074-5

[11] Webový server Peníze.cz http://www.penize.cz/produkty/platebni-karty/texty/1969/platebni-karty-a-jejich-druhy/?IDP=1& (elektronický zdroj) [cit. prosinec 2007]

[12] Webové stránky Idnes.cz http://mobil.idnes.cz/mob_tech.asp?r=mob_prakticky&c=A011207_0045726_mob_prakticky (elektronický zdroj) [cit. prosinec 2001]

[13] Webový server FinExpert.cz
http://www.finexpert.cz/default.aspx?section=17&server=1&article=18645
(elektronický zdroj) [cit. březen 2007]

[14] Webová verze zpravodaje ÚVT Masarykovy univerzity
http://www.ics.muni.cz/zpravodaj/articles/561.html
(elektronický zdroj) [cit. říjen 2007]

[15] Webové stránky ElisMendelu – studentský server
http://elis.mendelu.cz/metodika/ukazky/kapitola6.html
(elektronický zdroj) [cit. prosinec 2006]

[16] Webový portál Stavební technologie
http://www.stavebnitechnologie.cz/view.php?cisloclanku=2002041701
(elektronický zdroj) [cit. duben 2002]

[17] Webový archiv článků a přednášek J. Peterky (nezávislý konzultant a publicista)
http://www.earchiv.cz/b01/b0600001.php3 (elektronický zdroj) [cit. červen 2001]

[18] Webové stránky ING banky
http://www.ing.cz/cz/interbank/desatero-bezpecneho-internetoveho-bankovnictvi/
(elektronický zdroj) [cit. prosinec 2007]

[19] Webový server Měšec.cz
http://i.iinfo.cz/urs-att/Mesec.cz-studie_int.bankovnictvi-112002647608700.pdf
(elektronický zdroj) [cit. červen 2005]

[20] Webový server Peníze.cz http://www.penize.cz/zpravy/3525/internetova-banka-roku-startuje/ (elektronický zdroj) [cit. duben 2005]

[21] Webový server FinExpert.cz
http://www.finexpert.cz/Rubriky/Prime-bankovnictvi-v-Cesku/sc-17-sr-1-a-17385/default.aspx (elektronický zdroj) [cit. srpen 2006]

[22] Webové stránky Ceed (Centrum pro rozvoj a vzdělání)
http://www.ceed.cz/bankovnictvi/779vyvoj_elektornickeho_bankovnictvi.htm
(elektronický zdroj) [cit. prosinec 2007]

[23] Webový server Bankovnictví.ihned.cz http://bankovnictvi.ihned.cz/3-21386380-bankingu-900000_d-16 (elektronický zdroj) [cit. červen 2007]

[24] Webové stránky GE Money Bank http://www.gemoney.cz/ge/cz/1/prime-bankovnictvi/internet-banka (elektronický zdroj) [cit. prosinec 2007]

[25] Webový server peníze.cz http://www.penize.cz/zpravy/5553/ceske-banky-na-internetu-dohaneji-evropu/ (elektronický zdroj) [cit.listopad 2007]

[26] Webové stránky společnosti Cígler : http://www.money.cz/ (elektronický zdroj) [cit. prosinec 2007]

[27] Webové stránky informačního systému KASKÁDA : http://www.ekaskada.cz/ [cit. prosinec 2007]

[28] Webové stránky společnosti Stormware http://www.stormware.cz/pohoda/ [cit. prosinec 2007]

Seznam obrázků

Seznam tabulek