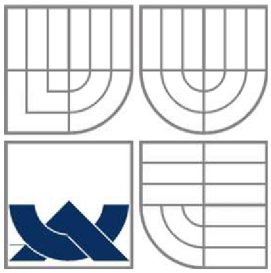
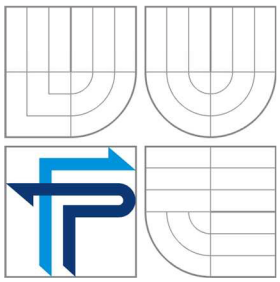


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA PODNIKATELSKÁ
ÚSTAV INFORMATIKY

FACULTY OF BUSINESS AND MANAGEMENT
DEPARTMENT INFORMATICS

NÁVRH ZABEZPEČENÍ FINANČNÍCH TRANSAKCÍ V ELEKTRONICKÉM BANKOVNICTVÍ

FINANCIAL TRANSACTION SECURITY IN ELECTRONIC BANKING PROPOSAL

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR

PETR VALINA

VEDOUCÍ PRÁCE
SUPERVISOR

Ing. KŘÍŽ JIŘÍ, Ph.D.

BRNO 2007

Vysoká škola: Vysoké učení technické v Brně | Akademický rok: 2006/2007

Fakulta: podnikatelská | Ústav: informatiky

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Petr Valina

6209R021 - Manažerská informatika

Ředitel ústavu v souladu se zákonem č. 111/1998 o vysokých školách, Studijním a zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských a magisterských studijních programů Vám zadává bakalářskou práci s názvem:

Návrh zabezpečení finančních transakcí v elektronickém bankovnictví

Financial transaction security in electronic banking proposal

Pokyny pro vypracování:

Úvod
Vymezení problému a cíle práce
Analýza problému a současné situace
Teoretická východiska práce
Vlastní návrhy řešení, přínos (efektivnost) návrhů řešení
Závěr
Seznam použité literatury
Přílohy

Rozsah grafických prací:	dle potřeby
Rozsah původní zprávy:	cca 40 stran

Seznam odborné literatury:

PŘADKA, M.: Elektronické bankovnictví. Praha, Computer Press 2000, 166 s. ISBN 80-7226-328-5
FRIMMEL, M.: Elektronický obchod: právní úprava. Praha, Prospektrum 2002, 321 s. ISBN 81-7175-114-6
SCHLOSSBERGER, O.: Elektronické platební prostředky. Praha, Bankovní institut vysoká škola 2005, 144 s. ISBN 80-7265-073-4
MÁČE, M.: Platební styk . Praha, Grada 2006, 220 s. ISBN 80-247-1725-5
GRUBLOVÁ, E.: Internetová ekonomika. Ostrava, Repronis 2002, 88 s. ISBN 80-7329-000-6

Vedoucí bakalářské práce:	Ing. Jiří Kříž, Ph.D.
Datum zahájení bakalářské práce:	31. října 2006
Datum odevzdání bakalářské práce:	31. května 2007

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
Fakulta podnikatelská
L. S.

Ing. Jiří Kříž, Ph.D.
Ředitel ústavu

Doc. Ing. Miloš Koch, CSc.
Děkan

V Brně dne: 16. února 2007

LICENČNÍ SMLOUVA
POSKYTOVANÁ K VÝKONU PRÁVA UŽÍT ŠKOLNÍ DÍLO

uzavřená mezi smluvními stranami:

1. Pan/paní

Jméno a příjmení: Petr Valina

Bytem: Nezvalova 20, Bruntál 79201

Narozen/a (datum a místo): 27.2.1984 v Bruntále

(dále jen „autor“)

a

2. Vysoké učení technické v Brně

Fakulta podnikatelská

se sídlem Kolejní 2906/4, 612 00, Brno

jejímž jménem jedná na základě písemného pověření děkanem fakulty:

.....

(dále jen „nabyvatel“)

Čl. 1
Specifikace školního díla

1. Předmětem této smlouvy je vysokoškolská kvalifikační práce (VŠKP):
   - □ disertační práce
   - □ diplomová práce
   - □ bakalářská práce
   - □ jiná práce, jejíž druh je specifikován jako .....

   (dále jen VŠKP nebo dílo)

Název VŠKP:	Návrh zabezpečení finančních transakcí v elektronickém bankovnictví
Vedoucí/ školitel VŠKP:	Ing. Jiří Kříž, Ph.D.
Ústav:	Ústav informatiky
Datum obhajoby VŠKP:	

VŠKP odevzdal autor nabyvateli v*:

- □ tištěné formě – počet exemplářů ……..
- □ elektronické formě – počet exemplářů ……..

* hodící se zaškrtněte

1. Autor prohlašuje, že vytvořil samostatnou vlastní tvůrčí činností dílo shora popsané a specifikované. Autor dále prohlašuje, že při zpracovávání díla se sám nedostal do rozporu s autorským zákonem a předpisy souvisejícími a že je dílo dílem původním.
2. Dílo je chráněno jako dílo dle autorského zákona v platném znění.
3. Autor potvrzuje, že listinná a elektronická verze díla je identická.

Článek 2
Udělení licenčního oprávnění

1. Autor touto smlouvou poskytuje nabyvateli oprávnění (licenci) k výkonu práva uvedené dílo nevýdělečně užít, archivovat a zpřístupnit ke studijním, výukovým a výzkumným účelům včetně pořizovaní výpisů, opisů a rozmnoženin.
2. Licence je poskytována celosvětově, pro celou dobu trvání autorských a majetkových práv k dílu.
3. Autor souhlasí se zveřejněním díla v databázi přístupné v mezinárodní síti
   - □ ihned po uzavření této smlouvy
   - □ 1 rok po uzavření této smlouvy
   - □ 3 roky po uzavření této smlouvy
   - □ 5 let po uzavření této smlouvy
   - □ 10 let po uzavření této smlouvy

   (z důvodu utajení v něm obsažených informací)
4. Nevýdělečné zveřejňování díla nabyvatelem v souladu s ustanovením § 47b zákona č. 111/ 1998 Sb., v platném znění, nevyžaduje licenci a nabyvatel je k němu povinen a oprávněn ze zákona.

Článek 3
Závěrečná ustanovení

1. Smlouva je sepsána ve třech vyhotoveních s platností originálu, přičemž po jednom vyhotovení obdrží autor a nabyvatel, další vyhotovení je vloženo do VŠKP.
2. Vztahy mezi smluvními stranami vzniklé a neupravené touto smlouvou se řídí autorským zákonem, občanským zákoníkem, vysokoškolským zákonem, zákonem o archivnictví, v platném znění a popř. dalšími právními předpisy.
3. Licenční smlouva byla uzavřena na základě svobodné a pravé vůle smluvních stran, s plným porozuměním jejímu textu i důsledkům, nikoliv v tísni a za nápadně nevýhodných podmínek.
4. Licenční smlouva nabývá platnosti a účinnosti dnem jejího podpisu oběma smluvními stranami.

V Brně dne: …….

…….. ……
Nabyvatel Autor

Abstrakt

Bakalářská práce analyzuje elektronické bankovnictví z hlediska využití a použitých technologií a z hlediska bezpečnosti. Nabízí srovnání konkrétních typů elektronického bankovnictví používaných v současné době. Nedílnou součástí je analýza možných hrozeb při používání elektronického bankovnictví a také návrh řešení, který upravuje interakci mezi bankou a klientem a navrhuje jejich chování, za účelem minimalizace bezpečnostních rizik.

Klíčová slova:

Elektronické bankovnictví, internetové bankovnictví, phishing, zabezpečení počítače, bezpečná práce s internetem, spyware

Abstract

Bachelor's thesis analyses electronic banking in the term of utilization, used technologies and with respect to security. It shows comparison of concrete types of electronic banking, which are being used at present. Analysis of possible risk by using electronic banking and solution proposal, which sets up interaction between bank and its client and makes behavior proposal for minimizing of security risks are integral part of this bachelor's thesis.

Keywords:

Electronic banking, internet banking, phishing, secure usage of computer, internet security, spyware

Bibliografické citace

VALINA, P. *Návrh zabezpečení finančních transakcí v elektronickém bankovnictví.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2007 72 s. Vedoucí bakalářské práce Ing. Jiří Kříž, Ph.D.

Čestné prohlášení

Prohlašuji, že předložená bakalářská práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem v práci neporušil autorská práva (ve smyslu zákona č. 121/2000 Sb. o právu autorském a o právech souvisejících s právem autorským).

V Brně, dne 31.5.2007 ……

podpis

Poděkování

Děkuji vedoucímu bakalářské práce Ing. Jiřímu Křížovi, Ph.D. za velmi užitečnou metodickou pomoc a cenné rady při zpracování bakalářské práce. Můj dík v neposlední řadě patří také mé rodině, která mi svojí vstřícností a tolerancí vytvořila skvělé podmínky nejen pro psaní této bakalářské práce, ale i pro samotné studium na FP VUT v Brně.

OBSAH

ÚVOD

Jak každý člověk dobře ví, v několika málo posledních letech proběhla obrovská expanze nejenom informačních a komunikačních technologií do života obyčejných lidí. Nebudu v úvodu popisovat, jak toto rozšíření nových technologií ovlivnilo naše životy, protože téměř v každém informačním médiu denně najdeme mnoho článků, které nám tyto nové trendy nebo samotné způsoby užití celkem obstojně popisují a radí, zda a jakým způsobem bychom je měli používat v běžném životě. Spíše se zaměřím na důvod, proč jsem si právě toto téma vybral.

Právě na rozšíření internetu a ostatních technologií, jako jsou mobilní telefony, bylo nutné v komerční sféře velmi brzo reagovat, aby si každá společnost, která se hodlá angažovat, mohla ukousnout onen pomyslný kus koláče. Nejinak tomu bylo i v bankovnictví. Peníze hrály, hrají a nepochybně budou hrát důležitou roli v našich životech, ať už si to přiznáme, či nikoliv. Proto vznikly bankovní ústavy, které se o naše jmění budou, ne zadarmo, starat. Tyto konkrétní bankovní ústavy musely samozřejmě nějakým způsobem reagovat na změny a nové trendy, některé byly úspěšné, jiné už méně, nicméně výsledkem je velké množství nabízených bankovních produktů, které využívají nejnovější technologie.

Časy, kdy si lidé své úspory schovávali pod polštář, nebo do postele jsou nenávratně pryč a protože každého zajímá, kde a za jakých podmínek budou jeho peníze v bezpečí, vzniká tato práce. V podstatě zde budu analyzovat bankovní produkty, které jsou v současné době dostupné na našem trhu z hlediska využitých technologií a dále se budu objektivně snažit analyzovat celkové riziko při konkrétním užití těchto služeb, zejména z pozice zákazníka, chcete-li klienta.

1 VYMEZENÍ PROBLÉMU, STANOVENÍ CÍLŮ A METOD

1.1 Vymezení problému

V současné době nabízí banky stávajícím, nebo potenciálním klientům řadu produktů využívající moderní technologické trendy, které jsou na první pohled bezpečnější, levnější a časově méně náročné. Stále více lidí tyto produkty začíná využívat v běžném životě a většina si neuvědomuje, že jsou jejich peníze v ohrožení.

Stejně jako v životě na ulici najdeme zloděje a lháře, výjimkou není ani cyberprostor, kde jsou uložené naše peníze. Tato skutečnost se až do nedávné doby jistým způsobem podceňovala, nebo přehlížela a nejen kvůli tomu vzrostl počet úspěšných útoků na naše majetky. Z hlediska vzájemné důvěry mezi bankou a klientem je nutné najít nejenom důvody a příčiny těchto finančních krádeží, ale také kvalitně a hlavně soustavně informovat klienty o tom, jak případným útokům předcházet.

1.2 Definování objektu výzkumu

V této práci budu analyzovat jednotlivé informační a komunikační technologie dostupné na našem trhu, ke kterým bankovní ústavy nabízejí své produkty v elektronickém bankovnictví. Dále se zaměřím na bezpečnost při konkrétním užitím dané služby, jeho výhody a nevýhody a přínos z hlediska časového, finančního a v neposlední řadě zhodnotím atraktivitu užití.

Známým faktem je to, že systém banky lze považovat za nejbezpečnější část přenosového řetězce a naopak největším rizikem je klientská stanice a její interakce uživatelem (klientem). Právě oprávněnost této teze, bude dalším bodem mé analýzy.

1.3 Cíle

Cílem této bakalářské práce je navrhnout komplexní řešení zabezpečení konkrétních služeb a finančních transakcí, které klient elektronického bankovnictví využívá.

Preferovaných výstupů této práce bude hned několik. Prvním výstupem bude celková recenze jednotlivých typů elektronického bankovnictví se zvláštním zaměřením na jeho nejprogresivnější část - internetové bankovnictví (internet banking).

Neméně důležitou součástí této práce bude snaha o popsání různých typů útoků, které můžeme v elektronickém (resp. internetovém) bankovnictví nalézt, jejich charakteristika, nebezpečnost a také způsob, jak tyto útoky odvracet a hlavně, jak jim předcházet.

Tato práce rovněž přináší úhel pohledu na problematiku vztahu bankovních ústavů k vlastním klientům, zodpovídá otázky, které bezprostředně souvisí s bezpečným užitím internetového bankovnictví.

Posledním zřejmým výstupem bude snaha o nalezení vhodného chování klienta, díky kterému by při užívání služeb elektronického bankovnictví měl jistotu, že je o jeho majetek v cyberprostoru dobře postaráno a nehrozí mu žádné akutní nebezpečí.

Narovinu zde prezentuji, že téma mé bakalářské práce je mi velice blízké, zajímá mě a jako každý rozumný člověk mám svůj názor. Proto, i přes snahu o bezprostřední objektivitu zkoumání a jednotlivých analýz, se nevyhnu subjektivním názorům postřehům na konkrétní problémy elektronického bankovnictví.

2 ANALÝZA SOUČASNÉHO STAVU

2.1 Elektronické bankovnictví

2.1.1 Objasnění pojmu elektronického bankovnictví

Elektronické bankovnictví (běžně používaným pojmem je e-banking) je nadřazeným pojmem pro služby, které využívá řada z nás v běžném životě. Nejznámější z těchto součástí je internetové bankovnictví, nebo Homebanking. O součástech elektronického bankovnictví bude další kapitola, nyní si můžeme vysvětlit samotný pojem.

E-banking je součástí technologického produktu pod názvem e-commerce, čímž se rozumí samotný prodej zboží nebo služeb přes celosvětovou síť internet, jednoduše řečeno, je to komplexní řešení obchodování využívající elektronické technologie. Samotný e-banking je jeden z poměrně nových nástrojů e-commerce, zajišťující klientům bankovních ústavů pohodlnou a časově nenáročnou správu svých účtů pomocí konkrétních elektronických médií. V současné době ho nabízí naprostá většina našich bank a řada jejich klientů si bez této služby neumí správu svých účtů dostatečně představit. Tímto je návštěva tradiční banky klientem omezena na absolutní minimum.

2.1.2 Vývoj elektronického bankovnictví

Za samotný počátek elektronického bankovnictví považujeme vznik debetních platebních karet, které zajišťovaly bez konkrétního užití peněz jako prostředku nákup produktu, nebo užití služeb. Tyto platební karty má na svědomí Western Union Telegraph Company a to v roce 1914. Klienti této společnosti mohli po předložení této platební karty posílat listovní zásilky a jim podobné produkty. V roce 1950 vydává Dinners Club International svým vybraným klientům první univerzální platební kartu pokrývající různé druhy služeb, které zajišťovala právě tato společnost. O rok později vydává platební kartu první banka Franklin National Bank, veškeré účetní operace zde

probíhají samozřejmě bez výpočetní techniky, kdy po předložení karty, byla zkontrolována její platnost a na papírovou účtenku zapsána dlužná částka, která byla později majiteli karty odečtena z účtu.

Nastává období studené války, kdy se světové mocnosti předhání ve vynalézání nových technologií a s určitou dávkou ironie, můžeme říct, že e-banking vděčí za svůj obrovský rozvoj právě studené válce. Zprvu nové technologie byly využívány víceméně pro nekomerční využití (zbraně, radarové a raketové systémy), ale banky velmi pozorně sledovali tyto invence a velmi brzo je začali využívat. V roce 1967 pustila do komerčního provozu banka Barclays Bank první bankovní automat (bankomat), umístěn byl v severním Londýně a byl klienty hojně využíván, později se začal jako první bankovní automat sériově vyrábět. Výstavbu a spuštění prvního ATM (Automatic Teller Machine) automatu má na svědomí Luther George Simjian v roce 1939, nicméně problémy tehdejší doby a celkový nezájem o jeho služby se postaral o stažení automatu ze scény.

V dnešní době převažují v České republice karty od společností EuroCard/MasterCard a VISA . Debetní nebo kreditní kartu užívá nebo má ve vlastnictví 70% populace starší 15let a můžou použít jeden z 3500 bankomatů po celé ČR a bezhotovostně platit na více než 50000 místech. Nejhojnější službou, ke které klienti našich bank platební karty užívají je výběr hotovosti, naproti tomu v USA jsou platební karty z více jak 60% využívány k bezhotovostnímu platebnímu styku, jehož služby nejsou tak striktně zpoplatněné. U nás se v posledních letech ubírají zákazníci k podobnému trendu využití platebních karet.

Přibližně do roku 1994 bylo tedy možné bezhotovostně platit kartou u vybraných obchodníků, nebo používat k výběru hotovosti bankomat. Pokud tedy chtěl klient využít jiné bankovní služby (trvalý příkaz, převod peněz), musel zajít do tradiční banky, tam vyplnit potřebné formuláře a počkat, než bankovní úředník zkontroluje podle podpisového vzoru totožnost klienta a jeho práva k užití účtu a konkrétní transakci zaúčtuje. Tento postup byl velmi běžný, ale pro klienta časově velmi náročný.

Banky proto hledají možnost dalších druhů komunikace se svými klienty a technologie jim jdou výraznou měrou naproti. S rozšířením telefonních ústředen a jejich následnou digitalizací, vzniká další odvětví elektronického bankovnictví a to, telefonní bankovnictví (phonebanking nebo telebanking), které je hojně využívané i v současné době. Zajišťuje komunikaci prostřednictvím telefonu s bankovním úředníkem, který vyřídí požadované bankovní služby, nebo při užití tónové volby, zde probíhá přihlášení k bankovní evidenci a terminálu operací a klient si požadované služby může skrze zmiňovanou automatickou ústřednu vyřídit sám. S phonebankingem úzce souvisí i GSM-banking, jenž využívá pro přenos dat GSM sítě a mobilních telefonů a především využívá služeb tzv. SMS zpráv (Short Message Service – krátké textové zprávy).

Dalším milníkem v prolomení ostychu při užití elektronického bankovnictví byl rozvoj výpočetní techniky v posledních třech desetiletích. Výpočetní technika dosáhla požadované kvality a hlavně začala být sériově vyráběna a cenou přístupná téměř každé domácnosti. Výpočetní technika na konci devadesátých let minulého století proniká do soukromého a pracovního života každého člověka a banky opět byly nuceny na tento celosvětový trend reagovat. Pokud přičteme i rozšíření celosvětové sítě WWW (World Wide Web – internet) a její privatizaci v roce 1993 (dříve byla určená výhradně k akademickým a vojenským účelům), vzniká tím velice příhodná kombinace pro rychlý rozvoj elektronického bankovnictví a vznikají jeho další odvětví jako internetbanking a homebanking (tyto dva termíny nemůžeme zaměňovat). Tyto produkty elektronického bankovnictví umožňují předat bance požadavky klienta v elektronické podobě, čímž je výraznou měrou zvýšena efektivnost práce. To zapříčiňuje vznik bank, které s klientem komunikují pouze přes elektronická média (Expandia banka – nynější eBanka). Internetové bankovnictví je v současné době nejrozšířenější službou e-bankingu, nicméně některé produkty byly předem odsouzené k záhubě, protože jejich vysoký bezpečnostní standart snižoval uživatelský komfort. Právě o tyto dvě položky v elektronickém bankovnictví jde nejvíce: přilákat klienty na snadnou dostupnost služeb, ale přitom jim garantovat absolutní bezpečnost jejich transakcí a operací s bankovním účtem. Výsledkem je, ne vždy vhodné hledání kompromisů na úkor bezpečnosti. [2]

2.1.3 Výhody elektronického bankovnictví

Elektronické bankovnictví se díky nejmodernějším technologickým trendům stává stále populárnějším a to nejen v ČR, patří mezi nejdynamičtěji se rozvíjející oblasti bankovních služeb jako celku. Pojďme si proto shrnout největší rozdíly mezi tradiční bankou a elektronickým bankovnictvím:

1. *Odlišný způsob komunikace mezi klientem a bankou* – elektronické bankovnictví zajišťuje vzájemnou komunikaci mezi klientem a bankou pomocí moderních informačních a komunikačních kanálů, tradiční banka preferuje osobní kontakt mezi klientem a bankou
2. *Kvalita služeb* – v tradiční bance provádí určené operace bankovní úředník, ikdyž plně kvalifikovaný, nemůže zvládat služby v takovém rozsahu jako výpočetní technika
3. *Dostupnost* – vstoupit do elektronické banky můžete takřka kdykoliv, kdy vám to technika dovolí, kdežto do tradiční banky jste odkázán na provozní hodiny.
4. *Náklady na provoz* – diskutabilní je to, jestli při užití elektronického bankovnictví ušetří na bankovních poplatcích klient, nicméně banky na financování provozu rozhodně vynaloží méně prostředků.
5. *Časová náročnost* – při užití např. internetbankingu stačí několik málo minut a požadované bankovní operace jsou provedeny, klient pouze několik málo minut čeká na server, která jeho operace provede. Naproti tomu u tradiční banky, která upřednostňuje osobní kontakt, musí klient vyplnit několik formulářů, vystát řadu a až potom bankovní úředník jeho požadavek provede. [2]

Všechny tyto rozdíly nahrávají jednoznačně elektronickému bankovnictví, čímž se stává stále populárnějším. Zřejmá jednoduchost, časová nenáročnost a pohodlí zaručují, že e-banking bude hrát v našich životech stále větší a důležitější roli.

Jedinou diskutabilní oblastní je bezpečnost prováděných transakcí. Banky zaručují stávajícím i budoucím klientům absolutní bezpečnost a kvalitní ochranu, používají nejmodernější metody šifrování přenesených dat, ale i přesto útoky na klientské účty

rostou a rovněž rostou i ty úspěšné. Jak se proti jednotlivým útokům bránit, jak jim předcházet, to bude předmětem dalších kapitol. V následujících kapitolách se podrobně rozepíši o jednotlivých formách elektronického bankovnictví, o bezpečnosti a možnostech využití.

2.2 Druhy elektronického bankovnictví

2.2.1 Platební karty

Platební karty jsou nezbytnou součástí každého běžného účtu, umožňují nám pohodlný výběr hotovosti z bankomatů a placení zboží bez hotovosti. Největší výhodou platební karty je, že eliminuje možné odcizení. Proti zneužití jinou osobou je platební karta chráněna čtyřmístným heslem PIN a při placení jste povinni se prokázat podpisovým vzorem. Samotná bezpečnost spočívá v tom, že při odcizení vaší karty, můžete okamžitě zablokovat její neoprávněné užívání a tím předejít zneužití vašich financí. Platební kartu si můžete taky nechat za poplatek pojistit u banky, která ji vydala.

Platební karta je identifikační doklad, jehož rozměry a fyzikální vlastnosti upravuje mezinárodní norma ISO 3554. Na přední straně karty je uvedeno jméno a příjmení držitele, doba její platnosti a její identifikační číslo. Na zadní straně je podpisový vzor a magnetický proužek a zpravidla taky číslo karty, které navíc obsahuje trojčíslí, které používáme při některých transakcích. Platební karta není majetkem držitele, ale banky.

Platební karty můžeme rozdělit dle několika kritérií:

1. Podle způsobu zúčtování

Debetní karty – jsou pevně svázány s běžným účtem. Při použití, ať je to platba u obchodníka nebo výběr z bankomatu, čerpáte své peníze uložené na bankovním kontu. Po provedení transakce odečte banka příslušnou sumu z vašeho účtu.

Kreditní karty – karta není napojená na běžný účet, ale na úvěrový účet. Jakákoliv transakce provedená za pomocí kreditní karty, znamená čerpání úvěru, který je povinen držitel karty ve stanovené lhůtě splatit.

Charge karty – fungují na stejném principu jako kreditní karty. Výjimkou je to, že banka vám na konci zúčtovacího období (konec měsíce) zaúčtuje všechny předchozí transakce a držitel je povinen tyto transakce splatit. Z čerpané částky není účtován žádný úrok.

Nákupní úvěrové karty – jsou to kreditní karty, které nevydávají samotné banky. Liší se hlavně cenou karty, úrokovou sazbou a omezené použitelnosti.

2. Podle způsobu provedení

Elektronické karty – jsou u nás nejrozšířenějším typem platebních karet. Patří zde VISA Electron, nebo Maestro. Jsou použitelné pouze pro transakce, které jsou online ověřeny v kartovém centru (platby u obchodníků disponujícím elektronickým platebním terminálem, výběr hotovosti z bankomatu). Nevýhodou je nízká použitelnost, protože ne každý obchodník vlastní elektronický platební terminál (přibližně 50%)

Embosované karty – základní charakteristikou těchto karet, jsou vyražené symboly na přední straně. Mohou být použity u obchodníků, kteří disponují pouze tzv. žehličkou (imprinter). Při použití vloží obchodník kartu do imprinteru, který obtiskne její údaje a vystaví šek, který zákazník podepíše. Embosované karty jsou lze použít na více místech než karty elekronické. Daní za tuto výhodu je ale vyšší cena za vydání, vedení či blokaci karty a jistá možnost zneužití karty i po nahlášení její ztráty či odcizení.

3. Podle vydávající asociace a třídy

Karty typu MasterCard – patří zde 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.

VISA - zahrnují elektronické karty VISA Electron, embosované VISA Classic, pro vyšší třídu klientů pak VISA Silver a VISA Gold. Nejvyšší kartou je VISA Platinum.

Diners Club, AMEX, JBC – určené pro movitější klientelu, jedná se o exkluzivní platební názor pro vyšší třídu klientů.

4. Podle použitelnosti

Domácí karty – použitelné jen na místech v ČR. Jsou označeny nápisem: valid only in the Czech Republic.

Mezinárodní karty – jsou použitelné nejenom na našem území. Většina dnešních karet je vydávána už jako mezinárodní. [10]

5. Podle použité technologie

Magnetický proužek – umístěn na zadní straně platební karty. Jsou na něm umístěny údaje o kartě a jejím držiteli. Bez těchto informací by nemohla být provedena žádná transakce. Magnetický proužek není tak bezpečný jako čip, proto na něm není uložen PIN.

Čipová technologie - Čip umožňuje díky vyššímu zabezpečení (využívajícímu dynamické šifrovací algoritmy) uložení PINu a použití karet pro elektronické transakce bez nutnosti ověření v centru (tzv. offline transakce).

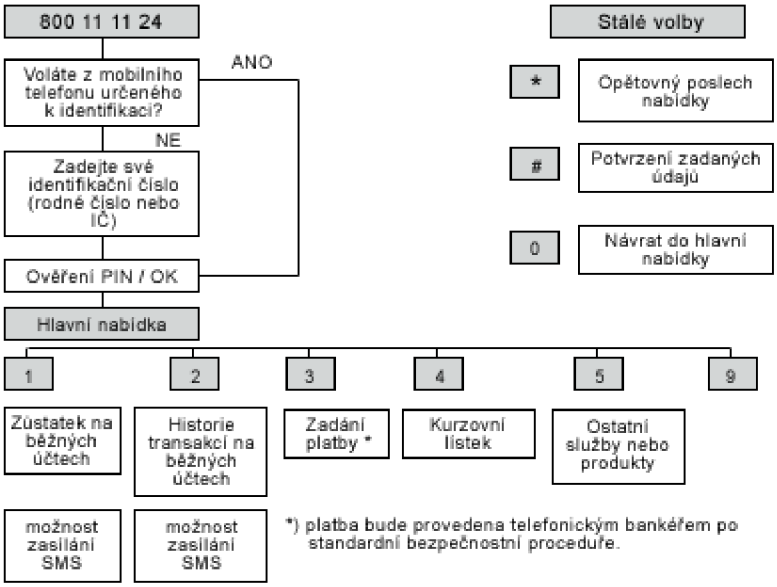
Hybridní karty – Obsahují magnetický proužek i čip. Toto řešení se používá v době přechodu z jedné technologie na druhou (magnetické→čipové) [10]

2.2.2 Telefonní bankovnictví

Pomocí této služby (phonebanking) můžeme provádět různé druhy bankovních operací, pasivní (zůstatek na účtu, zjištění pohybů na účtu, informace od banky) a aktivní (zadávání příkazů k úhradě, zadání příkazu k inkasu, zakládání termínovaných vkladů).

Phonebanking využívá pro komunikaci mezi klientem a bankou telefonní síť a přístroj (pevná linka, mobilní telefon). Ovládání je zpravidla velice jednoduché: klient vytočí číslo služby a po zadání PINu, nebo osobního číselného hesla a může pracovat se svým účtem. K dispozici má dvě možnosti, může využít služek telefonní operátorky (Call centrum), nebo telefonního automatu (IVR – Interactive Voice Response). Při zvolení služeb telefonního automatu, postupujete podobně jako například při používání hlasové schránky na mobilním telefonu, pomocí číselné tónové volby se pohybujete ve virtuálním prostoru telefonické banky a zadáváte požadované čísla účtů, resp. částky na klávesnici vašeho přístroje. Pokud zvolíte přepojení na telefonní operátorku, můžete jí slovně nadiktovat požadované transakce. [2]

Přístup do samotného systému je vázán na zadání čísla PIN, popřípadě osobního číselného hesla. Tento systém je snadno zneužitelný, pokud cizí osoba získá naše přístupová hesla.



Obr. 1 [2]

2.2.3 GSM banking

GSM banking je součást elektronického bankovnictví, jejíž vznik a vývoj je úzce spjat s rozšířením mobilních telefonů na našich trzích. Tato služba umožňuje klientovi ovládat svůj účet kdekoliv na světě a to pomocí mobilního telefonu GSM. Klienti mohou služeb GSM bankingu využívat hlavně pro pasivní operace, zřídkakdy pro aktivní operace, jako je zadávání trvalých příkazů. Klient komunikuje s bankou pomocí mobilního telefonu a na výběr má opět dva způsoby komunikace.

SMS banking – komunikace s bankou probíhá prostřednictvím SMS zpráv s pevně nadefinovanou strukturou (zpráva může vypadat například takto: ZUST_256348*11_056486_93597 – jde o pasivní operaci). Výhodou je, že lze použít u všech typů mobilních telefonů, naopak značnou nevýhodou SMS bankingu je jeho celková nepřehlednost a složitější manipulace se psaním SMS zpráv. Zabezpečení aktivních finančních transakcí probíhá dvěma různými způsoby: autentizačním kalkulátorem (PIN) nebo využitím elektronického klíče.

GSM SIM Toolkit – je uživatelsky daleko příjemnější služba. Po vložení bankovní SIM karty aktivovat služby GSM SIM banking Toolkit (služba musí být podporována operátorem – všichni tuzemští operátoři tuto službu v současné době podporují). Pomocí této služby může klient s bankou komunikovat prostřednictvím menu ve svém mobilním telefonu. Přístup klienta k operacím na účtu je obvykle vázán na PIN, který může být pevně generován, nebo vytvářen pomocí autentizačního kalkulátoru.

2.2.4 WAP banking

Prostřednictvím mobilního telefonu můžeme využívat nejenom GSM banking, ale také mladší variantu internetového bankovnictví (více v dalších kapitolách), tzv. WAP banking. WAP (Wirless Application Protocol) je vlastně obdoba internetových stránek pro mobilní telefony. Pomocí mobilních telefonů, které technologii WAP podporují, což je v současné době naprostá většina, se klient připojí do systému banky, kde se pomocí autorizačního klíče (ověření práv) přihlásí ke svému účtu a na displeji mobilního telefonu může pohodlným způsobem spravovat konkrétní účet. WAP využívá šifrovaného přenosu dat a nejenom proto můžeme konstatovat, že je tato služba minimálně riziková z hlediska bezpečnosti.

2.2.5 JAVA banking

Nejmladším členem rozsáhlé rodiny elektronického bankovnictví je bezesporu JAVA banking. Je to unikátní mobilní bankovnictví založené na bázi technologie JAVA. Nabízí se zde přímé srovnání s GSM bankingem. Zatímco GSM banking komunikuje pomocí SMS služby, JAVA banking používá ke komunikaci přenos dat prostřednictvím GPRS. Banka vytvoří JAVA aplikaci, kterou si klient stáhne do svého mobilního telefonu a potom se pomocí internetového rozhraní připojí sytému banky. Ochrana dat a bezpečnost je zajištěna vysokým standardem zabezpečení v podobě šifrované komunikace. Jedinou podmínkou pro užití této služby je to, že klient musí mít přístroj (PDA, mobilní telefon), který technologii JAVA podporuje.

2.2.6 PDA banking

PDA (personal digital assistant - *osobní digitální pomocník*) či palmtop je malý kapesní počítač, ovládaný obvykle dotykovou obrazovkou a perem (které se nazývá *stylus*). Původně měly PDA za cíl především pomoci s organizováním času a kontaktů. Současné PDA jsou velmi výkonné a zvládají i přehrávání videa a spoustu dalších aplikací. Připojení probíhá pomocí GPRS nebo WiFi sítí. Klient musí mít ve svém PDA mít nainstalovaný www prohlížeč. Nainstalovaný HTML prohlížeč však musí podporovat framy (rámce) a 128 bitový SSL protokol pro šifrování přenášených dat. Použití kapesního počítače k využívání bankovních služeb nabízí komfortní řešení správy klientských účtů. Výhodou je opět celková bezpečnost služby a nízká cena za uskutečněné transakce, protože klient platí za celkový objem přenesených dat, nikoliv za dobu připojení.

Obr. 2

2.2.7 Samoobslužná zóna

Jde zpravidla o terminál s dotykovým displejem, umístěný v bankovních prostorách. Banky o něm hovoří jako o automatizované přepážce, což naznačuje služby, které může klient využívat. Klient opět může komplexně ovládat a spravovat svůj účet, po vložení karty, která klienta identifikuje (někdy i otisk prstů) je zákazník přihlášen ke svému účtu a pomocí dotykového displeje a může provádět většinu aktivních i pasivních operací. Tato služba u nás není příliš rozšířená, z důvodu vysokých nákladů na koupi a

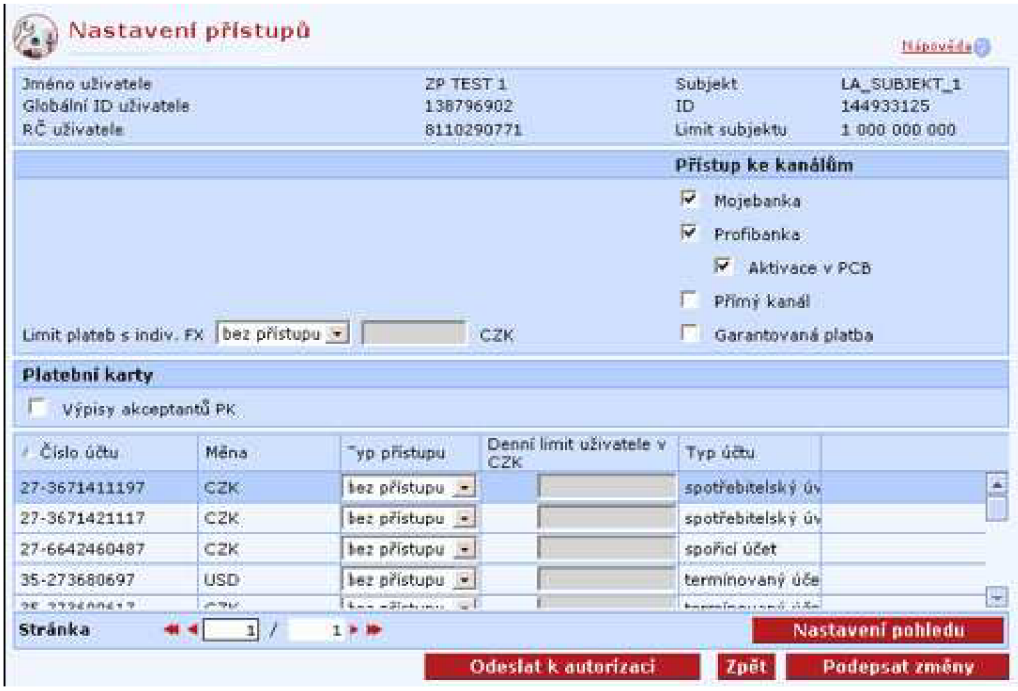
provoz automatu. Právě kvůli vysokým nákladům, bývá samoobslužná zóna spojována s provozem bankomatu.

2.2.8 Homebanking

Homebanking je určen klientům většiny bank jako prostředek k elektronické komunikaci. Slouží k realizaci bezhotovostního platebního styku pomocí počítače připojeného k internetu a nainstalování specializovaného programu vydaného bankou (tím se homebanking odlišuje od internetového bankovnictví, kde stačí mít pouze přístup k internetu). Umožňuje spojením přes internet kontrolovat stav účtu, průběh transakce, s jeho pomocí lze zadávat příkazy k úhradě, k inkasu a získávat další důležité informace.

Homebanking mohou klienti používat 24 hodin denně, 365 dní v roce, až na občasné výpadky bankovního systému a aktualizace některých bezpečnostních součástí. Systém obsahuje kontroly oprávněnosti přístupu. Přenášená data jsou chráněna digitálním podpisem a šifrováním. Digitální podpis v kombinaci s heslováním přístupů je základním kamenem bezpečnosti systému.

Je to jedno z nejvytíženějších odvětví elektronického bankovnictví u nás. Mezi klienty je tato služba oblíbena zejména pro možnost správy účtu z pohodlí domova, relativní časovou nenáročnost a vysokou přehlednost všech provedených transakcí. Další výhodou, je fakt, že program homebankingu lze propojit s účetním programem a importovat do něj potřebná data, což nám usnadní případné účetnictví – proto je homebanking využívaný nejčastěji pro firemní účely. Mezi hlavní nevýhody můžeme počítat opět relativní složitost celkového systému.



Obr. 3 [2]

2.2.9 Internetové bankovnictví

Na rozdíl od homebankingu, jediné co klient potřebuje pro napojení na bankovní systém, je počítač s připojením na internet. Pokud se chce tedy klient přihlásit ke svému účtu, musí se napojit na internetovou stránku, která je k tomuto důvodu vytvořena. Při podpisu smlouvy u užívání internetového bankovnictví dostane klient proti podpisu přihlašovací údaje (uživatelské jméno a heslo), s jejichž pomocí se snadno přihlásí ke svému účtu. Nezbytností pro užití internetového bankovnictví je užití elektronického klíče, který může mít uživatel uložený přímo ve svém počítači, nebo se může nacházet na čipové kartě (k čemuž ovšem klient potřebuje čtečku těchto karet připojenou k počítači).

Obr. 4 [6]

Elektronický klíč může mít také podobu autentizačního kalkulátoru. To ve zkratce znamená, že pro každou aktivní transakci je klientovi na určitou dobu vygenerován kód, který musí zadat, aby došlo k úspěšnému průběhu transakce. U této služby navíc odpadá mít nainstalovaný speciální software, s jehož pomocí operace provádíme. Tím se systém stává celkově jednodušším a tím pádem dostupnějším pro většinu obyvatel. Internetové stránky jsou velmi přehledné a bez jakéhokoliv předchozího nastudování jsou snadno a intuitivně ovladatelné.

Obr. 5

V současné době využívá služeb internetového bankovnictví přes 30% všech uživatelů internetu a tím pádem se tato služba stává nejrozšířenějším prostředkem elektronického bankovnictví (přímého bankovnictví). Proto se taky v současné době vedou ostré a důležité diskuze o komplexním zabezpečení tohoto produktu, o veškerých rizicích a nástrahách a o předcházení těchto útoků. Bankovní ústavy v tomto směru vedou tvrdý boj o klienta. Správně vycítili, že jejich klienti se už neorientují pouze podle vynaložených nákladů na správu účtu a jeho užívání, ale v poslední době se spíše přiklánějí na stranu kvalitního zabezpečení.

Následující kapitoly budou obsahovat shrnutí a analýzu všech bezpečnostních složek, budou vyhodnocovat možná rizika a způsoby ochrany, analyzovat důležitost všech ochranných bariér nejprogresivnějšího odvětví elektronického bankovnictví – internetového bankovnictví.

3 TEORETICKÁ VÝCHODISKA PRÁCE

3.1 Úvod do bezpečnosti internetového bankovnictví

Nedávné bezpečnostní incidenty související se zcizením identity v elektronickém bankovnictví nejsou ojedinělou záležitostí. Banky jsou stále cílem útoků, a proto je vhodné se zamyslet nad možnostmi zabezpečení, které by zabránily jakémukoliv zneužití. Ať už zneužití dat nebo krádeži prostředků z účtů. Pro úspěšné a bezpečné využívání elektronické komunikace s bankami pro manipulaci s finančními prostředky (a nejen s nimi) je nezbytné, aby v systému elektronických kanálů byly všechny bezpečnostní atributy přenášených zpráv byly zachovány od vzniku zprávy po její zpracování v cílovém systému. A to při komunikaci v obou směrech.

Obvyklým požadavkem bank je maximalizace pokrytí elektronických kanálů. U bankovních ústavů hrají důležitou roli při zavádění novinek legislativní požadavky.

Bezpečnostní ředitelé bank se neustále zabývají otázkou, jak zachovat klady elektronického bankovnictví a zároveň řešení zabezpečit proti zneužití. Tuto otázku můžeme charakterizovat jako hledání vhodného kompromisu mezi kvalitním zabezpečením a uživatelským komfortem především. Jednotlivé bankovní ústavy mezi sebou bojují o klienty a do nedávné doby sami sobě konkurovali zejména produkty, které by klientům co nejvíce zpříjemnil používaní elektronického bankovnictví. V minulých letech rapidně narostl počet útoků a banky byly nuceny začít uvažovat jinak: pokud klient nebude cítit, že jsou jeho finanční prostředky v bezpečí, těžko bude produkt používat. Proto zvolily jinou cestu, cestu garance nejvyššího zabezpečení. Začali mezi sebou komunikovat a společnou cestou se snaží zachovat nejen výhody klasického elektronického bankovnictví jako celku, ale snaží se i o to, aby elektronické bankovnictví neztratilo svou prestiž. Následující kapitola popíše a vysvětlí způsoby zabezpečení jednotlivých finančních transakcí v internetovém bankovnictví (jak banka chrání klienta před útoky).

3.2 Druhy zabezpečení

Systém banky lze považovat za nejbezpečnější část přenosového řetězce.

Základním úkolem elektronického bankovnictví je zajistit bezpečný přenos zpráv mezi klientem a bankou v obou směrech. Než začneme uvažovat o možných hrozbách, kde a jaké mohou nastat v elektronickém bankovnictví, podívejme se, jak vypadá obvyklý přenosový řetězec mezi klientem a bankou z hlediska bezpečnosti. K přenosu zpráv je využívána veřejná internetová síť, kde je ochrana zajišťována kryptografickými technikami, jako je elektronický podpis a šifrování v kombinaci s dalšími technologiemi. Pokud je počítač/klientská stanice připojen k internetu, proudí do něj data primárně prostřednictvím počítačové sítě. Součástí těchto dat může být rovněž nebezpečný software, který po spuštění v pracovní stanici může představovat bezpečnostní riziko pro uživatele, který jej spustil, a v případě, že jde o privilegovaného uživatele, rovněž ke všem prostředkům počítače. Musíme si nejprve ujasnit dva používané termíny při užívání internetového bankovnictví:

Autentizace (autentifikace) – ověření totožnosti uživatele
Autorizace – ověření práv pro vykonání určité činnosti, procesu autorizace předchází proces autentizace

Obě tyto techniky lze provádět několika způsoby a v souvislosti se zabezpečením internetového bankovnictví se skloňují ve všech pádech. Všeobecně platí, že systém zabezpečení internetového bankovnictví (resp. internet bankingu) není a ani nemůže být 100% bezpečný. V současné době neexistuje bezpečné internetové bankovnictví – maximalizovat lze pouze jeho ochranu. K zajištění bezpečnosti internetového bankovnictví musíme analyzovat a vyřešit 4 hlavní problémy:

1. Zabezpečení přenosu dat
2. Identifikace banky
3. Identifikace klienta
4. Bezpečnost klientského počítače

Dojde-li k selhání jednoho z předpokladů pro zajištění bezpečnosti, je zabezpečení považováno za neúspěšné a nedostatečné a útok je úspěšný.

3.2.1 Zabezpečení přenosu dat

K zabezpečení přenosu dat se používá protokol HTTP s nadstavbou SSL, protože právě tato nadstavba umí šifrovat přenášená data, kdežto protokol HTTP obstarává pouze autentizace pomocí uživatelského jména a hesla. Spojením těchto dvou protokolů vzniká šifrovaný protokol HTTPS. SSL je nadstavba pro protokol HTTP (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. Obvyklé servery a prohlížeče disponují implementací dostatečně kvalitních šifrovacích algoritmů. Většina bank se opírá o 128 bitové šifrování. Toto zabezpečení přenosu dat mezi bankou a klientem je

podle většiny počítačových expertů označováno za dostatečné. Pro případného schopného útočníka není velkým problémem zachytit komunikaci mezi těmito dvěma subjekty, ale útočník dostane odposlouchávaný materiál v zašifrované podobě a tudíž pro něj nepoužitelný (nezneužitelný).

3.2.2 Identifikace banky

V tomto případě řešíme, zda klient komunikuje opravdu s bankou a ne s útočníkem. Tuto jistotu můžeme úzkým způsobem spojovat s kvalitou SSL protokolu a s kvalitou užitých šifrovacích klíčů. V běžné praxi to znamená, že identifikace banky je ověřována SSL certifikátem, který je vydáván nezávislou institucí (nejčastěji VeriSign). Certifikáty společnosti VeriSign používá většina významných světových společností, v bankovním sektoru jsou certifikáty VeriSign samozřejmostí. Získáním certifikátu VeriSign každá společnost deklaruje vyšší úroveň kvality služeb a zabezpečení. SSL certifikát můžeme přirovnat k elektronickému průkazu totožnosti a je zpravidla uložen v internetovém prohlížeči. Certifikát může získat, rušit a obnovovat pouze uživatel oprávněný používat systém internetového bankovnictví. Správu certifikátů provádí registrační autorita.

3.2.3 Identifikace klienta

S identifikací klienta se setká pravděpodobně každý uživatel internetového bankovnictví hned na začátku. Tvoří jedinou překážku mezi klientem a bankovním účtem. Tento postup bývá také označován jako autentizace (ověření totožnosti) a nejčastěji bývá spojován s formou: uživatelské jméno/heslo (označováno jako slabá autentizace). Postupů jak samotnou autorizace vykonat je hned několik a liší se od sebe nejčastěji bezpečností, komfortností a časovou resp. finanční náročností. Jednotlivé možnosti autentizace zde popíšu:

1. *Kombinace jména a hesla* – klasická metoda ověřování totožnosti. Tato možnost je, co se týče bezpečnosti velice slabá. Heslo může útočník snadno vypozorovat nebo odposlechnout při přenosu přes síť. Při používání této metody je nutné volit silná hesla

(mnoho znaků), držet heslo v tajnosti před druhou osobou a po určité době heslo změnit z důvodu bezpečnosti. Existují různé variace této metody, nejbezpečnější a nejpoužívanější je metoda tzv. jednorázového hesla, kdy je vygenerováno heslo, které je možné použít právě na jednu konkrétní operaci.

2. Čipová karta (SmartCard) - Karta velikosti běžných bankovních nebo telefonních karet. Jednotlivé typy se liší především vnitřní architekturou. Karty SmartCard pro bankovnictví, identifikaci do počítače a uložení certifikátů obsahují kromě paměti i procesor. Uložené certifikáty, jiné identifikační informace popř. jiné informace a data jsou chráněna přístupovým heslem (PIN) a kryptografickými funkcemi. Při několika nesprávných zadání hesla se karta zablokuje, nelze použít odhad hesla hrubou silou. Pokud chce klient využívat výhod autentizace pomocí této čipové karty, musí mít na svém počítači mít připojenou čtečku těchto karet. Opět se zde setkáváme s poměrně vyššími náklady, které nám ale zaručují snížení rizikovosti neoprávněného přístupu a zvýšení celkové bezpečnosti užití služeb internetového bankovnictví. Zajímavé je i ochrana proti vnějším vlivům. Karty jsou velmi odolné proti vodě, mechanickému namáhání a elektromagnetickým polím.

Obr. 6 [5]

3. USB Token – pracuje na podobném principu jako čipová karta. Rozdílem je nižší rozšíření podpory u našich bankovních ústavů a celkové nižší náklady na použití. Stačí mít na počítači nainstalováno USB rozhraní.

Obr. 7 [5]

4. *Pomocí biometrie* - Biometrie je metoda autentizace založená na rozpoznávání fyzických charakteristik subjektu - živé osoby. Metoda vychází z přesvědčení, že některé fyzikální charakteristiky jsou pro každého živého člověka jedinečné a neměnitelné. V internetovém bankovnictví se používá nejčastěji metoda s použitím otisku prstů. Jakkoliv se zdá tato metoda zdánlivě bezpečná, podle expertu se stává dokonale bezpečnou až při kombinaci s jinou metodou autentizace (nejčastěji s čipovou kartou). [5]

Obr. 8 [5]

5. Harwarový klíč – jedná se o jednoduché zařízení připojované k portům počítače. Úspěšná detekce existence zařízení a jeho dalších parametrů potvrdí oprávnění k užití. Tato metoda autentizace bývá rovněž považována za bezpečnou.

6. Digitální certifikáty – jsou to elektronické dokumenty potvrzující totožnost. Důvěrnost a nezaměnitelnost certifikátu je chráněna digitálním podpisem. Při převzetí certifikátu obdrží klient soukromý a veřejný klíč. Nejčastěji bývají tyto certifikáty uloženy na pevném disku počítače.

7. Mobilním telefonem – další možností autentizace je užití mobilního telefonu. Zpravidla bývá zajišťována tak, že banka po zjištění požadavku přihlášení klienta na

účet, pošle uživateli jednorázové heslo (PIN), které se po úspěšném přihlášení, nebo po vypršení platnosti stává bezcenným. Tato metoda je v současné době používána spíše pro účely autorizace.

8. *Kombinace metod* – ikdyž je tato metoda až na posledním místě, její důležitost je nepopsatelná. Obecně platí, že při užití více jak dvou metod se stává proces autentizace zcela bezpečným, ovšem na úkor pohodlí zákazníka. Pokud se tedy banky rozhodnou kombinovat některé metody, zpravidla to bývají pouze dvě. I v tomto případě platí, že kombinace dvou metod zajišťuje několikanásobně větší zabezpečení, než metoda jedna.

Výše zmíněné metody bývají taktéž používány k autorizaci klienta. Při vstupu na samotný bankovní účet je nutné klienta prvně autentizovat, tím banka ověří totožnost zákazníka. Pokud chce klient provádět aktivní operace na účtu (finanční transakce) bývá často vyzván v autorizaci, která umožní požadované bankovní transakce provést.

K samotné autorizaci bývá často využíván tzv. autorizační kalkulátor. Autorizační kalkulátor je elektronické zařízení, které dokáže generovat jednorázová hesla pro přístup k bankovní aplikaci. Tato zařízení bývají synchronizována se systémy banky tak, aby obě strany generovaly stejné klíče. Ty pak uživatel opisuje do aplikace a ověřuje tak svou totožnost jednoduše tím, že dokáže, že je majitelem příslušného kalkulátoru. Generovaná hesla mívají obvykle návaznost na operace, které jsou pomocí klíče generovány a uživatel je tak nucen do kalkulátoru uvádět informace jako je číslo účtu, částka se kterou je manipulováno a podobně. Z tohoto důvodu je velmi obtížné podvrhnout uživateli falešné formuláře k potvrzení, protože pokud nejsou na obou stranách zadány stejné údaje, klíče jsou neplatné. Jedná se o jednu z nejbezpečnějších metod autorizace uživatele. [14]

Jinou metodou autorizace je generování jednorázových hesel. Proti autorizačnímu kalkulátoru je při ní ale uživatel přímo komunikuje s bankovním systémem s pomocí mobilního telefonu. Banka při požadavcích o autorizaci zašle klientovi SMS s potvrzovacím kódem, který je potřeba opsat zpět do aplikace. Součástí SMS bývá často také informace o tom, k čemu se konkrétní kód vztahuje. [14]

	Jméno a heslo	Certifikát	Čipová karta	SMS kódy	Kalkulátor
BAWAG Bank	ano				
Citibank	ano				
Česká spořitelna	ano		ano		ano
ČSOB	ano	ano	ano	ano	
eBanka		ano		ano	ano
GE Money Bank	ano	ano			
HVB Bank					ano
Komerční banka		ano	ano		
Poštovní spořitelna	ano	ano	ano	ano	
Raiffeisenbank	ano				
Volksbank	ano				
WSPK	ano		ano		
Živnostenská banka	ano	ano			

Tab. 1 [12]

	Certifikát	Čipová karta	SMS kódy	Kalkulátor
BAWAG Bank	ano			
Citibank				
Česká spořitelna		ano	ano	ano
ČSOB	ano	ano	ano	
eBanka	ano		ano	ano
GE Money Bank	ano			
HVB Bank				ano
Komerční banka	ano	ano	ano	
Poštovní spořitelna	ano	ano	ano	
Raiffeisenbank	ano		ano	
Volksbank	ano			
WSPK	ano	ano		
Živnostenská banka	ano			

Tab. 2 [12]

3.2.4 Bezpečnost klientského počítače

Jedním z nejpodstatnějších prvků internetového bankovnictví z hlediska bezpečnosti (nejenom) je klientský počítač. Zatímco předešlé tři problémy měl víceméně na starosti bankovní ústav, bezpečnost počítače má klient pouze ve svých rukou. Pro jakýkoliv kontakt s bankou je rozumné používat počítač, který je určen k ryze soukromým účelům. Velice nerozumné je používat, ke komunikaci s bankou, počítač umístěný v internetové kavárně, nebo na dalších veřejně dostupných místech. Samozřejmostí by měl být počítač vybavený:

1. Antivirovým programem - počítačový software, který slouží k identifikaci, odstraňování a eliminaci počítačových virů a jiného záškodného software (malware). K zajištění této úlohy používají dvě techniky:

A. Prohlížení souborů na lokálním disku, které má za cíl nalézt sekvenci odpovídající definici některého počítačového viru v databázi.

B. Detekcí podezřelé aktivity nějakého počítačového programu, který může značit infekci. Tato technika zahrnuje analýzu zachytávaných dat, sledování aktivit na jednotlivých portech či jiné techniky.

Úspěšnost závisí na schopnostech antivirového programu a aktuálnosti databáze počítačových virů, které si programy pravidelně, nejčastěji z Internetu, pravidelně stahují. [14]

2. Anti-spywarovým programem – nejprve si objasníme pojem spyware. Spyware je program, který využívá internetu k odesílání dat z počítače bez vědomí jeho uživatele. Tato činnost bývá odůvodňována snahou zjistit potřeby nebo zájmy uživatele a tyto informace využít pro cílenou reklamu. Nikdo však nedokáže zaručit, že informace nebo tato technologie nemůže být zneužita. Proto je spousta uživatelů rozhořčena samotnou existencí a legálností spyware. Důležitým poznatkem je, že spyware se šíří společně s řadou sharewarových (volně dostupných) programů a jejich autoři o této skutečnosti

vědí. Jakmile si program nainstalujete a spustíte, nainstaluje se do systému také spyware. Spyware je speciálním případem malware. Malware je označení programů, které na počítači běží bez vědomí uživatele a nějakým způsobem jej poškozují. [14]

Spyware představuje z hlediska bezpečnosti dat velkou hrozbu, narozdíl od virů odesílá různé informace (historii navštívených stránek, hesla) z vašeho počítače a poté vše zasílá určenému uživateli, který tyto informace dále zpracovává, jsou velice snadno zneužitelné. Anti-spywarové programy se tedy starají o detekci a celkovou eliminaci těchto záškodných programů. Navíc mnohdy účinně předcházejí „přichycení“ spywaru na klientském počítači. Tato prevence bývá označována jako nejdůležitější součást samotného zabezpečení.

3. Firewallem – jedná se o síťové zařízení, které slouží k řízení a zabezpečování síťového provozu mezi sítěmi s různou úrovní důvěryhodnosti, zabezpečení. Zjednodušeně se dá říct, že slouží jako kontrolní bod, který definuje pravidla pro komunikaci mezi sítěmi, které od sebe odděluje. Tato pravidla historicky vždy zahrnovala identifikaci zdroje a cíle dat (zdrojovou a cílovou IP adresu) a zdrojový a cílový port, což je však pro dnešní firewally už poměrně nedostatečné – modernější firewally se opírají přinejmenším o informace o stavu spojení a znalost kontrolovaných protokolů. [14]

3.3 Druhy útoků

Útoky na konta uživatelů lze rozdělit do pěti kategorií. V této části popíšu jakým Způsobem se snaží útočník an klienta vyzrát, metody obrany rozeberu až ve vlastním návrh zabezpečení. Pokud tady mluvím o útocích, běžně používaný termín v internetovém bankovnictví je rovněž podvod, nebo napadení. Všechny typy útoků mají jedno společné, snaží se neoprávněně získat přístup k účtu a nějakým způsobem klienta poškodit, nemusí jít nutně o krádež finančních prostředků, může se jednat o odposlech citlivých informací, což bývá v některých případech daleko nebezpečnější, než samotná krádež finančních prostředků. Upozorňuji, že jednotlivé typy útoků nejsou seřazeny ani podle nebezpečnosti, ani podle četnosti výskytu.

3.3.1 Odchycení přihlašovacích údajů od uživatele podvodem

V tomto případě potřebuje útočník mít na klientském počítači nahraný software, Který může nějakým způsobem ovládat, nebo odposlouchávat. Nejčastěji se jedná o spyware, nebo tzv. backdoor. Tyto aplikace parazitují na počítači a odesílají data třetí osobě, aniž by o tom poškozený klient věděl. Spyware jsem poslal o několik kapitol výše, teď bych se zabýval jeho nejbezpečnějšími formami. I spyware můžeme rozdělit do několika kategorií, některé internetové bankovnictví mohou jenom těžko ohrozit, jiné jsou k tomuto účelu speciálně naprogramovány, nebo modifikovány (upraveny).

1. Adware – pouze obtěžuje napadený počítač nevyžádanou reklamou (někdy chybně nazýván jako spam). Pro internetové bankovnictví neznamená téměř žádné ohrožení a víceméně, pouze uživateli znepříjemňují práci na počítači.

2. Hijacker – mění domovskou stránku v prohlížeči. Opět tento adware neznamená nebezpečí pro použití internetového bankovnictví.

3. *Dialer* – bez uživatelova vědomí přesměrovávají telefonní linku na drahé tarify. Pro internetové bankovnictví (IB) neznamenají žádné riziko, ikdyž pro napadenou stanici zjevný problém přináší.

4. *Browse helper object* – první vážné nebezpečí pro IB. Jedná se o knihovnu typu *.dll. Umožňují sledovat Internet Explorer a tímto způsobem mohou odečíst přihlašovací údaje a ty potom snadným způsobem zneužít.

5.Keystroke logger – programy, implantované do systému bez vědomí
oprávněného uživatele, monitorující specifické činnosti, o které projevuje útočník zájem. Tento nepřátelský software často instaluje nevědomky sám oprávněný uživatel, když instaluje z Internetu nebo zdarma distribuovaných CD jiné programy, se kterými jsou však tyto trojské koně spojeny (např. hry, či servisní
programy - utility). [11]

6. *Remote Administration* – to „nejlepší“ nakonec. Umožní útočníkovi sledovat kompletně celý systém a navíc i ovládat. Tento typ spywaru znamená akutní ohrožení pro napadený počítač z hlediska bezpečnosti všech citlivých dat.

Z popisu můžeme snadno zjistit, že některé typy představují pro internetové bankovnictví, a nejen pro něj, značné bezpečnostní riziko. Proti spywaru ovšem existuje vcelku jednoduchá ochrana i obrana. Dalším škodlivým softwarem je již výše zmiňovaný backdoor (zadní vrátka).
Jedná se o specifickou formu potlačení bezpečnostní ochrany systému. Muže být vytvořena samotným autorem distribuované aplikace, nebo dodatečně, prostřednictvím infoware, aby v případě potřeby posloužila pro vstup do systému bez nutnosti znát příslušná bezpečnostní hesla či kódy, instalovaná oprávněným uživatelem (tj. od specifického vzdáleného uživatele nevyžaduje běžné kontroly hesel). Jejím deklarovaným cílem, např. v souvislosti s operačním systémem Windows, je umožnění servisního přístupu odborníku firmy Microsoft do systému při aktualizaci některých aplikací. Zároveň se však jedná o ideální místo k průniku neoprávněné osoby.

3.3.2 Odchycení od „třetích“ stran

Jedná se o získání hesel, PINů a dalších dat např. o platební kartě od subjektů, kde byly použity k úhradě (např. z obchodu). Tento postup není běžně k útokům využívaný, pouze ho zde uvádím jako možnost útoku. V praxi to znamená, že si útočník všímá úkonů, které poškozený (potenciálně) provádí. Po např. úhradě nákupu platební kartou, se útočník zmocní čtecího zařízení na karty a z něho dostane potřebné identifikační údaje. Možné je taky napojení zmiňované čtečky karet na např. notebook a v reálném čase odposlouchávat přenos dat.

3.3.3 Nabourání do systému (hacking / cracking)

Neoprávněný průnik do konkrétního informačního systému, provedený zvnějšku, zpravidla ze vzdáleného počítače. Samotný průnik je podmínkou pro další

neautorizovanou činnost v rámci cílového systému. Pachatelé se zpravidla nepřipojují k objektu útoku (počítači) přímo, ale pres jeden i více internetových serveru v různých částech světa. Cílem takového postupu je podstatné snížení možnosti identifikace skutečného umístění počítače, který byl při útoku užit. Po spáchání cínu na cílovém počítači je často možno zjistit pouze internetovou adresu předchozího počítače, k němuž byl pachatel připojen (a do kterého učinil popsaný zásah). Jednotlivé případy takových incidentu se liší zejména, co se týče jejich motivace (vzrušení, zábava, msta, zvedavost, hmotný zisk). Samotný pojem „*hacking*“ bývá (zpravidla, ale nikoli výlučně) spojován s jinou než zištnou (či nezvratně ničivou) motivací; pojem „*cracking*“ bývá naopak užíván právě v případech, jejichž cílem je počitatelný zisk (resp. jejichž výsledkem je nevratná škoda). [14]

3.3.4 Rafinované útoky

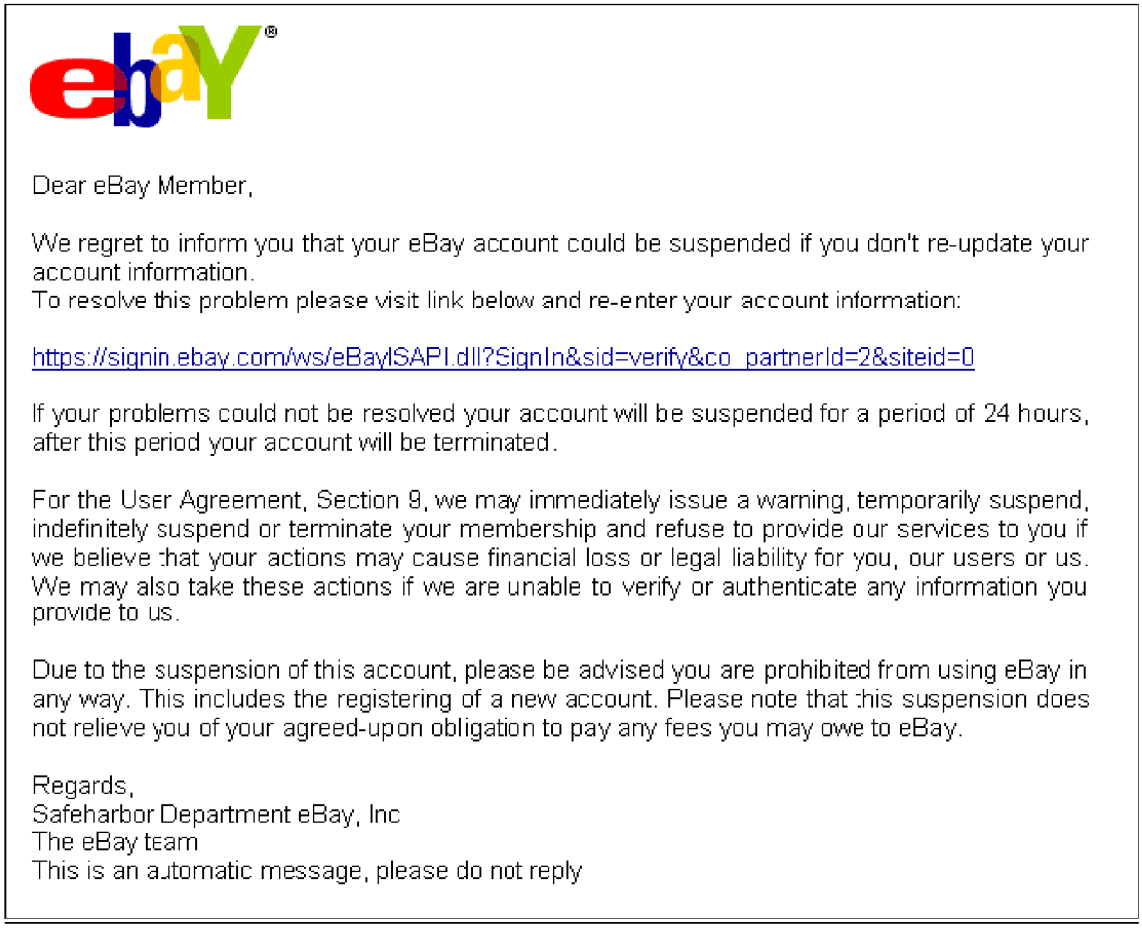
O rafinovaném útoku hovoříme v souvislosti s násilným získáním přístupových dat neoprávněným uživatelem. Může se jednat o psychické nebo fyzické vydírání, nebo neoprávněné odposlechy konkrétních komunikačních kanálů. Tyto typy útoků vyhodnocuji pro svou práci jako nedůležité, protože se v nich převážně nejedná o napadení softwarem. Za stručnou zmínku ovšem stojí.

3.3.5 „Dobrovolné“ zaslání přihlašovacích údajů

Na posledním místě (ne z hlediska důležitosti) popíšu tzv. dobrovolné zaslání přihlašovacích údajů klientem. V tomto nevinném nadpise tkví zdaleka nejnebezpečnější riziko napadení. Popíšu zde dva nejnebezpečnější útoky. Prvním z nich je:

1. Phishing - podstatou této metody, usilující o zcizování digitální identity uživatele, jeho přihlašovacích jmen, hesel, čísel bankovních karet a úctu apod. za účelem jejich následného zneužití (výběr hotovosti z konta, neoprávněný přístup k datum atd.), je vytvoření podvodné zprávy, šířené většinou elektronickou poštou, jež se snaží zmíněné údaje z uživatele vylákat. Zprávy mohou být maskovány tak, aby co nejvíce imitovaly důvěryhodného odesílatele. Muže jít například o padělaný dotaz

banky, jejíchž služeb uživatel využívá, se žádostí o zaslání čísla účtu a PIN pro kontrolu (použití dialogového okna, předstírajícího, že je oknem banky - tzv. **spoofing**). Tímto způsobem se snaží přistupující osoby přesvědčit, že jsou na známé adrese, jejímuž zabezpečení důvěřují (stránky elektronických obchodu, atd.). Tak bývají rovněž velice často zcizována například čísla kreditních karet a jejich PIN. [11]



Dear eBay Member,

We regret to inform you that your eBay account could be suspended if you don't re-update your account information.
To resolve this problem please visit link below and re-enter your account information:

https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerId=2&siteid=0

If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

Due to the suspension of this account, please be advised you are prohibited from using eBay in any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to eBay.

Regards,
Safeharbor Department eBay, Inc
The eBay team
This is an automatic message, please do not reply

Obr. 9 [11]

Modernějším a daleko nebezpečnějším „bratříčkem“ phisingu je pharming. Pokud konstatujeme, že nejlepší obranou proti phisingu je mít se na pozoru, proti pharmingu nám rozhodně pouhá opatrnost stačit nebude.

Pharming je takovým bratříčkem phishingu, mladším, sofistikovanějším a především nebezpečnějším. Ke své činnosti využívá překladu jména serveru na odpovídající IP

adresu, útočí tedy na DNS (Domain Name System). Pokud pak uživatel ve svém internetovém prohlížeči zadá adresu například www.lupa.cz, nedojde k překladu na odpovídající IP adresu 81.31.5.18, nýbrž nějakou jinou, podvrženou - a zde je kámen úrazu. Pokud by se totiž útočníkovi podařilo změnit DNS záznam výše zmiňované imaginární banky www.inetbanka.com, přesměruje se komunikace na jiný stroj, jiné stránky, které však na první pohled nelze rozpoznat od originálu. Nic netušící uživatel tedy zadá požadované přihlašovací údaje a bez větších překážek jimi obdaruje útočníka. [14]

Pokud je tedy uživatel internetový „laik“, rozhodně nemůže nic poznat. V současné době je to jeden z nejčastějších, nejnebezpečnějších a nejúspěšnějších útoků. O účinné obraně a ochraně budu opět psát v dalších kapitolách.

Pokud jste pozorně četli předcházející stránky, určitě je vám jasné, že není radno útoky proti internetovému bankovnictví podceňovat. Vzhledem k okolnostem, můžeme díky minimálnímu úsilí, zabezpečit svůj počítač takovým způsobem, abychom riziko napadení útočníkem snížili téměř na nulu. V internetovém bankovnictví obecně platí, více než jinde, že dokonalé zabezpečení, které by splňovalo podmínky neproniknutelnosti, neexistuje a nikdy existovat nebude.

3.4 Známý případ úspěšného útoku

Tato kapitola bude věnována útoku ze října minulého roku. Tento konkrétní útok má za následek několik stovek „vykradených“ a znehodnocených bankovních účtů. Útok zde v žádném případě nezveřejňuji jako návod na jeho uskutečnění, spíše jako odstrašující příklad.

Nejaktuálnějším útokem, který v poslední době bouřlivě rozvířil diskuzi právě na téma bezpečnosti (z důvodu vysokého počtu postihnutých klientů), se odehrál minulý rok a postihl klienty české spořitelny.

V e-mailových schránkách mnoha uživatelů českého internetu objevil na první pohled legitimní e-mail. Zpráva vyzývá uživatele k přechodu na nový bezpečnostní systém z důvodu množících se případů podvodů. Nabízí také přímý odkaz, na kterém by měl údajný systém běžet. E-mail obsahoval sdělení, jež vyzívá klienta k opatrnosti z důvodů neustále rostoucích útoků a dále ho pobízí ke kontrole svých bezpečnostních údajů, prostřednictvím přihlášení na svůj účet. Klient je poté odkázán na falešnou internetovou adresu s taktéž falešným přihlašovacím formulářem, který po něm vyžaduje uživatelské jméno, heslo a jakýsi doplňující bezpečnostní kód. Co klient ovšem netuší je to, že data jsou následně pod falešnou záminkou odeslána neoprávněné třetí osobě a s největší pravděpodobností následně zneužita v neprospěch majitele účtu.

4 NÁVRH ŘEŠENÍ

Samotný návrh řešení se bude dotýkat především internetového bankovnictví, jakožto nejpoužívanější služby elektronického bankovnictví. O zákazníkovi internetového bankovnictví zde budeme hovořit jako o klientovi, který odkoupí produkt u některé z tuzemských bank. Tento klient bude využívat internetové bankovnictví nejenom k tzv. pasivním operacím (zůstatek na účtu, podrobný přehled pohybu na účtu), ale také skrze tento produkt bude uskutečňovat samotné finanční transakce, tzv. aktivní operace (příkaz k úhradě, trvalý příkaz, nastavení inkasní platby). Proto, abychom mohli označovat tyto transakce jako bezpečné, tudíž adekvátně zabezpečené proti případným hrozbám musíme jednoznačně vymezit správné chování banky, která zajišťuje svoji identifikaci při přenosu, šifrování přenášených dat a identifikaci klienta, ale taky správné chování klienta při samotném procesu vlastní identifikace a při odesílání dat.

4.1 Chování banky

4.1.1 Zabezpečení zajišťující banka

Pro elektronické bankovnictví platí obecně, že zabezpečení ze strany banky je považováno za dostačující. Právě ono slovo „dostačující“ je velice ošidný pojem. Banky, které jsou v tomto případě subjekt prodávající zboží (službu) mají povinnost dokonale zabezpečit celý sektor elektronického bankovnictví. To se jim do jisté míry i daří. Úspěch kvality zabezpečení můžeme přičítat tomu, že banky jsou vysoce výdělečné organizace a mohou si do jisté míry dovolit investovat vysoké prostředky do vývoje, chcete-li vzniku dokonalého zabezpečení. Řada z nich také spolupracuje s celosvětově uznávanými bývalými hackery, kteří hledají drobné skulinky v systému zabezpečení přenosu a snaží se je nějakým způsobem opravit.

Banky v České republice používají k šifrování 128bitový symetrický klíč, který je z hlediska bezpečnosti naprosto dostačující. Některé banky postupně zavádějí dokonce 256bitové šifrování, které je o několik stupňů dokonalejší. Samotný tok dat, jedno ze tří slabých míst, které může potenciální útočník napadnout, v němž putují mezi bankou a klientem citlivé informace je tedy dostatečně kvalitně zabezpečena a dokonce i v případě, že by se třetí straně podařil tzv. odposlech dat, nebylo by možné tato data, díky šifrování žádným způsobem zneužít.

Druhým slabým místem, na které se může útočník zaměřit a které je v tomto případě nutné chránit je identifikace (autentizace) banky. Banky k této operace používají mezinárodně uznávané certifikáty (VeriSign, v ČR – První certifikační autorita), které klientovi bezezbytku zaručují, že komunikuje s bankou a v žádném případě ne s útočníkem. I v tomto směru tedy banky, z hlediska bezpečnosti, obstály a v obou případech zajišťují klientovi dokonalou bezpečnost. Pokud můžeme mluvit v tomto případě o vylepšení zabezpečení, musíme zmínit přechod všech složek elektronického bankovnictví na 256bitové šifrování, které zaručuje v daném případě přece jen o pověstný stupínek vyšší úroveň, tudíž kvalitu zabezpečení.

Je hluboce nemyslitelné, že by útočník prolomil (odposlech+překlad) zašifrovaný přenos mezi bankou a klientem, nebo že by se mu nějakým způsobem podařilo prolomit certifikát a tudíž zneužít identifikaci banky v přenosu dat. Muselo by se jednat o hrozivé selhání nejen lidského faktoru ve všech formách a na všech úrovních, ale taky o neuvěřitelné selhání techniky. Pravděpodobnost úspěšného útoku na tyto systémy zabezpečení můžeme s trochou nadsázky přirovnat k pravděpodobnosti sestrojení stroje času během následujících dvou týdnů.

Délka šifrovacího klíče		Podepsán autoritou
BAWAG Bank	128 bitů	VeriSign
Citibank	128 bitů	VeriSign
Česká spořitelna	128 bitů	VeriSign
ČSOB	128 bitů	První certifikační autorita
eBanka	128 bitů	VeriSign
GE Money Bank	128 bitů	VeriSign
HVB Bank	128 bitů	VeriSign
Komerční banka	128 bitů	VeriSign
Poštovní spořitelna	128 bitů	První certifikační autorita
Raiffeisenbank	128 bitů	VeriSign
Volksbank	256 bitů	VeriSign
WSPK	nezjištěno	VeriSign
Živnostenská banka	128 bitů	VeriSign

Tab. 3 [12]

4.1.2 „Politika“ banky

Problém samotného zabezpečení transakcí, které zajišťují banky, vidím jinde, než v kvalitě šifrování a certifikace. Celkem obstojně ho popisuje slovo „politika“.
Jedná se v prvé řadě o problém související s nátlakem banky na uživatele internetového bankovnictví. Zmiňovaný nátlak spočívá v tom, že banka staví klienta před otázku, zda zvolit komfort za cenu bezpečí, či naopak. Zde nastává prostor pro úvahy na téma, co by si měl chytrý uživatel IB zvolit, popřípadě jakým způsobem kompromis hledat a najít. Tato práce nabízí odpověď na danou otázku. Je zapotřebí přehodnotit *systém prodeje produktů internetového bankovnictví.*

Z odborných publikací, nebo článků na toto téma můžeme vyčíst dva postoje. Jeden, se kterým se ztotožní převážné procento uživatelů a redaktorů říká, *že klient internetového bankovnictví, který upřednostňuje svoje vlastní pohodlí před bezpečností, si nezaslouží*

ani jedno. Tato vhodně použitá parafráze známého výroku má rozhodně něco do sebe a nutí zainteresovaného člověka k zamyšlení. Druhým, bezpochyby taky vhodným, argumentem je to, *že klient využívá služeb internetového bankovnictví právě kvůli jeho komfortnosti.* Složité procesy autentizace a autorizace tuto pohodlnost velmi vzdalují. Můžu se zde rozepsat o hledání vhodného kompromisu, který by zajišťoval dostatečnou bezpečnost (minimální riziko úspěšného útoku) a rovněž onen potřebný uživatelův komfort. Rád bych se ovšem věnoval příčině, která si právě toto hledání kompromisu doslova vynucuje. Tomuto tématu se řada zmiňovaných publikací zdárně vyhýbá a také z tohoto důvodu bych zde rád prezentoval svůj názor.

Na vině jsou v tomto případě banky, které staví klienta do svízelné situace. Je to situace problematická nejenom v získání dostatečné bezpečnosti na úkor pohodlí využití služeb, ale také na úkor vynaložených peněžních prostředků na správu produktu, čili správu účtu. Mluvíme zde o tzv. nadstandardním zabezpečení, které nabízejí některé banky pro své klienty.

Nadstandardní zabezpečení (aktivace/zřízení)		
	PIN kalkulátor	Čipová karta + čtečka
BAWAG Bank	-	-
Citibank	-	-
Česká spořitelna	1 350 Kč	990 Kč
ČSOB	-	600 Kč
eBanka	89 Kč/měsíc	-
GE Money Bank	-	-
HVB Bank	-	-
Komerční banka	-	1 247 Kč
Poštovní spořitelna	-	-
Raiffeisenbank	-	-
Volksbank	-	-
WSPK	-	2000 Kč
Živnostenská banka	-	-

Tab. 4 [12]

Uvedu konkrétní příklad. Česká spořitelna nabízí standardní produkt IB, kde klient použije pro autentizaci pouze jméno a heslo. Tento typ zabezpečení je z mnoha důvodů (např. tzv. koukání přes rameno) nevyhovující. Pokud klient chce k autentizaci použít například PIN kalkulátor, musí si připlatit. Nejedná se pouze o administrativní poplatek,

jak můžeme vyčíst z tabulky. Nezpochybňuji fakt, že za kvalitnější služby se zpravidla platí víc, ale v tomto případě je to přinejmenším diskutabilní. Pokud tedy banka disponuje lepší technologií zabezpečení, proč ji nemůže nabídnout jako standardní způsob ochrany účtu? Samotný PIN kalkulátor lze pořídit řádově za stokoruny, proč se tedy banky snaží vydělat tímto způsobem na klientovi i z hlediska zabezpečení sytému? Tady vidím první problém v interakci mezi prodávajícím (bankou) a kupujícím (klientem). Napadá mě jednoduché řešení, banka nabídne klientovi k dispozici ten nejlepší systém zabezpečení, kterým disponuje. Místo bezplatného zavedení internetového bankovnictví zavede paušální poplatek v řádu desetikorun za zřízení této služby a zajistí tak svým klientům tu nejlepší péči, kterou jim je schopná nabídnout. Cílem této bakalářské práce není zkoumat, o kolik se v případě zavedení této inovace do praxe zvednou, nebo naopak sníží, příjmy banky. Jen je potřeba navrhnout komplexní řešení daného problému s jediným výstupem, zkvalitněním zabezpečení finančních transakcí. Paušální poplatky za zřízení toto rozhodně umožňují.

Nejedná se samozřejmě pouze o Českou spořitelnu, podobným způsobem hospodaří i mnoho jiných bank, nejenom u nás. Přinejmenším tato otázka otvírá další prostor k diskuzi. Pominu-li tedy fakt, že k jednomu produktu jsou nabízeny dva různé způsoby zabezpečení (jedno nevyhovující, druhé „nadstandardní“ a zpoplatněné), vzniká otázka jakým způsobem se stávající nebo potenciální klient o tomto způsobu řešení bezpečnosti dozví. Jako klient, využívající služeb internetového bankovnictví České spořitelny více než dva roky, mohu čestně prohlásit, že jsem nebyl při „kupování“ tohoto produktu obeznámen bankovní úřednicí o možnosti rozšíření zabezpečení s použitím nadstandardních služeb. Předpokládám, že v tomto ohledu nejsem rozhodně ojedinělý případ. Nezpochybňuji ovšem, že informace, které zde prezentuji, nebyly uvedeny ve smlouvě o vytvoření internetového bankovnictví, ale v zájmu banky by mělo být, poskytnout mi bezprostředně informace o zkvalitnění produktu. Tímto se dostáváme k dalšímu problému.

4.1.3 Komunikace mezi bankou a klientem

Je nedostatečná. Banky, které nabízejí svým klientům komfort v podobě internetového bankovnictví, musí být v úzkém kontaktu s klientem a pravidelně ho informovat nejenom o nových produktech, ale taky o rostoucích bezpečnostních rizicích, nových způsobech zabezpečení a nových technologiích. Banky musí brát v potaz, že většina jejich klientů není IT experty a taky nestudují nejnovější trendy ve výpočetní technice. Tomuto by měli komunikaci se zákazníkem přizpůsobit. Protože spravují citlivá data a finance svých klientů, měli by banky podle mého názoru projevit větší míru předvídavosti chování klienta. Souvisí to i s výše popisovaným problémem nabídky nadstandardních služeb klientům. Pokud by banka měla předvídat chování klienta, měla by mu nabízenou službu představit, vysvětlit přínos při zavedení této služby a všeobecně ho informovat o všech potřebných parametrech. Dle mého názoru je i tohle další podstatný problém z hlediska vztahu mezi bankou a klientem. Jako uživatel tří různých produktů internetového bankovnictví u tří různých tuzemských bank, si dovolím tvrdit, že na některých pobočkách chybí expert, který by se této problematice věnoval blíže. Běžní bankovní úředníci vás odkážou na internetové stránky, nebo na brožuru, která je vydána za tímto účelem. Pokud by se mohlo zdát, že zde uvedené problémy se zabezpečením přímo nesouvisí, rád tohle vysvětlím.

4.1.4 Prevence z pohledu bankovních ústavů

Nejenom v zubních ordinacích platí, že prevence je základ. Totéž můžeme parafrázovat při používání internetového bankovnictví a neklade se tomu v tomto případě o nic menší důraz. Jak důležitá by byla prevence, se mohli přesvědčit klienti, resp. banky po napadení phishingem. Pokud by s dostatečným předstihem informovaly své klienty o tom, že banka v žádném případě nekomunikuje s klientem prostřednictví e-mailu, ale zásadně písemně nebo osobním kontaktem, nemuselo by dojít k tolika úspěšným útokům. Jak už to tak bývá, všechno zlé, je k něčemu dobré a právě tento problém rozpoutal diskuzi na téma zabezpečení internetového bankovnictví. Pokud banky chtějí svého zákazníka dokonale ochránit, měly by splňovat následující kritéria:

1. *Technologie zabezpečení na dostačující úrovni (popsáno výše)*
2. *Nepodceňovat hrozbu útoku*
3. *Kvalitní komunikace s klientem*
4. *Předvídat chování klienta*
5. *Vypsání zásad bezpečné práce s internetovým bankovnictvím a distribuci těchto zásad klientovi (osvěta)*

Těchto pět jednoduše popsaných zásad je potřeba pro dokonalé zabezpečení celého procesu internetového bankovnictví z pohledu banky. Jinými slovy, při dodržení těchto postupů banka zajistí odpovídající kvalitu svého zabezpečení. Následuje poslední část komunikačního řetězce – klient (klientská stanice).

4.2 Chování klienta

Klient, resp. klientská stanice, je nejslabším článkem celého procesu internetového bankovnictví. I zde platí, že systém je tak slabý, jak je slabý jeho nejslabší článek. Proto je nutné zaměřit se na klienta, jeho stanici, která slouží ke spojení s bankou a vymezit jeho vhodné chování při práci s internetovým bankovnictvím. Běžný uživatel internetového bankovnictví není profesionální administrátor, proto mnohdy netuší, jaké možnosti počítač nabízí. S rozšířením trvalého internetu do našich domácností a rozvojem P2P sítí vzniká z bezpečnostního hlediska mnoho problémů. Pokud vezmeme v úvahu, že je klient postaven před samotný produkt IB s pevně stanoveným zabezpečením (systémem autentizace a samotné autorizace operací), je potřeba zajistit dvě věci, pro minimalizaci bezpečnostních rizik – zabezpečení klientské stanice a vhodné chování klienta při používaní IB.

4.2.1 Zabezpečení klientské stanice

1. Operační systém – uživatel využívá v naprosté většině MS Windows (95, 98, 200, XP, XP + SP2) přičemž platí, že verze starší, než MS Windows XP SP2 (SP – service

pack) jsou nevyhovující. Obsahují celou řadu mezer v bezpečnosti a ani jejich aktualizace nezabrání možným průnikům. Klient by tedy měl mít na svém počítači nainstalovanou minimálně tuto verzi operačního systému a pravidelně jej aktualizovat. Aktualizovat operační systém může klient okamžitě po vypuštění nové verze a to výhradně na stránkách distributora daného operačního systému. Zde jsou důvody proč užívat alespoň MS Windows XP SP2:

Ochrana počítače před nebezpečnými přílohami
Upozorněním na potenciálně nebezpečné přílohy pomáhá aktualizace SP2 chránit počítač proti virům, které se mohou šířit prostřednictvím aplikací Internet Explorer, Outlook Express (poštovní klient) a Windows Messenger.

Vylepšená ochrana osobních údajů při procházení webu
Použitím nastavení zabezpečení, které chrání počítač před soubory a obsahem stahovaným pomocí aplikace Internet Explorer, chrání aktualizace SP2 vaše soukromé informace.

Blokování potenciálně nebezpečných stahovaných souborů
Aplikace Internet Explorer sleduje stahování, přičemž informační panel upozorňuje uživatele na potenciálně nebezpečné stahované soubory a poskytuje možnost zablokovat soubory, které mohou způsobit škodu.

Omezení počtu obtěžujících automaticky otevíraných oken
Díky funkci blokování automaticky otevíraných oken, která umožňuje snížit množství nevyžádaného obsahu a reklam, které se automaticky otevírají při procházení webu, je práce na Internetu mnohem příjemnější.

Ochrana Bránou firewall od spuštění po ukončení činnosti systému
Výkonná integrovaná Brána firewall systému Windows je nyní ve výchozím nastavení zapnuta. Systém Windows XP je tak chráněn proti virům a červům, které se šíří prostřednictvím Internetu.

Opatření proti zhroucení způsobenými doplňky prohlížeče

Pomocí nového Správce doplňků v aplikaci Internet Explorer lze snadno zobrazit a ovládat nainstalované doplňky a omezit tak nebezpečí zhroucení aplikace, což omezí potíže při procházení webu.

Bez těchto oprav a aktualizací se používání prohlížeče internetových stránek stává nebezpečným.

2. *Internetový prohlížeč* – na straně klienta je prohlížeč velice důležitou součástí zabezpečení. Internetový prohlížeč bývá nejčastěji ohrožen chybou při samotném vývoji a umožňuje třetí osobě zaútočit na klientův počítač a např. přesměrovat data. Klient si může vybrat z mnoha prohlížečů, ale nejrozšířenější jsou Internet Explorer, Mozilla Firefox, Opera a Konqueror. Všechen tento software samozřejmě vychází v aktuálních verzích a je pouze volbou klienta, který z nich zvolí.

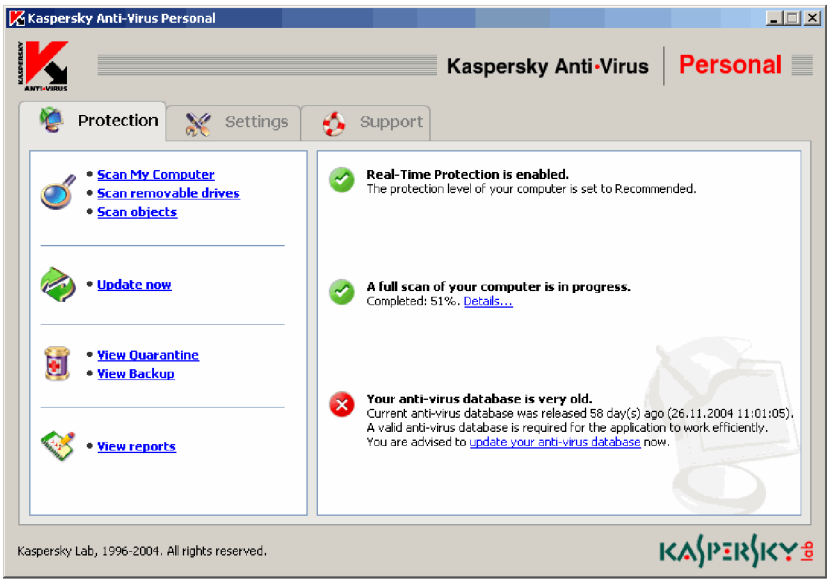
Prohlížeč	Počet objevených chyb	Z toho nezáplatováno
Internet Explorer 6.x	82	31
Mozilla Firefox 1.x	19	7
Opera 8.x	5	0
Konqueror 3.x	10	1

Tab. 5 [12]

Z tabulky můžeme vyčíst, že nejrozšířenější IE významně zaostává za svými alternativními kolegy. Nejenom v počtu chyb, ale taky v rychlosti oprav jednotlivých složek zabezpečení a rychlosti vývoje nových verzí. Všechny chyby samozřejmě nejsou kritické, ale o samotném softwaru vypovídají mnoho. Pokud tedy banka podporuje jiný prohlížeč, měl by si klient vybrat ten nejbezpečnější. V tomto případě by klient měl zvolit Operu 8. x (a vyšší verze).

3. Ochrana proti virům a spyware – jaké škody může tento software napáchat na našem počítači, jsem popsal v předešlých kapitolách. V této kapitole popíšu obranu proti tomuto záškodnickému softwaru. K dispozici je řada antivirových a anti-spywarových programů s propastně rozdílnou kvalitou. Představím tedy dostatečně kvalitní software, který zaručuje klientovi spolehlivou ochranu, ať už preventivní, nebo samotné léčení napadeného počítače. Jedním z nejlepších produktů na trhu je:

Kaspersky antivirus – tento antivirový produkt disponuje několika výjimečnými přednostmi. V prvé řadě má velmi kvalitní rezidentní štít, který bývá označován za nejdůležitější součást antiviru. Jednoduše řečeno, zabraňuje tomu, aby byl počítač infikován. Pokud z jakéhokoliv důvodu tento rezidentní štít selže, následuje práce pro samotný antivirový program. Kaspersky antivirus důkladně prověří stávající data na disku, bezpečně detekuje případnou infekci, oddělí ji od nenapadených souborů a zvolí nejvhodnější způsob léčby. V některých případech stačí soubor pouze vyléčit, někdy je nutné celý soubor nenávratně odstranit z disku. Tento antivirus disponuje především, pohodlným uživatelským rozhraním, má intuitivní ovládání a také působí proti spywaru, adwaru, atd. Poslední předností tohoto programu, kterou bych zde rád vystihl je minimalizace falešných poplachů (ikdyž počítač bezpečně napaden není – antivirový program hlásí infikaci), což leckterý uživatel jistě ocení. Protože je tento program určen pro komerční využití, neustále vycházejí nové verze s aktualizovanou databází škodlivého softwaru a jeho zneškodnění.



Obr. 10

Alwil Avast – dalším zajímavým produktem je tento antivirový program. Jeho nespornou výhodou je to, že je zdarma k dispozici pro domácí užití. Pyšní se kvalitním scanem zaměřeným hlavně na síťovou komunikaci vyprodukovanou internetovými viry (tzv. červi). I přes nekomerční využití v domácí sféře, stejně jako v předchozím případě vycházejí v krátké době aktualizované databáze, které obsahují nejnovější verze virů. Tento program rovněž obsahuje rezidentní štít, ale podle mnohých expertů nedosahuje kvalit jako u Kaspersky antiviru. Při likvidaci případné infekce jsou využívány dříve sesbírané informace o jednotlivých souborech, ale i kontroly pevného disku, které se spouští v momentě, kdy je případná havěť jen stěží aktivní. Pro mnoho uživatelů bude používání Alwil avastu poměrně náročné, vzhledem ke komplikovanosti nastavení při testech (scanech) a léčeních. Se vším případně pomůže nápověda a žádného zodpovědného klienta služeb internetového bankovnictví by neměla prvotní nesrozumitelnost s ovládáním odradit od jeho užití.

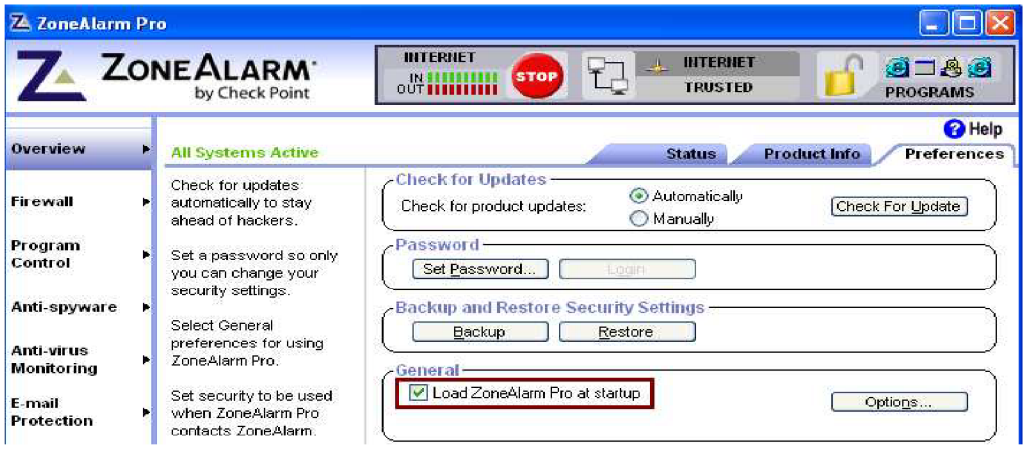
Obr. 11

Doporučuji vhodně mezi sebou tyto dva antivirové programy kombinovat. To znamená, bez okolků scanovat pevný disk prostřednictvím obou programů, pouze rezidentní štít by měl zůstat zapnutý pouze jeden. V tomto případě doporučuji využít služeb rezidentního štítu u kaspersky antivirus. Klient rovněž nesmí zapomenout software pravidelně aktualizovat (s důrazem na slovo pravidelně).

4. Firewall – je nejčastěji v podobě tzv. personálního firewallu a měl být taktéž výbavou uživatele přistupujícího k internetu. Přítomnost firewallu je téměř nutností v momentě, kdy je uživatel k Internetu připojen veřejnou IP adresou a jeho počítač je tak přímo dosažitelný odkudkoliv z Internetu._Uživatel služeb internetového bankovnictví by se tedy měl připojovat k internetu přes firewall, což je program nebo technické zařízení, které minimalizuje rizika neoprávněného přístupu k vašemu počítači z internetu. Firewall zpracovává pouze vámi povolené dotazy do internetu a všechna ostatní potencionálně nebezpečná data odfiltruje. Důležitým sdělením je to, že firewall zabudovaný ve Windows XP SP 2 nestačí! Nebrání odchozímu spojení a je možné ho určitým způsobem obejít (přelstít). Firewall pro domácí (osobní) využití lze zdarma získat na stránkách výrobce nebo distributora. Doporučuji využívat *Kerio Personal*

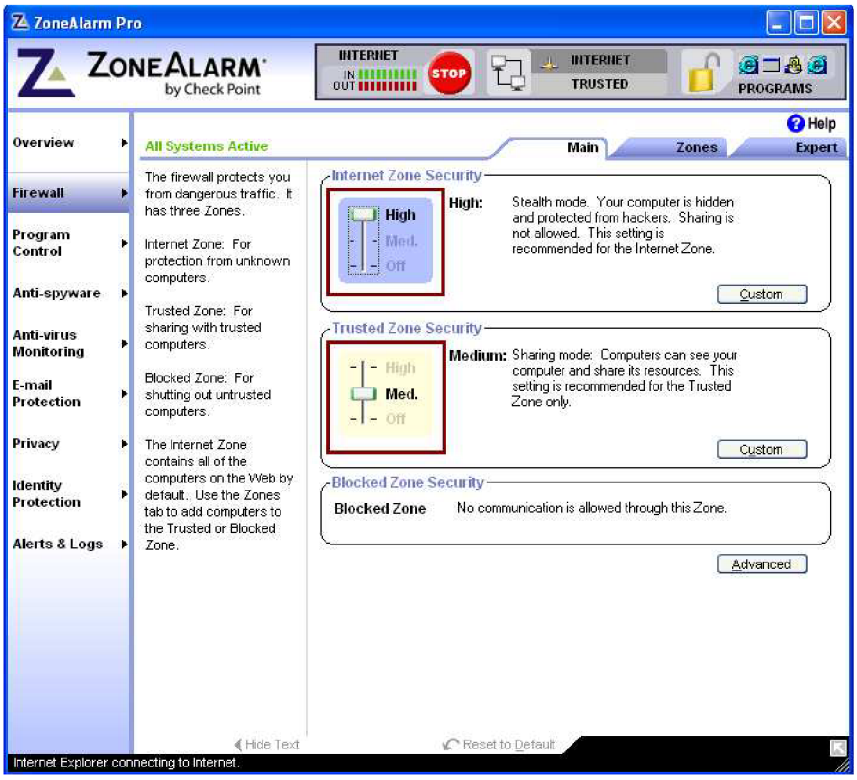
Firewall a Zone Alarm Firewall. Z vlastní zkušenosti se přikláním ke druhému produktu, hlavně z důvodu snadnějšího a pohodlnějšího ovládání. Z hlediska bezpečnosti jsou na tom oba dva zmiňované firewall produkty obdobně velice dobře a zajišťují uživateli bezpečnou ochranu před útoky „z venku“. Neméně důležité je mít firewall správně nastaven a to tak, že případné útoky na IP adresu budou správně detekovány a filtrovány. Ukážeme si to na příkladu užití firewallu od ZoneAlarm, konkrétně pro verzi ZoneAlarm 7.0.337.000 Pro.

Po instalaci, musíme nastavit charakteristiku počítače. To znamená nastavit několik parametrů, jako jsou třeba, zda je počítač připojen do místní sítě, kolik na něm pracuje uživatelů, jaká jsou rizika, a jednou z posledních položek je, jestli si zvolíme automatické, nebo manuální nastavení filtrování procesů. Je jednoduché se spoléhat na automatické nastavení, nicméně pokud chce mít uživatel takřka dokonalou jistotu o bezpečnosti, je vhodnější zvolit ruční nastavení. Po nastavení charakteristik do prohlížeče je firewall automaticky spuštěn. Jako první doporučuji nastavit automatické spuštění po startu operačního systému.



Obr. 12

Poté nastavíme citlivost firewallu, pro připojení do internetu doporučuji nejvyšší opatrnost (high), pro připojení do tzv. Trusted Zone (viz. další stránky) si vystačíme se střední opatrností (medium).



Obr. 13

Základem firewallu je paketový filtr, který rozhoduje podle stanovených pravidel, jaké pakety pustí směrem dovnitř, nebo ven. Pravidla si můžeme nastavovat několika typy způsobů. Můžeme využít obecná pravidla, která platí pro všechny programy, nebo pravidla přísná, kde povolíme, resp. zakážeme konkrétní porty u konkrétních programů. Ze začátku je doporučeno používat obecná pravidla, než si uživatel zvykne a nabere zkušenosti, později může přejít k přísnějším pravidlům. Příkladem takového obecného pravidla může být toto nastavení:

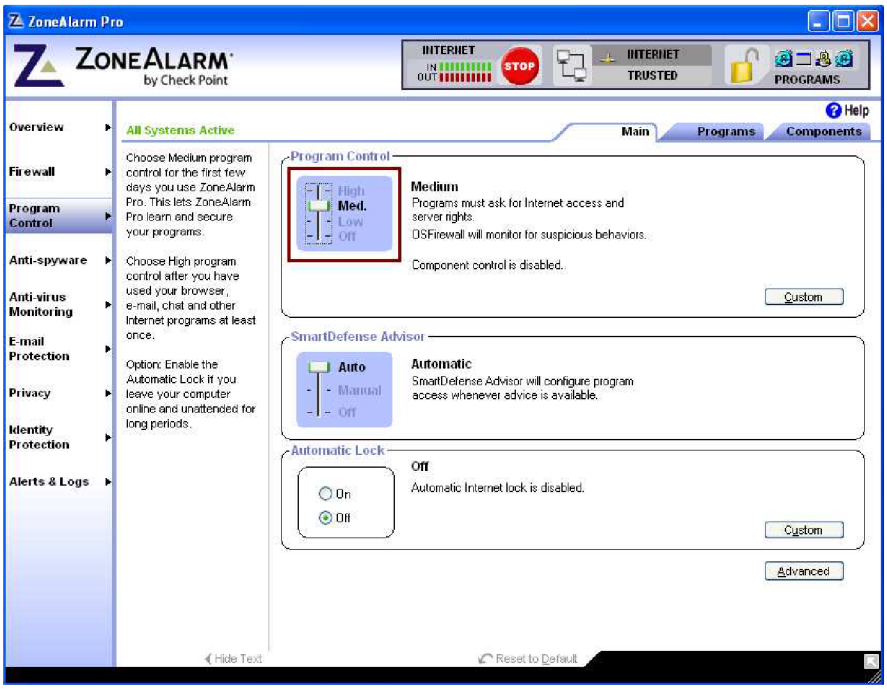
- *typ: obecné*
- *směr: dovnitř*
- *protokol: TCP a UDP*
- *cílový port: 135 - 139, 445*
- *adresa vzdálených počítačů: odkudkoliv*
- *akce: blokovat*

Toto nastavení blokuje příchozí (dovnitř) připojení na TCP a UDP portech 135 – 139 a 445 (sdílení v síti). Pro nastavení přísnějších pravidel je vhodné využít databázi portů,

která je umístěna přímo v počítači, nebo na internetových stránkách, kde je po zadání termínu do vyhledávače snadno dostupná. Příkladem přísnějšího pravidla je toto nastavení firewallu:

- *program: explorer.exe (internetový prohlížeč)*
- *směr: ven*
- *protokol: TCP*
- *cílový port: 21, 80, 443, 8000, 8080*
- *adresa vzdálených počítačů: kamkoliv*
- *akce: povolit*

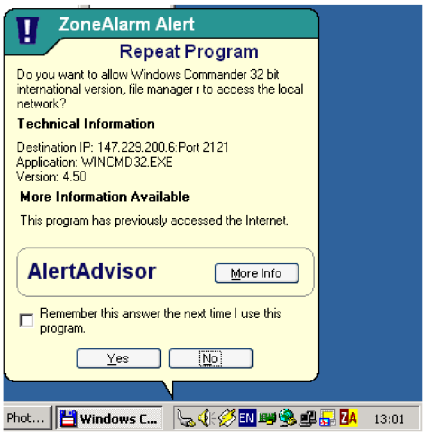
Upravuje stav povolení akce pro použitý program explorer.exe a odchozí data na portech 21, 80, 443, 8000, 8080 v protokolu TCP. Nastavení firewallů u rozdílných počítačů je velice různorodé, proto nelze jednoznačně nadefinovat správné nastavení, pouze doporučit určité metody k jeho dosažení. Pokud není uživatel počítačový expert, doporučuji následovné logické zacházení s firewallem. Nastavení chování firewallu při pokusu programu o přístup do internetu na položku medium. Toto nastavení zajistí, že pokud bude program vyžadovat připojení k internetu nebo síti, zeptá se uživatele, zda chce toto připojení povolit.



Obr. 14

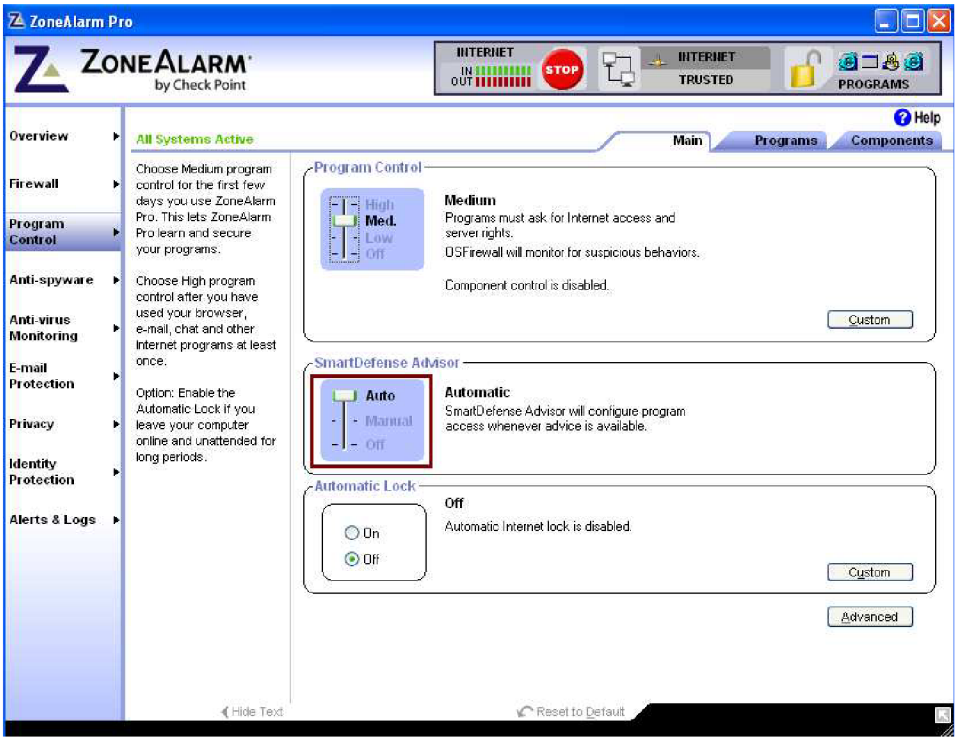
Pokud uživatel ví, že program, který má být povolen právě spustil, logicky povolí přístup. Naopak, pokud mu program, jenž povolení vyžaduje, bude neznámý, povolení zakáže (může si vybrat, zda natrvalo, nebo pouze dočasně) a tím se fakticky vyhne připojením nežádoucích programů do sítě internet.

Pokud uživatel uvidí, že se nějaký program s podezřelým názvem snaží o připojení, doporučuje se nakouknout do Wintask process library (databáze procesů, které MS Windows využívá, dostupná na internetu) a pokud tam proces nenajde, musí ho zakázat. V případě, že po nějaké době zjistí, že omezil nějaký bezpečný proces, může program dodatečně povolit.



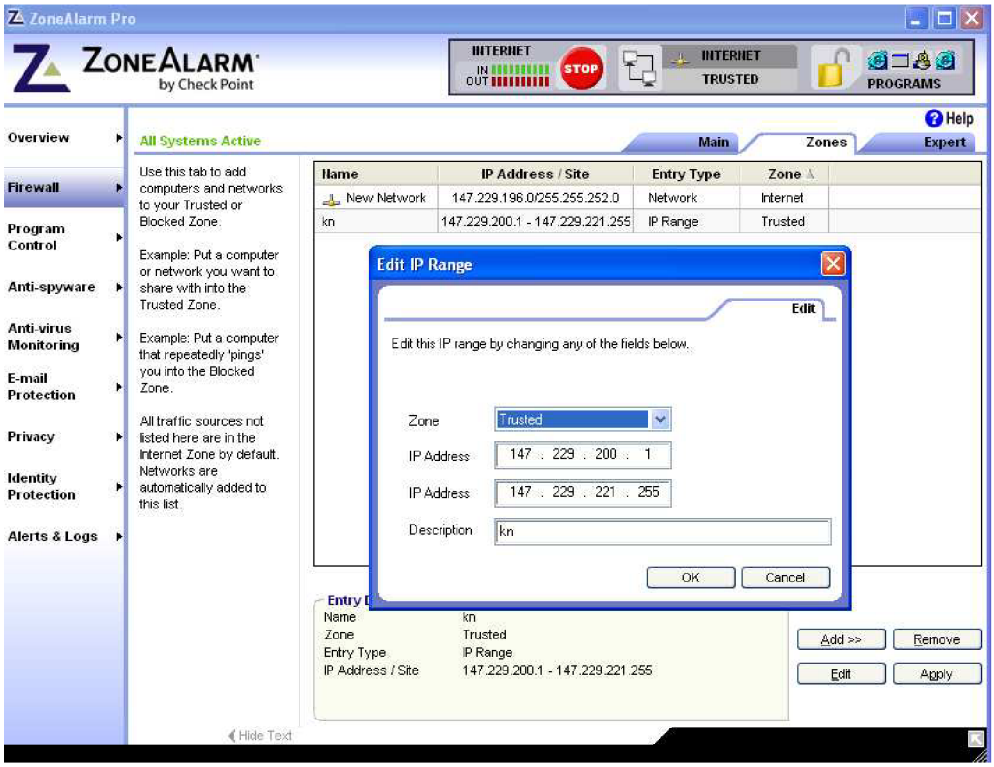
Obr. 15

Dalším důležitým nastavením firewallu, je tzv. sledování spuštěných programů. Tento proces zajistí, že viry nebo malware nebudou moci bez povšimnutí spustit prostřednictvím povoleného programu jiný, který by již byl pro uživatele nebezpečný. V ZoneAlarm firewallu má toto sledování programů název SmartDefence a zapíná se automaticky. Pouze doporučuji zapnout tzv. SmartDefence advisora (nastavení: auto), který nás v případě problému upozorní a tento problém vysvětlí.



Obr. 16

Pokud je počítač připojen k místní síti, zbývá už pouze přidat tuto síť do důvěryhodných položek, aby s ní mohl počítač (resp. síťová karta) komunikovat. Zadání probíhá vypsáním intervalu povolených IP adres, které budou označeny jako „trusted“ (ověřené). Tím zajistí uživatel bezproblémovou komunikaci s počítači připojenými ve stejné síti. Těmito kroky je firewall nastaven a připraven k použití.



Obr. 17

Tím by byla uzavřena kapitola: ochrana klientské stanice. Aby tato ochrana byla bezezbytku dokonalá, musí se každý uživatel těchto produktů dopodrobna seznámit s jejich možnostmi, jejich ovládáním a případně jejich nedostatky. Pokud bude mít uživatel tyto softwarové zabezpečení pouze nainstalované na svém osobním počítači a nebude si vědět rady s jejich správným použitím, bezpečnost počítače může být významně ohrožena. Počítač může být kvalitně zabezpečen, dostatečně zabezpečen může být i přenos dat, ba dokonce i identifikace banky, pokud uživatel nebude dodržovat zásady bezpečného užití internetového bankovnictví, opět bude celý proces významně oslaben.

4.2.2 Bezpečné užití internetového bankovnictví

1. V každém případě se přihlašovat ke službám internetového bankovnictví z tzv. „bezpečného“ počítače. Jedná se o počítače, u kterých můžete ovlivnit jejich bezpečnostní nastavení, a mají k němu přístup jen důvěryhodné osoby. V žádném případě by se klient neměl přihlašovat do systému prostřednictvím počítačů umístěných v internetových kavárnách nebo hernách.

2. Klient si musí vybrat nejdokonalejší zabezpečení IB, které mu banka je ochotná poskytnout a neohlížet se na komfort a cenu. Nevyhovující je autentizace pouze pomocí jména a hesla, odpovídající je užití čipových karet nebo tokenů. Musí také požadovat jednoznačnou možnost autorizace jednotlivých transakcí (pomocí SMS zpráv).

3. Klient se musí bezpodmínečně vždy po ukončení práce s internetovým bankovnictvím odhlásit ze svého účtu, aby zamezil neoprávněnému užití. Banky nabízejí proces automatického odhlášení ze systému, který je v tomto případě velice vhodným prostředkem ke zvýšení kvality zabezpečení. Přehled časových intervalů nabízí následující tabulka:

BAWAG Bank	5 min.
Citibank	5 min.
Česká spořitelna	max. 20 min.
ČSOB	20 min.
eBanka	není
GE Money Bank	5 min.
HVB Bank	5 min.
Komerční banka	5 min.
Poštovní spořitelna	20 min.
Raiffeisenbank	není
Volksbank	30 min.
WSPK	30 min.
Živnostenská banka	30 min.

Tab. 6 [12]

Pokud je doba automatického odhlášení příliš krátká, značným způsobem omezuje uživatele v práci, naproti tomu, pokud je příliš dlouhá, zvyšuje tak riziko zneužití.

Vhodným kompromisem se zdá být nastavení automatického odhlašování na cca 15 minut.

4. Za žádných okolností nemůže klient prozradit přístupové jméno a heslo, ani rodinnému příslušníkovi ani pracovníkům banky. Tímto je zčásti ochrání před zneužitím třetí stranou.

5. Nepoužívat jednoduchý PIN, vždy zvolit nejdelší možnou délku a jako PIN neudávat snadno odvoditelné čísla (telefonní číslo, datum narození, po sobě jdoucí posloupnost čísel).

6. PIN si nikam nezaznamenávat. Zcela nevhodný je záznam na papírky, do počítače, v peněžence, do diáře, v telefonu, na čipové nebo platební kartě. Originál obálky, která obsahovala PIN, zničte nebo uschovejte na bezpečném místě (např. v trezoru). PIN neukládejte ani na místo, kde ukládáte jiné osobní dokumenty. Pokud už tedy musí být PIN uschován, nikdy na stejném místě jako uživatelské jméno.

7. Při používání počítače *nikdy* nepovolte zapamatování hesla. Tento „nešvar“ moderních internetových prohlížečů se může snadno stát tragickým.

8. Pravidelně měnit používaná hesla. Toto opatření opět snižuje riziko, že budou citlivá data zneužita třetí stranou.

9. Pokud klient využívá služeb podpisového certifikátu, měl by se vyvarovat jeho uložení na pevný disk počítače, nebo v horším případě na internetu.

10. Nikdy nestahovat z internetu „neznámé“ soubory (zejména s příponou *.exe). To úzce souvisí s tím, že klient by měl navštěvovat pouze důvěryhodné stránky na internetu a vyhnout se stránkám s diskutabilním obsahem. Tyto soubory mohou jako vedlejší produkt nainstalovat na počítač nebezpečný software.
11. Neotvírat e-mailové zprávy od neznámých adresátů, nebo zprávy s podezřelým názvem či obsahem. V žádném případě nespouštět přílohy takovýchto e-mailových

zpráv. Zprávy okamžitě smazat. Nikdy nereagovat na e-mail, který po vás bude požadovat sdělení vašich osobních údajů, hesla nebo PINu. Banky touto formou s klientem zásadně nekomunikují.

12. Klient by si měl ověřit certifikát stránky, na které se k účtu přihlašuje (v pravém dolním rohu okna v případě internetového prohlížeče MS Internet Explorer 6 a v pravém horním rohu okna v případě Internet Explorer 7 zkontrolujte zobrazení ikony „zámku“). Nenechte se napálit symbolem zámku, který se objeví přímo na internetové stránce. Pro podvodníky je snadné zkopírovat obrázek zámku. Vy musíte hledat ten, který se objevuje v rámu okna prohlížeče Internet Explorer. Po najetí kurzoru se v IE vypíše zpráva jakou technologii šifrování je přenos zabezpečen.

Obr. 18

13. Pokud stránka nebude reagovat na zadání přihlašovacích údajů obvyklým způsobem, nebo se při přihlašování do služeb internetového bankovnictví objeví nějaké podezřelé chovaní, musí klient bezpodmínečně kontaktovat banku. Může zde jít o přesměrování na jiné, nebezpečné stránky (viz. phishing a pharming).

14. Pokud banka podporuje zasílání SMS zpráv při jakémkoliv pohybu na účtu, klient by si měl tuto službu aktivovat. Případně se obrátit na banku, která tuto službu podporuje a zajišťuje.

Běžný klient je postaven před celou řadu otázek. Správných odpovědí je hned několik. V této souvislosti se samotných zabezpečením, nevidím největší hrozbu v technologii, ale v lidském faktoru. Pokud selže první stupeň zabezpečení, je na řadě druhý a třetí atd., pokud ale selže lidský faktor, znamená to v mnoha případech prolomení bariéry mezi úspěšným a neúspěšným útokem. V návrhu zabezpečení bych vystihl slovo

„prevence“, v tomto případě to znamená o problému hovořit, nevyhýbat se mu a řešit ho. Často tento postup přinese kýžené odstranění (vyřešení) problému.

Důležitým faktorem při předcházení útokům je nepodceňovat riziko hrozby. Všeobecně platí, že modernizace probíhá v důsledku hledání slabých míst produktu a zvyšování nároků. Je vcelku pozdě otevřít téma zabezpečení elektronického bankovnictví až po úspěšných útocích z roku 2006. V zabránění útoků stačilo pouze dostat do podvědomí uživatelů informaci, že banka s klientem prostřednictvím e-mailových služeb nekomunikuje. To jsou přesně ty podceňované faktory hrozeb. Jakákoliv manipulace s penězi, ať už v peněžence nebo v cyberprostoru je nebezpečná a vždycky byla. Proto není na místě podceňovat riziko ani v internetovém bankovnictví, jakkoliv se tato služba může jevit na první pohled bezpečná. Analýza a návrh odhalili dle mého názoru, dostatečné množství bezpečnostních mezer a je v zájmu poskytovatelů internetového bankovnictví tyto mezery odstranit a s tím odstranit i starosti klientům.

5 PŘÍNOS NÁVRHU ŘEŠENÍ

Návrh řešení jasně definoval pravidla pro bezpečné užití, jak připojení k internetu, tak využití internetového bankovnictví. Pokud klient tyto pravidla bude striktně dodržovat a řídit se jimi, je šance hrozby minimální. Nemyslím, že hrozby v souvislosti s internetovým bankovnictvím návrh zabezpečení podcenil, nebo naopak přecenil. Poctivě popsal všechny aspekty zabezpečení, v závislosti na jejich kvalitě v celkovém řetězci obrany proti útokům. Pokud mám brát v potaz kompletní přínos práce jako celku, rád bych zde uvedl, že přináší objektivní pohled na použité a dostupné technologie v elektronickém bankovnictví. Kapitola s názvem „chování banky“ vysvětluje problémovost komunikace mezi bankou a klientem a obsahuje subjektivně laděnou úvahu nad prací bankovních ústavů v naší republice. Celkově jsem se snažil o jasnou, stručnou a objektivní analýzu vymezených problémů, které při práci s elektronickým bankovnictvím vznikají, jejich odstranění. Jsem si vědom, že k dokonalé bezpečnosti elektronického bankovnictví není potřeba pouze definovat

hrozbu a její možné odstranění. Důležité je rovněž, zamyslet se nad příčinou samotného útoku, kde vznikla skulinka k jeho úspěšnému provedení a jak těmto útokům do budoucna předcházet. Právě tento model řešení jsem se ve své práci snažil uplatnit. Dost možná někomu pomůže.

6 ZÁVĚR

Elektronické bankovnictví bude vždy rizikovou formou obchodování. Stejně jako jakákoliv jiná forma elektronického obchodování, stejně jako jakákoliv jiná forma obchodování a stejně tak jako jakákoliv jiná manipulace s financemi. Vždy budou taky existovat hrozby, které můžou ovlivnit nebo omezit zmiňovanou manipulaci. Nemůžeme ovšem dovolit, aby míra ohrožení byla tak vysoká, že by celkově zamezila jakékoliv manipulaci s financemi v různých formách a při různých příležitostech. Neodpustím si parafrázovat známé rčení: „pokud existuje útok, existuje i obrana“. V elektronickém bankovnictví bychom mohli toto rčení upravit a to tak, že pokud existuje hrozba (nikoliv útok), musíme najít obranu. Tato práce se o to snažila. Na úplný závěr bych rád uveřejnil některé mýty, se kterými byla tato práce konfrontována.

1. **Zvýšení bezpečnosti modelu zabezpečení bude výhodné pro obě strany.**
   Banky musejí dbát na dostupnost a použitelnost svého zabezpečení a zejména na časovou náročnost. Mezi těmito procesy a samotných zabezpečením musí nalézt vhodný kompromis, protože ne vždy použití nejvyššího stupně zabezpečení je nejvhodnější.

2. **Současné zabezpečení konkrétních ústavů je dost kvalitní, aby odolalo přímým útokům.**
   Nikdy nelze podceňovat neuskutečněné útoky. Musí platit pravidlo, že je nepřijatelné vynalézt novou ochranu až po prolomení bezpečnostních bariér.

3. **Experti IT mohou okamžitě přijít na novou, dosud nepoznanou metodu zabezpečení a tu začlenit do běžného provozu.**

Bohužel nemohou. Nelze očekávat, že se ze dne na den změní zabezpečení jednotlivých bank. Tento proces si vyžádá mnoho dnů testování ve virtuálním prostředí a až pak může plynule a nenásilně přejít do provozu využitelného v praxi.

7 SEZNAM POUŽITÉ LITERATURY A DALŠÍCH PRAMENŮ

Knihy a publikace:

[1] PŘÁDKA, M., KALA, J. *Elektronické bankovnictví: rady a tipy.* 1. vyd. Praha: Computer Press, 2000. 166 s. ISBN 80-7226328-5.

[2] PEKÁRKOVÁ, L. E*lektronické bankovnictví, jeho možnosti a další vývoj.* Brno, 2006, 60 s. Bakalářská práce na Ekonomicko-správní fakultě Masarykovy Univerzity. Vedoucí diplomové práce Ing. Jan Krajíček.

[3] DOSEDĚL T. *Počítačová bezpečnost a ochrana dat*. 1. vyd. Brno: Computer Press, 2004. 122 s. ISBN: 80-251-0106-1.

Elektronické zdroje:

[4] RAŠEK L. – MAYEROVÁ T. Bezpečnost elektronické komunikace. *IT Systems* [online]. 2006, č. 11 Dostupné z <http://casopis.systemonline.cz/5919-bezpecnost-elektronicke-komunikace.htm>.

[5] *Předpoklady zabezpečení* [online]. c2007 Dostupné z <http://www.adminxp.cz/security/index.php?aid=187>.

[6] BOUŠKOVÁ, K. *Internetové bankovnictví: jsou vaše peníze v bezpečí?* [online]. Publikováno 22.9.2006. <http://www.penize.cz/zpravy/4684/internetove-bankovnictvi-jsou-vase-penize-v-bezpeci/> ISSN 1213-2217.

[7] VONDRÁŠEK, J. Důvěra v bezpečí a rizika v současném prostředí elektronického podnikání. *DSM* [online] 2001, č. 1 Dostupné z <http://www.dsm.tate.cz>.

[8] BITTO, O. *Rhybaření střídá pharming* [online[. Publikováno 31.3.2005 <http://www.lupa.cz/clanky/rhybareni-strida-pharming/>.

[9] BEDNÁŘ, V. *Pharming je zpět a silnější* [online] Publikováno 23.3.2007 <http://www.lupa.cz/clanky/pharming-je-zpet-a-silnejsi/>.

[10] *Platební karty a jejich druhy* [online] c2007 <http://www.penize.cz/produkty/platebni-karty/texty/1969/platebni-karty-a-jejich-druhy/?IDP=1>.

[11] JIROVSKÝ, V. *Základní definice, vztahující se k tématu kybernetických hrozeb* [online] <http://www.mvcr.cz/bezpecnost/informacni/zakladni_info.pdf>.
[12] ZÁMEČNÍK, P. – KRČMÁŘ, P. *Analýza zabezpečení internetového bankovnictví v České republice* [online] Publikováno 29.6.2005 <http://i.iinfo.cz/urs-att/Mesec.cz-studie_int.bankovnictvi-112002647608700.pdf>.
[13] ŽALOUDNÍKOVÁ, V.: Bezpečnost internetového bankovnictví: skutečnost, nebo mýtus? *iDnes.cz* [on-line] 2004. Dostupné z: <http://fincentrum.idnes.cz/>.
[14] *Wikipedia* Dostupné z <http://www.wikipedia.cz>

Seznam obrázků a tabulek:

Seznam příloh:

8 PŘÍLOHY

8.1 Příloha první

Nejdelší šifrovací klíč

- Volksbank (256 bitů)

Největší počet možností autentizace klienta

- eBanka, Česká spořitelna (3 způsoby)

Největší počet možností autorizace platby

- eBanka (3 způsoby), Česká spořitelna (2 způsoby + "žádná")

Nejdelší povinné uživatelské jméno

- Citibank (16 znaků - číslo platební karty)

Nejrychlejší informace o neoprávněném vstupu na účet

- GE Money Bank, Živnostenská banka (volitelné SMS info při vstupu na účet)

Nejdelší doba odhlášení od účtu

- eBanka, Raiffeisenbank (nikdy nedojde k automatickému odhlášení)

Nejnižší maximální denní limit transakcí

- GE Money Bank (10 tis. Kč u aplikace s nižší úrovní zabezpečení)

Nejvyšší minimální poplatek při zřízení internetového bankovnictví

- HVB Bank (490 Kč - platí se za autentizační kalkulátor)

Nejvyšší cena za nadstandardní zabezpečení

- WSPK (2 000 Kč za umístění certifikátů v USB tokenu)

Nejdražší roční obnova podpisového certifikátu

- Česká spořitelna (320 Kč)

Nejlevnější SMS zprávy při změně stavu účtu

- Česká spořitelna (0 Kč)

[12]

8.2 Příloha druhá

Dobry den vazeni klienti!

Leto roku 2006 bylo pro Banku nejzavaznejsim z hlediska poctu nelegalnich operaci.
Cim dal vice maji podvodnici zajem o duvernou informaci nasich zakazniku.
Velke mnozstvi lidi se na nas obraci s zadosti zamezit vzniku nebezpeci ztraty peneznich prostredku z uctu.
S ohledem na soucasny stav vyhlasuje Banka nasledujici mesic za mesic boje s frodem.
Do 1.listopadu musi vsechny nasi klienti aktivovat novy system bezpecnosti vlastnich uctu.

Provedli jsme velkou praci pro zlepseni bezpecnosti. System byl zkontrolovan uznavanymi odborniky v oboru elektronickych plateb, a vsechny nezavisli experti potvrdili ucinnost systemu proti frodu. Z duvodu nebezpeci mozneho zneuziti techto udaju podvodniky nejsou tyto data zverejnena v otevrenych zdrojich.
Vy jste byl (a) zvolen (a) jako jeden z ucastniku finalniho stadia testovani systemu.
V soucasne dobe Vam navrhujeme vyuzit odkaz https://www.servis24.cz/ebanking-s24/ a standardnim zpusobem prihlaseni do Internet bankingu aktivovat novy bezpecnostni system.

V aktualnim stadiu provozu jsou mozne nektere nesrovnalosti.
Pripoustime jejich existenci, a proto prosim nezasilejte dodatecne popisy vznikajicich potizi, prace na jejich odstraneni jiz probihaji.
Musime Vas informovat o bezpodminecnem pouziti noveho systemu od listopadu, v opacnem pripade budou Vase ucty zablokovany do okamziku uplne identifikace Vasi osoby. Proto doporucujeme v nejkratsi mozne dobe prejit na novy bezpecnostni standard.
S pozdravem, Oddeleni Banky pro ochranu pred frodem (záměrně bez interpunkce) [8]

8.3 Příloha třetí

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 (automatická ústředna)	- Nepřetržitý provoz – dostupnost 24 hodin denně, 7 dní v týdnu.	- 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 využívá 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 sofware 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 - Spojení s bankou je možné z kteréhokoli počítače připojeného k síti internet - Relativně snadná obsluha - Další výhody stejné jako u *HomeBankingu (viz výše)* – přehlednost, hromadné příkazy atd	- Na rozdíl od Homebankingu jej nelze propojit s účetním softwarem - Není tak operativní, jako například GSM Banking (internet není mobilní)

[2]