**Mendelova univerzita v Brně**
**Provozně ekonomická fakulta**

# Možnosti zabezpečení proti sociálnímu inženýrství v oblasti elektronického bankovnictví

## Bakalárska práca

**Vedoucí práce: Ing. Stratos Zerdaloglu** **Ondrej Kubričan**

**Brno 2017**

**Poďakovanie**
**Týmto by som chcel poďakovať vedúcemu mojej bakalárskej práce Ing. Stratosovi Zerdaloglu, hlavne za jeho cenné pripomienky a rady, ktorými prispel k skvalitneniu práce, za trpezlivosť a podporu.**

**Čestné prohlášení**

Prohlašuji, že jsem tuto práci: **Možnosti zabezpečení proti sociálnímu inženýrství v oblasti elektronického bankovnictví**vypracoval/a samostatně a veškeré použité prameny a informace jsou uvedeny v seznamu použité literatury. Souhlasím, aby moje práce byla zveřejněna v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů, a v souladu s platnou *Směrnicí o zveřejňování vysokoškolských závěrečných prací.*

Jsem si vědom/a, že se na moji práci vztahuje zákon č. 121/2000 Sb., autorský zákon, a že Mendelova univerzita v Brně má právo na uzavření licenční smlouvy a užití této práce jako školního díla podle § 60 odst. 1 Autorského zákona.

Dále se zavazuji, že před sepsáním licenční smlouvy o využití díla jinou osobou (subjektem) si vyžádám písemné stanovisko univerzity o tom, že předmětná licenční smlouva není v rozporu s oprávněnými zájmy univerzity, a zavazuji se uhradit případný příspěvek na úhradu nákladů spojených se vznikem díla, a to až do jejich skutečné výše.

V Brně dne 20. května 2017 _____

**Abstract**

Kubričan, O. The Security options against social engineering in electronic banking. Bachelor thesis. Brno: Mendel University, 2017.
Bachelor thesis deals with social engineering methods in relation to electronic banking. It points to the security features and defense mechanisms of Internet banking and analyzes them in selected banks of the Czech Republic. After the analysis suggests increasing the security of online banking.

**Keywords**

E-banking, internetbanking, social engineering, phishing, safety, authentication.

**Abstrakt**

Kubričan, O. Možnosti zabezpečení proti sociálnímu inženýrství v oblasti elektronického bankovnictví. Bakalářská práce. Brno: Mendelova univerzita v Brně, 2017.
Bakalárska práca sa zaoberá problematikou metód sociálneho inžinierstva vo vzťahu k elektronickému bankovníctvu. Poukazuje na ochranné prvky a obranné mechanizmy internetového bankovníctva a analyzuje ich vo vybraných bankách ČR. Na základe výsledkov analýz navrhuje zvýšenie zabezpečenia internetového bankovníctva.

**Klíčová slova**

Elektronické bankovníctvo, internetové bankovníctvo, sociálne inžinierstvo, phishing, bezpečnosť, autentizácia.

# Obsah

# 1 Úvod a cieľ práce

## 1.1 Úvod

V posledných rokoch rozvoj informačných a komunikačných technológií napreduje rýchlym tempom. Prispôsobiť sa museli aj finančné inštitúcie, ktoré začali ponúkať služby prostredníctvom internetu. Tento nový spôsob komunikácie medzi klientom a bankou bol základom pre vytvorenie elektronického bankovníctva. Hlavným cieľom bolo zjednodušiť či spohodlniť klientom spravovanie svojich financií. Ľudia už nemusia dlhé hodiny vyčkávať v radách v banke kvôli záležitostiam, ktoré si môžu urobiť sami z pohodlia domova. Taktiež banky vďaka tomu znížili svoje náklady. Táto technológia výrazne zrýchlila transakcie medzi ľuďmi či inštitúciami. Avšak paralelne so vznikom elektronického bankovníctva vzniklo aj množstvo rizík a hrozieb. Hackeri nachádzajú spôsoby ako prekonávať zabezpečenie tohto systému s cieľom získať citlivé informácie alebo peniaze. Metódy, ktoré využívajú sú metódy sociálneho inžinierstva. Využívajú dôveru ľudí, pretože práve človek je najslabším článkom v zabezpečení tohto systému.

## 1.2 Cieľ práce

Cieľom tejto bakalárskej práce je zhodnotenie súčasného stavu zabezpečenia internetového bankovníctva vo vybraných finančných inštitúciách Českej republiky a navrhnúť riešenie bankám na zvýšenie bezpečnosti a ochrany voči sociálnemu inžinierstvu.

# 2 Sociálne inžinierstvo

Ak sa opýtate ľudí, či sa stretli alebo vedia, čo znamená termín sociálne inžinierstvo, väčšina ľudí ho nepozná alebo je ich odpoveď nesprávna. Žijeme v dobe, ktorá sa vyznačuje pokročilou technológiou a systémami, ktoré využíva väčšina inštitúcií, domácností, firiem a pod. A keďže každá technológia či systém má svoje slabé stránky, priblížme si pre správne pochopenie význam tohto pojmu.

Čo je vlastne sociálne inžinierstvo?

Pre tento termín sa používa množstvo definícií. Mitnick (2003) definuje sociálne inžinierstvo (sociotechniku) ako ovplyvňovanie a presvedčovanie ľudí s cieľom oklamať ich tak, aby uverili, že sociotechnik je osoba s totožnosťou, ktorú predstiera a ktorú si vytvoril pre potreby manipulácie. Vďaka tomu je schopný využiť ľudí, s ktorými komunikuje, poprípade dodatočné technologické prostriedky k získaniu potrebnej informácie.

Sociotechnika je teda vlastne umenie klamu, manipulácia ľudí za účelom získania určitej informácie. Presvedčenie človeka, že situácia je úplne iná než v skutočnosti. Človek nespozná, že ho skontaktoval podvodník. Na základe umelo vytvorených indícií má pocit, že komunikuje s niekým dôveryhodným. Týmto podvodníkom je človek, ktorý využíva sociotechnické praktiky vo svoj prospech, tzv. sociotechnik. (Kuneš, 2016)

Sociotechnik, nazývaný aj sociálny inžinier, je osoba, ktorá využíva manipuláciu a presvedčovanie s cieľom získať dôverné informácie. Jednoducho povedané, jeho umenie spočíva v presvedčení ľudí, aby robili veci, ktoré by inak pre neznámych ľudí neurobili. (Mitnick, 2003) Najdôležitejšie pre sociotechnika je, aby získal pred útokom čo najviac dostupných informácií, či už je to štruktúra firmy, mená zamestnancov a šéfov firmy, používaný žargón a pod. Pri manipulácii ľudí využíva základné vlastnosti ľudskej povahy (Sociální inženýrství, 2016):

- Autorita - ľudia majú tendenciu podriadiť sa osobe s vyššou funkciou
- Sympatie - sú rôzne spôsoby získania sympatií: spoločné názory, záujmy...
- Vzájomnosť - obeť ľahšie vyhovie, keď pre ňu sociotechnik predtým niečo vyrieši
- Dôslednosť - ľudia sa ľahšie podriadia, ak predtým verejne vyhlásili svoju podporu a angažovanosť v určitej záležitosti
- Spoločenský súhlas - kontaktuje obeť a spýta sa, či má čas vyplniť dotazník, ktorý už všetci pred ním vyplnili
- Vzácna príležitosť - sociotechnik zašle mail k zaregistrovaniu, napr. prvých 500 ľudí získa niečo zdarma

Najznámejšou osobnosťou v oblasti sociálneho inžinierstva je nepochybne hacker **Kevin Mitnick**. Je vlastne osobou, ktorá po prvýkrát definovala pojem sociálne inžinierstvo a paradoxne bol jednou z najhľadanejších osôb v histórii FBI za trestné činy v tejto oblasti. Tvrdil, že nikdy nemal zo svojich činov finančný prospech

a robil to len zo zvedavosti. Trest si odpykával do roku 2000. Po prepustení na slobodu sa z neho stal profesionálny počítačový konzultant a je expertom na bezpečnosť počítačových systémov. Vo svojej knihe Umění klamu popisuje svoje začiatky a v neposlednom rade aj tému obrany proti útokom. (Mitnick, 2003)

## 2.1 Metódy sociálneho inžinierstva

Dnes už existuje veľké množstvo metód sociálneho inžinierstva, a preto si priblížme pár najznámejších a najčastejších metód používaných sociotechnikmi.

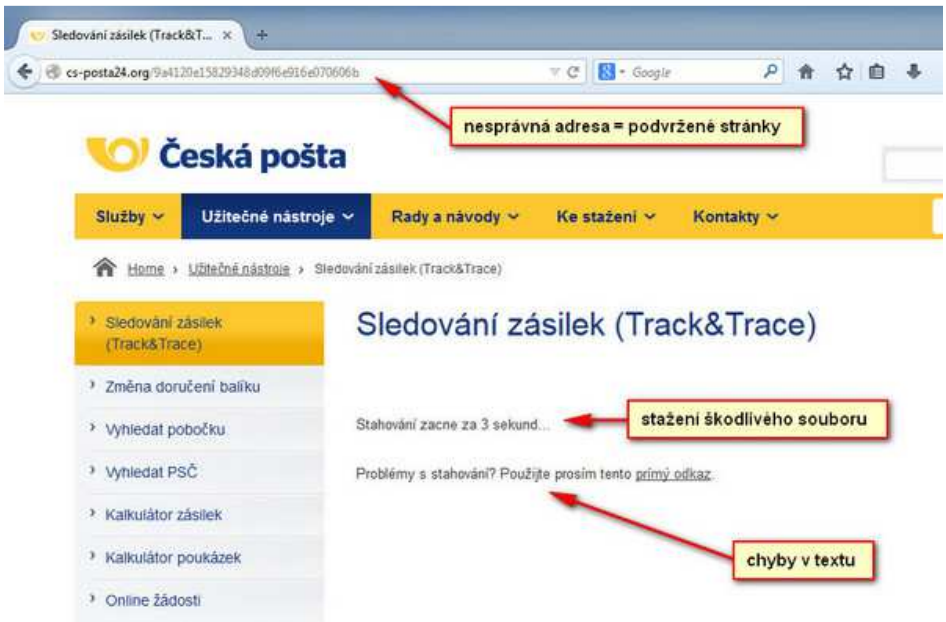
### 2.1.1 Phishing

Slovo phishing je evolúciou slova fishing v dialekte hackerov, ktorý často zamieňali písmeno *f* písmenom *ph*. Slovo vyplýva zo skutočnosti, že užívatelia (phish = ryby), sú lákané napodobenou komunikáciou do pasce alebo na "háčik", prostredníctvom ktorej získavajú dôverné informácie.

Phishing je forma sociálneho inžinierstva, v ktorej sa útočník (phisher), pokúša podvodne získať od oprávneného užívateľa dôverné alebo citlivé osobné údaje prostredníctvom napodobňovania elektronickej komunikácie dôveryhodnej alebo verejnej organizácie automatizovaným spôsobom.

Takáto komunikácia je najčastejšie vykonávaná prostredníctvom e-mailov, ktoré navedú užívateľa na podvodné webové stránky, ktoré zbierajú osobné údaje v dotazníkoch. Najčastejšie údaje zbierané phishermi sú čísla kreditných kariet, heslá a národné identifikačné čísla. (Jakobsson, 2007)

Obr. 1 Príklad phishingovej stránky




Zdroj: servis.eset.cz

Počiatok phishingu sa datuje už od roku 1995, kde to začalo so spoločnosťou America Online (AOL). Objavili sa programy, ktoré automatizovali proces phishingu v súvislosti s údajmi o účte a platobných kartách. Phishery napodobňovali administrátora AOL, obetiam oznamovali, že sa objavil problém s vyúčtovaním a je potreba obnoviť údaje o platobnej karte a prihlasovacích údajoch. Tieto pokusy boli vskutku úspešné, pretože spojenie osobného počítača a pripojenie k internetu bolo novinkou. Útoky phishingu proti finančným inštitúciám bol po prvýkrát zaznamenaný v júli 2003 (E-loan, Citibank). (James, 2007)

James (2007) vo svojej publikácii poukazuje na 3 najbežnejšie a najobľúbenejšie metódy útoky používané phishermi:

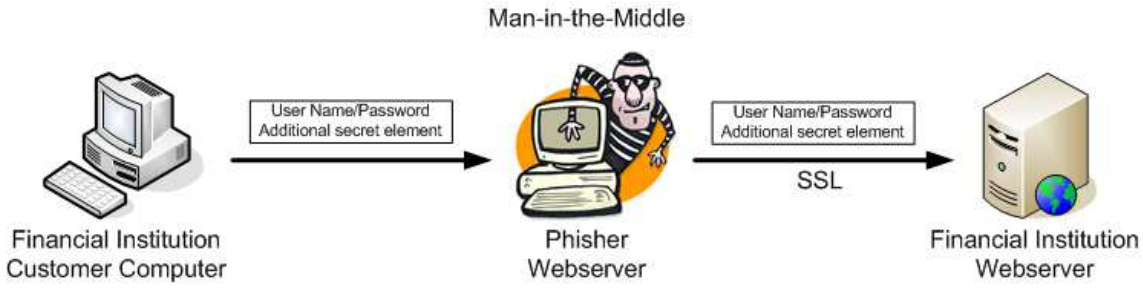
- **falošná identita** - najobľúbenejšia a najjednoduchšia metóda podvodu. Vyžaduje vybudovanie falošnej stránky, ku ktorej je príjemca lákaný. Takáto stránka obsahuje grafický materiál zo skutočnej webovej stránky a môže byť dokonca so skutočnou stránkou prepojená.
- **presmerovanie** - najčastejšie sa objavuje v súvislosti so stránkami Amazon a PayPal a predstavuje zvyčajne e-mail, ktorý obsahuje grafiku skutočnej stránky a prihlasovacie nástroje v nej. Ak sa obeť prihlási prostredníctvom presmerovacieho odkazu v e-maile, užívateľské dáta sú odoslané na nepriateľský server, zatiaľ čo užívateľ je presmerovaný na skutočnú stránku a vo veľa prípadoch ich systém prihlási na skutočnú stránku pomocou techniky Prostredník (Man-in-the-middle - MITM). Obeť zvyčajne ani nepostrehne, že bola vystavená phishingu vďaka plynulosti útoku presmerovania.
- **vyskakovacie okná** - ide v zásade o odkaz v rámci e-mailovej správy, ktorý viedol k nepriateľskému vyskakovaciemu oknu. Za vyskakovacím oknom sa ale skrýval skutočný cieľ, a to, že sa útočníci snažili ukradnúť dáta z počítača. Ide o pomerne elegantný a kreatívny trik, no dnes už pomerne neúčinný vďaka blokovaču vyskakovacích okien, ktorý majú prehliadače nainštalované už v základe.

Typy phishingových útokov podľa Jacobssena (2007):

- Klamlivý phishing - sú zasielané klamlivé e-maily, ktoré vyzývajú "vykonať určitú akciu" a požadujú kliknutie na priložený link.
- Phishing založený na Malwarey - je všeobecne typ phishingu, ktorý zahŕňa beh zákerného softwaru na užívateľovom zariadení. Má mnoho podôb. Phishery napríklad nabádajú otvoriť e-mail alebo stiahnuť súbor zo stránky. Ak to užívateľ vykoná, stiahne software, ktorý môže obsahovať malware, ktorý odcudzí osobné informácie.
- Phishing založený na DNS ("Pharming") - odkazuje všeobecne na formu phishingu, ktorá narúša integritu procesu vyhľadávania pre doménové meno.
- Obsah zavádzajúci phishing - odkazuje na vloženie škodlivého obsahu na legitímne stránky. Tento obsah môže presmerovávať na iné stránky, inštalovať malware na užívateľov počítač alebo vložiť rámec obsahu, ktorý presmeruje dáta na phishingový server.

- Man-in-the-middle phishing - v tomto type útoku je pozícia phishera medzi užívateľom a legitímnou stránkou. Správy zasielané stránkam sú namiesto toho posúvané phisherom, ktorý zachytia cenné informácie a následne posunú správy legitímnym stránkam a spätné odozvy stránok spať k užívateľovi.
- phishing zameraný na vyhľadávače - vytvorenie stránky pre falošné produkty, indexovanie týchto stránok vyhľadávačmi, a následné vyčkávanie, kým užívatelia vložia ich súkromné informácie ako proces pri objednávke, prihlásení alebo platení.

Obr. 2 MITM phishing

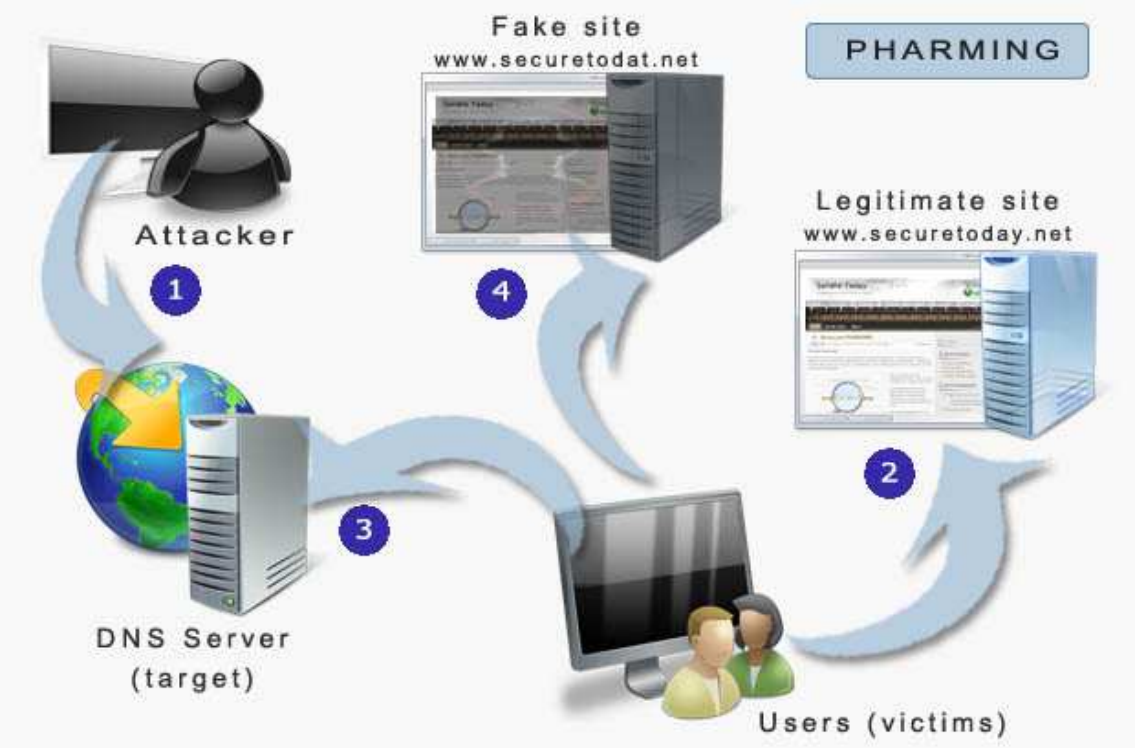



Zdroj: ebankingabersicher.ch

### 2.1.2 Pharming

Pharming je ďalšia z metód sociálneho inžinierstva. Je sofistikovanejšou a omnoho nebezpečnejšou formou phishingu. Ide taktiež o podvodnú techniku získavania citlivých údajov užívateľa. Princíp spočíva v napadnutí DNS serveru (Domain Name System) a prepísanie IP adresy. DNS server prekladá doménové meno na IP adresu (napr. po zadaní www.seznam.cz preloží DNS server na IP adresu 77.75.77.39). Užívateľ zadá správnu adresu, ale napadnutý DNS server nepreloží na správnu IP adresu, no na webové stránky s IP adresou útočníka - väčšinou na nerozoznanie od originálu. (Kohout, 2016) Útočník tak môže získať napr. prihlasovacie údaje zákazníka. V horšom prípade môžu slúžiť aj ako prostredník medzi užívateľom a skutočným systémom internetového bankovníctva - prostredník tak môže korektne preposielať iba autorizačné údaje, zatiaľ čo informácie vzťahujúce sa k samotnej transakcii (číslo účtu, veľkosť prevedenej čiastky) už môžu byť zmanipulované. (Matyáš, 2008)

Obr. 3 Schéma pharmingu




Zdroj: securetoday.net

### 2.1.3 Hoax

Hoax môžeme zaradiť medzi ďalšie metódy sociotechniky. Pochádza z anglického slova, ktoré v preklade znamená falošná správa, výmysel, kanadský žart..

V elektronickej komunikácii sa jedná o poplašnú správu, ktorá napr. varuje pred neexistujúcim nebezpečím, počítačovým vírusom, prosí o pomoc alebo chce iba pobaviť. Často je v správe dôraz na ďalšie preposielanie priateľom a známym - reťazová správa. Väčšinou práve podľa tejto žiadosti sa dá hoax identifikovať. (Kohout, 2016)

### 2.1.4 Baiting

Baiting môžeme porovnať k útoku pomocou Trojského koňa v reálnom svete. Namiesto dreveného koňa je použité médium (CD,DVD,USB..) s programom k "dobytiu" počítača obeti.

Útočník nechá médium s lákavým nápisom alebo dokumentom na mieste, kde ho obeť najpravdepodobnejšie nájde. Potom nechá už pracovať zvedavosť. Skôr či neskôr sa nájde niekto, kto ho vloží do svojho počítača. Tak dôjde k aktivácii škodlivého kódu, s jeho pomocou získa útočník prístup k počítaču alebo dokonca celej firemnej počítačovej sieti. (Kuneš, 2016)

### 2.1.5 SCAM419

SCAM419 je druh podvodu, ktorý je známy v Českej republike skôr pod názvom "Nigérijské dopisy". Tento druh podvodu existoval už vo forme klasických listov a s rozvojom e-mailovej komunikácie umožnil osloviť milióny užívateľov vo veľmi krátkom období a za nízke náklady.

Princíp spočíva v tom, že vás osloví neznámy človek, a povie vám, že zdedil, získal alebo dokonca spravuje niečí majetok vo výške niekoľko miliónov dolárov a potrebuje vašu pomoc pri jeho prevode zo krajiny. Samozrejme je za túto pomoc sľúbená odmena vo výške niekoľko desiatok percent z celkovej sumy. Obeť však musí neustále platiť nečakané administratívne poplatky a prevod majetku sa stále oddialuje.

S rozvojom internetových služieb podvodníci vymýšľajú čoraz dôveryhodnejšie praktiky. Niekedy sú to falošné ponuky neexistujúcich produktov, podvodné inzeráty na predaj lacných automobilov alebo prenájom bytov. Taktiež to môžu byť nešťastia iných, katastrofy a pod. Veľmi často bývajú podvody prepracované do najmenších detailov, ako sú napríklad profesionálne vytvorené stránky neexistujúcich spoločností a bankových inštitúcií. Obetiam bývajú zasielané falošné dokumenty a certifikáty. K získaniu peňazí a zameteniu stôp slúžia tzv. biele kone. (*Co je to SCAM 419, 2016*)

### 2.1.6 Pretexting

Pretexting je definovaný ako praktika prezentovať seba samého za niekoho iného za účelom získania osobných informácií. Je to viac, než len vytvoriť lož. V niektorých prípadoch to môže byť až vytvorenie novej identity a následne ju využiť k manipulácii pre prijímanie informácií.

Pretexting možno tiež využívať na vydávanie sa za človeka v určitých pracovných miestach, ktoré nikdy predtým nerobil. Sociálny inžinier využíva množstvo zámienok, ktoré získava výskumom, aby presvedčil obeť k získaniu potrebných informácií. Najdôležitejším aspektom k získaniu informácií je dôvera. Solídna zámienka je nevyhnutnou súčasťou k získaniu dôvery. Ak má alias, príbeh alebo identita diery alebo nedostatok dôveryhodnosti, obeť sa s najväčšou pravdepodobnosťou nedá nachytať. (The Social Engineering Framework: Pretexting*, 2016*)

## 2.2 Reálne a možné dopady metód SI

V histórii počítačov a internetu sa objavilo množstvo ničivých vírusov, ktoré ovplyvnili vnímanie bezpečnosti. V nasledujúcom texte som na priblíženie vybral 5 vírusov z najničivejších vírusov histórie.

V roku 1999 vírus Melissa (typ: malicious) v podobe e-mailu zasiahol odhadom 20% počítačov na celom svete. Predmet znel "dôležité" a po otvorení prílohy sa na zariadeniach začali nekontrolovateľne otvárať webové stránky s obsahom pre dospelých. Vírus našťastie nebol nijak škodlivý a jeho šírenie sa podarilo zastaviť. Tvorca vírusu bol po týždni chytený, dostal 20 mesiacov väzenia a 5000 dolárov pokuty. (Napáchali miliónové škody: Toto je 5 najničivejších vírusov histórie, 2016)

Vírus I LOVE YOU (máj 2000) bol snáď najnebezpečnejší počítačový vírus v podobe červa. Bol sa schopný samostatne replikovať. Šíril sa prostredníctvom e-mailu a napádal počítače po celom svete. Bol to milostný list od tajného ctiteľa, čo ho robilo ešte lákavejším. Práve príloha tohto e-mailu po otvorení spôsobila, že sa e-mail sám rozoslal prvým 50tim kontaktom v adresári počítača. Vírus spôsobil škodu približne 10 miliárd dolárov a napadol skoro 10 % počítačov na celom svete pripojených k internetu. (5 most dangerous computer viruses of all time, *2017)*

V roku 2003 vírus známy ako Sapphire (typ: červ) napadol 75 tisíc užívateľov pomocou DoS (Denial of Service) útoku. Zameral sa na zraniteľné miesto, ktoré našiel v Microsoft SQL a rýchlo sa rozšíril. DoS útoky preťažujú siete nezmyselnými požiadavkami až nakoniec sieť spadne. (The Most Destructive Malware of All Time, *2017).* Tento vírus spôsobil globálny výpadok internetu. Celkovo bolo zasiahnutých niekoľko miliónov serverov. Tie nemohli spracovať toľko požiadaviek a internet sa stal prakticky nefunkčným. Celková škoda sa odhaduje na vyše 1,2 mld dolárov. V Severnej Kórei bol napr. nefunkčný internet, v Portugalsku sa cca 300tisíc ľudí nemohlo naň pripojiť, nefungovali bankomaty v krajinách, v Seatlli nefungovala tiesňová linka. Páchatelia neboli dostihnutí. (Napáchali miliónové škody: Toto je 5 najničivejších vírusov histórie, 2016)

V roku 2004 sa objavil červ "My doom" a stal sa najrýchlejšie šíriacim sa e-mail červom od vzniku I LOVE YOU. Šíril sa sám tak, že vyzeral ako chyba prenosu e-mailu a obsahoval prílohu samého seba. Otváral zadné dvierka umožňujúce vzdialený prístup a spúšťal DoS útoky na spoločnosť SCO Group. Verilo sa, že bol vytvorený práve s cieľom rozvrátiť SCO kvôli sporu o vlastníctvo nejakého linuxového kódu. Odhadované škoda je 38,5 miliardy dolárov. Autor je neznámy, avšak predpokladá sa, že bol platený za jeho vytvorenie, pretože obsahoval správu: Nič osobné, robím si len svoju prácu, je mi to ľúto. (10 Most Destructive Computer Viruses*, 2017)*

V roku 2007 sa vírus Mebroot dostal do zariadení prostredníctvom odkazu na webovú stránku a taktiež pracoval v tichosti. Dochádzalo ku krádežiam citlivých informácií. Vírus kontroloval aktivitu užívateľa a odchytával zadané informácie.

Boli ukradnuté informácie o približne 500tisíc bankových účtoch. Tvorcov nechytili. (Napáchali miliónové škody: Toto je 5 najničivejších vírusov histórie, 2016)

Pozrime sa aj na prítomnosť. V roku 2015 boli zaznamenané tieto kybernetické útoky (Kyberzločinci útočia so zámerom znásobiť svoj zisk, 2016):

- malvér Carbanak bol najväčším útokom, ktorý zasiahol viac ako 100 bankových domov vo vyše 30 krajinách a útočníkom sa podarilo ukradnúť viac ako jednu miliardu dolárov
- US Office of Personnel Mangement v USA zaznamenal krádež informácií o bezpečnostných previerkach, odtlačkov prstov, detailné osobné informácie o miliónoch federálnych pracovníkov
- v Austrálii a UK unikli dáta vo veľkých retailových firmách, ukradnuté boli aj mimo iné informácie o kreditných kartách; taktiež poskytovatelia internetových služieb zaznamenali únik dát, pričom náhrada škody sa ráta vo výške 30 mil libier

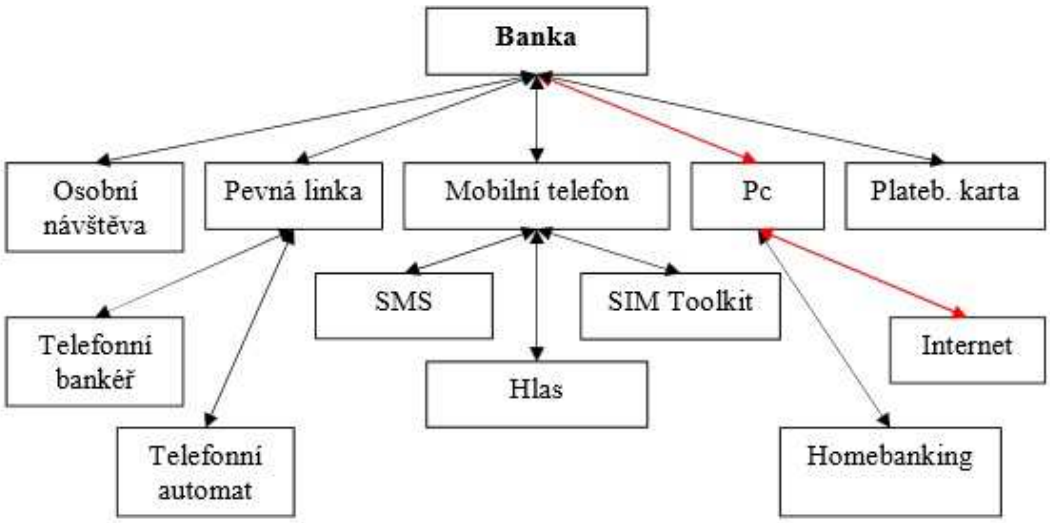
Spoločnosť Kaspersky Lab na základe analýz publikovala predpovede hrozieb kybernetických útokov na rok 2017 (Kaspersky Lab: Čo nás čaká v roku 2017? Útoky, ktoré nezanechajú stopy…, 2016):

- pribudnú aktivity kyberzločincov, ktorí kradnú dáta s dobrými úmyslami, resp. v mene vyššieho dobra
- špionáž prenikne do mobilov
- nárast kybernetických sabotáží
- rastie záujem o nelegálne preniknutie do platobných systémov a ich zneužitie na kriminálne aktivity
- komodifikácia finančných útokov
- rast informačnej vojny

# 3 Elektronické bankovníctvo

Prvým impulzom pre vznik elektronického bankovníctva bolo obmedzenie komunikácie bánk s klientom na úrovni osobnej komunikácii, väčšinou prostredníctvom bankových pobočiek alebo ich zástupcami. Avšak vďaka rýchlemu technologickému rastu a pokroku od polovice 20. storočia sa situácia mení. Do popredia sa dostala veľká škála komunikačných prostriedkov, ktoré dnes už každý z nás pozná a využíva. Hovorím predovšetkým o internete a mobilných telefónoch. Dôvody, ktoré podnecujú tieto rýchle zmeny a vývoj je zníženie nákladov a zvýhodnenie služieb pre klientov. (Přádka, 2000)
Možnosti, ktoré má banka k dispozícii na komunikovanie s klientom je v dnešnej dobe veľa a banka si vyberá najvhodnejšie kombinácie z komunikačných prostriedkov podľa svojho uváženia.

Obr. 4 Možnosti komunikácie klienta a banky




Zdroj: Přádka (2000)

## 3.1 Platobné karty

Platobné karty sú moderným nástrojom bezhotovostného platobného styku, ktoré sa využívajú hlavne k výberu hotovosti a umožňujú uhrádzať spotrebné výdaje. Platba prostredníctvom kariet je najrozšírenejším spôsobom platieb. Ich vzhľad, fyzikálne vlastnosti a obsahové náležitosti sú štandardizované v medzinárodnom meradle. (Máče, 2006)

Tab. 1 Náležitosti platobnej karty

| | |
|---|---|
| Označenie vydavateľa | Názov a logo príslušnej banky |
| Číslo platobnej karty | 16-19 numerických znakov (2 znaky - druh karty, 5 znakov - identifikácia vydávajúcej banky, ostatné - identifikácia držiteľa karty) |
| Časť čísla BIN | 4 znaky - čísla BIN (Bank Identification Number), tj. číslo pridelené kartovou asociáciou danej banke |
| Platnosť platobnej karty | Udanie začiatku a konca platnosti alebo iba konca platnosti karty |
| Meno držiteľa karty | Max. 27 znakov, u služobných kariet aj názov podniku |
| Podpisový prúžok | Vzor podpisu držiteľa karty na zadnej strane karty |
| Záznam dát | |

Zdroj: Máče (2006)

### 3.1.1 Druhy platobných kariet

Platobné karty môžeme deliť podľa rôznych hľadísk (Matyáš, 2008):

1. podľa spôsobu zúčtovania
   - debetné karty
   - kreditné karty
   - charge karty
   - nákupné úverové karty
2. podľa spôsobu prevedenia
   - embosované
   - elektronické
3. podľa vydavateľskej asociácie
   - 3.1. banky a bankové asociácie
     VISA
     MasterCard
     Maestro
   - 3.2. finančné spoločnosti
     Japan Credit Bureau
     American Express
     Dinners Club
   - 3.3. ostatné

letecké spoločnosti
obchodné domy
atd.

4. podľa použitej technológie
   - karty s magnetickým prúžkom
   - čipové karty
   - hybridné karty

### 3.1.2 Výhody a nevýhody platobných kariet

Za výhody platobných kariet pre klienta môžeme považovať:

- rýchly a jednoduchý prístup k finančným prostriedkom
- vyššia bezpečnosť v porovnaní s hotovosťou
- úspora času a poplatkov spojených so zmenou hotovosti
- tuzemské alebo medzinárodné použitie
- výhodnejší kurz pre zúčtovanie platieb
- vysoká osobná prestíž
- doplnkové služby pre držiteľa karty
- núdzové služby pri strate karty (Schlossberger, 2005)

Na druhej strane, nevýhody platobných kariet:

- poplatky spojené s vystavením karty
- poplatky spojené s používaním karty
- riziko zneužitia karty v prípade straty (Máče, 2006)

### 3.1.3 Platba platobnou kartou

Dnes už málo využívaný spôsob platby v obchodných sieťach je platba pomocou zariadenia, ktorý sa nazýva **imprinter**.

Imprinter sa využíva v obchodoch, kde akceptujú platobné karty avšak nevyužívajú elektronický platobný terminál. Toto zariadenie je dodávané bankou obchodníkovi zároveň s podpisom zmluvy o akceptácii platobných kariet. Imprinter akceptuje iba embosované karty, čo je veľký handicap pre dané obchodné miesto.

Toto zariadenie funguje týmto spôsobom:
Pri platení sa vloží karta do imprinteru, na ktorom je pripravený identifikačný štítok obchodníka a naň sa položí predajný doklad (účtenka). Následne sa prejde rukoväťou so zabudovanými prítlačnými valčekmi vpravo a späť. Údaje z karty a zo štítku sa vytlačia na účtenku. Po doplnení sumy a podpisu držiteľa, obchodník dá vrchný diel držiteľovi karty. Ten má originál účtenky, 1. kópia je pre obchodníka

a 2. kópiu zasiela svojej banke, s ktorou má zmluvu o akceptácii platobných kariet. Spracovateľská banka potom obdŕžané účtenky typuje do vlastného systému, ktoré sú následne predané na zúčtovanie. (Schlossberger, 2005)

Jedným z najviac rozšírených a používaných elektronických zariadení, čo sa týka obchodných sietí, v oblasti platobných kariet je **platobný terminál** (EFT POS - Electronic Funds Transfer at Point Of Sale). Tieto terminály slúžia k vykonávaniu bezhotovostných platieb prostredníctvom platobných kariet.

Skladá sa zo štyroch základných častí:

- základná jednotka - obsahuje zobrazovaciu jednotku (displej), numerickú klávesnicu, čítačku magnetických (poprípade čipových) kariet, procesorovú jednotku, pamäťové bloky a ďalšie moduly
- tlačiareň - zaisťuje tlač klientskych potvrdeniek, výsledok denných uzávierok...
- PIN PAD - zariadenie určené predovšetkým k zadávaniu PIN. Jeho súčasťou je väčšinou aj čítačka na čipové karty, numerická klávesnica, kryptovací procesor zaisťujúci kódovanie zadaného PIN. PIN môže byť zadávaný u niektorých terminálov priamo na klávesnici v základnom module (prenosný terminál).
- komunikačný modul a napájací zdroj - komunikačný modul obsahuje modem, ktorý zaisťuje prostredníctvom stanoveného komunikačného protokolu prenos dát - správ medzi platobným terminálom a autorizačným centrom (Schlossberger, 2005)

S rozmachom siete Internet, ktorá je v súčasnej dobe celosvetovo využívaná, sa začali realizovať obchody vo virtuálnom prostredí. Účastníci obchodu majú zníženú možnosť overenia vzájomnej identity, ako to bolo pri realizácii platby platobnými kartami medzi obchodnými partnermi v kamenných predajniach. Dodatočné overovanie je možné len s použitím iného komunikačného kanálu, a tento proces sa môže v neposlednom rade predražiť.

Pri platbe platobnou kartou prostredníctvom internetovej siete existuje riziko zneužitia súkromných informácií. Rôzne nekalé praktiky sú dnes smutnou realitou a je nutné s nimi počítať. S rastúcim objemom transakcií na Internete prostredníctvom platobných kariet sa najväčšie medzinárodné asociácie snažia tieto situácie systémovo riešiť.

V polovici 90. rokov bol asociáciami MasterCard a VISA predstavený systém **SET** (Secure Electronic Transaction). Tento systém predpokladal k zaisteniu funkčnosti štyri dôležité komponenty:

- osobného správcu platobnej karty (tzv. peňaženku - e-wallet),
- digitálny certifikát,
- digitálnu pokladňu u obchodníka (merchant server),

- bankovú "platobnú bránu" (payment gateway).

Tento systém však vinou svojej technologickej náročnosti a komplikovanosti (ako pre držiteľov karty, tak pre obchodníkov) a značnej nákladnosti na prevádzku sa príliš nerozšíril. Dnes už sa prakticky nevyužíva. (Schlossberger, 2005)

Neskôr asociácie ponúkli vydavateľským bankám možnosť vydávania tzv. **virtuálnych kariet**. Nejedná sa o kartu v pravom slova zmysle. Ide o číslo karty, jej platnosť a kód CVV alebo CVC. Všetky tieto dáta sú iba v papierovej forme. Údaje potrebné k uskutočneniu transakcií sú vytlačené do špeciálnych obálok. Má nastavený nižší čerpací limit ako klasická platobná karta. Zaisťuje pomerne vysokú bezpečnosť. Virtuálne karty sa nedajú použiť k iným typom transakcií ako k transakciám v sieti Internet.

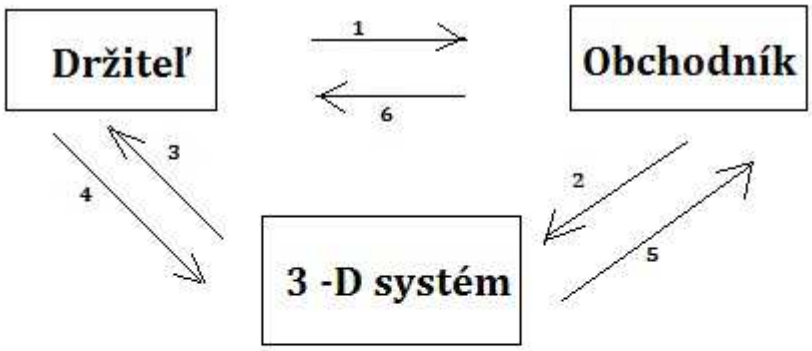
V roku 2001 zaviedol MasterCard novú metódu pre uskutočňovanie transakcií v prostredí Internet "**MasterCard SecureCode**" a VISA svoj systém "**Verified by VISA**".

Obidva systémy sú založené na tom, že pri voľbe použitia platobnej karty držiteľom v sieti Internet je automaticky vyzvaný k zadaniu osobného tajného hesla, nie PIN karty. Heslo držiteľ získava na stránkach svojej banky v procese tzv. Registrácie. Toto heslo je mimo kontrolu obchodného miesta. Obdrží iba informácie, či je transakciu možné zrealizovať.

Systém pracuje s modelom **3D Secure** - Three Domain Secure:

- 1. doména - *vydavateľ karty* - metóda overenia držiteľa je v kompetencii a zodpovednosti vydavateľa karty
- 2. doména - *platobný systém* - protokol, ktorý spojuje doménu vydavateľa karty a obchodníka, sa uskutočňuje prostredníctvom UCAF (Universal Cardholder Authentication Field) alebo 3DSET
- 3. doména - *obchodník* - metóda overenia obchodníka je v kompetencii a zodpovednosti banky obchodníka (Acquirera) (Schlossberger, 2005)

Obr. 5 Schéma vykonania transakcie




1. Držiteľ zvolil platbu kartou
2. Obchodník žiada 3D systém o verifikáciu držiteľa
3. 3D systém žiada držiteľa o zadanie dát ohľadom platobnej karty
4. Držiteľa zadá požadované dáta v kryptovanej podobe
5. 3D systém overí kartu povolí/zamietne transakciu
6. Obchodník informuje držiteľa o výsledku

Zdroj: Schlossberger (2005)

### 3.1.4 Autorizácia bankových operácii

**Podpis držiteľa karty**

Pri platbe kartou sa ešte stále môžeme stretnúť s autorizáciou pomocou podpisu. Aj keď je táto metóda na ústupe, ešte stále úplne nezanikla. Prežívať bude vďaka imprintérom.

Plus tejto metódy je rýchla a jednoduchá platba.

Mínusom je nemožnosť dôveryhodného skontrolovania podpisu zo strany obchodníka, podpis sa dá ľahko naučiť.

**Autorizácia pomocou PINu**

Autorizácia pomocou PINu je prevládajúca metóda autorizácie. Cieľom bánk by malo byť dosiahnutie 100% transakcií týmto spôsobom.

Výhodou je jednoznačné rozhodnutie o správnosti či nesprávnosti autorizácie.

Nevýhodou sú zlé typy terminálov a ergonomika pracoviska pokladničného miesta.

**Autorizácia platieb pomocou elektronického podpisu na báze PKI**

Obchodník aj zákazník majú svoj účet v KB. Pri platení sa vytvorí elektronický prevodný príkaz, ktorý sa štandardným spôsobom podpíše. Je odoslaný do banky, kde sa overí likvidita účtu a vykoná sa verifikácia transakcie. Ak je všetko v poriadku, banka vygeneruje potvrdenie platby na platobný terminál.

Dôvodom pre zavedenie tohto systému bolo zvýšenie úrovne zabezpečenia platieb a v neposlednom rade aj zníženie poplatkov pre obchodníka účtovaných medzinárodnými združeniami za operácie so štandardnými platobnými kartami.

**Autorizácia pomocou SMS jednorazového hesla**

Metóda predpokladá, že klient je držiteľom mobilného telefónu. Tento spôsob je vhodný pre rôzne typy elektronického bankovníctva obsluhovaného z PC a nie pre platenie bežnou platobnou kartou na POS terminály v obchodnej sieti.

**Autorizácia pomocou biometriky**

Tento spôsob je málo rozšírený a v porovnaní s inými produktmi pre svoju zložitosť a náročnosť na vybudovanie databáze s biometrickými prvkami taktiež veľmi drahý. (Matyáš, 2008)

Platobné karty sú v elektronickom bankovníctve kapitola sama o sebe. Elektronické bankovníctvo (nazývané aj priame) umožňuje klientovi banky vykonávať bankové operácie so svojím účtom, či sledovať pohyby na účte pomocou telekomunikačnej či dátovej siete pohodlne z domova či kancelárie. Cieľom banky je ponúknuť pre klienta pohodlnejší spôsob obsluhy účtu a hlavne znížiť náklady na prepážkovú prevádzku.

Produkty pre elektronické bankovníctvo sa líšia u jednotlivých bánk napríklad rôznym stupňom zabezpečenia. Sú to napríklad:

- Internet banking,
- Home banking,
- TV banking,
- WAP banking,
- GSM banking a iné. (Matyáš, 2008)

## 3.2 Internet banking

Internet banking umožňuje komunikáciu klienta banky prostredníctvom počítača pripojeného na internetovú sieť. Klient sa prihlasuje do systému banky a po overení oprávnenosti k vykonávaniu požadovaných úkonov prostredníctvom elektronického kľúča alebo cez elektronické podpisy a digitálne certifikáty, môže priamo zadávať pokyny banke. (Dvořák, 2005)

Na disponovanie účtom používa špeciálnu internetovú stránku banky. Vďaka internetovému bankovníctvu majú klienti možnosť spravovať svoje financie 24 hodín denne a to kdekoľvek, kde je kvalitné a bezpečné internetové pripojenie. Môže mať aj pasívnu verziu, ktorá umožňuje iba nahliadať na stav produktu. (*Co je internetové bankovnictví, 2016*).

Nakoľko internetové prostredie nie je celkom bezpečné, banky sa snažia zaistiť maximálnu ochranu prenášaných dát pri komunikácii so svojimi klientmi. Pri tom používajú tieto prvky zabezpečenia:

- autentizačný kalkulátor

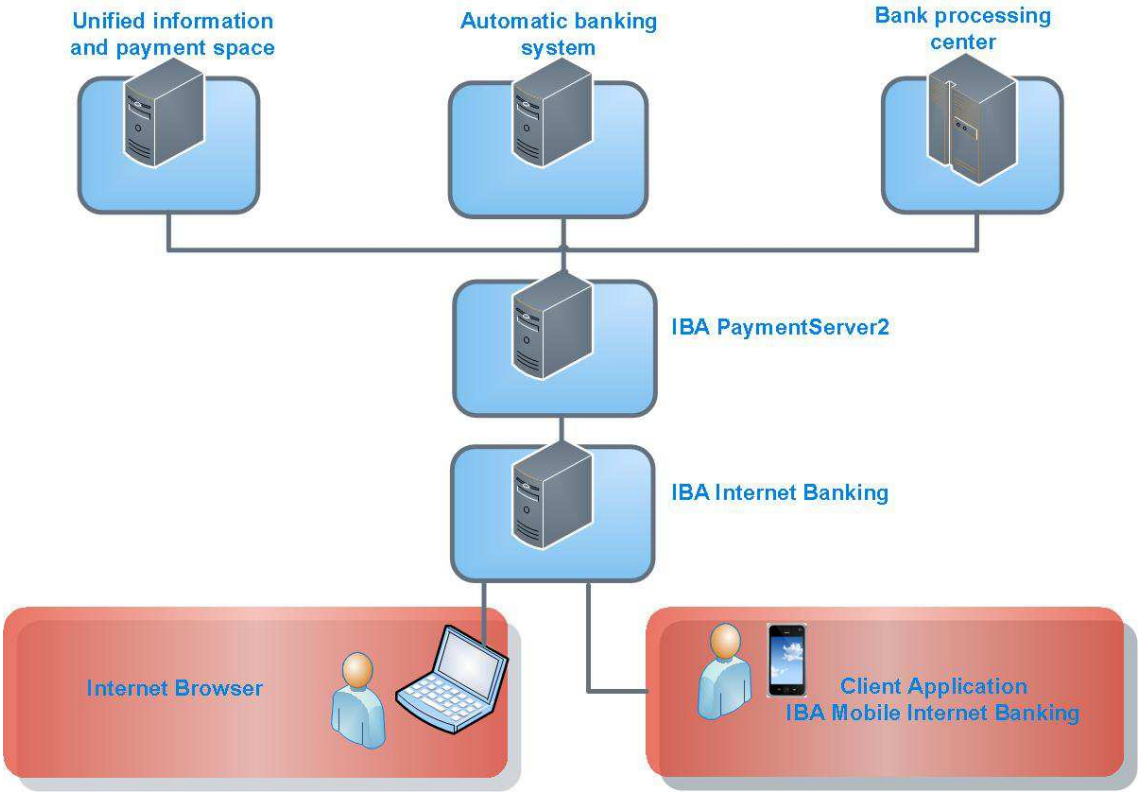
- autentizačná SMS poslaná ako bežná SMS - banka zašle na registrovaný mobilný telefón autentizačný kód prostredníctvom SMS, ten sa prepíše ručne do určeného pola v internetovom bankovníctve.
- Autentizačná SMS zaslaná ako šifrovaná SMS SIM-TOOLKIT - banka zašle na registrovaný mobilný telefón autentizačný kód prostredníctvom šifrovanej SMS, ten sa ručne prepíše dom určeného pola v internetovom bankovníctve. Pre prečítanie šifrovanej SMS je potrebné mať SIM kartu podporujúcu bankové aplikácie, SIM vyžaduje zadanie tzv. BPIN.
- podpisový certifikát - banková operácia sa potvrdí podpisovým certifikátom. To je heslom chránený šifrovaný súbor, ktorý je uložený na disku v počítači, alebo na prenosnom disku (USB, CD, DVD...)
- podpisový certifikát uložený na čipovej alebo optickej karte - banková operácia sa potvrdí podpisovým certifikátom na čipovej alebo optickej karte. K potvrdeniu potrebujete špeciálnu čipovú kartu a čítačku čipových kariet. Tá je vo variante buď pre notebooky alebo pre stolné počítače.
- podpisový certifikát uložený na USB tokene - banková operácia sa potvrdí podpisovým certifikátom na špeciálnom USB tokene. K potvrdeniu operácie potrebujete špeciálny USB token, ktorý vo svojom úložisku bezpečne uchová podpisový certifikát. Vydanie tokena je spoplatnené.
- TAN kódy - banka vám zašle poštou zoznam tzv. TAN kódov. Tento kód tvorí unikátne, spravidla 6-miestne číslo, ktorým sa potvrdí banková operácia. TAN kód je po potvrdení neplatný a pri ďalšej operácii je potrebné použiť nový.
- užívateľské meno a heslo - po prihlásení do internetového bankovníctva možno vykonávať bankové operácie bez nutnosti ďalšieho potvrdzovania inými bezpečnostnými prvkami. (*Internetové bankovnictví, 2016*)

Prvá časť systému internetového bankovníctva obsahuje funkcie dostupné klientom a sadu procesov, ktoré podporujú vnútorné a vonkajšie interakcie pomocou systému.

IBA Internet Banking zabezpečuje výmenu informácií prostredníctvom medzinárodného finančného protokolu IFX (Interactive Financial Exchange s 1.7) s platobným systémom PS2, ktorý je v spolupráci s nasledujúcimi externými systémami:

- jednotný informačný a platobný priestor, ktorý riadi interakcie pomocou protokolu Raschet (bieloruský platobný systém)
- spracovateľské centrum banky
- automatizovaný bankový systém

Obr. 6 Schéma Internet Banking




Zdroj: IBA Internet Banking System (2016)

## 3.3 Home banking

Home banking je založený na prepojení osobného počítača klienta, na ktorom je nainštalovaný špeciálny software, s počítačom banky. Typickým znakom je to, že klient pri tejto forme sťahuje určité dáta z databázy banky a sám ich spracováva. Bezpečnosť je založená na fyzickej ochrane prístupu k počítaču pripojenému k banke a prostredníctvom hesiel a šifrovania odoslaných správ. (Dvořák, 2005)

Bol obľúbený do konca 90 rokov, keď ešte internetové bankovníctvo nebolo tak rozšírené a nebola v neho ešte taká dôvera. Preferujú ho klienti, ktorí nechcú alebo nemôžu používať prístup cez internet. Pre potvrdenie bankovej operácie používa podpisový certifikát. Dáta sú prenášané buď využitím internetu cez šifrované SSL spojenie, alebo priamym spojením s modemom banky.

## 3.4 GSM banking

GSM banking je založený na komunikácii s bankou prostredníctvom mobilných telefónov, ktorá môže byť založená buď na báze kľúčových slov v SMS správe, prostredníctvom technológie SIM Toolkit alebo aj s využitím technológie WAP. Bezpečnosť je zaisťovaná systémom hesiel a šifrovaním zasielaných správ. (Dvořák, 2005)

Základným prvkom je banková aplikácia uložená na karte, ktorá sprostredkováva cez intuitívne rozhranie komunikáciu medzi bankou a klientom. Prístup k správam banky či zaobchádzanie s účtom je zabezpečené prístupovým bankovým PINom. Komunikácia je šifrovaná.

# 4 Možnosti zabezpečenia internetového bankovníctva

V dnešnej dobe je internet banking základnou službou každej banky. A ako žiaden systém nie je dokonalý, musia dbať banky na to, aby čo najviac znížili možnosť napadnutia a prelomenia bezpečnosti tohto systému.
Bezpečnosť internetového bankovníctva zahrňuje tri aspekty:

- identifikáciu banky
- identifikáciu klienta
- zabezpečenie prenosu dát

Identita banky je overovaná certifikátom, ktorý vydáva nezávislá inštitúcia (najčastejšie VeriSign). Klient má tak istotu, že stránky, prostredníctvom ktorých komunikuje s bankou patria skutočne jej. Zabezpečenie zo strany banky je teda dostatočne zabezpečené a k prelomeniu ochrany dochádza najčastejšie v dôsledku chýb a neopatrnosti klientov, ktoré útočník nemá problém využiť vo svoj prospech.

Prenos dát je v bankách riešený vysokoúrovňovým šifrovaním a dá sa považovať za dostatočne bezpečný. (*Jak je to s bezpečností internetového bankovnictví?, 2016)*

V tejto kapitole sa budeme venovať teda hlavne zabezpečeniu identifikácie klienta banky.

## 4.1 Identifikácia a autentizácia klienta

Identifikácia a autentizácia sú nutné k zaisteniu priradenia užívateľovi zodpovedajúce bezpečnostné atribúty (napr. jeho identita, príslušnosť ku skupinám užívateľov, role, bezpečnostná úroveň integrity).

Jednoznačná identifikácia autorizovaných užívateľov a správne priradenie bezpečnostných atribútov užívateľom a subjektom je z hľadiska presadenia bezpečnostných politík kritická. Tieto funkcie sa zaoberajú určením a verifikáciou identity jednotlivých užívateľov, určením ich oprávneniam k interakcii s účtom a správnym priradením bezpečnostných atribútov každému autorizovanému užívateľovi. (Hanaček, 2000)

V podstate existujú 3 základné metódy autentizácie užívateľov, ktoré sa líšia typom prostriedkov používaných pri autentizácii. Tieto metódy môžu byť založené na niečom, čo:

- daný užívateľ pozná - tajná informácia, napr. PIN, heslo alebo prístupová fráza
- daný užívateľ vlastní - predmet, token napr. platobná karta
- daný užívateľ je - biometrická informácia napr. odtlačok prstu

Všetky tieto metódy majú svoje výhody aj nevýhody. Aby sa čo najviac eliminovali nevýhody týchto metód, volí sa ich vzájomná kombinácia. Použitím dvoch metód

z týchto troch uvedených skupín sa označuje ako dvojfaktorová autentizácia a použitie všetkých troch metód ako trojfaktorová autentizácia. V súčasnosti sa najčastejšie používa dvojfaktorová autentizácia.

Pre zabezpečenie vstupu môžeme teda použiť viaceré metódy:

- užívateľské meno a heslo
- autentizačné tokeny
- certifikáty
- biometriky (Matyáš, 2008)

### 4.1.1 Užívateľské meno a heslo

Autentizácia pomocou hesla je v súčasnej dobe asi najjednoduchším spôsobom a zároveň nie veľmi bezpečným. Užívateľ predkladá systému heslo spoločne so svojou identifikáciou - užívateľským menom (loginom). Systém tieto údaje kontroluje s dátami uloženými k danému užívateľovi. Preukázanie znalosti hesla je vyhodnotené systémom ako korektné preukázanie identity. Heslo by malo obsahovať reťazec netriviálnych znakov (8 - 12) - kombinácia malých a veľkých písmen a číslic - odolnejšie voči možnému slovníkovému útoku alebo útoku hrubou silou. Heslá je dobré meniť pravidelne po niekoľkých mesiacoch používania.

Pre zvýšenie bezpečnosti internet bankingu sa zaviedla doplnková služba - autorizačná SMS. Predpokladom je vlastníctvo mobilného telefónu. Po zadaní užívateľského mena a hesla je klientovi zaslaná autorizačná SMS s kódom, ktorý zadá užívateľ do príslušného poľa pre autorizáciu. (Matyáš, 2008)

### 4.1.2 Autentizačné tokeny

Autentizačné tokeny sú zariadenia, ktoré môžu užívatelia neustále nosiť pri sebe a ich vlastnenie je nevyhnutné pre autentizáciu do systému. Tokeny majú buď špecifické fyzikálne vlastnosti (tvar, elektrický odpor, kapacít...), obsahujú tajné informácie (kvalitné heslo, kryptografický kľúč..), alebo sú dokonca schopná vykonávať niektoré výpočty (zvyčajne kryptografické).

Jedným z týchto tokenom je autentizačný kalkulátor. Je to špeciálne zariadenie. Môže byť založené na tajomstve, ktoré je uložené v kalkulátore a na autentizačnom servery, alebo synchronizovaných hodinách. Ďalšia dôležitá vlastnosť je komunikácia s užívateľom. Rozhranie môže byť klasické (klávesnica a displej) alebo špeciálne (napr. optické rozhranie umožňujúce snímať dáta priamo z obrazovky počítača). Väčšinou využívajú protokol výzva - odpoveď.

Autentizačné kalkulátory sú používané bankami v oblasti internet bankingu a sú považované za jednu z najbezpečnejších metód. Po zadaní PINu je vygenerované heslo, ktoré je časovo obmedzené a slúži k autentizácii. Tento kalkulátor je zosynchronizovaný so systémom v banke, aby generoval rovnaké heslo vpisované užívateľom. Zhodou hesla sa preukáže užívateľ, že je majiteľom kalkulátoru. (Matyáš, 2008)

Obr. 7 Autentizačný kalkulátor

Zdroj: alsoft.cz

### 4.1.3 Certifikáty

Kvôli vyššej bezpečnosti bývajú k autentizácii užívateľov tiež často využívané prostriedky asymetrickej kryptografie (najmä digitálny podpis). Užívateľ väčšinou vlastní kľúčový pár (verejný a súkromný kľúč), kde je verejný kľúč certifikovaný príslušnou autoritou (bankou). Súkromný podpisový kľúč je bežne uložený na kryptografickej čipovej karte, kde prístup chráni PIN. Všetky operácie vyžadujúce digitálny podpis užívateľa preto prebiehajú vo vnútri čipovej karty, ktorá im poskytuje zabezpečené výpočetné prostredie. Pri používaní čipových kariet je potrebné vlastniť čítačku kariet. (Matyáš, 2008)

### 4.1.4 Biometria

Biometria je automatizované rozpoznávanie ľudských jedincov na základe ich charakteristických anatomických rysov (napr. tvár, odtlačok prstu, dúhovka, sietnica) a behaviorálnych rysov (chovanie: dynamické vlastnosti podpisu, chôdza). (Drahanský, 2011)

Biometrické vlastnosti delíme do dvoch kategórií (Drahanský, 2011):

- anatomické vlastnosti: odtlačok prstu, tvár, dúhovka, sietnica oka, geometria ruky, dlaň, termogram tváre/ruky, dentálny obraz, podpis (statická forma), tvar ucha, DNA...
- behaviorálne vlastnosti: hlas/reč, mimika tváre a pohyby pier, podpis (dynamická forma), dynamika stisku kláves, chôdza

Biometrické techniky môžeme využiť pre dve rozdielne aplikácie, a to pre autentizáciu či verifikáciu identity (užívateľa) a pre identifikáciu užívateľa. Môžeme využiť teda meranie pomocou fyziologických vlastností ľudského tela alebo pomocou chovania človeka, pričom sa jedná o meranie automatizovaným spôsobom.

Niektoré technológie sú zatiaľ v štádiu vývoju (napr. analýza pachov), no iné sa dajú využívať a sú komerčne dostupné (napr. odtlačok prstu). Systémy založené na fyziologických vlastnostiach sú obvykle spoľahlivejšie a presnejšie než systémy založené na chovaní človeka, pretože sú lepšie opakovateľné a nie sú podstatnejšie ovplyvňované psychickým či fyziologickým stavom (stres, choroba). (Matyáš, 2008)

Aby sa dal biometrický systém využiť v praxi, je potrebné najskôr uskutočniť niekoľko základných krokov.

**Fáza registrácie**

Počas tejto etapy sa užívateľ registruje do biometrického systému poskytovaním dát reprezentatívnych biometrických vzoriek nazývaných šablóny alebo etlóny. Snímanie daného vzorku prebieha viackrát a k vytvoreniu šablóny sa použije najlepší snímok.

V šablóne nie je uložený biometrický vzor ako taký (obraz odtlačku prstu), ale iba zodpovedajúci matematický kód, ktorý vznikol z nasnímaného vzorku extrakciou jeho unikátnych znakov.

Šablónu je potrebné vhodne uchovať. Môže by uložená priamo v snímacom zariadení, vhodný je tiež token. Ďalšou možnosťou je centrálna databáza na vzdialenom počítači. Tu však musí byť zaistená bezpečná komunikácia medzi snímacím zariadením a daným počítačom.

**Fáza verifikácie/identifikácie**

Po vytvorení databáze šablóny môžeme pokračovať k verifikácii alebo identifikácii užívateľa. Z biometrického vzoru získaného pomocou snímacieho zariadenia sa opäť vytvorí šablóna, a tá je porovnávaná s uloženým etalónom.

Určovanie zhody v prípade biometrických systémov sa líši od iných autentizačných techník. Napríklad pri autentizácii heslom dostaneme vždy jednoznačnú odpoveď, či je heslo správne alebo nie. U biometrie však nikdy nenastane stopercentná zhoda medzi uloženou referenčnou šablónou a práve získanou. Stanovuje sa teda prahová hodnota, pri ktorej sú porovnávané šablóny považované za zhodné. (Bitto, 2005)

## Chyby biometrických systémov

Veľký dôraz pri využívaní týchto systémov je kladený na vysokú bezpečnosť a spoľahlivosť technológie. Bohužiaľ ani biometria nie je stopercentne bezpečná.

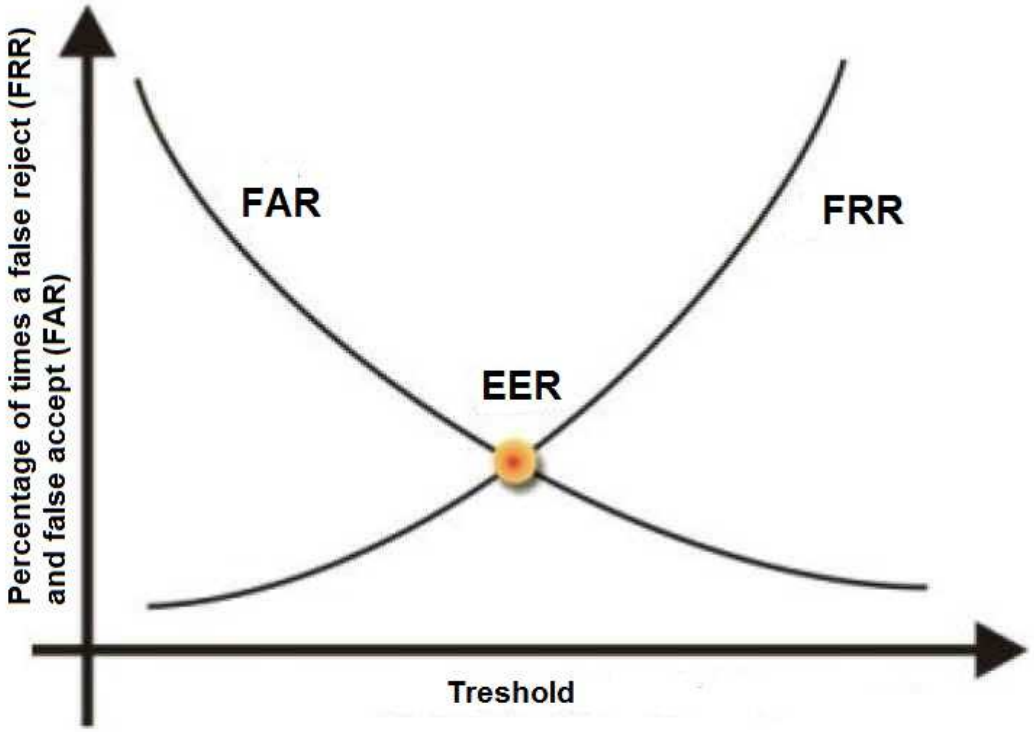
Referenčná šablóna je teda získaná ako najreprezentatívnejší vzor. Pri následnej identifikácii nezískame úplnú zhodu. Z tohto dôvodu môže dôjsť k chybám:

- **chybné prijatie** - podvodník je nesprávne identifikovaný ako oprávnený užívateľ
- **chybné odmietnutie** -autorizovaný užívateľ nie je rozpoznaný a je označený ako podvodník

Výskyt týchto chýb je spätý s vlastnosťami konkrétneho systému a nastavenou úrovňou zabezpečenia. Ak je prahová hodnota príliš vysoká, dochádza najčastejšie k chybným odmietnutiam. Na druhej strane pri nízkej prahovej hodnote sa môžeme stretnúť s chybným prijatím.

V praxi sa tieto chyby neuvádzajú v absolútnych číslach, ale v ich relatívnych ekvivalentoch. Sú to miera chybného prijatia (False Acceptance Rate, FAR) a miera chybného odmietnutia (False Rejection Rate, FRR). Vyjadrujú pravdepodobnosť výskytu danej chyby v percentách. (Bitto, 2005)

Obr. 8 Závislosť FAR a FRR na prahovej hodnote




Zdroj: Bitto (2005)

Čím je nižšia FAR, tým je vyššia FRR a naopak. Obidve miery sú závislé na nastavenej prahovej hodnote. Toto nastavenie závisí na konkrétnom spôsobe použitia biometrického systému v praxi podľa toho, či je väčšou škodou chybné prijatie alebo chybné odmietnutie. Priesečník FAR a FRR, čiže hodnota, pri ktorej sa rovnajú, je označená ako miera rovnej chyby (Equal Error Rate, ERR). Podľa tejto miery môžeme približne určiť bezpečnosť biometrického systému, avšak FAR a FRR majú ďaleko vyššiu vypovedajúcu hodnotu. (Bitto, 2005)

V Českej republike, biometrické systémy v oblasti bankovníctva a internet bankingu, ešte stále čakajú na svoj vstup do tejto sféry. Z prieskumu agentúry SC&C pre Českú bankovú asociáciu (ČBA) vyplýva, že biometrické overovanie údajov, napr. prostredníctvom odtlačku prstu alebo skenu sietnice očakáva v budúcnosti v bankovníctve 52% Čechov. (Většina Čechů očekává v budoucnu větší využití biometrie v bankovnictví, 2016)

Obr. 9 USB so snímačom odtlačku prstu

Zdroj: http://tech.sme.sk

# 5 Metodika

Praktická časť bakalárskej práce bude analyzovať zabezpečenie internetového bankovníctva vybraných finančných inštitúcií, pôsobiacich na území Českej republiky. Následne bude prevedená komparácia sledovaných bánk s cieľom určiť, ktorá je najlepšie zabezpečená. Porovnávanie bude vykonávané pomocou troch kritérií: spôsob autentizácie, informovanosť klientov o bezpečnosti používania a bezpečnostný limit pre automatické odhlásenie z aplikácie internetového bankovníctva. Poradie bánk bude určené pomocou metódy viackritérialneho rozhodovania.

V kapitole sedem predložíme návrh na zvýšenie zabezpečenia internetového bankovníctva pomocou využitia biometrických systémov. Budú vybrané štyri biometriky, ktoré porovnáme na základe viacerých kritérií a vyberieme najvhodnejšie riešenie.

# 6 Analýza zabezpečenia u vybraných bánk v ČR

V nasledujúcej kapitole vypracujem analýzu zabezpečenia internetového bankovníctva zameranú na bezpečnosť identifikácie (autentizácie) klienta u piatich vybraných bankách, pôsobiacich na území Českej republiky. Väčšina bánk používa na zabezpečenie dvojfaktorovú autentizáciu. U jednotlivých bánk nájdeme rozdielne možnosti identifikácie užívateľov. Analyzované banky boli vybrané podľa rôznej veľkosti[1].

Tab. 2 Porovnanie veľkosti vybraných bánk

| Názov banky | Počet klientov | Objem vkladov |
|---|---|---|
| **ČSOB** | 2,9 mil | 676,2 mld |
| **KB** | 1,6 mil | 650 mld |
| **Raiffeisenbank** | Cca 500 tis. | 173 mld |
| **Air Bank** | 343tis. | 57,6 mld |
| **Sberbank** | 86 tis. | 48,7 mld |

Zdroj: Vlastné spracovanie podľa vzoru - zpravy.aktualne.cz

Tabuľka 2 umožňuje porovnať počet klientov a objem vkladov jednotlivých bánk (údaje z roku 2015). Z tabuľky je zrejmé, že najväčšia z porovnávaných subjektov, či už počtom klientov alebo objemom vkladov, je banka ČSOB. Na druhej strane, najmenšou bankou je Sberbank.

## 6.1 Československá obchodná banka, a.s. (ČSOB)

ČSOB pôsobí v Českej republike ako univerzálna banka, ktorá bola založená štátom v roku 1964 ako banka pre poskytovanie služieb v oblasti financovania zahraničného obchodu a volnomenových operácií s pôsobnosťou na československom trhu. V roku 1999 bola privatizovaná väčšinovým vlastníkom a od roku 2007 sa stala jediným vlastníkom - belgická KBC Bank. (O ČSOB a skupině, 2016)

ČSOB ponúka službu internetového bankovníctva - ČSOB InternetBanking 24.

### 6.1.1 Autentizácia užívateľa

Autentizácia užívateľa sa môže vykonať tromi spôsobmi:

- identifikačným číslom, PIN a SMS kľúčom,
- identifikačným číslom, PIN a Smart kľúčom,
- certifikátom k elektronickému podpisu uloženým na čipovej karte.

[1] Veľkosť bánk je určená v závislosti na počte klientov banky a objemu vkladov

V prvých dvoch prípadoch je nutné zadať identifikačné číslo (8-miestne) a PIN (5-miestny), ktoré pridelí klientovi banka pri zriadení služby. Následne je potrebné zadať SMS kľúč zaslaný SMS správou do mobilného telefónu. Tento kľúč je v podobe kombinácie malých písmen a číslic (napr. abc-f2x-4n9) a je nutné ho zadať do 10 minút (prvý prípad). Druhý prípad - namiesto SMS kľúča načítame aplikáciou QR kód a následne získaný kód prepíšeme do polí a potvrdíme.

Tretí prípad - prihlásenie čipovou kartou vyžaduje certifikát uložený na čipovej karte a zaregistrovaný v systéme ČSOB pri zriadení služby. Pred prihlásením zasunieme čipovú kartu do nainštalovanej čítačky kariet a stlačíme tlačidlo prihlásiť. V priebehu prihlásenia zadáme PIN k čipovej karte. Následne dôjde k overeniu elektronického podpisu systémom a prihlásenie certifikátom. (S internetem šetřím svůj čas a peníze, 2016)

### 6.1.2 Analýza ČSOB InternetBanking 24

Banka ČSOB ponúka autentizáciu pomocou mena a hesla (s overením SMS kľúča). Pri zadaní nesprávneho SMS kľúča 5 krát po sebe dôjde k zablokovaniu účtu. Bezpečnostný limit pre jeho zadanie je 10 minút. Za pozitívne považujem aj ponuku druhej, vyššej možnosti zabezpečenia, a to pomocou elektronického podpisu uloženého na čipovej karte. Ak po prihlásení nevykonáme do 20 minút žiadnu operáciu, aplikácia nás automaticky odhlási. Zabezpečenie internetového bankovníctva preto hodnotím veľmi dobre. Využitie dvojfaktorovej autentizácie patrí k zatiaľ využívanému maximu. Na druhej strane, využívanie mena a hesla považujem za slabú stránku. Tento prvok jednofaktorovej autentizácie patrí k najmenej bezpečným. Paradoxne ho používatelia radi využívajú, najmä pre jeho jednoduchosť. Čo sa týka informovanosti používateľov ČSOB InternetBankingu 24 o možných bezpečnostných zabezpečeniach, nástrahách a ich predchádzaniu, na webovej stránke internetového bankovníctva môžeme nájsť informácie a vyznačené upozornenia o aktuálnych pokusoch napádania IB. Taktiež tu nájdeme bezpečnostné odporúčania, ktoré by mali klienti dodržiavať, napríklad aktualizácie operačných systémov, antivírusových programov atď. V ponuke je aj odkaz na zásady pre bezpečné používanie ČSOB elektronického bankovníctva. Po prihlásení do IB v sekcii správy môžeme nájsť správy zasielané bankou, ktoré sa mimo iné týkajú aktuálnych útokov na klientov ČSOB (napr. podvodné e-maily zasielané menom spoločnosti).

## 6.2 Komerčná banka, a.s. (KB)

Komerčná banka vznikla v roku 1990 vyčlenením obchodnej činnosti z bývalej Štátnej banky československej na území Českej republiky. V roku 1992 sa transformovala na akciovú spoločnosť. KB vlastní francúzska spoločnosť Société Générale. Do roku 2012 vyhrala päťkrát prestížne ocenenie Banka roku v jedenásťročnej histórii tejto ankety. Ako prvá banka ponúkla zdarma nástroj zameraný na ochranu proti sociálnemu inžinierstvu. (Historie spoločnosti, 2016)

KB ponúka službu internetového bankovníctva - MojaBanka.

### 6.2.1 Autentizácia užívateľa

Autentizácia užívateľa je možná iba prostredníctvom:

- certifikátu v súbore a hesla,
- certifikátu na čipovej karte a PIN.

Systém teda neumožňuje autentizáciu pomocou mena a hesla a tým zvyšuje zabezpečenie autentizácie. Certifikát je vygenerovaný na pobočke banky a je možné uložiť ho v počítači. Bez neho nie je možné prihlásenie do internetového bankovníctva. K aktivácii je potrebné heslo určené bankou (možnosť zmeny). Následne musíme zadať jednorazový SMS kľúč. (prvý prípad)

V druhom prípade je certifikát uložený na čipovej karte. Je potrebné zaobstarať si čítačku čipových kariet a komponenty nainštalovať do počítača. Súčasťou procesu je zadávanie PIN kód. Hlavnou výhodou čipovej karty je, že certifikát z nej sa nedá žiadnym spôsobom skopírovať. (Certifikáty, 2016)

### 6.2.2 Analýza MojaBanka

Za silnú stránku internetového bankovníctva Komerčnej banky považujem vyradenie autentizácie pomocou identifikačného mena a hesla. Sústredí sa na zabezpečenie pomocou certifikátu, či už uloženého priamo v počítači, alebo na čipovej karte. Certifikát uložený v počítači má nižšiu úroveň bezpečnosti. Pri napadnutí sa k nemu hacker môže jednoducho dostať. Pre vyššiu ochranu je teda lepšie mať certifikát uložený na čipovej karte. Ak nedôjde k strate čipovej karty je prakticky nemožné zneužitie certifikátu. Ak klient nevykoná žiadnu akciu v bezpečnostnom limite 20 minút, dôjde k automatickému odhláseniu. Nevýhodou pre klientov môže byť zložitosť prihlasovania sa do systému a taktiež prenášanie čítacieho zariadenia čipovej karty pri prihlasovaní z verejného počítača. Informácie pre klientov o bezpečnom používaní internetového bankovníctva MojaBanka ponúka KB na svojich stránkach. Priamo pri prihlasovaní sa nachádzajú aktuálne a dôležité informácie o možných zmenách a najmä o hackerských útokoch a podvodoch. Taktiež odkaz s názvom Společně bezpečně, kde môžeme nájsť okrem aktuálnych hrozieb desatoro bezpečnosti, návody ako chrániť svoje zariadenia a podobne. Ponúka aj nástroj na stiahnutie, ktorý je zameraný na ochranu proti metódam sociálneho inžinierstva.

## 6.3 Raiffeisenbank, a.s.

Raiffeisenbank pôsobí na českom trhu od roku 1993. Ponúka široké spektrum bankových služieb súkromnej aj firemnej klientele. Banka sa zameriava predovšetkým na náročnejšiu klientelu, ktorá má záujem o vysokú kvalitu služieb, aktívnu správu svojich financií a profesionálne poradenstvo. Väčšinovým akcionárom banky je rakúska finančná inštitúcia Raiffeisen Bank International AG (RBI). Prestížny medzinárodný magazín EMEA Finance vrámci cien Europe Banking Awards vyhlá-

sil Raiffeisenbank za najlepšiu banku v Českej republike za rok 2015. (Profil a historie Raiffeisenbank v ČR, 2016)

### 6.3.1 Autentizácia užívateľov

Autentizáciu zabezpečuje niekoľko nástrojov:

- klientske číslo a autentizačný kód,
- mobilný elektronický kľúč,
- mobilný elektronický kľúč SMS,
- osobný elektronický kľúč.

Banka po overení klientskeho čísla (prihlasovacie meno) a autentizačného kódu (heslo) zistí, kto sa prihlásil k internetovému bankovníctvu. Úspešne overená identita klienta sa následne používa ku kontrole oprávnenia k manipulácii s účtom.

Mobilný elektronický kľúč zabezpečuje prístup na účet prostredníctvom telefónu s funkciou SIM Toolkit. Prístup je chránený špeciálnym osobným identifikačný číslom (BPIN), a komunikácia s bankou prebieha šifrovane.

Mobilný elektronický kľúč SMS slúži prostredníctvom telefónu, ktorý nepodporuje funkciu SIM Toolkit, alebo je používané zahraničné číslo. Pre prístup k účtu cez internet je potrebný teda mobilný telefón a štvormiestny číselný kód I-PIN. Tento kód dáva banka na pobočke pri aktivácii mobilného elektronického kľúča SMS a môže byť kedykoľvek zmenený.

Osobný elektronický kľúč je univerzálnym hardwarovým prostriedkom k zabezpečeniu prístupu na účet. Tento kľuč je možné využiť kdekoľvek nezávisle na pokrytí mobilnej siete a technického vybavenia použitého počítača. Osobný elektronický kľúč je chránený proti zneužitiu štvormiestnym PINom. (Bezpečnost internetového bankovnictví, 2016)

### 6.3.2 Analýza internetového bankovníctva Raiffeisenbank

Silnou stránkou je určite rôznorodosť a prepracovanosť autentizácie pomocou elektronických kľúčov. Dva fungujú prostredníctvom mobilných telefónov a osobný elektronický kľúč je pre prihlasovanie prostredníctvom počítača. Po zadaní štvormiestneho PIN kódu nám tento kalkulátor vygeneruje kľúč, ktorý stačí prepísať do internetového formuláru. Zabezpečenie prostredníctvom elektronických kľúčov patrí k najvyšším zabezpečeniam v dvojfaktorovej autentizácii. Na druhej strane stále používa identifikáciu prostredníctvom mena a hesla. Ďalším mínusom môže byť neprítomnosť bezpečnostného limitu, kde pri nečinnosti nedôjde k automatickému odhláseniu. Informácie pre klientov o bezpečnosti môžeme nájsť na webových stránkach banky. Pri každej metóde autentizácie aj autorizácie sa nachádzajú odporúčania pre zaistenie bezpečnosti. Nájdeme tu i zásady a pokyny o bezpečnom používaní internetového bankovníctva, aktuálne správy, avšak ku všetkým informáciám o bezpečnosti sa musíme preklikať. Chýba tu viditeľné upozornenie.

## 6.4 Air Bank, a.s.

Air Bank vznikla v roku 2011. Je člen skupiny PPF (jednej z najväčších investičných a finančných skupín v strednej a východnej Európe) a medzinárodnej skupiny Home Credit Group. Väčšinu klientov získala banka z tradičných veľkých bánk aj vďaka jednoduchému prechodu medzi bankami. Banka ponúka úročenie peňazí do 100 000 Kč aj na bežnom účte s rovnako výhodnou sadzbou ako na šporiacom účte. (O první bance, kterou můžete mít rádi, 2016)

### 6.4.1 Autentizácia užívateľov

Autentizácia užívateľov v internetovom bankovníctve Air Bank ponúka túto ochranu:

- užívateľské meno a heslo

Vstup do intenetbankingu je teda chránené užívateľským menom, ktoré si volí klient sám na pobočke pri tvorbe zmluvy, a heslom, ktoré si tak isto volí klient sám. Pre heslo existujú určité pravidlá, ktoré je nutné dodržať (veľké, malé písmená, číslice, špeciálne znaky...). Pre overenie prihlásenia je možné dobrovoľne si zvoliť autorizačnú SMS pre vyššiu ochranu. (Bezpečnost a soukromí, 2016)

### 6.4.2 Analýza internetového bankovníctva Air Bank

Zabezpečenie internetového bankovníctva Air Bank je najmenej bezpečný spôsob. Využíva iba jednofaktorovú autentizáciu prostredníctvom mena a hesla. Používateľ má 5 pokusov na opravu v prípade zlého zadania prihlasovacích údajov. Z toho po treťom neúspešnom pokuse zadáva dátum narodenia. Po piatich neúspešných pokusoch musí klient kontaktovať banku a odpovedať na autentizačné otázky. Táto autentizácia je síce jednoduchý a pohodlný spôsob no najjednoduchší na prelomenie. Hackeri prostredníctvom phishingových metód dokážu zistiť tieto údaje a už im nič nestojí v ceste. V prípade slabého hesla môžu použiť aj útok hrubou silou, ktorý dokáže prelomiť heslo za pár hodín. Pozitívom je ponuka prvku vyššej ochrany, aj keď iba voliteľne. Bezpečnostný limit pri nečinnosti je nastavený na 20 minút, ktorý nás následne automaticky odhlási. Čo sa týka informácií o bezpečnosti, na prihlasovacej stránke do internetové bankovníctva Air Bank je upozornenie, aby sme si pred prihlásením skontrolovali, či sme na legitímnej stránke banky. A to v troch krokoch: neprišli sme na túto stránku prekliknutím z mailu, v adresnom riadku je adresa podľa napísaného vzoru a certifikát je vystavený na meno Air Bank a.s. Ďalej tu nájdeme odkaz na rady a návody o bezpečnosti, ako napríklad: pravidelne aktualizovať prehliadač, antivírusový program, operačný systém.

## 6.5 Sberbank CZ, a.s.

Potom ako vlastníci Volksbank International AG a predstavitelia medzinárodnej bankovej skupiny Sberbank úspešne dokončili vyjednávania o predaji v roku 2012, v roku 2013 sa spoločnosť Volksbank CZ, a.s. premenovala na Sberbank CZ, a.s. (Volksbank CZ, a.s. se mění na Sberbank CZ, a.s, 2016)

Sberbank CZ je dcérskou spoločnosťou Sberbank Europe AG, ktorá je súčasťou Skupiny Sberbank. Je to moderná banka s komplexnou ponukou produktov a služieb pre fyzické osoby, malé a stredné firmy a aj veľké korporácie. Posledné štyri roky sa drží na prvých troch priečkach v kategórii Klientsky najprívetivejšia banka. (Představení banky, 2016)

Sberbank Cz ponúka internetové bankovníctvo - Sberbank Online Banking

### 6.5.1 Autentizácia užívateľov

Autentizácia je možná pomoc dvoch funkcií:

- elektronický kľúč
- podpisový certifikát

Prvé prihlásenie vyžaduje vloženie prihlasovacieho mena, ktoré dostaneme v bezpečnostnej obálke od banky pri založení účtu. Ďalej zadáme Token kód s dĺžkou 6 číslic, ktorý je vygenerovaný elektronickým kľúčom (tokenom). Klikneme na Prihlásiť a nastavíme vlastný, štvormiestny PIN kód. Pri druhom prihlásení už zadávame len prihlasovacie meno a do druhého pola náš zvolený PIN plus vygenerovaný token kód, ktorý vygeneruje elektronický kľúč, čiže vkladáme desaťmiestny kód.

Pri funkcii podpisový certifikát sú dve možnosti. Ak používame pasívny prístup vložíme iba prihlasovacie meno a heslo, ktoré dostaneme v bezpečnostných obálkach na pobočke banky. Pre použitie aktívneho prístup si po vložení prihlasovacieho mena a hesla vytvoríme podpisový certifikát. Doporučené uloženie pre väčšiu bezpečnosť je na prenosnom médiu (napr. USB kľúč). Následne zvolíme meno a heslo pre certifikát podľa vlastného výberu. Heslo musí mať minimálne 5 a maximálne 20 znakov. (Sberbank Online Banking: Jak jej zvládnout, 2016)

### 6.5.2 Analýza Sberbank Online Banking

Sberbank Online Banking ponúka na výber z dvoch najvyšších spôsobov zabezpečenia dvojfaktorovej autentizácie, a to certifikát a elektronický kľúč. Práve preto ju radím na prvé miesto v zabezpečení z vybraných bánk. Používa síce aj prihlasovacie meno a heslo, ale iba pri prvom prihlásení a vytvorení certifikátu, preto nepovažujem tento spôsob za slabú stránku. Pri chybnom vložení PIN kódu (3 krát) alebo token kódu (10 krát) je potrebné navštíviť pobočku banky a žiadať o reaktiváciu tokenu. Z dôvodu zdokonalenia bezpečnosti sa aplikácia po 15 minútach nečinnosti automaticky odhlási. Informácie o aktuálnych hrozbách môžeme nájsť priamo na prihlasovacej stránke Online Banking-u. Ďalej sa tu nachádza odkaz

na bezpečnosť s online bankovníctvom, kde sa používateľ dozvie pokyny a rady, ako bezpečne postupovať pri prihlasovaní. Taktiež si môže stiahnuť PDF súbor, tzv. užívateľskú príručku, kde sa okrem iného nachádza aj bezpečnostné desatoro.

## 6.6 Výber optimálne zabezpečenej banky

Pre výber optimálnej banky z pohľadu zabezpečenia použijem metódu viackriteriálneho rozhodovania. Kritériá, podľa ktorých je zabezpečenie bánk posudzované, sú spôsob autentizácie, informovanosť klientov o aktuálnych hrozbách a bezpečnostných opatreniach, bezpečnostný limit pre odhlásenie z aplikácie pri nečinnosti.

Pre výpočet váh jednotlivých kritérií som využil metódu poradia. Kritéria sú zoradené podľa dôležitosti. Autentizácia je prvá v poradí z troch kritérií, preto má priradené tri body. Celkový počet priradených bodov všetkým kritériám je teda 6. Následne jednotlivé váhy vypočítame podielom počtu priradených bodov a celkového počtu bodov.

Tab. 3 Výpočet váh

| Kritérium | Poradie | Body | Váhy |
|---|---|---|---|
| **Autentizácia** | 1. | 3 | 0,5 |
| **Informačná bezpečnosť** | 2. | 2 | 0,33 |
| **Bezpečnostný limit** | 3. | 1 | 0,17 |

Ďalej ohodnotím každé kritérium samostatne u jednotlivých bánk, a to pomocou priradenia bodov. Bodovacia stupnica je od 0 po 5, pričom 0 znamená, že dané kritérium banka neposkytuje. 1 až 5 značia kvalitu kritéria, pričom 1 je najnižšia a 5 najvyššia kvalita.

Tab. 4 Hodnotenie kritérií u jednotlivých bánk

| Banka / Kritérium | ČSOB | KB | Raiffeisenbank | Air Bank | Sberbank |
|---|---|---|---|---|---|
| **Autentizácia** | 3 | 4 | 4 | 1 | 5 |
| **Informačná bezpečnosť** | 5 | 5 | 3 | 4 | 5 |
| **Bezpečnostný limit** | 3 | 3 | 0 | 3 | 4 |

V tabuľke číslo 4 vidíme body, ktoré získali banky v jednotlivých kritériách. Čo sa týka autentizácie jednotlivých bánk, najviac bodov, a to päť, získala Sberbank. Ponúka najvyššie zabezpečenie z vybraných subjektov vďaka využitiu certifikátov a elektronických kľúčov. Najmenej, jeden bod, získala Air Bank, pretože využíva jednofaktorovú autentizáciu pomocou mena a hesla. KB a RB banky dostali zhodne po 4 body. Patria k vysoko zabezpečeným systémom, no zaostávajú využitím prvku jednofaktorovej autentizácie u RB a zameraním sa len na jeden spôsob autentizácie u KB. ČSOB má tiež vyššiu úroveň zabezpečenia, meno a heslo doplnené autorizačnou SMS, preto dostala s 3 body.
Informačná bezpečnosť zahŕňa informovanosť klientov o možných hrozbách. Hodnotil som informácie na prihlasovacích stránkach do internetového bankovníctva, či už aktuality o hrozbách, bezpečnostné informácie a pokyny atď. Všetky banky obstáli nadpriemerne. Sberbank, ČSOB a KB dostali po 5 bodov. Na prihlasovacej stránke nájdeme bezpečnostné pokyny a opatrenia, ktoré majú klienti dodržiavať, ďalej aktuality o nových hrozbách a útokoch a odkazy na ďalšie bezpečnostné rady. Air Bank chýbali na stránke aktuálne informácie o hrozbách, preto dostala 4 body a Raiffeisenbanke nechýbali síce žiadne informácie, no je treba sa k nim preklikávať, takže 3 body.
Bezpečnostný limit pre automatické odhlásenie s aplikácie pri nečinnosti využívajú okrem RB všetky banky. KB, ČSOB a Air Bank majú 20 minútový limit a Sberbank má 15 minútový. Podľa môjho názoru, čím menší limit tým lepšie, preto 3 a 4 body.

Následne body jednotlivých bánk vynásobíme príslušnými váhami, sčítame pre všetky kritéria a dostaneme celkové hodnotenie vybraných bánk, ktoré môžeme vidieť v nasledujúcej tabuľke 5. Najlepšie v hodnotení zabezpečenia dopadla Sberbank s 4,83 bodmi, ďalej KB, ČSOB, RB a najhoršie Air Bank s 2,33 bodmi.

Tab. 5 Celkové hodnotenie bánk

| **Banka** | | **ČSOB** | **KB** | **RB** | **Air Bank** | **Sberbank** |
|---|---|---|---|---|---|---|
| **Kritérium** | **Váhy** | | | | | |
| **Autentizácia** | 0,5 | 3 | 4 | 4 | 1 | 5 |
| **Informačná bezpečnosť** | 0,33 | 5 | 5 | 3 | 4 | 5 |
| **Bezpečnostný limit** | 0,17 | 3 | 3 | 0 | 3 | 4 |
| **Body celkom** | | **3,66** | **4,16** | **2,99** | **2,33** | **4,83** |

# 7 Návrh zvýšenia zabezpečenia autentizácie internetového bankovníctva

Žiadny systém nie je úplne bezpečný. Ani najmodernejšia technológia nezaručuje stopercentné zabezpečenie a ochranu proti poškodeniu, napadnutiu či preniknutie do systému. Pritom najslabším článkom nie je ani tak technológia, ale človek, ktorý ju využíva.

Ako môžeme vidieť z predchádzajúcej kapitoly, zabezpečenie autentizácie internetového bankovníctva využívané bankami je zabezpečenie pomocou dvojfaktorovej autentizácie. Avšak postupom času ani takto vysoká forma zabezpečenia nebude dostatočná. Hackeri, respektíve sociálni inžinieri, tak ako banky zdokonaľujú svoje zabezpečenia, aj oni zdokonaľujú svoje znalosti a spôsoby k dosiahnutiu svojho cieľa, ktorým je prekonanie zabezpečenia tohto systému a získanie či už osobných informácii alebo finančných prostriedkov.

Môj návrh pre zvýšenie zabezpečenia autentizácie internetového bankovníctva spočíva v prechode z dvojfaktorovej autentizácie na trojfaktorovú.
Z kapitoly 4.1 vieme, že autentizačné metódy sú založené na tom, čo poznáme (PIN, heslo), čo vlastníme (karta, kalkulátor) a na tom, čo sme (biometrická informácia). Trojfaktorová autentizácia používa jednu metódu z každej z uvedených skupín. Táto forma je maximum z hľadiska bezpečnosti, ktorú môžeme v oblasti autentizácie využiť. Usporiadanie systému by malo byť také, že biometrická informácia je ideálne zosnímaná pomocou tokenu. PIN alebo heslo je zadané do zariadenia pod kontrolou autentizačného serveru a mimo iné slúži k zahájeniu autentizácie v autentizačnom serveri. K tejto autentizácii je potrebná spolupráca tokenu podmienená úspešným overením biometrickej informácie.
Postup môžeme popísať takto:

- užívateľ vloží token do autentizačného zariadenia
- užívateľ zadá do autentizačného zariadenia PIN, ktorý je zaslaný priamo do tokenu a nikam inam
- token overí PIN
- užívateľ vloží svoju biometrickú informáciu do tokenu
- token spracuje biometrickú informáciu a porovná ju so vzorom, ktorý má v sebe uložený
- token začne komunikáciu protokolom typu výzva - odpoveď so systémom, ku ktorému sa užívateľ autentizuje; pre tento účel sú použité dôverné dáta (kľúče, náhodné čísla), ktoré generuje iba token
- po úspešnom ukončení protokolu výzva - odpoveď je užívateľ autentizovaný

Ak dôjde pri bodoch 3, 5, 6 k chybe, bude autentizácia ukončená neúspechom. (Matyáš, 2008)
Rozdielom medzi dvoj a trojfaktorovou autentizáciou je teda využitie biometrie.

## 7.1 Využitie biometrie

Slovo biometria vzniklo spojením dvoch gréckych slov *bio* a *metric*, kde bio znamená život a metric znamená meranie. Biometria teda meria určité charakteristiky človeka. Biometrické systémy slúžia k automatickej identifikácii alebo overeniu identity človeka na základe jeho unikátnych merateľných fyziologických alebo behaviorálnych vlastností. (Bitto, 2005)

## 7.2 Biometria ruky

Ľudská ruka poskytuje niekoľko unikátnych a zároveň merateľných vlastností. Najznámejšia a najrozšírenejšia z nich je odtlačok prstu. Okrem toho môžeme merať aj geometriu ruky, dynamiku podpisu, dynamiku písania na klávesnici, vzor krvného riečišťa, tvar lôžku nechtu alebo absorpčné spektrum ľudskej kože. V nasledujúcom texte sa oboznámime s odtlačkami prstov a dynamikou podpisu. (Bitto, 2005)

### 7.2.1 Odtlačok prsta

Technológia odtlačku prsta má bohatú históriu najmä vo forenznej sfére. Vďaka daktyloskopii bolo odhalených veľa zločincov. V roku 1880 publikoval Angličan Henry Faulds článok. ktorý sa zaoberal snímaním odtlačkov prstov pomocou atramentu. Je považovaný za prvého človeka, ktorému sa podarilo získať odtlačok prsta z predmetu. Za prvý kriminálny prípad vyšetrený vďaka odtlačku prstu sa považuje vražda dvoch detí v Argentíne roku 1892.

Ak sa pozrieme bližšie na bruška prstov, uvidíme drobné preliačiny a vyvýšeniny. Vznikajú tak, že škára vybieha proti pokožke v takzvaných papilách - papilárne línie. Ako prvý popísal jednotlivé typy charakteristických vzorov papilárnych línií Jan Evangelista Purkyně, keď ich klasifikoval do deviatich základných vzorov. Z tohto delenia vychádza novodobá klasifikácia, ktorá rozoznáva tri základné vzory:

- oblúk - papilárne línie vytvárajú jednoduché oblúky; vzor neobsahuje žiadne tzv. delty - útvary, v ktorých sa papilárne línie rozbiehajú do troch smerov
- vír - pap. línie vytvárajú kruhové, oválne alebo špirálové obrazce s jadrom v strede; vzor musí obsahovať aspoň 2 delty s aspoň jednou samostatne prebiehajúcou líniou
- slučka - pap. línie vytvárajú slučku; medzi deltou a stredom musí byť aspoň jedna prebiehajúca línia

Identifikácia je založená na nájdení a porovnaní tzv. markantov, ktoré papilárne línie vytvárajú. Existuje niekoľko druhov markantov, napr. body (veľmi malé ryhy), ostrovčeky (ryhy o málo väčšie ako body ležiace v priestore medzi rozdvojenou ryhou) či mostíky (malé ryhy spojujúce dve susedné ryhy).

Pri rozpoznaní odtlačku prstu sa používajú dva základné princípy:

- skúmanie podľa globálneho vzoru
- skúmanie podľa podrobností (Bitto, 2005)

Výhody:

- relatívne lacná metóda - základný snímač stojí cca 2500Kč
- odtlačok prsta je u každého človeka jedinečný, stály (v čase sa takmer nemení)
- rýchlosť snímania je vysoká (Biometrické systémy, 2011)
- niektoré snímače sú malé, prenosné
- špecializované snímače sa nedajú oklamať umelo vytvoreným odtlačkom (Biometrie otisku prstu, 2016)

Nevýhody:

- jednoduché získanie a napodobenie odtlačku prstu
- u niektorých snímačov môže byť problém pri poškodení či znečistení prstu

### 7.2.2 Dynamika podpisu

Táto biometrická technika spočíva v tom, že namiesto vizuálnej podoby so vzorom dochádza k porovnávaniu vlastného priebehu písania. Meria sa predovšetkým rýchlosť, tlak na podložku, štýl jednotlivých ťahov a pod. Táto technika patrí medzi behaviorálne charakteristiky. Klasický podpis sa dá naskenovať a zneužiť. Oproti tomu systémy merajúce dynamiku podpisu porovnávajú podpis so vzorom v štyroch rozmeroch naraz. K tradičným dvom dimenziám roviny pribúda ešte tlak špeciálneho podpisového pera na podložku a čas.
Výhody:

- taktiež relatívne lacná metóda (cca od 3000 Kč)
- vysoká užívateľská prijateľnosť
- nenapodobiteľnosť
- rýchlosť snímania podpisu je prijateľná

Nevýhody:

- nepresnosť podpisovania
- premenlivosť v čase (Bitto, 2005)

## 7.3 Biometria hlavy

Taktiež ako ruka, aj hlava obsahuje niekoľko unikátnych charakteristík. Snímanie očnej dúhovky alebo sietnice patrí medzi najpresnejšie formy biometrie. Ďalej poznáme rozpoznávanie tváre alebo overenie hlasu. V nasledujúcom texte si priblížime očnú dúhovku a overenie hlasu. (Bitto, 2005)

### 7.3.1 Očná dúhovka

Očná dúhovka, čo sa týka podobnosti, je u každého človeka jedinečná. Niet divu, že sa stala ďalšou formou biometrických technológií. Ide o pigmentovanú membránu obklopujúcu zrenicu oka, ktorej štruktúra je jedinečná a v čase sa nemení. Identifikácia osôb na základe merania unikátnych vlastností dúhovky sa považuje za jednu z najpresnejších biometrických techník.

Dúhovka má niekoľko jasne viditeľných vonkajších charakteristík - záhyby, škvrny, ryhy, krypty a pod. Identifikácia biometrickými systémami je založená na digitalizácii týchto rysov a ich následným porovnaním s registračnými vzormi uloženými v databázach.

- krypty: veľmi tmavé miesta, kde je dúhovka pomerne tenká
- radiálne ryhy: začínajú blízko zornice a paprskovito vybiehajú smerom k okraju dúhovky
- pigmentové škvrny: náhodné zhluky pigmentových buniek pri povrchu dúhovky
- pigmentové záhyby: vznikajú ako dôsledok vystupujúcej spodnej vrstvy dúhovky v blízkosti zornice

Digitálna kamera umiestnená vo vnútri snímacieho zariadenia spraví čiernobiely snímok ľudského oka, ktorý sa vyznačuje vysokým rozlíšením. Fotografia je ďalej spracovávaná softwarom, ktorý lokalizuje vnútorné a vonkajšie okraje dúhovky a dochádza k výpočtu šablóny.
Výhody:

- jedinečnosť dúhovky u človeka
- veľká presnosť v identifikácii
- dúhovka sa v čase nemení
- užívateľmi vysoko prijateľná forma
- snímanie prebieha bez kontaktu - vysoko hygienické
- dúhovka je dobre chránená voči externým vplyvom

Nevýhody:

- vysoká cena zariadenia
- vysoké obstarávacie náklady systému

- možnosť zmeny dúhovky vplyvom ochorení (Bitto, 2005)

### 7.3.2 Overenie hlasu

Táto biometrická technológia je založená na odlišnostiach vokálneho traktu jednotlivých osôb. Tvar a rezonancia ústnej dutiny, hlasiviek, jazyka a zubov dokážu jednoznačne sformovať náš biometrický odtlačok. Prvé pokusy verifikácie hlasom prebehli už v 70. rokoch a v dnešnej dobe je táto technológia intenzívne skúmaná a zdokonaľovaná.

Rozpoznávanie a overovanie hlasu nie sú rovnaké prístupy. V prípade rozpoznávania hlasu človek vysloví slovo, systém následne prehľadá databázu a určí, ktoré slovo odpovedá danej výslovnosti. Pri overovaní hlasu je užívateľom vyslovená fráza porovnaná s registračným vzorom a systém určí mieru zhody. Pomocou samotného rozpoznania hlasu je systém schopný určiť, čo bolo povedané, nie však kto to povedal.

V priebehu fázy registrácie každý užívateľ vytvorí svoj vzor, tzv. "odtlačok hlasu". Z bezpečnostného hľadiska je jasné, že dlhšie vety a frázy poskytujú vyšší stupeň zabezpečenia ako krátke slová.

V priebehu identifikácie je človek vyzvaný, aby vyslovil svoju vetu. Lepšiu bezpečnosť poskytujú systémy, ktoré vo fázy registrácie požadujú niekoľko rôznych fráz a pri identifikácii vyberú náhodne niektorú z nich.

Výhody:

- nízka hardwarová náročnosť
- nízke náklady
- jedinečnosť hlasu človeka
- vysoká užívateľská prijateľnosť

Nevýhody:

- vysoká závislosť na aktuálnom stave hovoriaceho (choroba)
- nízka presnosť zariadenia
- hlas sa mení v čase
- vysoká možnosť zneužitia (Bitto, 2005)

## 7.4 Zhrnutie biometrických systémov

Biometrické systémy tvoria najvyšší stupeň zabezpečenia. Ako súčasť trojfaktorovej autentizácie sú teda najlepšou možnosťou pre využitie v oblasti zabezpečenia internetového bankovníctva. Aby mohli byť využiteľné v praxi, musia byť čo najviac prijateľné pre užívateľa. V nasledujúcej tabuľke ohodnotím jednotlivé vlastnosti biometrických systémov.

Tab. 6 Hodnotenie vlastností biometrických systémov

| **Biometria** | **Jedinečnosť** | **Presnosť** | **Zmena v čase** | **Užívateľské prijatie** | **Cena** | **Možnosť zneužitia** |
|---|---|---|---|---|---|---|
| **Odtlačok prstu** | V | V | N | S | N | S |
| **Dynamika podpisu** | V | N | S | V | N | N |
| **Očná dúhovka** | V | V | N | V | V | N |
| **Overenie hlasu** | S | N | V | V | N | V |

| **Biometrie** | CELKOM |
|---|---|
| **Odtlačok prstu** | V |
| **Dynamika podpisu** | S |
| **Očná dúhovka** | V |
| **Overenie hlasu** | N |

Zdroj: vlastné spracovanie podľa vzoru Bitto (2005)

V tabuľke 10 sme hodnotili jednotlivé vlastnosti hodnotami Nízka (N), Stredná (S) a Vysoká (V).

Z celkového hodnotenia môžeme vidieť, že najlepšie hodnotenie získali odtlačok prstu a očná dúhovka. Pri voľbe vhodného biometrického systému musíme brať v úvahu jednotlivé vlastnosti. Vidíme, že jedinečnosť týchto dvoch biometrík je vysoká, čo znamená, že každý človek má unikátny odtlačok prstu a očnú dúhovku. Taktiež presnosť snímania je na vysokej úrovni čo znižuje percento chybného prijatia a odmietnutia. Hodnota zmeny biometriky v čase je nízka. V tomto prípade je nízka hodnota tejto vlastnosti považovaná kladne, pretože nemusíme tak často meniť šablónu, s ktorou systém porovnáva práve nasnímaný vzor.
Pri odtlačku prsta môže byť problém vo vyššej miere možnosti zneužitia. Snímač odtlačku prstu môže byť oklamaný umelo vytvoreným odtlačkom. Túto mieru zneužitia môžeme znížiť využívaním špeciálnejších zariadení na snímanie odtlačkov

prstov, ktorý okrem iného kontroluje živosť tejto časti tela. Samozrejme zníženie miery možnosti zneužitia je vykúpené vyššou cenou zariadenia.
Čo sa týka očnej dúhovky, miera zneužitia je nízka čiže možnosť prekonania systému je veľmi malá. Jediným nedostatkom je vysoká cena.

Dynamika podpisu získala stredné a overenie hlasu získalo dokonca nízke hodnotenie. Je to spôsobené nízkou mierou presnosti a vysokou mierou zmeny v čase a nestálosti. To znamená, že sa nedokážeme podpísať alebo povedať uloženú frázu rovnakým spôsobom. Vidíme, že nízke hodnotenie je aj napriek dobrej prijateľnosti a ceny. Overenie hlasu získalo o niečo nižšie hodnotenie oproti dynamike podpisu vďaka vysokej miery možnosti zneužitia.

Z predchádzajúceho textu teda môžeme usúdiť, že na zabezpečenie pomocou biometrických systémov je vhodné využiť fyziologické typy biometrie pred behaviorálnymi. Najlepšími kandidátmi sú odtlačok prstu a očná dúhovka.

# 8 Diskusia

V diskusii zhodnotíme spôsoby autentizácie vybraných bánk a na základe skutočností uvedených v kapitole 5 ohodnotíme a porovnáme zabezpečenie vo vybraných finančných inštitúciách. Ďalej zhodnotím a zdôvodním návrh riešenia z kapitoly 6.

V tabuľke 9 môžeme vidieť súhrnný prehľad spôsobov zabezpečenia autentizácie internetového bankovníctva jednotlivých bánk.

Tab. 7 Spôsoby autentizácie u jednotlivých bánk

| | **Spôsoby autentizácie** | | | | |
|---|---|---|---|---|---|
| **Banka** | **Meno a heslo** | **SMS kód** | **Čipová karta** | **Certifikát** | **Elektronický kľúč** |
| **ČSOB** | ✓ | ✓ | ✓ | | |
| **KB** | | | ✓ | ✓ | |
| **Raiffeisen** | ✓ | | | | ✓ |
| **Air Bank** | ✓ | | | | |
| **Sberbank** | ✓ | | | ✓ | ✓ |

Ako môžeme vidieť, všetky sledované banky okrem jednej ponúkajú ako minimálne zabezpečenie autentizáciu užívateľov pomocou mena a hesla, čo je paradoxne najmenej bezpečný spôsob, avšak zatiaľ stále najviac obľúbený pre klientov. Jedine Komerčná banka tento spôsobom autentizácie nevyužíva. Okrem Air Bank, všetky sledované banky používajú okrem tohto minimálneho zabezpečenia aspoň jeden spôsob vyššieho zabezpečenia.

Mohli by sme si myslieť, že najmenšie zabezpečenie budú mať banky, ktorú sú najmenšie alebo najnovšie. Tak isto môžeme usúdiť, že tieto banky budú mať najmenej klientov. Nie je to však úplne tak.

Ako môžeme vidieť z tab. 8, najmenšie hodnotenie zabezpečenia internetového bankovníctva má Air Bank, ktorá používa iba meno a heslo(voliteľne SMS). Umiestnila sa na poslednom mieste, avšak s cca 350 000 klientmi sa neradí medzi najmenšie banky na trhu. Nenáročným klientom toto zabezpečenie nevadí väčšinou kvôli jeho jednoduchosti a nulovým poplatkom, čím ho robí prívetivejším.

Najmenšou bankou je Sberbank (cca 90 000 klientov), ktorej zabezpečenie získalo najviac bodov z pozorovaných subjektov. Banka pre zabezpečenie využíva elektronický kľúč, ktorý sa radí k najbezpečnejšiemu spôsobu z doposiaľ využívaných spôsobov zabezpečenia. Navyše je ešte skombinované so 4miestnym kódom vlastného výberu. Taktiež využíva ako alternatívu zabezpečenie podpisovým certifikátom, ktorý patrí k veľmi vysokému spôsobu zabezpečenia. Spolu s prehľadnými a aktuálnymi bezpečnostnými informáciami a bezpečnostným limitom pre odhlásenie sa umiestnila na prvom mieste.

Čo sa týka najväčších bánk z nášho výberu, Komerčná banka a Československá obchodná banka, ich zabezpečenie sa radí k tým vyšším.

ČSOB ponúka síce zabezpečenie pomocou mena a hesla, je však doplnené autorizačnou SMS. Ako alternatívu používa autentizáciu čipovou kartou s certifikátom.
KB využíva vysoké zabezpečenie prostredníctvom certifikátov, či už certifikát v súbore alebo na čipovej karte. Certifikáty sú chránené heslami a jediný spôsob zneužitia je pri strate nosiča certifikátu. Taktiež bezpečnostné informácie a limit sú na vysokej úrovni.

Raiffeisenbank využíva podobne ako Sberbank zabezpečenie prostredníctvom elektronických kľúčov, takže ju môžeme zaradiť medzi banku s najlepším zabezpečením pomocou autentizácie. No na rozdiel od ostatných subjektov, bezpečnostné informácie nenájdeme pri prihlasovaní do aplikácie. K týmto pokynom a aktualitám sa musíme preklikávať. Bezpečnostný limit pre automatické odhlásenie banka nevyužíva. Kvôli týmto nedokonalostiam sa banka prepadla až na štvrté miesto.

Tab. 8 Prehľad vybraných bánk

| Banka | Autentizácia | Body | Umiestnenie |
|---|---|---|---|
| **ČSOB** | Meno a heslo, SMS, čipová karta | 3,66 | 3. |
| **KB** | Certifikát | 4,16 | 2. |
| **Raiffeisenbank** | Meno a heslo, elektronický kľúč | 2,99 | 4. |
| **AirBank** | Meno a heslo | 2,33 | 5. |
| **Sberbank** | Elektronický kľúč, certifikát | 4,83 | 1. |

Ako návrh pre zvýšenie zabezpečenia autentizácie internetového bankovníctva som vybral trojfaktorovú autentizáciu, ktorá je vyšším stupňom doposiaľ používanej dvojfaktorovej, a maximom, ktoré môžeme využiť. Tento vyšší stupeň predstavuje zakomponovanie biometrického systému do systému zabezpečenia.

V kapitole 6 som predstavil niektoré z biometrík, ktoré sú použiteľné ako súčasť trojfaktorovej autentizácie. Následne som ich na základe viacerých kritérií porovnal, ohodnotil a vybral najlepšie riešenie z ponúkaných možností.

Zavedenie tohto systému do praxe by znamenalo na strane banky zakúpenie či vytvorenie potrebného softwaru, vytvorenie manuálu na používanie systému, propagačné materiály, zaškolenie pracovníkov a iné. To všetko sprevádzané zvýšenými nákladmi, čo by sa odrazilo v cenách služieb bánk. Na strane klientov by to znamenalo zakúpenie potrebného príslušenstva, zaškolenie zamestnancami banky, možné predĺženie prihlasovania sa do systému. Uplatnenie trojfaktorovej autentizácie by znamenalo zníženie úspešných pokusov o preniknutie do systému.

# 9 Záver

V literárnej rešerši sme sa oboznámili s formami komunikácie, ktoré využívajú banky pre interakciu so svojimi klientmi a taktiež metódy sociálneho inžinierstva, ktoré využívajú hackeri na prelomenie zabezpečenia tejto komunikácie s cieľom získať súkromné a citlivé informácie či peniaze pre svoj prospech.

Hlavným cieľom tejto bakalárskej práce bolo zhodnotiť súčasný stav zabezpečenia internetového bankovníctva vo vybraných finančných inštitúciách Českej republiky. Zamerali sme sa najmä na zabezpečenie internetbankingu zo strany klienta práve preto, že je najviac zraniteľná. K vybraným bankám sme pristupovali najprv jednotlivo a to zanalyzovaním ich zabezpečenia. Následne sme pre ich porovnanie využili metódu viackritérialneho rozhodovania. Boli vybrané 3 kritéria zabezpečenia, a to autentizácia, informačná bezpečnosť a bezpečnostný limit pre automatické odhlásenie. Jednotlivým kritériám sme určili váhy podľa ich dôležitosti. Pridelili sme im body podľa kvality, samostatne pre každú banku. Po dodatočných výpočtoch sme mohli vidieť, že najhoršie zabezpečenie z vybraných finančných inštitúcií má AirBank a naopak najlepšie dopadla Sberbank.

Doplňujúcim cieľom bolo celkovo zhodnotiť systém zabezpečenia a navrhnúť riešenie pre zvýšenie bezpečnosti. Celkovo hodnotím zabezpečenie bánk pozitívne. Každá banka ponúka (minimálne voliteľne) dvojfaktorovú autentizáciu, ktorá je zatiaľ využívaným maximom v možnostiach zabezpečenia. Avšak, čo je dnes vysoké zabezpečenie, zajtra už nemusí byť dostačujúce. Tak ako hackeri zlepšujú a inovujú svoje techniky prenikania systémom zabezpečenie, je potrebné viac a viac zvyšovať bezpečnosť. Našim návrhom je zvýšiť dvojfaktorovú autentizáciu na trojfaktorovú s pomocou využitia biometrických systémov. V kapitole 6 sme sa zoznámili s niektorými formami biometrie a na základe zhodnotenia viacerých kritérií týchto biometrík sme vybrali ako najvhodnejšie formy odtlačok prsta a snímanie očnej dúhovky. Taktiež by sa mali banky sústrediť na školenie svojich zamestnancov a na zvyšovanie informovanosti klientov v oblasti bezpečného používania internetového bankovníctva, či už prostredníctvom mailov alebo školení verejnosti.

Aj keď ešte žiadna väčšia banka tento systém nevyužíva, myslím si, že navrhnuté riešenie bude vďaka technologickému pokroku možné využiť v praxi bez väčších problémov.

Podobný systém založený na trojfaktorovej autentizácii by sa mal totiž začať využívať v indickom bankovom sektore. Do 30. júna by mali prejsť na biometrickú autentifikáciu založenú na Aadhaar systéme pre elektronické platobné transakcie. (India's Banks Must Move to Aadhaar-Based Biometric Authentication, 2017)

# 10Literatura

*5 most dangerous computer viruses of all time*. TechWorm [online]. Kavita Iyer, 2017 [cit. 2017-04-10]. Dostupné z: https://www.techworm.net/2016/02/5-most-dangerous-computer-viruses-of-all-time.html

*10 Most Destructive Computer Viruses*. HONGKIAT [online]. Azwan Jamaluddin [cit. 2017-04-10]. Dostupné z: http://www.hongkiat.com/blog/famous-malicious-computer-viruses/

*Bezpečnost a soukromí*. Airban*k* [online]. [cit. 2016-11-30]. Dostupné z: https://www.airbank.cz/co-vas-nejvic-zajima/rubrika/bezpecnost-a-soukromi

*Bezpečnost internetového bankovnictví*. Raiffeisen BANK [online]. [cit. 2016-12-01]. Dostupné z: https://www.rb.cz/informacni-servis/doplnkove-informace-k-produktum/bezpecne-bankovnictvi/bezpecnost-internetoveho-bankovnictvi

*Biometrické systémy zaměřené na rozpoznávání tváře, jejich spolehlivost a základní metody pro jejich tvorbu*. *Posterus* [online]. SULOVSKÁ KATEŘINA, 2011 [cit. 2016-12-08]. Dostupné z: http://www.posterus.sk/?p=11511

*Biometrie otisku prstu.* Biometric [online]. [cit. 2016-12-08]. Dostupné z: http://www.biometricke-ctecky.cz/biometriky/otisk-prstu/

BITTO, ONDŘEJ. *Šifrování a biometrika, aneb, Tajemné bity a dotyky*. Kralice na Hané: Computer Media, 2005. ISBN 80-86686-48-5

Certifikáty. *KB* [online]. [cit. 2016-11-30]. Dostupné z: https://www.kb.cz/cs/prime-bankovnictvi/certifikaty/vyzvednuti-a-prodlouzeni-certifikatu/

*Co je internetové bankovnictví*. Peníze.cz [online]. [cit. 2016-10-21]. Dostupné z: http://www.penize.cz/80347-co-je-internetove-bankovnictvi

*Co je sociální inženýrství?* PCWorld [online]. KUNEŠ J., 2012 [cit. 2016-10-15]. Dostupné z: http://pcworld.cz/internet/co-je-socialni-inzenyrstvi-1-dil-44361

*Co je to SCAM 419*. SCAM419 [online]. JOSEF DŽUBÁK & HOAX.CZ [cit. 2016-10-20]. Dostupné z: http://hoax.cz/scam419/co-je-to-scam-419

DRAHANSKÝ, MARTIN A FILIP ORSÁG. *Biometrie*. [Brno: M. Drahanský], 2011. ISBN 978-80-254-8979-6.

DVOŘÁK, PETR. *Bankovnictví pro bankéře a klienty*. Praha: Linde, 2005. Vysokoškolská učebnice. ISBN 80-7201-515-X.

HANÁČEK, PETR. *Bezpečnost informačních systémů: metodická příručka zabezpečování produktů a systémů budovaných na bázi informačních technologií*. Praha: Úřad pro státní informační systém, 2000. ISBN 80-238-5400-3.

*Historie společnosti*. KB [online]. [cit. 2016-11-30]. Dostupné z: https://www.kb.cz/cs/o-bance/o-nas/historie-spolecnosti/

*India's Banks Must Move to Aadhaar-Based Biometric Authentication*. BANK INFO SECURITY [online]. Geetha Nandikotkur, 2017 [cit. 2017-04-30]. Dostupné z: http://www.bankinfosecurity.com/indias-banks-must-move-to-aadhaar-based-biometric-authentication-a-9785

*Internetové bankovnictví*. Měšec.cz [online]. [cit. 2016-10-22]. Dostupné z: http://www.mesec.cz/bankovni-ucty/prime-bankovnictvi/internetove-bankovnictvi/pruvodce/

JAKOBSSON, MARKUS. A STEVEN MYERS. *Phishing and countermeasures: understanding the increasing problem of electronic identity theft*. Hoboken, N.J.: Wiley-Interscience, c2007. ISBN 9780471782452.

*Jak je to s bezpečností internetového bankovnictví?* Lupa.cz [online]. 2006 [cit. 2016-11-25]. Dostupné z: http://www.lupa.cz/clanky/jak-je-to-s-bezpecnosti-internetoveho-bankovnictvi/

JAMES, LANCE. *Phishing bez záhad*. Praha: Grada, 2007. ISBN 978-80-247-1766-1.

*Kaspersky Lab: Čo nás čaká v roku 2017? Útoky, ktoré nezanechajú stopy….* Android portal [online]. 2016 [cit. 2016-12-13]. Dostupné z: http://androidportal.zoznam.sk/2016/11/kaspersky-lab-co-caka-rok-2017-utoky-nezanechaju-stopy/

KOHOUT, ROMAN A RADEK KARCHŇÁK. *Bezpečnost v on-line prostředí.* Karlovy Vary: Biblio Karlovy Vary, z.s., 2016. ISBN 978-80-260-9543-9.

*Kyberzločinci útočia so zámerom znásobiť svoj zisk*. Webnoviny.sk [online]. WBN/PR, 2016 [cit. 2016-12-13]. Dostupné z: http://www.webnoviny.sk/slovensko/clanok/1123651-kyberzlocinci-utocia-so-zamerom-znasobit-svoj-zisk/

MATYÁŠ, VAŠEK A JAN KRHOVJÁK. *Autorizace elektronických transakcí a autentizace dat i uživatelů*. Brno: Masarykova univerzita, 2008. ISBN 978-80-210-4556-9.

MÁČE, MIROSLAV. *Platební styk: klasický a elektronický*. Praha: Grada, 2006. Osobní a rodinné finance. ISBN 80-247-1725-5.

MITNICK, KEVIN D. A WILLIAM L. SIMON. *Umění klamu*. Gliwice: Helion, 2003. ISBN 83-7361-210-6.

*Napáchali miliónové škody: Toto je 5 najničivejších vírusov histórie*. Živé [online]. MOLČAN ĽUBOŠ, 2016 [cit. 2016-12-13]. Dostupné z: http://www.zive.sk/clanok/117288/napachali-milionove-skody-toto-je-5-najnicivejsich-virusov-historie

*O ČSOB a skupině*. ČSOB [online]. [cit. 2016-11-30]. Dostupné z: https://www.csob.cz/portal/o-csob/o-csob-a-kbc/o-csob-a-skupine

*O první bance, kterou můžete mít rádi*. Air Bank [online]. [cit. 2016-12-01]. Dostupné z: https://www.airbank.cz/o-air-bank/

*Představení banky*. Sberbank [online]. [cit. 2016-12-01]. Dostupné z: https://www.sberbankcz.cz/o-bance/predstaveni-banky

*Profil a historie Raiffeseinbank v ČR*. Raiffeisen BANK [online]. [cit. 2016-12-01]. Dostupné z: https://www.rb.cz/o-nas/o-spolecnosti/profil-a-historie-raiffeisenbank-v-cr

PŘÁDKA, MICHAL A JAN KALA. *Elektronické bankovnictví: rady a tipy*. Praha: Computer Press, 2000. Praxe manažera. ISBN 80-7226-328-5.

*Sberbank Online Banking: Jak jej zvládnout*. Sberbank Online Banking [online pdf]. [cit. 2016-11-30]. Dostupné z: https://ob.sberbankcz.cz/VBCZIBS32/ControllerServlet

SCHLOSSBERGER, OTAKAR A LADISLAV HOZÁK. *Elektronické platební prostředky*. Praha: Bankovní institut vysoká škola, 2005. ISBN 80-7265-073-4.

*Sociální inženýrství*. Security-Portal.cz [online]. 2004 [cit. 2016-10-16]. Dostupné z: http://www.security-portal.cz/clanky/soci%C3%A1ln%C3%AD-in%C5%BEen%C3%BDrstv%C3%AD

*Sociální inženýrství*. Národní centrum kybernetické bezpečnosti [online]. [cit. 2016-10-16]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/doporuceni/2486-socialni-inzenyrstvi/

*S internetem šetřím svůj čas a peníze*: *ČSOB InternetBanking 24*. ČSOB [online]. [cit. 2016-11-30]. Dostupné z: https://www.csob.cz/portal/documents/10710/36574/csob-ib24-prirucka-zkrac.pdf

*The Most Destructive Malware of All Time*. The DATACENTER Journal [online]. Lauren Sporck, 2015 [cit. 2017-04-10]. Dostupné z: http://www.datacenterjournal.com/most-destructive-malware-of-all-time/

*The Social Engineering Framework: Pretexting*. Security through education [online]. [cit. 2016-10-20]. Dostupné z: http://www.social-engineer.org/framework/influencing-others/pretexting/

*Většina Čechů očekává v budoucnu větší využití biometrie v bankovnictví.* Měšec.cz [online]. Doskočilová V., 2016 [cit. 2016-11-30]. Dostupné z: http://www.mesec.cz/aktuality/vetsina-cechu-ocekava-v-budoucnu-vetsi-vyuziti-biometrie-v-bankovnictvi/

*Volksbank CZ, a.s. se mění na Sberbank CZ, a.s*. Sberbank [online]. [cit. 2016-12-01]. Dostupné z: https://www.sberbankcz.cz/novinky/oznameni-rebranding

# 11Seznam obrázků

# 12 Seznam tabulek