# Počítačová kriminalita a její prevence v bankovním sektoru

Cyber crime and its prevention in the banking sector

Bc. Roman Poloch

Diplomová práce

2010

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2009/2010

# ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

| | |
|---|---|
| Jméno a příjmení: | **Bc. Roman POLOCH** |
| Studijní program: | **N 3902 Inženýrská informatika** |
| Studijní obor: | **Bezpečnostní technologie, systémy a management** |
| Téma práce: | **Počítačová kriminalita a její prevence v bankovním sektoru** |

Zásady pro vypracování:

1. **Proveďte obecnou literární rešerši a analýzu na téma počítačová kriminalita.**
2. **Analyzujte počítačovou kriminalitu v bankovním sektoru.**
3. **Specifikujte způsoby prevence před počítačovou kriminalitou v bankovním sektoru.**
4. **Navrhněte způsob zabezpečení před počítačovou kriminalitou v bankovním sektoru.**
5. **Materiál opatřete tabulkou a obrázkovou dokumentací.**

Rozsah práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:


1. **MATĚJKA, Michal. Počítačová kriminalita. vyd. Praha : Computer Press, 2002. 106 s. ISBN 80-7226-419-2.**
2. **VLČEK, Martin. Počítačové právo. vyd. Praha : C. H. Beck, 1995. 261 s. ISBN 80-7179-009-5.**
3. **POŽÁR, Josef. Informační bezpečnost. vyd. Plzeň : Vydavatelství a nakladatelství Aleš Čeněk, 2005. 309 s. ISBN 80-86898-38-5.**
4. **ČANDÍK, Marek. Základy informační bezpečnosti. vyd. Zlín : Univerzita Tomáše Bati, 2004. 107 s. ISBN 8073182181.**
5. **MUSIL, Stanislav, RNDr. Počítačová kriminalita. vyd. Zlín : Institut pro kriminologii a sociální prevenci, 2000. 107 s. ISBN 80-86008-80-0.**
6. **LANCE, James. Phishing bez záhad. Praha : Grada Publishing, a.s., 2007. 281 s. ISBN 978-80-247-1766-1.**
7. **JIROVSKÝ, Václav. Kybernetická kriminalita. vyd. Praha : Grada Publishing, a.s., 2007. 284 s. ISBN 80-247-1561-9.**
8. **Allen Harper, Shon Harris, Chris Eagle, Jonathan Ness, Michael Lester. Hacking - manuál hackera. vyd. Praha : Grada Publishing, a.s., 400 s. ISBN 978-80-247-1346-5.**


Vedoucí diplomové práce: **Ing. Roman Šenkeřík, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **19. února 2010**

Termín odevzdání diplomové práce: **7. června 2010**

Ve Zlíně dne 19. února 2010


prof. Ing. Vladimír Vašek, CSc.
*děkan*

doc. RNDr. Vojtěch Křesálek, CSc.
*ředitel ústavu*

## ABSTRAKT

Cílem diplomové práce je přiblížit problematiku počítačové kriminality, která se vyskytuje v bankovním sektoru. Za prvé provedu obecnou rešerši počítačové kriminality. Poté se zaměřím na různorodost forem počítačové kriminality v bankovním sektoru. Dále zde uvedu způsoby prevence a ochrany před touto kriminalitou. V praktické části práce je specifikován způsob zabezpečení před počítačovou kriminalitou v bankovním sektoru pomocí zavedení bezpečnostní politiky banky. Po zavedení bezpečnostní politiky byla provedena analýza hrozeb a cílů bezpečnostního prvku jménem „firewall“. Tato analýza je znázorněna v tabulce.



Klíčová slova:

Všechna klíčová slova jsou vysvětlena v textu diplomové práce.



## ABSTRACT

The thesis aims to bring the issue of cyber crime, which occurs in the banking sector. Firstly, make a general search cyber crime. I shall discuss the variety of forms of computer Crime in the banking sector. Furthermore, here the means of prevention and protection against this crime. The practical part is specified way of security against cyber crime in the banking sector through the establishment of security policy bank. Following the introduction of safety Policy analysis was made of threats and security objectives of the element name "Firewall". This analysis is shown in the table.



Keywords:

All keywords are explication in text diplom work.

Chtěl bych velmi poděkovat vedoucímu diplomové práce panu Ing. Romanu Šenkeříkovi, Ph.D., za vedení mé diplomové práce, za jeho ochotu, trpělivost a pomoc při jejím zpracování.

**Prohlašuji, že**

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

**Prohlašuji,**

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně

…….

podpis diplomanta

# OBSAH

# ÚVOD

Počítačová kriminalita je odvětvím trestné činnosti. Vyskytuje se ve všech vyspělých zemích, které využívají výpočetní techniku a vzrůstá v nich informační průmysl.

V dnešní době se výpočetní technika užívá k většině činnostem. Je to nastroj k řízení správy státu, bankovním odvětví, technickém průmyslu, zdravotnictví či v armádě a dalších odvětvích lidské činnosti. Prostřednictvím počítačových systémů lze shromažďovat informace do databází, které jsou pak využitelné k usnadnění práce. Databáze se můžou pomocí počítačové sítě navzájem propojit, poté mohou napomáhat ke komunikaci mezi jednotlivými státy světa.

Při poškození počítačových systémů, které jsou celostátně vytvořené, může dojít k dezorganizaci mnoha sfér společenského života. Zpracované informace mají totiž stejnou cenu jako finance, majetek či jiný produkt lidského práce.

Počítačová kriminalita má několik odlišností od té „klasické“ kriminality. Odlišnosti je zejména ve způsobu provedení, typ pachatele a následně i jeho odhalování. Tento trestný čin může být spáchán během krátkého časového úseku. Tím se rozumí, že pachatel může vytvořit např. předdefinovaný program, který má naprogramovaný sled příkazů. Tento program může vykonat pouhým stisknutím tlačítka na klávesnici všechny tyto příkazy. Z toho vyplývá, že v počítačové kriminalitě jsou pachatelé rychlejší než v klasickém případu kriminality. Rychlost se samozřejmě odvíjí od použitého počítačového vybavení tedy na výkonu počítače. Dalším nezanedbatelným rozdílem bývá prolomení vzdálenosti mezi pachatelem a místem činu. Prolomením vzdálenosti je myšleno, že počítačová kriminalita může být vykonávána na velké vzdálenosti, aniž by se pachatel zvednul od svého počítače. Z charakteristiky vyplývá, že pachatelé těchto činů jsou většinou lidé s nadprůměrnou inteligencí, vyšším vzděláním a také s velkým zájmem o techniku v oblasti počítačů či jsou zběhlí v počítačovém programování. Pachatelé se nesnižují k násilným činům, či nevyužívají zbraně, proto bývá na místě činu málo důkazního materiálu, který v konečném důsledku nenapomáhá k vyšetření činu počítačové kriminality tak moc, jak by bylo zapotřebí. Přenosy informací v počítačových sítích jsou uskutečňovány pomocí datových paketů, které se ve většině případů nezaznamenávají a nearchivují. Výjimkou jsou již počítačové sítě ve větších firmách, které již využívají bezpečnostní standarty a svou komunikaci na síti archivují. Tyto firmy by měly mít poté větší přehled o uživatelích dané počítačové sítě. V případě výskytu

počítačové kriminality v jejich sítí mohou lépe dohledat slabý prvek v sítí a pro příště ho lépe zabezpečit. Pachatelé počítačové kriminality využívají čím dál tím lepší techniku a z pohledu pachatel versus ochrance je to nikdy nekončící boj.

# I. TEORETICKÁ ČÁST

# 1 POČÍTAČOVÁ KRIMINALITA

## 1.1 Úvod do počítačové kriminality

Počítačová kriminalita je dnes aktuálním jevem. O informace byl vždy velký zájem, i když v minulosti byly informace uchovávány v papírové podobě. V minulosti bylo zvykem vyzrazení informací nazývat pojmy jako vyzvídání, vyzrazování či špionáž. Hlavně podle uplatnění ukradených informaci. Z toho plyne, že by se mohlo hovořit o informační kriminalitě, která je lidmi chápaná lépe než počítačová kriminalita.

Pojmem počítačová kriminalita se obvykle označují ty trestné činy, které jsou zaměřené proti počítačům a stejně tak i trestné činy páchané prostřednictvím počítače. Počítačová kriminalita je definována velmi obecně jako trestný čin namířený proti počítačovému systému nebo trestný čin, při kterém je použita výpočetní technologie. Mnoho lidí chápe počítačovou kriminalitu jako aktivitu, která vede k manipulaci v počítačovém systému (čtení dat bez autorizace, manipulace, vymazání nebo přepis dat či zneužití dat). Tento jev se nazývá „počítačová defraudace“ a je to jedna z metod počítačové kriminality. Metoda má za cíl získat výhodu či peníze pro vlastní neoprávněnou potřebu.

Členské státy Evropské Unie se dohodly na definici počítačové kriminality: „je to nemorální a neoprávněné jednání, které zahrnuje zneužití údajů získaných prostřednictvím ICT[1] nebo jejich změnu“. Počítače ve své podstatě nelze chápat jako novou trestnou činnost, ale poskytuje novou technologii a nové vylepšené způsoby páchání již známých trestných činů jako špionáž, neoprávněné užívání cizí věci či vydírání.

Charakteristika počítačové kriminality má řadu odlišných rysů od té „klasické“ kriminality. V mnoha případech počítačové kriminality se neobjeví takový prvek, jako je brutální násilí, použití střelné zbraně, újma na zdraví osob. Jestliže u „klasické“ kriminality se trestný čin odehrává v časovém horizontu minut, hodin, dnů, pak trestný čin v oblasti počítačové kriminality může proběhnout v několika vteřinách a pachatel nemusí být ani přímo přítomen na místě činu.

Další možná charakteristika pro počítačovou kriminalitu je z pohledu značné ztráty, ať již přímo v podobě financí nebo v podobě zneužití nabytých informací. Počítačovou kriminalitu charakterizuje i skryté chování trestné činnosti. Poté tato kriminalita často bývá spjata s názvem „zločin bílých límečků".

Počítačová kriminalita souvisí i s ochranou informací a dat v informačních systémech. Pokud je hovořeno o počítačové kriminalitě, musí pachatel vykonat za pomocí počítače nebo jiné moderní výpočetní technologie čin, který naplňuje skutkovou podstatu trestného činu. Tudíž musí čin spáchaný pachatelem dosahovat určitého stupně nebezpečí pro společnost definovaný trestním zákoníkem.

Trestné činy spáchané pomocí výpočetní techniky bylo zapotřebí sjednotit a členit. Evropská Rada jedno takové členění odsouhlasila a tím i sjednotila legislativu v evropských zemích, protože trestná činnost provozována pomocí počítačové techniky má v širším důsledku mezinárodní charakter.

Evropská rada rozčlenila počítačovou kriminalitu takto[2]:

V minimálním seznamu trestných činů v počítačové kriminalitě je obsaženo:

- počítačové podvody,
- počítačové falzifikace,
- poškozování počítačových dat a programů,
- počítačová sabotáž,
- neautorizovaný přístup,
- neoprávněný průnik,
- neoprávněné kopírování autorsky chráněného programu,

---

1 ICT ( z anglického Information and Communication Technologies), je označení o informační a komunikační technologie.

[2] Úmluva Rady Evropy o počítačové kriminalitě, [citováno 23. 11. 2001], Convention on Cybercrime - ETS no. 185. Dostupný z http://conventions.coe.int/

- neoprávněné kopírování fotografie.

Volitelný seznam trestných činů zahrnuje:

- změna v datech nebo počítačových programech,
- počítačová špionáž,
- neoprávněné užívání počítače,
- neoprávněné užívání autorsky chráněného programu.

Když Evropská rada vymezila jednání v počítačové kriminalitě do těchto dvou seznamů, došlo k podstatnému vymezení trestných činů, které jsou stíhány v evropských zemích. Minimální seznam vymezuje jednání, která by měla být zakotvena do právních řádů v jednotlivých zemích Evropské unie. Volitelný seznam obsahuje jednání, která by měla být kvalifikovaná jako trestné činy. Počítačová kriminalita byla touto klasifikací shrnuta do srozumitelnější roviny. Vyšší stádium této kriminality je kyberterorismus, který vyplývá z počítačové kriminality, ale na rozdíl od ní vyvolává strach širších mas obyvatel.

## 1.2 Počítačová kriminalita v České republice

Počítačovou kriminalitu v České republice rozšířily dva momenty a tím se rozmohla i tato zákonem postižitelná činnost. Dva momenty, které rozšířily počítačovou kriminalitu jsou: 1. nástup PC (osobních počítačů), 2. vznik počítačových sítí (vzdálená komunikace mezi PC). Velký třesk počítačové kriminality způsobila miniaturizace počítačů a jejich cenová dostupnost. Velké sálové počítače ze zabezpečeného prostředí se osvobodily díky technologické modernizaci a miniaturizaci až do podoby dnešních přenosných počítačů či kapesních počítačů. Tento moment miniaturizace a zároveň cenové dostupnosti změnil i podmínky pro páchání trestných činů s využitím počítače.

Česká republika v letech 1991-1992 došla k zařazení zcela nových skutkových podstat z hlediska počítačové kriminality. Tyto podstaty jsou zakotveny v ustanovení § 257a – poškození a zneužití záznamu na nosiči informací a § 178 – neoprávněné nakládání s osobními údaji.

Ustanovení byla zapotřebí zakotvit do zákonu, protože se začaly objevovat čím dál víc propracovanější činy naplňující skutkovou podstatu trestného činu za využití výpočetní techniky. V letech, kdy vstupovalo ustanovení v platnost, se již začaly objevovat počítačové útoky na bankovní sektor České republiky.

### 1.2.1 Podvody

Technologická inovace počítačů zvyšuje rozmanité možnosti podvodníkům. Podvodníci za pomoci a využití počítačů usnadňují svou činnost a zvyšují účinnost klasické trestné činnosti. Podvody jsou hlavní trestnou činnosti České republiky v oblasti hospodářství. Podvodníci za využití výpočetní techniky udali nový rozměr tohoto trestného činu.

Základní výhody podvodu vykonaných za pomoci počítačů jsou:

- Útočník či podvodník má možnost infiltrace do informačního systému a přemazat či dokonce vymazat data skladované v těchto systémech. Po teoretické strance za sebou nezanechají žádné stopy.
- Velká část populace z psychologického pohledu důvěřuje výsledkům, které zpracoval počítač. Těmto informacím důvěřují a považují je za prioritně správné. Slepá důvěra v informace na počítači vede k tomu, že trestné činy tohoto typu jsou úspěšné. Podvodníci spoléhají na tuto důvěru obyvatelstva.

Aspekty, které zapříčiňují velkou úspěšnost podvodu, můžeme rozdělit:

- zvyšující zkušenosti a znalosti pachatelů podvodů,
- obtížnou permanentní kontrolou výpočetních systémů,
- způsobem a námahou provedení, protože práce a operace s počítačovými daty a jejich modifikace pro zkušené programátory nejsou tak obtížné jak reálný čin, kde musí pachatel být na místě činu (např. bankovní loupež, krádež ).

### 1.2.2 Padělky

Inovace ve výpočetní technice napomohla zločincům tím, že zločinci využívají ke své práci grafické počítačové programy pro profesionální grafickou úpravu padělků. Pomocí

těchto programů např. vytvářejí falešné doklady, technické průkazy pro kradená auta či jiné doklady. Možností využití grafických programů je nepřeberné množství. Jsou zaznamenány i padělky cenných papírů nebo různých bankovních dokumentací.

Zločinci se nyní zaměřují na moderní druhy padělků a to vytváření kopií elektronických karet: telefonních, kreditních (úvěrových), debetních (platebních).

### 1.2.3 Počítačové podvody v bankovním sektoru

V posledních deseti letech se v bankovnictví ČR zaznamenala minimálně desítka zveřejněných bankovních počítačových zločinů. Všechny tyto zločiny, které byly udělány s využitím počítače, měly podobný cíl - manipulaci s bankovními záznamy ( účty, soubory převodních příkazů).

Je nutno podotknout, že spousta těchto zločinů není zveřejňována z důvodu utajení. Banky nechtějí tyto případy zveřejňovat , aby nedošlo k zdiskreditování pověsti banky. Samozřejmě na finančním trhu operují i spousty jiných firem jako pojišťovny, leasingové společnosti, obchodníci s cennými papíry apod.. V soukromém sektoru existuje ještě více firem, kde jsou počítačově zpracovávány finanční převody či účetnictví firmy. V těchto firmách, které mají horší zabezpečení než banky, je větší riziko vystavení útočníkům.

Útočníkům napomáhá i fakt, že probíhá mnohem víc denních bankovních transakcí než před deseti lety. Toto napomáhá ke skrytosti individuálních útoků na účty, než tomu bylo kdykoliv předtím. Pachatel při útocích musí mít znalosti o účtu, jeho stavu a operacích s ním. Další metodou může být manipulace s desetinnými čárkami, manipulace s kurzy, zvýšení poplatků. Obrovské množství transakcí tyto individuální činy maskují.

Banka se brání proti skrytým metodám okrádáni většinou kontrolou svého informačního systému. Banka má mít standardizované pracovní postupy a samozřejmě je musí dodržovat. Zajišťovat vnitřní kontrolní mechanismy, využívat interní a externí finanční audit či bezpečnostní audit.

### 1.2.4 Pyramidové hry

Pyramidové hry jsou zástupcem dnes už legendárních případů počítačových finančních her. Již předchozí známé tzv. „letadla“ se s využitím výpočetní techniky znásobily do mnoha tisíců účastníků. Základní podstata tkví v přerozdělování finančních zdrojů

vložených účastníky do hry. Finanční kapitál se rozdělí ve prospěch hráčů a zčásti ve prospěch zřizovatele hry. Při registraci hráčů se jim podle pořadí přiřadí priorita. Jejich priorita hodně souvisí i s pravděpodobností, že neskončí hru se ztrátou. Tyto hry nezaručují zisk, jedná se pouze o to, kdy se do hry registrujete a čekáte na finance od uživatelů, kteří se registrují po vás. Zřizovatel hry určí pravidla, která v konečném důsledku nedodrží pro své vlastní obohacení.

### 1.2.5 Porušování autorských práv

Nelegální využití výpočetní techniky se neustálilo pouze na technickém vybavení počítače tzn. hardwaru, ale útočníci využívají také programové vybavení počítače tzn. software. Útočníci se soustřeďují na dva druhy duševního vlastnictví, které je chráněno autorským zákonem. Prvním druhem jsou audiovizuální nahrávky a druhým druhem jsou počítačové programy.

Průzkum majitelů největších softwarových firem ukázal na to, že každý druhý software v ČR se využívá nelegálně.

Příklady způsobů nelegálního zásahů do autorských práv:

- Nejběžnější je využití licence softwaru patřícího zaměstnavateli pro soukromé využití (podnikání).
- Dalším způsobem je zásah do programů jiných osob, následné přepracování těchto programů a vydávaní za své. Přepracované programy jsou i distribuovány dalším subjektům.
- Poté jsou i situace, kdy firmy zakoupí pouze jednu licenci softwaru na jeden počítač, ale program je zkopírován do ostatních počítačů určených k podnikání.
- Na trhu se vyskytují i padělky softwarových produktů.
- Programátoři vedou stále spory o licenční práva mezi sebou a jejich zaměstnavateli.

### 1.2.6 Počítačové viry

Nejvíce medializovaným počítačovým zločinem je infikování počítačů počítačovým virem. V moderní době se objevují nebezpečné viry a tzv. makroviry.

Kriminalita vztahující se k počítačovým virům má dvě fáze: zaprvé je vytvořen (naprogramován) program. Při vytvoření viru na počítači programátora, nelze ještě hovořit

o trestném činu. Pokud tento vytvořený vir programátor nepoužije pro infikování počítačů. Až teprve poté co infikuje programátor jakýkoliv informační systém, dochází k naplnění skutkové podstaty trestného činu a tudíž se z programátora stává pachatel, který je již ze zákona postižitelný.

### 1.2.7 Zneužití osobních dat

Nyní se ukládají všechny informace do informačních databází a na přenosné nosiče či na externí disky. Zájem o tyto informace vyvolává i zájem pachatelů o obsah těchto informačních databází z důvodů jejího pozdějšího prodeje.

Zájem pachatelů je o dvě oblasti:

- Osobní údaje a data občanů,
- Hospodářsky využitelné údaje.

Pro velký výskyt těchto případů zcizení osobních údajů bylo zapotřebí zavést zákon o ochraně osobních údajů.

### 1.2.8 Trestná činnost spojená s Internetem

Internet a s ním spojená trestná činnost se dá kategorizovat do dvou částí:

- Veškeré shromažďování či zpřístupňování informací, které jsou choulostivé a mohou vytvořit újmu nebo založit trestný čin či mohou být nelegálně využity – informační trestná činnost,
- Provedení trestné činnosti v internetovém prostředí – tzv. internetová trestná činnost.

#### *1.2.8.1 Informační trestná činnost*

Komunikační médium jako je internet může uchovat spoustu informací, ale také sbírat data o uživatelích. Běžným způsobem sběru informací jsou různé registrace na internetových portálech. Některé portály ani nejsou oprávněny tyto data uchovávat. Uživatele nemají žádnou kontrolu, jak je s jejich daty nakládáno. Uživatelé si za zneužití svých dat částečně mohou sami svou neopatrností a důvěrou v pochybné internetové portály.

#### *1.2.8.2 Internetová trestná činnost*

Na internetu se dá trestná činnost dělit na:

- Zásahy do zdrojových kódů jinými lidmi vytvořených programů a databází.
- Porušování autorských práv vědomým kopírováním cizího díla (např. zkopírovaný zdrojový kód WWW stránek, vkládat a distribuovat cizí díla na svých stránkách bez souhlasu majitele.
- Neoprávněné využití počítače či informačního systému za využití identifikačních údajů jiné osoby.
- Získaní cizích dat neoprávněně, získávání utajovaných informací – špionáž s použitím počítače
- Zakázané šíření pornografie. Tento trestný čin spadá do skutkové podstaty, pokud jsou šířeny prvky pedofilie nebo pokud je pornografie přístupná mladistvým osobám.
- Trestné činnosti jako tzv. „letadla“ neboli pyramidy.
- Jeden z trestných činů, který je na internetu souvisí s podporou a propagací hnutí směřujících k potlačení práv a svobod občanů.
- Další trestný čin, který se na internetu vyskytuje,je zneužití platebních a obchodních systémů. Toto zneužití nastává v internetových obchodech či jiných platebních portálech. Zprvu byly zneužívány platební karty, ale nyní se využívají techniky vylepšené metody jako phishing (viz. kapitola 2.1 ) a pharming (viz. kapitola 2.2 ).
- Na internetu se mohou objevit i pomluvy a diskreditace osob. Pomluvy jsou trestným činem pokud ten, kdo je šíří, ví o jejich nepravdivosti či jimi poškodí dobré jméno osoby.

### 1.2.9 Softwarové pirátství

Softwarové pirátství neboli počítačové pirátství je jednou z trestné činnosti, kterou pachatel úmyslně zkopíruje programové vybavení (software). Pachatel poté tento software distribuuje a prodává dál za účelem zisku nebo provozuje prácí za účelem zisku pro jinou osobu.

**Druhy softwarového pirátství:**

#### *1.2.9.1 Pirátství koncových uživatelů*

Jsou to případy, kdy uživatelé si neoprávněně kopírují originální software.

Pirátství koncových uživatelů lze dělit:

- Nainstalování softwaru na více PC i když má majitel pouze jednu zakoupenou licenci.
- Neoprávněné kopírování CD,DVD či Blue-ray za účelem jejich distribuce.
- Opatření softwaru určeného pro školství nebo verze softwaru, která není určena pro komerční využití pro neoprávněnou distribuci těchto softwaru.
- Vypůjčování si mezi uživateli CD nebo DVD se softwarem.

#### *1.2.9.2 Nadužívání softwaru typu klient – server*

Pirátství tohoto typu se vyskytuje ve firmách, kdy jedna uživatelé připojení na síti používají ve stejný čas jednu centrální kopii programu bez zakoupené multilicence.

#### *1.2.9.3 Internetové pirátství*

Pirátství na Internetu je trestný čin, pokud na stránkách internetu je zdarma ke stažení licencovaný software.

Na Internetu muže narazit na tyto formy internetového pirátství:

- webové stránky, které nabízejí volně a zcela zdarma licencovaný software ke stažení
- aukční stránky na Internetu, které nabízejí padělaných licencovaný software (např. software nabízen pod jinou značkou)
- sítě pro výměnu dat (Peer-to-Peer), které umožňují sdílení a následný přenos programů či audiovizuálních souborů, které jsou chráněny autorskými zákony

#### *1.2.9.4 Nahrání na pevný disk*

Tento jev se objevuje při prodeji nových počítačů. Systém spočívá v tom, že firma nahraje operační systém na počítač bez platné licence. Firma si tímto zatraktivní prodej počítače, ale porušuje zákon o autorských právech.

#### *1.2.9.5 Padělání softwaru*

Tato počítačová kriminalita spočívá v tom, že dochází k nelegálnímu kopírování, vytváření napodobenin a následný prodej těchto nelegálních kopií vydáváním za originální produkt, který je chráněný autorskými právy. Když je software zabalen do ochranné folie je snadno zjistitelné, zda je software padělán. Zabalený software musí obsahovat licenční smlouvu, nálepku, registrační kartu a bezpečnostní znaky.

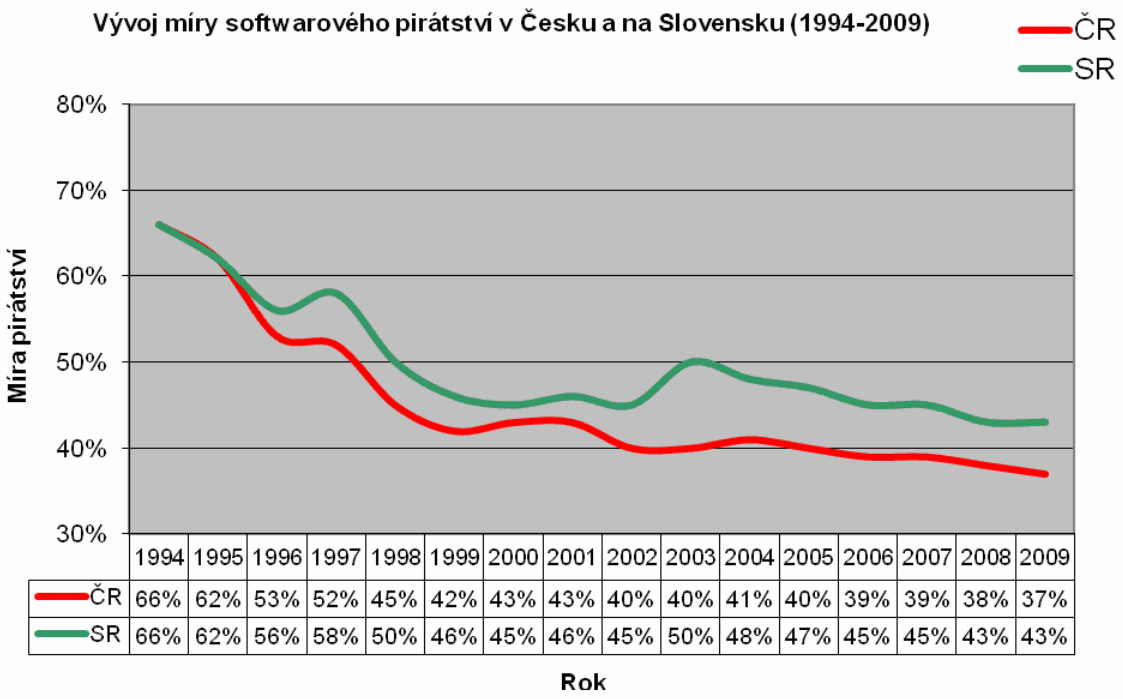
***Faktory ovlivňující míru softwarového pirátství***

Firmy vytvářející software se snaží co nejvíce minimalizovat ztráty, které vytváří softwaroví piráti. Velký podíl na snížení ztrát je prodej značkových notebooku či PC s předinstalovaným softwarem. Tento předinstalovaný software je tzv. OEM software. OEM se distribuuje společně s hardwarem za nižší a pro uživatele cenově výhodnějších částek. Jednou z dalších možnosti jak snižovat softwarové pirátství mají vlády každého státu. Tuto možnost je zapotřebí chápat jako správně vykonstruovanou zákonnou základnu pro dodržování autorských práv.

Samozřejmě s přibývajícím počtem uživatelů se softwarové pirátství rozrůstá. Tuto skutečnost zapříčinila větší gramotnost nových uživatelů a rozmach Internetu. Riziko softwarového pirátství vzniká v zemích, kde se k novému počítači nainstaluje volně šiřitelný OS (Linux, FreeDos apod.), protože valná většina uživatelů není zvyklá na tyto OS a nainstaluji si nelegální kopii OS Windows.

***Softwarové pirátství ČR v číslech***

Organizace s název BSA (Business software alliance) se snaží celosvětově o potlačení softwarového pirátství. Vznik této organizace se datuje na rok 1988. Hlavní zakladatelé byli největší výrobci softwaru v USA. V České republice působí od roku 1993 dceřiná společnost BSA CS v Praze. Každým rokem tato společnost vydává studii míry vývoje softwarového pirátství mezi Českou republikou a Slovenskem. Zároveň studie BSA obsahuje i porovnání míry softwarového pirátství států Evropské unie. Samozřejmě tato studie neobsahuje všechny případy softwarového pirátství, protože řada případů není zaevidována. Případy domácího softwarového pirátství je obtížné řešit či evidovat.




| | 1994 | 1995 | 1996 | 1997 | 1998 | 1999 | 2000 | 2001 | 2002 | 2003 | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ČR | 66% | 62% | 53% | 52% | 45% | 42% | 43% | 43% | 40% | 40% | 41% | 40% | 39% | 39% | 38% | 37% |
| SR | 66% | 62% | 56% | 58% | 50% | 46% | 45% | 46% | 45% | 50% | 48% | 47% | 45% | 45% | 43% | 43% |

Graf 1 - Vývoj míry softwarového pirátství v České republice a na Slovensku [zdroj: www.adsl.cz][3]

Na grafu je jasně vidět, že míra softwarového pirátství ustupuje a daří se zdárně tuto kriminalitu potlačovat. Jak již bylo zmíněno, graf obsahuje pouze zjištěné činy pirátství a na spoustu těchto trestných činů se ani nepřijde.

[3] BSA tisková zpráva [citováno 21.5.2010]. Dostupná z http://www.adsl.cz/archiv/kratke-zpravy/piratskeho-softwaru-v-cesku-ubylo-nelegalne-se-ho-podle-bsa-uziva-37-187.html

***Míra pirátství v jednotlivých státech Evropské unie***

| Pořadí | Země | Rozdíl | 2009 | 2008 | 2007 | 2006 | 2005 | 2009 $M |
|---|---|---|---|---|---|---|---|---|
| *1.* | Lucembursko | 0% | 21% | 21% | 21% | | | $ 30 |
| *2.* | Rakousko | 1% | 25% | 24% | 25% | 26% | 26% | $ 212 |
| *3.* | Belgie | 0% | 25% | 25% | 25% | 27% | 28% | $ 239 |
| *4.* | Finsko | -1% | 25% | 26% | 25% | 27% | 26% | $ 175 |
| *5.* | Švédsko | 0% | 25% | 25% | 25% | 26% | 27% | $ 304 |
| *6.* | Dánsko | 1% | 26% | 25% | 25% | 25% | 27% | $ 203 |
| *7.* | Velká Británie | 0% | 27% | 27% | 26% | 27% | 27% | $ 1581 |
| *8.* | Německo | 1% | 28% | 27% | 27% | 28% | 27% | $ 2023 |
| *9.* | Nizozemsko | 0% | 28% | 28% | 28% | 29% | 30% | $ 525 |
| *10.* | Irsko | 1% | 35% | 34% | 34% | 36% | 37% | $ 125 |
| *11.* | Česká republika | -1% | 37% | 38% | 39% | 39% | 40% | $ 174 |
| *12.* | Francie | -1% | 40% | 41% | 42% | 45% | 47% | $ 2544 |
| *13.* | Portugalsko | -2% | 40% | 42% | 43% | 43% | 43% | $ 221 |
| *14.* | Maďarsko | -1% | 41% | 42% | 42% | 42% | 42% | $ 113 |
| *15.* | Španělsko | 0% | 42% | 42% | 43% | 46% | 46% | $ 1014 |
| *16.* | Slovensko | 0% | 43% | 43% | 45% | 45% | 47% | $ 65 |
| *17.* | Malta | 0% | 45% | 45% | 46% | 45% | 45% | $ 7 |
| *18.* | Slovinsko | -1% | 46% | 47% | 48% | 48% | 50% | $ 39 |
| *19.* | Kypr | -2% | 48% | 50% | 50% | 52% | 52% | $ 16 |
| *20.* | Itálie | 1% | 49% | 48% | 49% | 51% | 53% | $ 1733 |
| *21.* | Estonsko | 0% | 50% | 50% | 51% | 52% | 54% | $ 19 |
| *22.* | Litva | 0% | 54% | 54% | 56% | 57% | 57% | $ 31 |
| *23.* | Polsko | -2% | 54% | 56% | 57% | 57% | 58% | $ 506 |
| *24.* | Lotyšsko | 0% | 56% | 56% | 56% | 56% | 57% | $ 24 |
| *25.* | Řecko | 1% | 58% | 57% | 58% | 61% | 64% | $ 248 |
| *26.* | Rumunsko | -1% | 65% | 66% | 68% | 69% | 72% | $ 183 |
| *27.* | Bulharsko | -1% | 67% | 68% | 68% | 69% | 71% | $ 115 |
| | | | | | | | | |
| Celkem | Evropská unie | | 35% | 35% | 35% | 36% | 36% | $ 12 469 |

Tabulka 1 - Míra pirátství v jednotlivých státech Evropské unie [zdroj: www.adsl.cz][4]

Tabulka vypovídá o velkých finančních ztrátách, které způsobuje softwarové pirátství v Evropské unii. Česká republika se svými výsledky míry pirátství, která je za rok 2009 37%, řadí na 11. místo.

[4] BSA tisková zpráva [citováno 21.5.2010]. Dostupná z http://www.adsl.cz/archiv/kratke-zpravy/piratskeho-softwaru-v-cesku-ubylo-nelegalne-se-ho-podle-bsa-uziva-37-187.html

## 1.3 Trendy vývoje

Někteří uživatelé ICT jsou samozřejmě zločinci. Počítačovou kriminalitu v dnešní době vyvíjí uživatelé, kteří z ní žijí a berou jí jako hlavní zdroj obživy, z čehož plyne stále narůstající zapojení uživatelů do sítě organizovaného zločinu. Dnes profesionální zločinci používají modernější a stále rafinovanější metody. Ochrana proti dnešním útočníkům musí být stále víc aktivní a progresivní.

Firmy, organizace či složky státní správy jsou na výpočetní technologii, počítačových sítích i internetu hodně závislé. Počet rodin využívajících služby internetu rapidně vzrostl a tím i počítačová gramotnost již od mladých let.Je samozřejmostí, že se vzrůstající internetovou sítí přibývá i útočníků využívající cestu internetu pro provozování své trestné činnosti.

Počítačovou kriminalitu lze charakterizovat možnými trendy:

- Moderní delikty již jdou spáchat pouze on-line. Jedná se o trestné činy či přestupky proti důvěrnosti a dostupnosti počítačových dat a informací. Útoky na počítačová data v ICT se nazývá Hacking. Počet napadení v Evropské Unii vzrostl velice rapidně. Počet evidovaných napadení převyšuje hodnotu 1500, samozřejmě spoustu napadení počítačových sítí napadený ani nezaznamená. Přibližně 70% napadení je za účelem zisku. V Evropě počítačová kriminalita v trestně právní kategorii má největší nárůst trestných činů.
- Další možnost vývoje trendů je u mobilních komunikačních systémů. Mobilní zařízení v dnešní době využívají operační systémy totožné se systémy používaných na počítačích. Útočníci již nemají obtíže se na tyto systémy zaměřit a veškeré údaje z mobilního zařízení zkopírovat či prohlížet. Podle odhadů při vzrůstu zájmů o tyto multimediální mobilní zařízení vzroste počet útoků na mobilní zařízení v každém roce pěti až desetinásobně.

- Nárůst a poté i zneužití sítí Wi-Fi[5]. Snadné napadení přenosných počítačů či mobilních zařízení. Bezpečnost sítí Wi-Fi se stále vyvíjí a vznikají stále modernější zabezpečovací kódy a zlepšuje se zašifrovaní datové komunikace v síti ( čím více má šifrovací kód bitů, tím bývá pro útočníka těžší na napadení ).

- Rozšíření spammingu[6] pomocí trojských koní a botů. Taktéž nárůst e-mailových červů. Spamming, který následně umožní stažení trojských virů, které nakazí nechráněné počítače, aniž by uživatelé počítačů vůbec rozpoznali, že jejich počítač odesílá citlivé data útočníkovi. Při takové infiltraci v počítači může útočník za pomocí tzv. „botů“ ovládat počítač.“Boti“ automatické programy pro ovládaní počítače na dálku využívané při správě vzdálených serverů. Podle odhadů počet těchto zákeřných „botů“ rapidně narůstá, až se spojí do jedné velké sítě tzv. bot network – botnet, která je podobná internetu. Potom se může útočník připojit kdekoliv ve světě a za pár vteřin provést rozsáhlý útok na mnoho počítačů.

- Nárůst phishingu. Phishing znamená rozesílání útočníkem falešné e-mailové zprávy ze zdánlivě oficiálních zdrojů. V e-mailech jsou výzvy, aby uživatel aktualizoval své stávající hesla např. do internetového bankovnictví, či zadat svůj PIN[7] či zadat své přihlašovací údaje do služby PayPal[8]. Poté se útočník za pomocí těchto vymámených osobních údajů zmocní financí oklamaných uživatelů.

- Trend vzrůstu je i u spywaru. Zločinci se zaměřují i na zisk formou nevyžádané reklamy, kdy útočníci rozesílají e-maily s odkazy na různé pochybné internetové obchody, kde se nabízí zboží za velice nízké částky. Uživatelé po zadání údajů své kreditní karty z důvodu platby svého vybraného zboží, přijdou o mnohem víc financí

---

[5] Wi-Fi (Wireles Fidelity): Bezdrátová technologie pro šíření dat („vzduchem“), vhodná pro tvorbu sítových infrastruktur tam, kde je výstavba klasické kabelové sítě nemožná.

[6] Spam je nevyžádané masově šířené sdělení (nejčastěji reklamní) šířené internetem.

[7] PIN je akronym z anglického personal identification number, což znamená osobní identifikační číslo. Jedná se o jedinečný identifikátor, pomocí kterého je možné se autorizovat např. platební karty, mobilní telefony, vstupní kódy apod.

[8] PayPal je internetový platební systém. Umožňuje přesuny peněz mezi účty, které jsou identifikovány emailovými adresami.Každý účet je propojen s jednou nebo více platebními kartami.

ze svého účtu, protože útočník použije získané informace z kreditní karty pro výběr co možná nejvyšší možné částky z účtu uživatele.

# 2 POČÍTAČOVÁ KRIMINALITA V BANKOVNÍM SEKTORU

Napadnout vnitřní počítačovou síť banky nelze bez nadprůměrných znalostí provést, proto se ve větším měřítku nestávají. Zpravidla útočníci napadnou banku zevnitř ( útočník musí být přítomen na počítači v bankovním domě ) nebo využívají nejslabší článek v bankovním sektoru, a to jsou klienti. V dnešní době se v bankovním sektoru vyskytuje především phishing. Útočnici došli již tak daleko, že používají jména a domény tvářící se jako domény předních bank světa.

## 2.1 Phishing

Phishing, tedy podvodné e-mailové zprávy, které mají vzbudit dojem, že byly odeslány z e-mailové adresy banky. Vždy je jejich cílem vylákat citlivé (zpravidla) bankovní údaje. E-mailová zpráva je většinou psána špatnou češtinou nebo v angličtině, obsahuje hypertextový odkaz na údajné stránky internetového bankovnictví vaší banky a vyzývá k zadání osobních bankovních údajů. Pravidlo zní: Nereagovat na nevyžádanou poštu, která se tváří jako zaslaná vaší bankou.

Klient banky se může nechat napálit podvodným e-mailem jako např. potvrzení platby, zrušení nevyžádané platby, výzva k aktualizaci platnosti účtu, k aktualizaci bezpečnostních údajů, vidinou náhlé výhry nebo jen prostým varováním před podvodnými e-maily. Ukázky podvodných e-mailů viz. obrázek 1,2.

Cílem internetové stránky, na něž vás hypertextový odkaz v podvodném e-mailu odkáže, je vyzvání k zadání přístupových kódů k internetovému bankovnictví či identifikační čísla a PIN u platebních karet. Stránky jsou velmi často profesionálně vytvořené a v důsledku vypadají přesně jako internetové bankovnictví vaší banky.

Při podezření na podvodný e-mail či podvodné nestandardní chování stránek internetového bankovnictví je dobré kontaktovat vaší banku. Z důvodů zvětšení a zlepšení prevence proti této trestné činnosti. Nedoporučuje se kontaktovat uvedené číslo na podezřelých stránkách, které může patřit útočníkovi.

Nemyslete si, že vaší e-mailovou adresu útočník nemůže získat a takový e-mail vám nemůže zaslat. Útočníci e-mailové adresy generují pomocí programu nebo je kupují od

dalších útočníků zabývající se rozesíláním nevyžádané reklamy. Banky pomocí e-mailové služby neposílají výzvy k zadávaní citlivých údajů na internetu.

Využívaní internetového bankovnictví kterékoliv banky je zpravidla bezpečná a komfortní služba pro klienty za předpokladu, že dodržují základní bezpečnostní pravidla:

- dodržování bezpečnostních doporučení banky,
- nikdy se nepřihlašovat do služby z neznámých nebo veřejně dostupných počítačů,
- chránit své přihlašovací údaje a zároveň tyto údaje nemít zapsány v počítači,
- nestahovat do svých počítačů soubory z neznámých zdrojů (z důvodu infiltrace škodlivými programy )
- aktualizovat antivirový systém na vašem počítači.

**Od:** Cesk? Sporitelna <ceskamsg1@cesk.cz>
**Předmět:** SERVIS 24 Internetbanking
**Datum:** 26.2.2008 04:45:29

ČESKÁ SPOŘITELNA

**Neúspěšná transakce / Payment Not Successful**

**Platební transakce zamítnuta - pokyn vydavatele karty**

Transakce byla odmítnuta na základě některého z uvedených důvodů:

- Vaší kartou není povoleno provádět internetové transakce
- Byl překročen limit pro internetové transakce
- Byl chybně zadán CVC2/CVV2 kód
- Na Vašem účtu není dostatek prostředků

Jdi na: Prehled aktivovanych produktu sluzby SERVIS 24 .
(pro okamžitý návrat klikněte zde).

Nyní budete přesměrován/a na stránky internetového obchodníka
(pro okamžitý návrat klikněte zde).

**The payment was declined at issuer's request**

Transaction was not successful due to one of the following reasons:

- Your card is not intended for shopping via Internet
- Limit for Internet transactions was exceeded
- Wrong CVC2/CVV2 entered
- Insufficient funds on your account

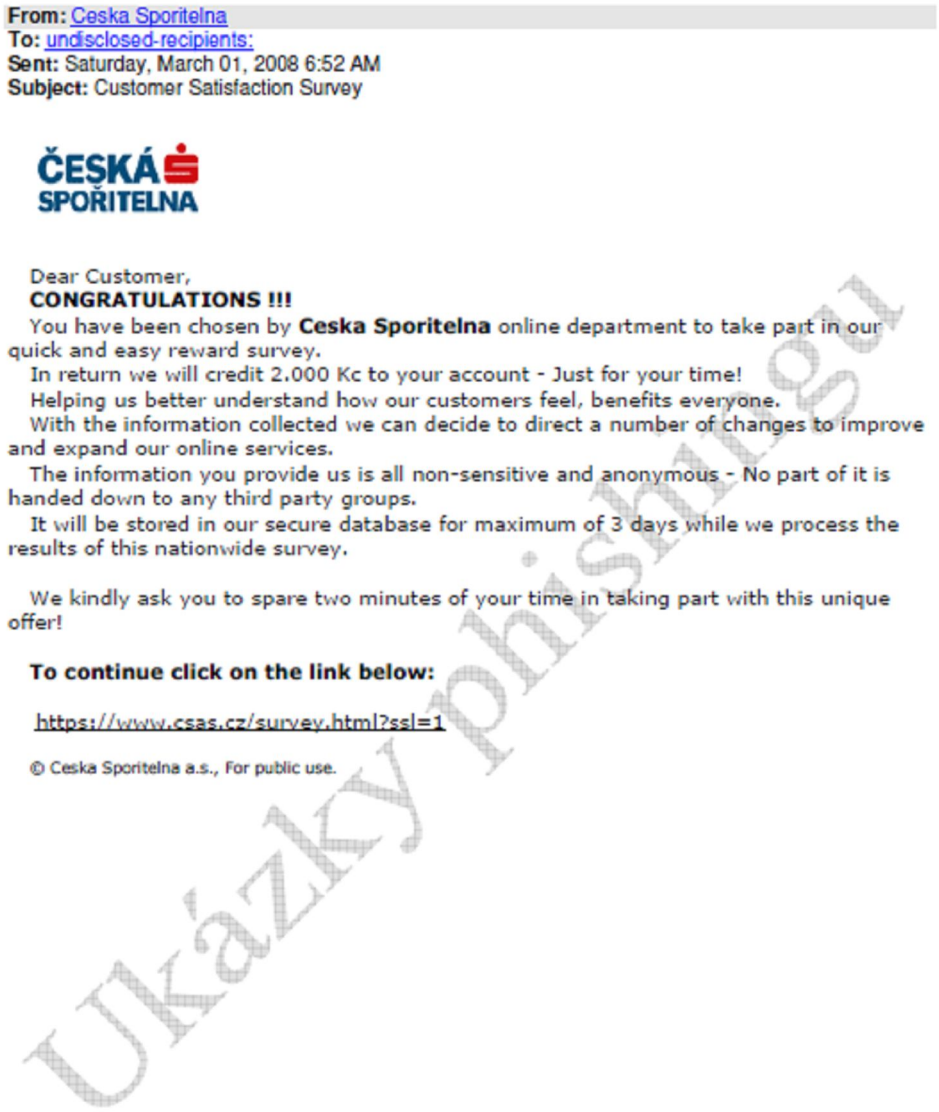
For further assistance please click here.

The Payment Service will redirect you to the Merchant Website
(or click here to be redirected immediately).



Obrázek 1 – ukázka phishingu [zdroj: www.csas.cz][9]

[9] Ukázky phishingových e-mailů, dostupná z http://www.csas.cz/banka/menu/cs/banka/nav7004_phishing_ukazky



**From:** Ceska Sporitelna
**To:** undisclosed-recipients:
**Sent:** Saturday, March 01, 2008 6:52 AM
**Subject:** Customer Satisfaction Survey

ČESKÁ SPOŘITELNA

Dear Customer,
**CONGRATULATIONS !!!**
You have been chosen by **Ceska Sporitelna** online department to take part in our quick and easy reward survey.
In return we will credit 2.000 Kc to your account - Just for your time!
Helping us better understand how our customers feel, benefits everyone.
With the information collected we can decide to direct a number of changes to improve and expand our online services.
The information you provide us is all non-sensitive and anonymous - No part of it is handed down to any third party groups.
It will be stored in our secure database for maximum of 3 days while we process the results of this nationwide survey.

We kindly ask you to spare two minutes of your time in taking part with this unique offer!

**To continue click on the link below:**

https://www.csas.cz/survey.html?ssl=1

© Ceska Sporitelna a.s., For public use.



Obrázek 2 – ukázka phishingu [zdroj: www.csas.cz][10]

[10] Ukázky phishingových e-mailů, dostupná z
http://www.csas.cz/banka/menu/cs/banka/nav7004_phishing_ukazky

## 2.2 Pharming

Pharming na rozdíl od phishingu využívá slabin počítače, který klient využívá. Cílem je (zjednodušeně) spustit v počítači klienta program, jenž se samovolně stáhl, když klient hledal informace na internetu a poté program bez tušení získává informace z napadeného počítače. Zde je již jen otázkou času, kdy si přečte útočník vše potřebné např. při snadném sledování úderů na vaší klávesnici pomocí ASCII[11] tabulky. Zde je taktéž na místě zmínit i možnosti grafické klávesnice pro zadávaní hesel, ale útočnici mohou sledovat i pohyby myši.

Pharming je dalším stádiem phishingu, modernějším, sofistikovanějším a především nebezpečnějším. Pharming k činnosti využívá překladu názvu serveru na odpovídající IP adresu (každý počítač je v síti rozpoznán tedy má svou jedinečnou adresu, která vypadá např.: 168.192.1.1.), útočí tedy na DNS[12]. Uživatel při zadávaní internetové adresy ve svém internetovém prohlížeči např. www.banka.cz, nedošlo by k překladu na odpovídající IP adresu zadané adresy, ale za pomocí útočníka na nějakou jinou k nerozeznání podobnou a zde vzniká problém, že uživatel nepozná rozdíl a automaticky vyplní své přihlašovací údaje, které se automaticky odešlou útočníkovi. Pro běžné uživatele by bylo obtížné si zapamatovat IP adresy počítačových serverů svých bank. Proto existuje tzv. DNS server, který tyto IP adresy převádí na srozumitelné adresy a naopak.

### 2.2.1 Obrana

Přepsání údajů zajišťují různé počítačové viry, např. trojské koně, které se do počítače klientů dostanou např. v e-mailech nebo v softwarech, které si instalují a taktéž samozřejmě z internetu. Jediná nejúčinnější ochrana před napadením takovéhoto viru či

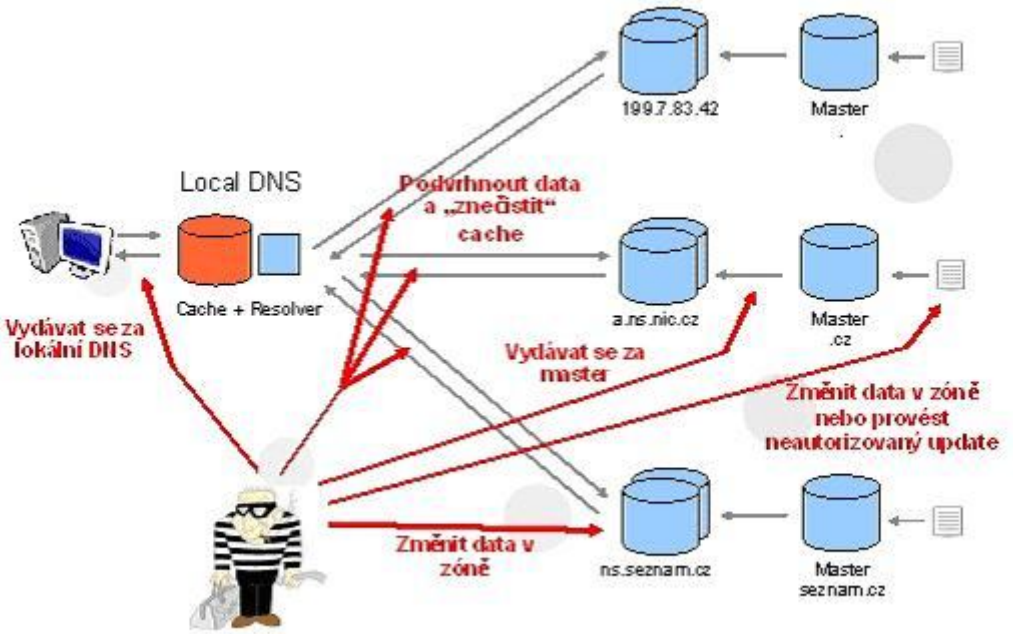
---

[11] ASCII je anglická zkratka pro American Standard Code for Information Interchange („americký standardní kód pro výměnu informací“). V podstatě jde o kódovou tabulku, která definuje znaky anglické abecedy, a jiné znaky používané v informatice.

[12] DNS (Domain Name System) je hierarchický systém doménových jmen, který je realizován servery DNS a protokolem stejného jména, kterým si vyměňují informace. Jeho hlavním úkolem a příčinou vzniku jsou vzájemné převody doménových jmen a IP adres uzlů sítě.

trojského koně je použití kvalitního antivirového systému a pak zajišťovat jeho pravidelnou aktualizaci. Samozřejmě, že dalším ochranou je použitý a dobře nakonfigurovaný firewall, nicméně obrana proti pharmingu v celosvětovém měřítku není jednoduchá.

## 2.3 Způsob útoku na DNS




Obrázek 3 – způsob útoku [zdroj: www.nic.cz ]

Jestliže-li se útočník bude vydávat za DNS tím,že se naboural do síťové cesty mezi klientem a DNS, klient má smůlu, i když má svůj počítač aktualizovaný a dobře zabezpečený. Poté, co klient zadá obvyklou adresu do prohlížeče, je mu načtena podvržená stránka a klient má jen velice málo možností rozpoznat, že není na stránkách banky, samozřejmě za předpokladu zhotovení dokonalé kopie stránky banky. Časem se zavede řešení formou tzv. DNSSEC, kde systém domén bude chráněn ověřovacími certifikáty.

Počítačoví útočníci využívají nejslabšího článku v bankovním sektoru a to jsou klienti. Banky se snaží chránit před těmito útočníky a dávají do ruky klientovi ověřovací nástroje, které jsou více bezpečnější než jen uživatelské jméno a heslo. Samozřejmě, že každý bezpečnostní prvek není zcela bezpečný.

Zprvu se zdálo řešení jednoduché a klientům se zavedl další bezpečnostní prvek a to ověření podle certifikátu na čipové kartě. Čas prokázal, že i tento bezpečnostní prvek není

zcela bezpečný. I přesto se stávalo, že se objevovaly neoprávněné transakce, které byly autorizovány klientem a byly odeslány z klientova počítače, u něhož právě sedí.

Každý bezpečnostní prvek má nedostatky – zda už se jedná o ověřující SMS zprávy, PIN kalkulátor či jiné. Vždy budou útočníci napřed a najdou způsob, jak se ke klientovým financím dostat.

Nesmí se opomenout, že každé internetové bankovnictví stojí na vnitřním bankovním systému. Systémy by měly hlídat, zda jsou transakce v pořádku. Pro upřesnění systém hlídá např. chování klienta a vyhodnocuje a varuje při nestandardních transakcích. Tedy pokud se na učtu nikdy nepřeváděly peníze do bank např. do Karibiku či jiné rizikové destinace, zřejmě bude banka kontaktovat majitele účtu při takovémto převodu.

## 2.4 Skimming

Skimming je útok, který počítačoví útočníci provádí cíleně z důvodu zkopírovat informace z magnetického proužku platební karty. Kopírování informací z magnetického proužku může dojít v čtečce, kterou útočník umístil u vstupu do prostoru, kde je umístěn bankomat nebo až ve čtečce umístěné přímo na samotném bankomatu. Poté když útočník zkopíruje magnetický proužek musí získat ještě PIN. Pro tento účel může použít např. repliku klávesnice (resp. PINpadu), která je nastražena na originální klávesnici na bankomatu. Pod replikou klávesnice se skrývá zařízení podobné mobilnímu telefonu, které má v sobě pamětní kartu např. SD[13], která v sobě zaznamená zadané PIN. Útočník poté jen vyčká na nashromážděné data a vyzvedne si paměťovou kartu ze skimmovacího nadstavce a ze zařízení pod replikou klávesnice. Útočníkovi poté již nic nebrání vytvořit kopii kreditní karty a poté provést výběr v bankomatech. Může být i ještě jedna cesta jak získat PIN a to odpozorováním. K tomuto účelu je použito nainstalování kamery nad klávesnici bankomatu.

Místa napadení skimmingem mohou být různorodá, dochází k nim zejména v barech, restauracích, také na čerpacích stanicích nebo i v hotelových zařízení. Útočník, který chce

[13] Secure Digital ( zkratka SD) je paměťová karta o určité velikosti udávané v jednotkách informací Byte, používaná v přenosných zařízeních včetně digitálních fotoaparátů, přenosných počítačů a mobilních telefonech.

provést skimming osobně, k tomu využívá různé triky, výmluvy nebo manipulační nátlaky na majitele karty. Hlavním účelem je odvedení pozornosti majitele karty, aby útočník mohl kartu zkopírovat přes přenosné skimmovací zařízení. Dále tyto data z zařízení mohou útočníci použít při platbách bez přítomnosti karty nebo k výrobě kopie karty. Poté dochází z útočníkovy strany s transakcím bez vědomí majitele karty. Jak již bylo zmíněno, útočníci instalují své zařízení i na bankomaty. Tento typ je pro útočníka pohodlnější a proto se masivně rozrůstá.

### 2.4.1 Technologie skimmingu

Každé skimmovací zařízení instalované útočníkem se skládá ze dvou částí. Jedna umožňuje kopírovat informace z kreditní karty a s druhým zařízením útočník získá PIN. Zařízení nainstalováno na otvoru ( viz. obrázek 4), do které se vsouvá kreditní karta na bankomatu, není na první pohled poznat od originálního prvku bankomatu. Poté již útočník pomocí kamery ( viz. obrázek 5) či fotoaparátu ( umístěny např. v liště nad klávesnici, kde je vyvrtána nepatrná díra, kterou je vidět na klávesnici ) synchronizuje získaná data pomocí časového uložení informace a má data pro vytvoření kopie kreditní karty. V dnešní době již tento způsob útočníci ještě zdokonalili, protože bankomaty jsou stále víc kamerově střeženy, tak útočníci instalují své vlastní bankomaty. Je to jednoduchý způsob bankomat informace z karty zkopíruje i s klientovým vlastnoručně zadaným PINem a na displeji vypíše informaci: „ Z důvodu nedostatečné hotovosti v bankomatu Vám nemůžeme vydat finance.“ , „ Mimo provoz“ nebo podobné informace, které v majiteli karty nevzbudí pocit že zadal informace do nebezpečného bankomatu. Tyto falešné bankomaty jsou navíc od těch originálních téměř k nerozeznání. Falešné bankomaty se již několik měsíců objevují v zahraničních bankovních sítích. V dnešní době dorazily i k nám do České republiky. Nejvíce falešných bankomatových terminálů se objevilo v Praze. Spousta klientů ani neví, že jim byly informace z kreditní karty zkopírovány, protože útočník nemusí ihned provést výběr. Někteří útočníci vyčkávají až několik měsíců, než provedou výběry z kreditní karty klienta z důvodu zamaskování podezření na neoriginální bankomat.

Obrázek 4 – skimmovací nástavec [zdroj: www.ics.muni.cz][14]

Obrázek 5 – kamera v nástavci snímá zadávání PINu [zdroj: www.ics.muni.cz][15]

[14] Útoky na platební systémy [ citováno 1.10.2007] dostupná z http://www.ics.muni.cz/bulletin/articles/562.html

[15] Credit card skimming [ citováno 19.3.2009] dostupná z http://izismile.com/2009/03/19/credit_card_skimming_be_carful_11_pics.html

### 2.4.2 Obrana a vývoj

Všechny banky začínají více zvyšovat bezpečnost svých klientů potažmo bankomatů pomocí tzv. FDI (Fraudulent Device Inhibitor) bezpečnostního modulu ( viz. obrázek 6). Modul ztěžuje útočníkům skimming karet, tedy kopírování informací z platební kartě. FDI moduly se již instalují na bankomaty. Modul, který byl nainstalován na bankomat, omezil či zamezil skimming karet. Podle odborníků ale tento modul vše nevyřeší a časem přijdou útočníci i na skimmovací nástavec pro tento modul. V dnešní době tento modul využívají ve všech vyspělých státech světa jako základní bezpečnostní prvek na bankomatech. Mimo nových bezpečnostních prvků bankovní domy do svých bankomatů vkládají informativní obrazovky, kde upozorňují na tuto problematiku a tím i zvyšují preventivní chování klientů.

Obrázek 6 – Ochranný nástavec (anti-skimming) [zdroj: www.ics.muni.cz][16]

Podle odborníků největší bezpečnostní prvek, který by zabránil skimmingu, bude implementován snad za několik let. Tento prvek tkví v tom, že všechny banky přejdou z karet s magnetickým proužkem na karty osazené čipem. Banky do přechodu na čipové karty

[16] Útoky na platební systémy [ citováno 1.10.2007] dostupná z http://www.ics.muni.cz/bulletin/articles/562.html

nechtějí ještě investovat, protože pro banky je výhodnější nahradit klientovi škodu, než investovat do této technologie. Klientům nezbývá než být obezřetní a všímat si veškerých maličkostí na bankomatu, samozřejmostí je i chránit výhled na klávesnici, kde zadáváme PIN. Jednou možností je taktéž provádět výběr z jednoho stálého bankomatu, na který jste zvyklí a při podezření s jeho neoprávněnou manipulací kontaktovat dotyčnou banku.

# II. PRAKTICKÁ ČÁST

# 3 ZPŮSOB PREVENCE

Způsobů počítačové kriminality v bankovním sektoru je rozmanité množství. Útočník může využít i kombinaci způsobů, ale cílem zůstávají vždy finance. Jak již bylo zmíněno, pro bezpečnost je nejslabším článkem v bankovním sektoru klient. Banky mohou klienty jen varovat před způsoby počítačové kriminality a apelovat na jejich obezřetnost. Banky se chrání hlavně prevencí a zavaděním své bezpečnostní politiky, kterou musí zaměstnanci banky a samozřejmě i banka striktně dodržovat.

Bezpečnostní politika je v praktické části rozebrána se zohledněním prvků, na které banka musí dbát při zavádění této prevence. Po tomto preventivním opatření se banka musí zaměřit na aktivní ochranu své počítačové sítě. Pro aktivní ochranu vnitřní bankovní sítě se využívá bezpečnostního prvku „firewall“. Tento prvek musí odpovídat základní bezpečnostní politice. Při dodržení bezpečnostní politiky se musí prvek nakonfigurovat pro optimální ochranu. Pro konfiguraci zde specifikuji bezpečnostní hrozby a bezpečnostní cíle. Specifikaci je pro detailní představu zanesena do tabulky, kde na každou bezpečnostní hrozbu musí být vytvořen odpovídající bezpečnostní cíl.

## 3.1 Bezpečnostní politika ICT

### 3.1.1 Ochrana a bezpečnost informační a komunikační technologie

Ochrana a bezpečnost ICT obsahuje veškeré počítačové vybavení banky (od serverových sálů po osobní počítače a ostatní terminály), počítačovou komunikační síť, která počítače propojuje, uchovávané data na místních discích, softwarové programy a výstupy vytvořené počítačem, systémový software a procesy, kterými jsou vyvíjeny, zaváděny a spravovány nové aplikace jednotlivých produktů, včetně aplikací samotných.

Základními principy bezpečnosti ICT :

- integrita – lze provést pouze autorizované změny dat a programů,
- důvěrnost - informacím banky mají přístup pouze osoby k tomu oprávněné,
- dostupnost - informace jsou dostupné ve stanoveném místě a čase,
- autentičnost – možnost ověřit pravdivost a správnost informací kdykoliv,

- přímá odpovědnost – zde je jednoznačně určitelné kdo, kdy, jak (odkud) provedl operaci či zásah do bankovního systému.

Každá informace v bance uložená či vytvořena ICT se dělí z hlediska hodnoty na tyto kategorie:

- ZVLÁŠTĚ DŮVĚRNÉ (ZD) – tyto informace, by mohly mít značnou a trvalou škodu a chod či pověst banky, pokud by byly zneužity, neoprávněně upraveny nebo prozrazeny. Samozřejmě hrozí i možnost ztráty konkurenceschopnosti, pokud by se tyto zvláště důvěrné informace dostaly do rukou konkurenční banky.
- DŮVĚRNÉ (D) - informace, jež by mohly uškodit pověsti a zájmům banky nebo způsobit finanční ztrátu, pokud by byly vyzrazeny, jiným způsobem zneužity nebo by se k těmto informacím dostala konkurence. Tyto informace a údaje jsou zakotveny v ustanovení zákona o bankách č. 21/92 Sb., § 38 odst. 1 (bankovní tajemství) (tj. informace o bankovních obchodech, peněžních službách včetně stavů na účtech apod.).
- VYHRAZENÉ (V) - ostatní informace, které jsou smyslu podnikového tajemství, tudíž nejsou určeny pro veřejnost. Informace tohoto typu jsou považovány za informace s nízkým rizikem, které výrazně či minimálně uškodí bance. Jsou vázány povinností zachování bankovního, firemního tajemství.
- OSTATNÍ INFORMACE - (MPV) materiály pro veřejnost – tyto informace nepotřebují žádné speciální zacházení jsou určeny pro veřejnost a nevyžadují ochranu proti neoprávněnému přístupu.

Při vytvoření dokumentů se musí zavést tzn. definovaná klasifikace dokumentů. Informace označené typem „Zvláště důvěrné a Důvěrné“ jsou omezené na určitou skupinu, která má právo tyto informace otevřít, číst či v nich zapisovat. Tato skupina je specifikována vlastníkem či správcem těchto informací, případně top managementem banky či jiným bezpečnostním úsekem vybraným top managementem. Ochranu dat a informací je nutno chápat komplexně, protože informace nelze zabezpečit pouze technologicky. Bezpečnostní úsek banky se musí zaměřit samozřejmě hlavně na režijní bezpečnost a předávat a vštěpovat bezpečnostní prevenci zaměstnancům.

### 3.1.2 Organizace a řízení

Po vydefinování hodnot informace je nutno dbát na organizační zajištění ICT ve všech jejich fázích, to znamená, že se musí provést i analýza bezpečnostních rizik spjatých s informačními systémy.

V analýze rizik se definuje::

- aktiva informačních systémů,
- hrozby, které na ně působí,
- slabá (zranitelná místa),
- pravděpodobnost realizace hrozeb a odhad jejich následků,
- protiopatření,

Analýza rizik dopadů, při zavádění nového systému, (subsystému, aplikace) pro stávající systémy instalované na počítačích. Tuto analýzu provede úsek bezpečnosti ICT, poté vydá prohlášení, zda nový systém nebude mít následky na starý. K identifikaci rizik slouží „Kniha rizik“.

Všechny povinnosti a pokyny pro jednotlivé oblasti a pracoviště ICT jsou prováděny formou vnitřních předpisů a pracovních postupů, ve kterých jsou jednoznačně určeny prováděné činnosti a odpovědnosti jednotlivých útvarů, pracovišť, pracovníků.

Z pravidla jsou nadefinovány:

- provozní řády pro zajištění řádného chodu systémů a podsystémů,
- režim zálohování a archivace,
- havarijní plány pro zajištění chodu systému v případě náhlé havárie,
- režim pohybu osob v prostorách s ICT (zaměstnanci, servisní organizace, dodavatelé, hosté),
- postupy pro řízení a kontrolu přístupů (způsob nakládání s autorizačními prostředky),
- postupy v případech narušení bezpečnosti ICT,
- standardizace tvorby, údržby dokumentace a nakládání s ní v oblastech ICT,

- pravidla pro správy programů a distribuce programů,
- normy a metody pro tvorbu programů i s kritérií pro testování a ověřování,
- proces zařazení programů do produkčního prostředí,
- zásady změnového řízení,
- pravidla pro práci s dokumenty, sestavami,
- postupy pro zabezpečení systému a dat při provádění kontroly a údržby technických zařízení,
- zásady antivirové prevence a postupy při odstraňování virové infekce.

Všechny pokyny a předpisy musí být v souladu s pravidly ochrany a bezpečnosti ICT.

Jednoznačně jsou definovány a určeny odpovědnosti za bezpečnost ICT v následujících oblastech:

- definování bezpečnostní politiky - metodické řízení oblasti bezpečnosti zpracovávaných dat a informací v informačních systémech banky a aktualizaci bezpečnostní politiky provádí útvar bezpečnosti
- implementace bezpečnostní politiky - architektura a vývoj programů, procedur a postupů informační technologie v souladu se zásadami bezpečnostní politiky provádí útvar učený top managementem
- vlastnictví jednotlivých systémů (produktů) – správce (vlastník) produktu má prvotní odpovědnost za integritu dat systémem zpracovávaných. Správce produktu je odpovědný za definici způsobu autorizace uživatelů užívajících jeho produkt
- denní správu a provoz příslušných systémů a aplikací – každé pracoviště má technika či správce ICT
- monitoring dodržování bezpečnostní politiky v ICT (tj. nastavení bezpečnostních atributů) provádí útvar učený top managementem

V rámci definice odpovědností musí být zajištěno oddělení správy informačního systému od vyhodnocování bezpečnostních záznamů, včetně kontroly přidělovaní přístupových práv.

### 3.1.3 Personální zabezpečení

Hlavním personálním zabezpečením je výběr zaměstnanců, kteří mají odpovědnost za informační a komunikační technologii, samozřejmě zaměstnanci musí splňovat kritéria odborné způsobilosti, důvěryhodnosti a spolehlivosti.

V případě nestandardního chování je nutné okamžitě realizovat opatření k zamezení fyzického i logického přístupu k zařízení ICT (např. zrušit oprávnění, zamezení přístupu, změnit bezpečnostní informaci). Zaměstnanci musí být seznámeni s bezpečnostními opatřeními včetně následků při porušení přijatých opatření. Zaměstnanci jsou povinni informovat své nadřízené o narušení bezpečnosti ICT, včetně podezření na narušení bezpečnosti ICT.

Všichni zaměstnanci mají definována přístupová práva v souladu s jeho pracovním zařazením, při změně pracovního zařazení musí být provedena změna přístupových práv z důvodu bezpečnosti. Bankou je vyhotoven odpovídající seznam pracovních pozic a k nim spjaté povinnosti pro bezpečnostní chování na ICT a taktéž ke každé pracovní pozici přidefinovaná přístupová práva. Všichni zaměstnanci banky absolvují školení v oblasti ICT. Toto školení musí obsahovat i zásady bezpečnosti a postupy chování při mimořádných situacích a haváriích na ICT.

### 3.1.4 Povinnosti uživatelů ICT

Pro zajištění funkčnosti informačního systému jsou uživatelé ICT povinni dodržovat zásady postupů, chování a činností souvisejících s provozem a správou informační a komunikační technologie. Při vzniku problému, závady a nestandardního projevu software a hardware jsou zaměstnanci banky povinni hlásit tuto skutečnost místním správcům bezpečnosti ICT.

Zaměstnanci musí dodržovat zejména tyto pravidla:

- pracovní postupy v oblasti informační a komunikační technologie,
- pravidla bezpečnosti a ochrany systému informační technologie,
- pravidla antivirové ochrany,
- neprovádět změny v jednotlivých prvcích informační technologie,
- nepřemisťovat či upravovat výpočetní techniku,

- neinstalovat či jinak upravovat nainstalovaný software.

### 3.1.5 Umístění ICT prvků

Ke klíčovým prvkům systému (např. výpočetní střediska, serverovny, a ostatní centra zajišťující bankovní operace) musí být zajištěna nepřetržitá a spolehlivá dodávka elektrické energie.

Dosahuje se toho následujícími způsoby či jejich kombinací:

- UPS (zdroj nepřerušitelného napájení),
- zdvojený zdroj dodávky elektrického proudu,
- záložní generátory.

Klimatizační i chladicí jednotky musí mít dostatečnou rezervu.

V klíčových místnostech musí být nainstalován detekční a poplašný systém monitorující zvýšení teploty či vlhkosti včetně detekce kouře, ohně či vody. Detekční a poplašný systém je připojen minimálně do dvou kontrolních míst , aby bylo zajištěno nepřetržité sledování. V případě potřeby musí být provedena okamžitě odpovídající opatření. Zaměstnanci odpovědni za kontrolu těchto místností musí být ihned schopni reagovat na jakýkoliv z poplachů.

### 3.1.6 Kontrola přístupu

Jsou stanovena pravidla, která platí pro klíčová místa (např. výpočetní střediska, komunikační místnosti.):

- přístup do důležitých oblastí musí být kontrolován vhodným přístupovým systémem, prostory budov jsou rozčleněny do bezpečnostních zón s alternativním přístupem a zvolí se prvek bezpečnosti např. pomocí magnetických nebo čipových karet,
- konkrétní klíčové místnosti výpočetních prostředků nesmějí být nápadně označeny,
- přístup do výpočetních středisek mají pouze zaměstnanci a oprávněné osoby.
- příchod a odchod všech zaměstnanců a hostů do chráněných oblastí musí být evidován i ostatní přesun zařízení a médií musí být evidován,

- veškeré zařízení v klíčové místnosti musí být přehledně zdokumentováno,
- technologické části a obsluha klimatizačních zařízení, na které závisí provoz výpočetní techniky mají být přístupné pouze oprávněným osobám.

### 3.1.7 Kontrola logického přístupu

Z důvodů logického přístupu jsou jasně definovány automatické postupy a kontrolní systémy, které musí byt striktně zavedeny pro řízený přístup k datům a funkcím informační technologie bankovní instituce. Nejdůležitější podmínkou je při logickém vstupu jednoznačná identifikace tzv. autentizace uživatele, který bude pracovat na informačních a komunikačních technologiích. Autentizace musí předcházet před začátkem práce s bankovním systémem. Oddělení bezpečnosti ICT má za úkol přidělit každému zaměstnanci přihlašovací jméno s heslem. Zaměstnanec si po prvním přihlášeni změní heslo na své. Heslo z bezpečnostních důvodu musí obsahovat alfanumerické znaky.

Z důvodu možnosti přístupu z jednoho zařízení do více systémů a aplikací tzn. metoda jednoho přihlášení – Single sign on, musí být zajištěno bezpečné a jednoznačné chování při předávaní údajů nutných pro autentizaci uživatele.

Při přihlášení uživatele musí být zadáno heslo nebo musí být využito jiného autentizačního nástroje, např. čipové karty apod.. V žádném případě nesmí být možnost přihlášení uživatele bez hesla.

Základní bezpečnostní pravidla, které se v bankovním sektoru vztahují na hesla, mají mít tyto následující kritéria:

- minimální délka hesla je 8 znaků (alfanumerické znaky),
- uživatel má mít možnost změny hesla,
- systémem uživatele musí informovat na životnost hesla (30 dnů) a poté nabídnout jeho změnu,
- uživatel při obdržení vygenerovaného hesla pro první přihlášení musí toto heslo změnit za nové,
- hesla musí být enkryptována (šifrována),
- heslo uživatel nesmí nikomu sdělovat a také jej nikde fyzicky uchovávat,

- při zadání autentizačních informacích musí být jejich přenos při kontrole se serverem chráněn šifrováním,
- systém musí hlídat historii 12. naposled užitých hesel u uživatele a během tohoto cyklu nesmí uživatel využít staré heslo, které používal (tzn. každý uživatel během roku vystřídá 12 neopakujících hesel),
- z důvodu bezpečnosti má systém při zadávání nového hesla zaveden slovník běžných slov, jmen, číselných posloupností, co nejsou dovolena využít.

Každá banka vede záznamy o všech změnách v jejich databázi logického přístupu a poté jsou tyto záznamy kontrolovány pověřeným pracovníkem. Vedou se samozřejmě kompletní záznamy úspěšných a neúspěšných přístupů do systému. Bezpečnostní úsek stanoví počet neúspěšných pokusů o přihlášení a poté je uživatel zablokován. Při nečinnosti uživatele v systému musí být tento uživatel automaticky odhlášen nebo musí dojít k ukončení jeho relace. Současně systém musí poskytovat aplikaci pro uzamčení relace uživatelem. Při opětovném odemčení relace musí aplikace vyžadovat opětovnou autentizaci přihlášeného uživatele.

Uživatelům jsou s ohledem na jejich pracovní zařazení nadefinována práva v bankovních systémech. Prává jsou zaměstnancům nadefinovány hromadně, takže jsou jejich uživatelské účty zařazeny do příslušných pracovních skupin. Při definování těchto skupin je požadováno oddělení pravomocí (např. práce s účty, schvalování transakcí, apod.). Nelze, aby jeden uživatel byl zařazen do všech pracovních skupin a tudíž by měl neomezená práva v systémech. Každý uživatel má zodpovědnost za transakce, které byly provedené pod jeho uživatelským účtem.

V systému jsou zavedeny i tzv. *speciální účty***.** Speciální účty jsou administrátorské účty operačních systémů či databází.. Tyto účty využívají nejvyšší (privilegovaná) oprávnění. V bankovním prostředí se nesmí používat standardně systémem přednastavené speciální účty až na výjimku, které jsou nastaveny výrobcem či dodavatelem systému z důvodu chodu systému. Zajištění bezpečného provozu je zapotřebí tyto speciální účty nově vytvořit a původní defaultní uzamknout, přejmenovat či zrušit.. Samozřejmostí je u těchto speciálních účtů definována politika silnějších hesel.

Ve všech systémech či aplikacích, které jsou připravovány do provozu se musí zajistit oddělení speciálních účtů určených pro správu systému či aplikace od účtů, které

slouží ke správě bezpečnosti či účtů pro vyhodnocování bezpečnostních auditních záznamů. V systémech by se měl objevit co nejmenší počet tzv. obecných (neadresných) uživatelských účtů, a to pouze na případy, kdy jsou tyto účty zapotřebí využít např. z technických důvodů, zaučování nováčků (nemají ještě přiřazeny autentizační informace). Použití takovýchto obecných uživatelských účtů musí být posouzeno a odsouhlaseno bezpečnostním útvarem banky.

### 3.1.8 Bezpečnost hardware

Útvar v bance zabývající se bezpečnosti ICT schvaluje dodavatelé hardware (výrobci renomovaných značek). Je to zásadní, protože zařízení mají přímý dopad na bezpečnost. Zařízení mají odpovídající úroveň bezpečnosti (např. hardwarová přístupová zařízení). Všechna zařízení by měla mít smluvně zajištěn servis a technickou podporu, která v bankovním sektoru odpovídá nepřetržitému režimu „nonstop“.

V hardwarových zařízeních nesmí existovat ani jedno místo, které by mohlo při výpadku vyřadit celý bankovní informační systém či podsystém. U klíčových částí systémového zařízení musí být zajištěna adekvátní záloha (např. primární a sekundární databázový archív osobních účtů).

### 3.1.9 Povinnost zabezpečit software

V bance a v jejich počítačích lze používat pouze verze systémového software podporované výrobcem. Po instalaci systémového software je potřeba zajistit jeho pravidelnou aktualizaci (zaprvé bezpečnostní záplaty a bezpečnostní aktualizace vydané výrobcem softwaru). Dalším krokem po aktualizaci systémového softwaru je otestování aplikací (zejména provozní aplikace). Změny na všech pracovních stanicích lze provést až po vyhodnocení dopadů aktualizace na bezpečnost informačních systémů.

Vstup do systémového nastavení nesmí být umožněn obecným uživatelům. Tento vstup do systému je omezen na speciální okruh uživatelů (správci systému). Příkazy, které nezasahují do primárních nastavení systému jsou umožněny (uživatelské nastavení). Veškeré změny v softwarovém vybavení pracovní stanice musí odpovídat bezpečnostním pravidlům a seznamu povoleného softwaru. Banky vydávají i směrnice, kde uvádějí seznam zakázaného softwaru (viz. tabulka 1) a porušení tohoto zákazu se bere jako hrubé porušení

bezpečnosti. Většinou jsou tyto zakázané software nebezpečné z důvodu, že využívají připojení na internet, sdílí data, či pouze odvádějí zaměstnance od pozornosti.

| *Název programu* | |
|---|---|
| Alcohol 120% | Google Desktop |
| AnyDVD | Google Earth |
| BitTorrent | ICQ |
| CloneCD | iTunes |
| CloneDVD2 | KazaA |
| Daemon Tools | Skype |

Tabulka 2 – Výčet některých zakázaných softwaru [zdroj: vlastní]

### 3.1.10 Softwarový vývoj

Při vývoji softwaru je nutné oddělit odpovědnost, pravomoci a povinnosti techniku tvořících či jinak spolupracujících na vývoji softwaru. Při vývoji nového nebo úpravě a aktualizaci staršího softwaru musí byt zajištěno oddělení vývojového, testovacího a produkčního prostředí z důvodu vymezení odpovědnosti.

Povinnosti vedoucích pracovníku při vývoji nového softwaru či při inovaci staršího softwaru je zajistit, aby všechny nově tvořené aplikace či prováděné inovace aplikací ve vztahu k bezpečnostním mechanismům byly vytvořeny v souladu s mezinárodně platnými normami (např. ISO normy, standardy banky). Tvorba a inovace se musí taky řídit podle požadavku odboru bezpečnost ICT banky. Změny v informačních systémech banky se mohou provést až po analýze dopadu změn na bezpečnost inovovaných systémů.

Pracovní prostředí a inovaci v nich je možné provádět pouze po schválení příslušného vlastníka či správce produktu. Při schválení změny v systému nesmí tato změna zasáhnout do integrity programového vybaveni systému. Všechny změny v systémech se mohou uskutečnit až po autentizaci uživatele. Samozřejmě, že všechny změny provedené v systémech, které by mohly ovlivnit pracovní prostředí, musí projít důkladným testováním a analýzou dopadu těchto změn na integritu systému.

Zaměstnanci, kteří se zabývají vývojem a inovaci, nesmí použit své přístupové právo pro zásahy do produkčního (pracovního) prostředí informačních systémů a databázi. Databáze a informační systémy využívají knihovny, proto práce a zásahy do zdrojových kódů těchto knihoven se může provádět až po odsouhlaseni těchto změn úsekem bezpečnosti, zároveň práce s těmito knihovnami se řídí podle striktních pravidel stanovených úsekem bezpečnosti.

Bezpečnostní rizika se musí správcem produktu za spolupráce s odborným útvarem zanalyzovat již při vytváření software tzn. ve vývojové fázi. Bezpečnostní rizika musí být eliminována a tato eliminace se provádí zavedením vhodných automatických i manuálních kontrol a postupů. V případě výměny dat mezi systémy musí existovat rozhraní, kde je zajištěna propojovací síť šifrováním a v systému určení musí byt identifikovány jejich místa určeni.

V každé aplikaci je zabudovaná kontrola integrity a taktéž musí být zavedena odpovídající systémová archivace zpráv, které lze využit k podávání zpráv využitelných pro řízení, správu a audit nebo i pro potřeby mimořádných šetření. Taktéž je zapotřebí při výpadku provést rychlé obnovení systému.

### 3.1.11 Bezpečnost dat

V bankovním sektoru se kladou specifikované požadavky na bezpečnost dat. Tyto požadavky se vztahují na všechny informace uložené, přenášené nebo jinak produkované kterýmkoli ze systémů informační technologie.

Každá informace, která je vyprodukována systémem informační technologie, musí mít striktně určenou klasifikační hodnotu (viz. kapitola 3.1.1 ). Klasifikační hodnotu provede příslušný vlastník informace, správce produktu, autor spolu s odborným úsekem pro tuto kvalifikaci.

Pro klasifikaci dat je nutné zohlednit následující požadavky:

- právní předpisy,
- možnost finančního odhalení a zneužití dat,
- význam pro řízení společnosti,
- náklady na získání a rekonstrukci dat,

- dostupnost a udržování informací,
- význam pro konkurenci, veřejné sdělovací prostředky.

Přístup k vytvořeným datům a jejich distribuce se musí omezit správcem produktů na základě kvalifikace informace. Správce při vytvoření dat musí taktéž určit i dobu jejich archivace. Samozřejmě omezení přístupu musí být nastaveno i na záložní kopie a výstupy určené k archivaci. Pro informace, které spadají do klasifikací, jsou určena pravidla a režimy s jejich zacházením ( tištěné i elektronické informace). Pro datové soubory, na které spadají klasifikace *zvláště důvěrné,* je nezbytně nutné zajistit vhodný způsob jejich dalšího zabezpečení (např. šifrováním). Ve všech bodech zpracování dat musí systémy a aplikace poskytovat prostředky zajišťující integritu dat. Tato integrita dat se zajišťuje např. pomocí kontrolních součtů, digitálního podpisu či kryptograficky.

### 3.1.12 Informační systémy a jejich provoz

Bankou je určen příslušný orgán, který dohlíží na provoz všech aplikací, systémového software a služeb komunikací ve vztahu k uživatelům. Zpracování dat v těchto systémech je zcela nezávislé na zaměstnancích provádějících vývoj systému. Režijní vedení a provoz informačních systémů musí být pravidelně prověřován a vyhodnocován jejich dopad na bezpečnost.

Úsekem bezpečnosti v bance je určen provozovatel informačního systému, ten odpovídá za dodržování pravidel ochrany a bezpečnosti informační a komunikační technologie.

Provozovatel klade důraz na:

- dodržování stanovené úrovně dostupnosti poskytovaných služeb,
- dodržování zásad fyzické bezpečnosti,
- bezpečnost distribuce dat, jejich archivace, zálohování či likvidace,
- kontroly logických přístupů všech provozních zaměstnanců pracujících na výpočetní technice.

V případech, kdy by mohla funkčnost systému selhat, musí být vypracovány havarijní plány a plány obnovy. Plány musí obsahovat i specifikaci alternativního opatření a postupy pro obnovu systému a aplikací, které vedou k minimalizaci ztrát a urychlí obnovu standardního systému. Pro případ nedostupnosti části či celého zpracujícího zařízení musí být zajištěno portfolio základních služeb náhradním způsobem.

Zásah podpory, která je vyžadovaná z důvodu kolize či pokud je vyžadovaná vzdálená diagnostika (třetí strany), může nastat pouze řízeným způsobem a o této činnosti se bude archivovat úplný revizní záznam. Vždy při zásahu servisních zaměstnanců je zapotřebí provést ochranu dat i programů před neoprávněným přístupem těchto zaměstnanců.

### 3.1.13 Komunikační sítě a jejich bezpečnost

Komunikační (datové) sítě slouží k přenosu dat a informací, které jsou nezbytné pro zajištění provozu banky.U dat přenášených po komunikační sítí (datový tok) musí být zajištěna jejich adekvátní ochrana a integrita těchto informací. Úsek bezpečnosti ICT banky je zodpovědný za provoz a infrastrukturu komunikačních sítí.

Úsek bezpečnosti v rámci komunikační sítě, kterou využívá banka pro přenos dat, musí implementovat prostředky a mechanizmy, které zajistí:

- správu sítě definovaným, řízeným zpětně kontrolovatelným a auditovatelným způsobem,
- zajištění výkonnosti sítě,
- zajištění odolnosti sítě proti poruchám (dynamický routing, redundance komunikačních tras),
- segmentaci sítě (implementaci VLAN, ACL – access listy),
- implementaci a využívání QoS (Quality of Service) na WAN části komunikační sítě,
- implementace monitorovacího systému přenášených dat (např. pomocí IDS systémů - Intrusion detection Systems).

***Havarijní plány a plány obnovy***

Při výskytu selhání funkčnosti komunikační sítě musí být vypracovány havarijní plány a plány obnovy. V těchto plánech musí byt specifikována alternativní opatření a následující postupy pro obnovu komunikační sítě z důvodu zajistit minimalizaci ztrát a rychlý návrat k běžnému provozního stavu.

Každý hardware a software v komunikačních sítí musí splňovat kritéria obecně stanovená v pravidlech ochrany a bezpečnosti ICT a samozřejmě vybavení musí být v souladu s dalšími definovanými normami a standardy platné v bance.

Do prvku infrastrukturních zařízení a prvku komunikační (datové) sítě se musí zajistit, aby se za všech okolností propojovala informační technologie řádné autentizovana a k síťovým prvkům přistupovali autorizovaní uživatele zařízení. Musí být zavedeny postupy umožňující vysledování případného místa a způsobu narušení bezpečnosti v komunikační síti.

Při propojení komunikační sítě s druhotnými subjekty (např. Internet, datové sítě dceřiných společností, datové sítě spolupracujících firem) je toto propojení možno zřídit pouze s využitím firewallu, který musí byt zaveden na straně banky i na straně připojeného subjektu. Z důvodu bezpečnosti při teto komunikaci (výměně dat) musí byt subjekty v síti jednoznačně identifikovány. Komunikační kanály musí být využity pouze pro komunikaci mezi připojenými subjekty za jiným účelem tato síť nesmí byt kvůli bezpečnosti použita.

### 3.1.14 Bezpečnostní auditní záznamy

Každá banka musí vest bezpečnostní auditní záznamy o všech prováděných činnostech a operaci, které jsou vykonány na terminálech. Banka musí mít k dispozici informace z bezpečnostních auditních záznamu pro událost, kdy je zapotřebí vyšetřit činy porušující důvěrnost, integritu a dostupnost, včetně nástrojů pro jejich vyhodnocování.

Základní informace, které se ukládají v bezpečnostních auditních záznamech musí obsahovat:

- přesný čas a identitu přihlášených a odhlášených uživatelů,
- počet neúspěšných pokusů o autentizaci uživatele,
- počet neúspěšných pokusů o přístup k datům,

- počet neúspěšných pokusů o provedení transakcí a neoprávněných operací,
- počet neúspěšných pokusů o přístup k prostředkům a datům, které souvisí s bezpečností,
- změny privilegií a bezpečnostních vlastnosti uživatelů,
- změny nastavení bezpečnostních, systémových parametrů,
- změny přístupových práv.

Zaznamenaná událost musí mít uvedeno:

- identifikace uživatele (uživatelský účet),
- identifikace terminálu nebo adresa sítě zařízení,
- datum a čas,
- další potřebné údaje o události (typ události, výsledek, apod.).

Řízení bezpečnostních auditních záznamů i informace uloženy v archivech musí být chráněny proti neautorizovanému přístupu a samozřejmě se nejvíc apeluje na ochranu před modifikací a zničení záznamu.

V bance se zavádí systémy a softwarové nástroje, které vytvoří mechanismus pro automatické vytváření archivu bezpečnostních auditních záznamů na externí médium (externí disky) v předem navolených intervalech, včetně nástrojů pro vyhodnocování a analýzu archivovaných záznamů.

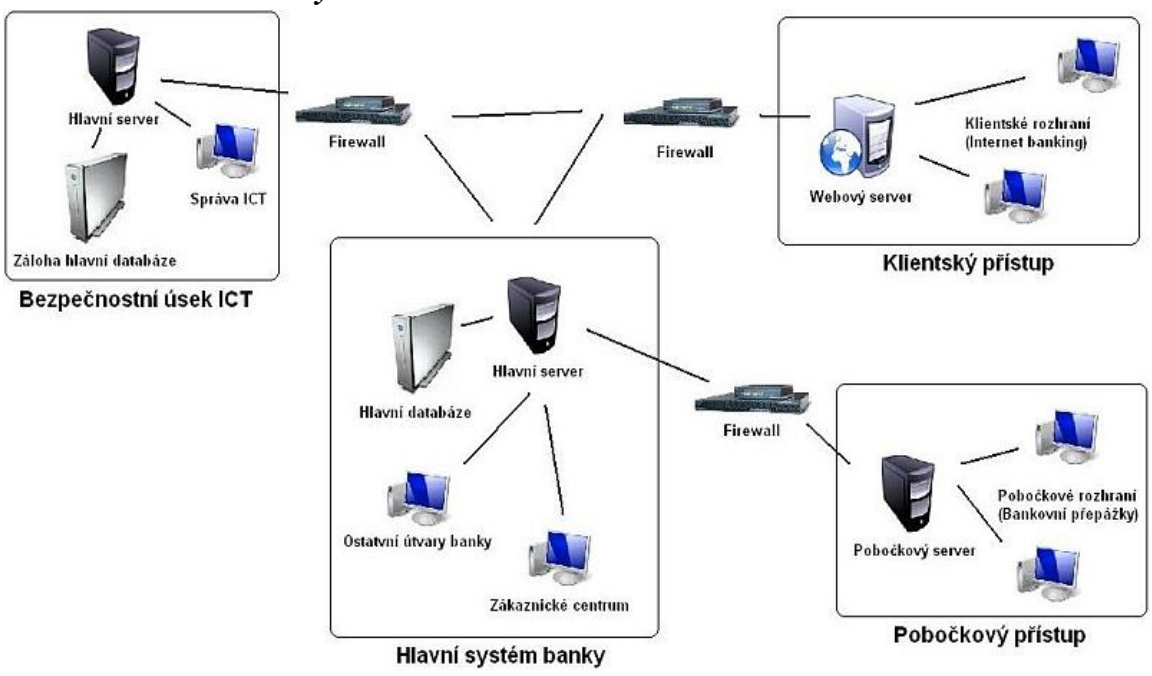
Některé vybrané systémy a aplikace, které zajišťují nepřetržitý chod v bance je potřeba chránit i před vnějším narušením. V těchto aplikacích je k dispozici detekční nástroj pro on-line monitorování bezpečnosti, který slouží k pravidelnému vyhodnocování průniku do systému a stanovení protiopatření.

# 4 NÁVRH PREVENCE POMOCÍ FIREWALLU

Firewall je určen k ochraně vnitřního systému banky od průniku útočníků z externí sítě. Systém firewallu slouží k ochraně vnitřních zdrojů od datových toků externích subjektů jako jsou servisní a dceřinné organizace či toky z Internetu. Je nutné oddělit externí síť, která má veřejně publikovaná data v demilitarizovaných zónách od vnitřní sítě banky, v niž jsou důvěrná data. Systém je nastaven, aby dělil jednotlivé bezpečnostní zóny, tím brání průniku z jednoho systému do druhého. Systémy pomohou při detekci potencionálního nebezpečí narušení důvěrných dat.

Inicializace systému je tvořena větším množstvím a druhy firewallů na různých systémových platformách pro eliminaci chyb jednoho výrobce firewallu. Při instalování systému je nutno postupovat tak, aby nebylo možno využít konfigurační nebo jiné chyby jedné části systému a tím obejít nastavení celého systému. Práva správců systému musí být rozdělena na rozdílné subjekty, protože žádný správce nesmí mít práva pro konfiguraci celého systému. Jednou z hlavní části systému je detekce možného bezpečnostního incidentu a podat o takovémto incidentu okamžité hlášení bezpečnostnímu úseku banky. Samozřejmě, že veškeré detekované události systémem jsou archivovány pro případný zpětný audit.

***Schéma ICT banky***




Obrázek 7 – Schéma ICT banky [zdroj: vlastní]

Ze schéma, které znázorňuje ICT banky lze jasně pochopit jak je bezpečnostní prvek firewall důležitý. Chrání komunikaci v bance na všech spektrech systémů. Komunikace z jednoho rozhraní do druhého musí projít přes bezpečnostně nakonfigurovaný firewall. Z tohoto důvodu je zapotřebí analyzovat bezpečnostní politiku a její pravidla. Poté co je určena bezpečnostní politika je nutné analyzovat bezpečnostní hrozby a cíle, kterým firewall musí čelit a zároveň poskytovat.

## 4.1 Bezpečnostní politika a její pravidla u firewallu

Je nutno zavést pravidla bezpečnostní politiky, která je zapotřebí striktně dodržovat. Bezpečnostní politika je označována písmenem „P“ a nadpisem.

*P.Šifrování*

Při používání funkcích a ochrany vzdálené administrace musí být zaveden šifrovací algoritmus Triple DES[17], a šifrovací modul musí vyhovovat standardu banky pro inicializaci a zapojení kryptografických modulů.

*P.Rozdělení NAT a DNS*

Ochrana před zneužitím útočníkem ve vnější sítí může být provedena ukrytím jmen a adres interních systémů. Realizace tohoto rozdělení je za pomocí využití překladu síťových adres (NAT[18]) a rozdělením DNS.

*P.Kontroly povolení*

Musí se dodržovat pravidla pro zpracování příchozího toku dat. V toku dat se musí blokovat všechny pakety a spojení, které nebyly vysloveně vyžádány či povoleny.

*P.Provozu IS*

IS banky a všechny jeho částí jako jsou protokoly a spojení na tento systém musí být z důvodu přístupů z vnější sítě blokovány firewallem.

---

[17] Triple DES je bloková šifra založená na šifrování Data Encryption Standard (DES), které aplikuje třikrát a tak zvyšuje její odolnost proti prolomení

[18] Network Address Translation překlad síťových adres

*P.Blokování síťových provozů*

Některé typy síťového provozu jsou z důvodu bezpečnosti vždy blokovány:

- Neautentizovaný zdrojový systém, který žádá o komunikaci a má jako adresu systému firewallu, tudíž se vydává za firewall banky.
- Příchozí paket dat ze zdrojovou adresou vnější sítě, který se vydává jako paket dat vytvořen na síti za firewallem banky.
- Pokus o komunikaci ze systému používajícího zdrojovou adresu která nezapadá do adresného prostoru definovaných dle RFC[19] pro soukromé sítě.
- Pokus o komunikaci z neautentizovaného zdroje obsahující SNMP[20] provoz.
- Pokus o komunikaci a příchozí provoz obsahující informaci řízeného směrování (IP source routing[21])
- Pokusy o komunikaci, kde cílová či zdrojová adresa obsahuje IP adresu 127.0.0.1.
- Pokusy o komunikaci, kde cílová či zdrojová adresa obsahuje IP adresu 0.0.0.0.
- Pokusy o komunikaci, která obsahuje "Broadcast Addresses" Např. rozsah IP adres použitý v síti představuje IP adresu sítě + rozsah IP adres použitelný pro připojená zařízení + IP adresu broadcastu. Pro představu: V síti 192.168.0.0/24 (maska 255.255.255.0) se používají tyto IP adresy:
    - IP adresa sítě: 192.168.0.0

[19] RFC Request for Comments (žádost o komentáře), která se používá pro označení řady standardů a dalších dokumentů popisujících Internetové protokoly, systémy apod. Jak už název napovídá, RFC jsou oficiálně považovány spíše za doporučení než normy v tradičním smyslu, přesto se podle nich řídí drtivá většina Internetu.

[20] Simple Network Management Protocol (SNMP) je součástí sady internetových protokolů. Slouží potřebám správy sítí. Umožňuje průběžný sběr nejrůznějších dat pro potřeby správy sítě, a jejich následné vyhodnocování. Na tomto protokolu je dnes založena většina prostředků a nástrojů pro správu sítě.

[21] Information Protocol Routing (IPR) je v informatice směrovací protokol umožňující směšovačům (routerům) komunikovat mezi sebou a reagovat na změny topologie počítačové sítě.

- IP adresa použitelná pro připojená zařízení: 192.168.0.1 - 192.168.0.254
- IP adresa broadcastu: 192.168.0.255

*P.Bezpečnosti OS*

Při implementaci firewallu do Operačního systému (např. UNIX, Windows) musí být operační systém aktualizován a odstraněny z něho nadbytečné aplikace a zabezpečen proti útokům, které jsou běžné na tyto operační systémy. Záplaty a bezpečnostní opravy musí být včas inicializovány.

*P.Zálohy*

Jednou ze součástí bezpečnostních pravidel je zálohování systému firewallu. Tato záloha je prováděna přes interní zařízení, které je připojeno na firewall (např. externí disky, flash paměti či záloha na Blue-ray[22] disky). Zálohy se musí provádět pravidelně a za bezpečnostního dozoru. Zálohy se musí střežit, aby se nedostaly nepovolaným osobám do rukou, protože poté by mohli útočníci mít čas přijít na potenciální slabé místo průchodu do sítě.

*P.Zmírnění dopadů*

Banky se musejí připravit i na scénář, kdy se budou muset vypořádat s narušeními. Toto narušení může vzniknout i přes zabezpečení systémů firewallem a nelze se mu vyhnout. Banka musí zřídit tým, který se bude zkoumat jednotlivé narušení systému a analyzovat jejich dopady na bezpečnost. Tým je povinen po útoku vytvořit bezpečnostní záplatu místa, kudy útočník narušil systém.

[22] Blu-ray disk patří k třetí generaci optických disků, určených pro ukládání digitálních dat. Disky umožňují záznam dat s celkovou kapacitou až 25 GB u jednovrstvého disku, 50 GB u dvouvrstvého disku až po 80 GB u oboustranné dvouvrstvé varianty.

## 4.2 Analýza požadavků a opatření

Je zapotřebí uvést a zanalyzovat vztah bezpečnostní hrozby působící na služby a technické prostředky firewallu a bezpečnostní cíle, které stanoví eliminaci identifikovaných bezpečnostních hrozeb. Bezpečnostní hrozby jsou označeny písmenem „H“ a bezpečnostní cíle písmenem „C“. Jednotlivé hrozby a cíle jsou označena písmenem „H“ nebo „C“ a nadpisem.

### 4.2.1 Hrozby působící na zařízení a služby firewallu

*H.Neoprávněná osoba*

Pokus útočníka obejít zabezpečení firewallu, aby mohl přistoupit k bezpečnostním či ostatním funkcím poskytovaným firewallem a využít je ve svůj prospěch.

*H.Opakované přihlášení*

Opakované pokusy o uhádnutí autentizačních údajů za účelem použití údajů k vedení útoku na firewall útočníkem.

*H.Získané ID údaje*

Hrozba, kdy se do „rukou“ útočníka dostanou platné identifikační a autentizační údaje pro přístup k funkcím poskytované firewallem.

*H.Podvrh uživatele/objektu*

Útočník by mohl z vnější sítě pokoušet obejít bezpečnostní politiku podvržením autentizačních dat a vydáváním se za legitimního uživatele či objekt vnitřní sítě.

*H.Nepřípustné informace*

Při zaslání nepřípustné informace či škodlivého programu přes firewall do vnitřní sítě, by mohlo zapříčinit zneužití zdrojů vnitřní sítě útočníkem.

*H.Chyby funkčnosti*

Možným výskytem chyb ve funkčnosti firewallu by mohla neautorizovaná osoba sledovat informační toky z firewallu. Útočník může získat zbytkovou informaci z předchozí komunikace nebo interní údaje firewallu.

*H.Datové sítě*

Útočník nebo vnější ICT může být schopný vidět, měnit nebo vymazat informace související s bezpečností, které jsou posílány po datové síti mezi vzdáleně umístněným administrátorem a firewallem.

*H.Nečinění kontroly záznamu*

Není prováděna zpětná kontrola auditních záznamů a proto nesou odpovědnost osoby, které nejednaly podle bezpečnostních pravidel, a tím umožní útočníkovi uniknout odhalení.

*H.Konfigurace firewallu*

Útočník může číst, modifikovat, nebo zničit z bezpečnostního hlediska velice důležitá konfigurační data firewallu.

*H.Auditních záznamů*

Útočník chce vniknout do vnitřního systému a způsobit ztrátu auditních záznamů nebo zabránit dalšímu ukládání auditních záznamů.Útočník v systému provede akce, které vedou k vyčerpání kapacity zařízení pro ukládání dat, tím se snaží maskovat svoji činnost.

*H.Zkušeného útočníka*

Zkušený útočník s vysokým potenciálem, který se může pokusit obejít bezpečnost firewallu, aby získal přístup k chráněným datům.

*H.Špatné konfigurace*

Možnost neschopného servisu z důvodu nekvalifikovaných zaměstnanců. Např. nevhodná konfigurace firewallu nebo správa nedostatečně chráněným způsobem autorizovanou či neautorizovanou osobou. Tuto hrozbu je zapotřebí eliminovat při personálních náběrech specializovaných zaměstnanců.

### 4.2.2 Bezpečnostní cíle pro firewall

*C.Identifikace*

Dříve než firewall poskytne přístup ke svým funkcím, musí jednoznačně identifikovat a autentizovat identitu všech uživatelů.

*C.Zajistit nezneužití*

Firewall musí zabránit opakovanému použití autentizačních dat uživatelům pokoušejícím se autentizovat na firewall z připojené sítě.

*C.Jistit komunikaci*

Musí se zajistit, aby firewall přenášel tok všech informací mezi uživateli vnitřní sítě připojené k firewallu a mezi uživateli vnějších sítí připojených k firewallu. Důležité je zajistit, že nejsou přenášeny zbytkové informace z předchozích informačních toků.

*C.Chránit při výpadku*

Při restartování firewallu nebo výměně některých technických části (servisní zásah) musí být zajištěny zdroje firewallu i jiné zdroje na připojené síti, která jsou firewallem chráněna.

*C.Šifrování a dešifrování*

Při komunikací firewallu s administrátorem zajišťující jeho správu na dálku, musí být zajištěna komunikace šifrovacím a dešifrovacím zařízením.

*C.Sebeobrany*

Jednou z hlavní funkcí firewallu musí být ochrana sama sebe proti pokusům neautorizovaných uživatelů o infiltraci, deaktivaci nebo před zásahy do bezpečnostních funkcí firewallu.

*C.Ukládání záznamů*

Další prioritní funkce firewallu je zajišťovaní pořizování auditních záznamu o událostech vztahujících se k bezpečnosti. Tyto záznamy jsou pro pozdější vyhodnocování nebo revize. Všechny záznamy obsahují přesné datumy a časy. Firewall musí poskytovat prostředky k vyhledávání a třídění auditních záznamů podle uživatelem zadaných vlastností.

*C.Kontroly toku dat*

Důležitou součástí firewallu je zajišťování informačních toků procházející jím z důvodu identifikace uživatele, který tok dat obdržel či vyslal. Správci musí implementovat použití bezpečnostních funkcí spojených s auditem.

*C.Zabezpečení správy*

Firewall musí být zajištěn funkcemi, které umožní,, aby se do něho přihlásili pouze administrátoři, kteří ho systémově spravují. Tuto funkci zajištění muže plnit heslo, PIN či čipová karta k počítači apod.

*C.Externích uživatelů*

Správcům musí umožňovat firewall prostředky k řízení a k omezení přístupu oprávněných externích uživatelů k bezpečnostním funkcím firewallu.

*C.Zkouška útokem*

Musí proběhnout testování firewallu, zda je odolný pro útočníkovi s průměrnými útočnými znalostmi.

*C.Fyzická ochrana*

Systém a součástí firewallu musí být fyzicky a bezpečnostně zabezpečen.

*C.Loajální zaměstnanci*

Banka musí již při výběru administrátorů musí zkoumat jejich minulost z důvodu bezpečnosti. Poté administrátoři nesmí chovat nepřátelské úmysly a jsou povinni dodržovat všechny směrnice. Samozřejmě je nutno brát v potaz, že i loajální administrátoři mohou udělat chybu.

*C.Zaručeného průchodu*

Veškerá komunikace a informace musí proudit mezi vnitřní a vnější sítí pouze přes firewall.

*C.Přímého připojení*

Pokud firewallu podporuje na svém zařízení přímé spojení pomocí externího zařízení (např. znaková/grafická konzole) je nutné toto spojení mít pod kontrolou. Kontrola znamená archivace všech komunikací s takovýmito zařízení.

*C.Kontrola servisních přístupů*

Vzdálené připojení přes vnitřní i vnější síť mohou provádět jen administrátoři, kteří zajišťují správu firewallu.

*C.Podmínky bezpečnosti*

Instalace, správa a provoz firewallu musí splňovat a zajišťovat bezpečnost banky a její sítě.

*C.Aktualizace bezpečnosti*

Bezpečnostní politiky a praktiky jsou podle aktuální situace upravovány a aktualizovány dobře vyškolenými administrátory.

### 4.2.3 Analýza působení bezpečnostních hrozeb na bezpečnostní cíle

| Hrozby [H] + Politika [P] / Cíle [C] | H.Neoprávněná osoba | H.Opakované přihlášení | H.Získané ID údaje | H.Podvrh uživatele/objektu | H.Nepřípustné informace | H.Chyby funkčnosti | H.Datové sítě | H.Nečinění kontroly záznamu | H.Konfigurace firewallu | H.Auditních záznamů | H.Zkušeného útočníka | P.Šifrování |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| C.Identifikace | X | | | | | | | | | | | |
| C.Zajistit nezneužití | | X | X | | | | | | | | | |
| C.Jistit komunikaci | | | | X | X | X | | | | | | |
| C.Chránit při výpadku | X | | | | | | | | X | | | |
| C.Šifrování a dešifrování | X | | | | | | X | | | | | X |
| C.Sebeobrany | X | | | | | | | | X | X | | |
| C.Ukládaní záznamů | | | | | | | | X | | | | |
| C.Kontroly toku dat | | | | | | | | X | | | | |
| C.Zabezpečení správy | X | | X | | | | | | | X | | |
| C.Externích uživatelů | X | | | | | | | | | | | |
| C.Zkouška útokem | | | | | | | | | | | X | |

Tabulka 3 - Působení bezpečnostních hrozeb na bezpečnostní cíle [zdroj: vlastní]

# ZÁVĚR

Počítačová kriminalita zasahuje do všech činnosti lidského života. Z pohledu organizovaného zločinu je počítačová kriminalita jednou z nejvýnosnějších trestných činností. Útočníci a pachatele jsou rafinovanější a profesionálnější, protože se kriminální metody modernizují a jsou vždy o krok napřed oproti orgánům, které tyto způsoby trestné činnosti vyšetřují.

Práce se zabývá počítačovou kriminalitou v bankovním sektoru. Jsou zde uvedeny způsoby, kterých útočníci využívají pro své obohacení. Zároveň je zde upozorněno na problém, který vytvářejí sami klienti bank svou neopatrností a důvěrou v prostředky bankovnictví na internetu. Spoustu počítačové kriminality (Pharming, Phishing) vytvářejí klienti neznalí bezpečnostních pravidel chování na počítači. V práci je rozebrána i metoda tzv. Skimmingu, kdy útočníci využívají nepozornost klientů banky pro zkopírování jejich platebních karet a následnému jejich použití pro zisk pachatelů.

Bankovní sektor České republiky může klientům jen doporučit, aby byli opatrní při manipulaci se svými účty ( použití internetového bankovnictví, výběry z bankomatu). Banky taktéž využívají síť poboček a své Internetové stránky pro předávání informací klientů jako jsou např. brožury bezpečnosti práce na PC či ukázky podvodných e-mailů apod..

V bankovním sektoru se již počítá s nepozornosti klientů a je to rizikový faktor. Banky se chrání hlavně prevencí a zavaděním své bezpečnostní politiky, kterou musí zaměstnanci banky a samozřejmě i banka striktně dodržovat. Z tohoto důvodu jsem se v praktické části zaměřil na analýzu bezpečnostní politiky a vytvořil jsem bezpečnostní politiku, kterou by se banky měly řídit. Bezpečnostní politika by měla zohledňovat všechny nebezpečné faktory pro narušení bezpečnostní ochrany. V práci je využito způsobu ochrany bankovní informační sítě pomocí technického prvku Firewall. U tohoto prvku jsou analyzovány hrozby působící na zařízení a služby s bezpečnostními cíly pro firewall. Tato analýza je graficky znázorněna v tabulce pro lepší představu působení hrozeb na cíle, které jsem si navrhl a specifikoval.

Počítačovou trestnou činnost není možné zcela potlačit nebo vymýtit. Eliminaci těchto činů z části zajišťují bezpečnostní opatření, která v konečném pohledu budou prolomeny útočníky. Jednou z povinnosti vlády a zákonodárců je modernizovat zákony zabývající se touto trestnou činností z důvodu jejich potlačení. Všeobecně se v názorech

odborníků a znalců objevuje určitá skepse v trendech počítačové kriminality a limitů jejího odhalování. Nejvíce názorů se ovšem shoduje k přesunutí daleko více sil do prevence či obrany počítačů a informačních systémů, protože toto je jediná možnost, jak nad touto trestnou činností zvítězit. V České republice současná trestně právní úprava není tak moderní jako v předních státech Evropské unie, proto je zapotřebí trestní úpravu aktualizovat a modernizovat, což je obtížné z důvodu rychle modernizace těchto trestných činů.

# SUMMARY

Computer-related crime affects all activities of human life. View of organized crime, cyber crime is one of most profitable criminal activity. Attackers and criminals are sophisticated and professional, because criminal methods modernized, and are always one step ahead of authorities, these methods investigating crime.

This work deals with cyber crime in the banking sector. Are listed ways that attackers use to their enrichment. At the same time there to the problem, which themselves produce their bank clients lack of caution and confidence in the banking resources of the Internet. Lot cyber crime (Pharming, Phising) provide clients knew safety rules of conduct on the computer. The work is analyzed and method called skimming, where the attackers used inattention bank's clients copy of their credit cards and their subsequent use for profit offenders.

Czech banking sector clients can only recommend that they cautious when handling their bills (using Internet banking, ATM withdrawals). Banks also use a network of branches and their website for transmitting information to clients such as safety brochures on a PC or examples of fraudulent e-mails, etc..

The banking sector has been calculated with the client's inattention and it is a risk factor. Banks are mainly protects the prevention and implementation of its security policy to the Bank's employees and of course the bank strictly adhered to. For this reason, I focused on the practical part of the analysis of security policy and created a security policy that the banks would be governed. The security policy should take into account all the dangerous factors for breach of security protection. In my work I use a means of protecting the banking computer network Firewall with technical element. For this element, I analyzed the threats to the operating facilities and services with the security objectives for the firewall. This analysis graphically illustrate my table for a better understanding of threats to the operation of goals that I have designed and specified.

Cyber crime can not be completely suppress or eradicate. Elimination of such acts of providing security measures in final view will be broken by attackers. One of the responsibilities of government and lawmakers to modernize the laws dealing with this crime because of their suppression. Generally the views of professionals and experts appears certain skepticism in the trends of cyber crime and its limits detect. Most views are of

course identical to přesutí far more energy into prevention or defense of computers and information systems, because this is the only way to win this criminal activity. In the Czech Republic of contemporary criminal law is not as advanced as the leading European Union states, therefore it is necessary to update the presentation of criminal and modernize, which is difficult because of rapid modernization of the criminal offenses.

# SEZNAM POUŽITÉ LITERATURY

***Monografie:***

[1] MATĚJKA, Michal. Počítačová kriminalita. vyd. Praha : Computer Press, 2002. 106 s. ISBN 80-7226-419-2.

[2] VLČEK, Martin. Počítačové právo. vyd. Praha : C. H. Beck, 1995. 261 s. ISBN 80-7179-009-5.

[3] POŽÁR, Josef. Informační bezpečnost. vyd. Plzeň : Vydavatelství a nakladatelství Aleš Čeněk, 2005. 309 s. ISBN 80-86898-38-5.

[4] ČANDÍK, Marek. Základy informační bezpečnosti. vyd. Zlín : Univerzita Tomáše Bati, 2004. 107 s. ISBN 80-73182-18-1.

[5] MUSIL, Stanislav, RNDr. Počítačová kriminalita. vyd. Zlín : Institut pro kriminologii a sociální prevenci, 2000. 107 s. ISBN 80-86008-80-0.

[6] LANCE, James. Phishing bez záhad. Praha : Grada Publishing, a.s., 2007. 281 s. ISBN 978-80-247-1766-1.

[7] JIROVSKÝ, Václav. Kybernetická kriminalita. vyd. Praha : Grada Publishing, a.s., 2007. 284 s. ISBN 80-247-1561-9.

[8] Allen Harper, Shon Harris, Chris Eagle, Jonathan Ness, Michael Lester. Hacking - manuál hackera. vyd. Praha : Grada Publishing, a.s., 400 s. ISBN 978-80-247-1346-5.

[9] DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. vyd. Brno : Computer Press, 2004. 187 s. ISBN 80-251-0106-1.

[10] POLOCH, Roman. Způsoby páchání a vyšetřování počítačové kriminality, bakalářská práce. Universita Tomáše Bati ve Zlíně. rok. 2008.

***WWW stránky:***

[11] Stránky ministerstva vnitra. [Online] www.mvcr.cz.

[12] Ochrana autorských práv. [Online] MICROSOFT.COM. http://www.microsoft.com/cze/piratstvi/default.mspx.

[13] Business software alliance. [Online] BSA.COM. http://w3.bsa.org/czechrepublic.

[14] Počítačová (informační) kriminalita a úloha policisty při jejím řešení - materiál z přílohy časopisu POLICISTA č. 3/1998 [Online] http://www.spsmvbr.cz/osobni/jedlicka/poc_krim/pocitace.htm.

[15] Ukázky phishingu. [Online] Česká spořitelna. http://www.csas.cz/banka/menu/cs/banka/nav7004_phishing_ukazky

[16] Stránky otevřeného on-line slovníku Wikipedie [Online] Wikimedia Foundation Inc. http://cs.wikipedia.org/wiki/ICT. http://cs.wikipedia.org/wiki/Wi-Fi. http://cs.wikipedia.org/wiki/Spam. http://cs.wikipedia.org/wiki/Paypal. http://cs.wikipedia.org/wiki/Ascii. http://cs.wikipedia.org/wiki/DNS. http://cs.wikipedia.org/wiki/Secure_Digital. http://cs.wikipedia.org/wiki/TripleDES. http://cs.wikipedia.org/wiki/Network_address_translation. http://cs.wikipedia.org/wiki/RFC. http://cs.wikipedia.org/wiki/SNMP. http://cs.wikipedia.org/wiki/Routing_Information_Protocol. http://cs.wikipedia.org/wiki/Blu-ray.

[17] Phishing stručně. [Online] Česká spořitelna. http://www.csas.cz/banka/menu/cs/banka/nav7001_phishing_strucne.

[18] Počítačová kriminalita a banky. [Online] Petr Zámečník. 21.4.2008. http://www.investujeme.cz/clanky/pocitacova-kriminalita-a-banky-kdo-vede/.

[19] BSA tisková zpráva. [Online] BSA.COM. 21.5.2010. http://www.adsl.cz/archiv/kratke-zpravy/piratskeho-softwaru-v-cesku-ubylo-nelegalne-se-ho-podle-bsa-uziva-37-187.html

# SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

| | |
|---|---|
| ASCII | American Standard Code for Information |
| CD | Compact Disc |
| DES | Data Encryption Standard |
| DNS | Domain Name System |
| DVD | Digital Video Disc |
| GB | Gigabyte |
| ICT | Information and Communication Technologies |
| ID | Identification |
| IS | Information System |
| NAT | Network Address Translation |
| OS | Operation System |
| PayPal | Internetový platební systém |
| PC | Personál Computer |
| PIN | Personal Identification Numer |
| RFC | Request for Comments |
| SD | Secure Digital |
| SNMP | Simple Network Management Protocol |
| Wi-Fi | Wireles Fidelity |

# SEZNAM OBRÁZKŮ

# SEZNAM GRAFŮ A TABULEK

# SEZNAM PŘÍLOH

Příloha P1: Vypálené CD s touto prací.