Bezpečnosť informačných technológií v bankovníctve

Erik Fogaš

Bakalářská práce
2016

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2015/2016

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Erik Fogaš**
Osobní číslo:	**A13010**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Bezpečnost informačních technologií v bankovnictví**
Téma anglicky:	**The Safety of Information Technology in the Banking Sector**

Zásady pro vypracování:

1. **Zpracujte rešerši literatury a pramenů, které se vztahují ke zpracovávanému tématu.**
2. **Vymezte zkoumanou oblast (fenomenologie, etiologie) včetně právních aspektů, sociálních a historických souvislostí.**
3. **Analyzujte a charakterizujte moderní trendy a postupy, které jsou využívány k eliminaci vnitřních a vnějších bezpečnostních hrozeb v bankovním sektoru.**
4. **Tvůrčí část bakalářské práce zaměřte na syntézu; výstupy výzkumu a analytické části využijte pro vlastní návrhy a opatření, výstupy zpracujte do grafů a tabulek.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **BRABEC, F. Ochrana bezpečnosti podniku. Praha: Eurounion spol. s r.o., 1996. 203 s. ISBN 80-85858-29-0.**
2. **DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. vyd. Brno : Computer Press, 2004. 187 s. ISBN 80-251-0106-1.**
3. **JAŠEK, Roman. Informační a datová bezpečnost. Zlín: Univerzita Tomáše Bati ve Zlíně. Fakulta managementu a ekonomiky, 2006.140 s.ISBN 80-7318-456-7.**
4. **LÁTAL, Ivo. Ochrana informací, dat a počítačových systémů. 1. vyd. Praha: Eurounion, 1996, 238 s. ISBN 80-85858-32-0.**
5. **MATĚJKA, Michal. Počítačová kriminalita. Vyd. 1. Praha: Computer Press, 2002, x, 106 s. ISBN 80-7226-419-2.**
6. **POŽÁR, Josef. Informační bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005, 309 s. Vysokoškolské učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 80-86898-38-5.**

Vedoucí bakalářské práce: **PhDr. Mgr. Stanislav Zelinka**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **23. února 2016**

Termín odevzdání bakalářské práce: **30. května 2016**

Ve Zlíně dne 16. února 2016

L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Jan Valouch, Ph.D.
ředitel ústavu

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně, dne …….

podpis diplomanta

ABSTRAKT

Úvod bakalárskej práce je venovaný informačnej bezpečnosti v bankovníctve a vymedzením jej pojmov. Ďalej práca špecifikuje najčastejšie hrozby a využívané programy na ohrozenie bezpečnosti v bankovom sektore. V praktickej časti sa práca zaoberá analýzou zabezpečenia významných bánk na Slovensku. Záver je zameraný na nový návrh autentizácie a autorizácie pomocou použitia biometrických systémov.

Klíčová slova:

bankovníctvo, bezpečnosť, internetbanking, hrozby, platobné karty, smartbanking, autentizácia, autorizácia

ABSTRACT

The introduction of this bachelor's thesis presents the protection of information systems in banking and explanation of important terms. In the following part, the thesis particularize the most common threats and programms, which can be used to endanger the security of banking sector. In the practical part, the thesis looks more into the security of important banks in Slovakia. The conclusion focuses on authentization and authorisation through the use of biometric systems.

Keywords:

banking, safety, internet banking, threats, payment card, smartbanking, authentication, authorization

Poďakovanie

Týmto by som sa chcel poďakovať vedúcemu bakalárskej práce pánovi PhDr. Mgr. Stanislavovi Zelinkovi za cenné rady, pripomienky a odborné vedenie v priebehu spracovania tejto bakalárskej práce. Ďalej patrí poďakovanie mojím rodičom za podporu počas štúdia.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Žijeme v dobe, ktorá ide neustále dopredu, vyvíjajú sa nové technológie, o ktorých ľudia nemajú žiadne predstavy. Z roka na rok prichádzajú nové informačné technológie, ktoré prechádzajú každým rokom veľkým vývojom. Rovnako ako sa vyvíjajú informačné technológie vo všetkých odvetviach, je tomu tak aj v bankovom sektore. Sektor, ako sú banky je veľmi dôležitý, preto sú nútení, aby sa prispôsobovali technickému vývoju. Je to spôsobené tým, že v dnešnej dobe existuje niekoľko bánk, ktoré si konkurujú a rovnako je to aj zo strany požiadaviek od ich klientov. Ľudia čoraz viac využívajú elektronické bankovníctvo. Môže ísť o vyberanie peňazí z bankomatov alebo transfer peňazí pomocou internetového bankovníctva a ku kontrole zostatkov na účte. V súčasnosti sú banky u ľudí veľmi obľúbené a určite tomu bude tak aj naďalej. Obľúbenosť bude neustále narastať.

Cieľom bakalárskej práce je spracovanie problematiky bezpečnosti internetového bankovníctva a poukázať na riziká, ktoré prináša. Pokúsime sa predstaviť a ukázať pravidlá, ktoré by mali zamedziť vzniku prichádzajúcich rizík. Tieto riziká môžu ohroziť banku, tak aj ich klientov.

Bakalárska práca tvorí päť kapitol. V prvej kapitole sú popísané a vymedzené základné pojmy, popisujúce informačnú bezpečnosť, systém spolu s procesom a na záver šifrovanie.

Druhá kapitola je zameraná na právny rámec bezpečnosti a nábeh moderného bankovníctva v porovnaní s minulosťou. Ďalej popisuje zabezpečenie osobných dát a informácií, kde sa zameriavame na pojem autentizácia a jej druhy a ukázať užívateľovi, ako zaobchádzať s citlivými údajmi. Sú tu popísané programy, ktoré sa využívajú na ohrozenie bezpečnosti a vymedzenie pravidiel v sieti internet.

V tretej kapitole sú rozoberané hrozby a riziká. Začiatok poukazuje na zabezpečenie prenosu dát a spôsoby autentizácie, ktoré banky v súčasnosti využívajú. Spomenuté a rozobrané sú aj spôsoby prelomu bezpečnosti.

Praktická časť je zameraná na analýzu bezpečnosti internetového bankovníctva v piatich najznámejších bankách na Slovensku. Ich základné zabezpečenie je spracované v tabuľkách. Posledná časť je zameraná na internetové bankovníctvo, smartbanking, bezkontaktné platobné karty a bankomaty, kde sú nové návrhy a opatrenia, v ktorých sú popísané výhody a nevýhody dnešného zabezpečenia a následne nového modelového návrhu.

I. TEORETICKÁ ČASŤ

1 INFORMAČNÁ BEZPEČNOSŤ

Každý jeden z nás si môže pojem bezpečnosť vysvetliť inak. Záleží, akú bezpečnosť má na mysli. Dokážeme sa ale zhodnúť, že bezpečnosť nám zaručuje určitý druh istoty a zmenšuje ľuďom cítenie na možné ohrozenie. Každý sa chce cítiť bezpečne po celý svoj život. Existujú tri skupiny, do ktorých môžeme zaradiť ochranu.

1. život, zdravie,
2. majetok (hmotný aj nehmotný, každý majetok, ktorý má určitý vzťah k predmetom),
3. informácie, dáta, znalosti [1].

Ľudia si myslia, že keď používajú dostatočne silné heslá, tak to stačí pre zabezpečenie informačných systémov. Dôležité je zabezpečiť systém ako jeden celok. Vonkajšie a vnútorné ohrozenie je priamo úmerné kvalite, ktorá je prevádzaná bezpečnostnou politikou každého štátu. Bezpečnostnú politiku je možné definovať ako analýza bezpečnostných hrozieb a rizík, v rámci možnosti výberu a v poslednom rade efektivita protiopatrení ku zníženiu rizík. Každý štát sa snaží reagovať na dynamický, ale aj dramatický vývoj bezpečnostného prostredia v uplynulom období.

Zvyšovanie rýchlosti a kvality informačného procesu má na starosti rýchle rozšírenie informačných a komunikačných technológií. Preto je veľmi potrebné, aby sa dbalo na pozornosť a dostatočne sa venovať ochrane dát a informácií v informačných systémoch. Netreba zabúdať ani na útočníkov, ktorí sa tiež snažia a hľadajú nové spôsoby a cesty útokov na informačné systémy za cieľom zničenia, zmeny alebo snahu dostať sa do týchto systémov. V súčasnej dobe sa jedná o trestnú činnosť, ktorá sa nazýva kybernetická kriminalita. Táto kriminalita ohrozuje dôležité pojmy, ako sú dôvernosť, integrita a dostupnosť počítačových systémov. Nejedná sa len o tieto, ale spadá sem aj bezpečnosť rozhodujúca o kritických infraštruktúrach štátu. Rýchlosťou akou sa vyvíjajú dnešné technológie vznikajú rôzne druhy problémov, ktoré vyplývajú z kybernetickej kriminality a odrážajú rozdiely v znalostiach. Nastávajú tu zložité forenzné problémy, ktorým musia vyšetrovatelia a štátny zástupcovia čeliť. Je to kvôli tomu, pretože digitálne procesy vznikli s nehmotnou a prechodnou povahou digitálnych dôkazov. Okrem toho je potrebné zmysluplné vyšetrovanie a stíhanie kybernetickej kriminality, časté sledovanie kriminálnych aktivít, ktoré môžu vychádzať aj za hranice štátu, čo ďalej komplikuje situáciu a vedeniu otázkam týkajúcich sa právomocí.

Informačná bezpečnosť je označenie pre aktivitu, ktorá smeruje k ochrane informácií. Jedná sa o ochranu informácií a dát pred negatívnymi udalosťami. Jedná sa o stratu, úniku, odcudzeniu, zneužitiu, zničeniu, zmeny alebo narušeniu celistvosti, dôvernosti a dostupnosti. Chránené informácie môžu mať rozličnú podobu napr. môže ísť o elektronickú, tlačenú, ale existujú aj také informácie, ktoré je možné odpozorovať z logistických procesov. Zneužitie informácie hrozí nielen z vonkajšieho prostredia, ale vo väčšej miere sem spadá aj vnútorné prostredie (organizácia). Informácie sú pre organizáciu kľúčovým zdrojom. Pokiaľ by sme o ne prišli, v inom prípade, ak by sa informácie dostali do rúk konkurencie, dalo by sa to nazvať ako koniec fungovania a podnikania. O informácie môžeme prísť na svojom počítači, na serveri, alebo počítačovej sieti. Informačnú bezpečnosť možno označiť ako celkový pohľad na organizáciu, ktorá pomáha spoznávať a chrániť si svoje dáta. Snaží sa nasmerovať k praktickým opatreniam a k eliminácií zníženia škôd, pri mimoriadnych udalostiach. Informačná bezpečnosť chráni informácie ako celok. Je potrebné vytýčiť a pochopiť, aké informácie daná organizácia má a aká je ich hodnota. Súčasťou informačnej bezpečnosti, je riadenie bezpečnosti. Je potrebné si uvedomiť fungovanie organizácie a na základe toho navrhnúť fungujúci a efektívny systém riadenia informačnej bezpečnosti. Ďalším faktorom je aj dlhodobá funkčnosť a rozvoj systému, ktorý bude reagovať na zmeny organizácie a jej okolia. Pomocou zavedenia dobre fungujúceho systému, je možné minimalizovať riziká patriace k úniku informácií. Ďalej tento systém pomáha znižovať náklady na informačné a komunikačné technológie a následnej efektivite procesov. Veľkú úlohu zohráva aj pri rozhodovacích procesoch. Tieto systémy riadenia, by mali zlepšiť situáciu v interných službách a procesov a navyše procesov a služieb pre klientov organizácie alebo štátnej inštitúcie. Okruhy činností riadenia informačnej bezpečnosti v organizácií [2]:

1. **Potrebné si stanoviť pravidlá so zachádzaním s informáciami** - kto, kedy, ako, prečo má prístup k dátam alebo informáciám.
2. **Stanovenie riadenia prístupu k dátam a informáciám** - potrebné vedieť, kto ku ktorým informáciám môže a kto nesmie. Vedieť, či je ochrana proti podvodom.
3. **Riešiť bezpečnosť zariadení proti strate a odcudzeniu** - pracovník stratí alebo mu ukradli počítač, je potrebné vedieť, čo sa stane. Mal dáta zálohované?
4. **Ochrana proti napadnutiu alebo odcudzeniu informácií** - rieši otázku o dostatočnom zabezpečení siete proti kybernetickým útokom.

5. **Uložené dáta z pohľadu havárie** - ochrana proti haváriám, zničenie serverov (požiar, kolaps disku), schopnosť obnoviť dáta [3].

Riadenie informačnej bezpečnosti má na zodpovednosť manažér bezpečnosti (CSO). Vlastník, štatutárny orgán organizácie má najvyššiu zodpovednosť [3].

1.1 Základné pojmy informačnej bezpečnosti

Do informačnej bezpečnosti zasahuje mnoho nových pojmov a definícií, preto je potrebné si tieto definície vysvetliť a hlavne správne pochopiť danú problematiku. Informačné systémy sú ohrozované väčším množstvom hrozieb a je potrebné dopredu vedieť, že im hrozí nebezpečie. Ak dôjde k poškodeniu, ktoré bolo spôsobené prírodnými vplyvmi, dokážeme ho rýchlo zistiť. Pokiaľ by došlo k nelegálnemu úniku informácií alebo dát, tak veľmi ťažko by sa dokazoval únik. V prípade, že k úniku dôjde, tak majiteľ informačného systému nechce o tom komunikovať, pretože sa skresľujú informácie a z danej situácie vyplynie, že o nič nejde. Útoky preto bývajú neodhalené a ak sa aj podarí časť útokov odhaliť, tak nikdy sa nedostanú k verejnosti, aby ten, kto sa postaral o únik informácií, nevedel k akému úspechu sa dopracoval a pokiaľ ide o užívateľa, tak ten nechce stratiť svoju dobrú povesť.

1.1.1 Aktívum

Medzi aktíva sa zaraďujú všetky hmotné, ale i nehmotné majetky. Pre majiteľa v organizácií v informačnom systéme je aktívum všetko, čo má pre neho určitú hodnotu. Pre každého človeka, majiteľa organizácie sú najväčšou hodnotou dáta a informácie. Pokiaľ by o ne prišiel ,alebo by boli zneužité na iné účely, danej osobe alebo majiteľovi by spôsobili obrovské škody. Preto by malo byť každé aktívum vhodným spôsobom chránené. Aktíva sa rozdeľujú na hmotné a nehmotné.

Hmotné aktíva vznikajú za pomoci výpočtovej techniky a komunikačnými technológiami (počítače, diskové pole, servery, aktívne sieťové prvky). Pokiaľ by majiteľ potreboval zistiť hodnotu týchto aktív, zistí to jednoducho a to stanovením ich obstarávacej ceny.

Medzi nehmotné aktíva sa zaraďujú dáta a programové vybavenie. Nie sú to žiadne veci fyzického druhu. Sú to napríklad operačné systémy, patenty, ochranné známky, programové nástroje pre riadenie informačného systému a v poslednom rade aplikačné programy. Dôležitou súčasťou nehmotných aktív je dátová základňa [4].

1.1.2 Bezpečnosť

Vo všeobecnosti pomenováva stav, keď pri vykonávaní bežnej práce alebo s čím sa stretávame nespôsobuje ujmu, v prípade možnej ujmy je minimalizovaná a je akceptovateľná. Ide o vlastnosť objektu, subjektu, ktorá určí stupeň ochrany proti škodám, ktoré môžu vzniknúť.

1.1.3 Hrozba

Hrozbu možno definovať ako udalosť, ktorá môže pôsobením spôsobovať narušenie dôvernosti, hodnotu aktíva, integritu. Hrozba často poukazuje na objektívny jav, ktorý je identifikovateľný a reálne začína deštrukčne pôsobiť. Hrozby môžu spúšťať ako ľudia, tak aj vplyv techniky (porucha zariadenia) alebo prírodné javy (voda, oheň). Medzi ľudské hrozby patria teroristi, zločinci (jednotlivci, skupina) a nadšenci do počítačových systémov [5].

1.1.4 Ocenenie rizík

Pri ocenení rizík sa vyhodnocujú hrozby, ktoré môžu určitým spôsobom napádať informačný systém. Pokiaľ by hrozilo, že systém bude reálne vystavený určitému riziku, musí dokázať definovať úroveň tohto rizika, ktoré môže nastať a včas ho minimalizovať alebo dokázať mu zabrániť. Hlavným cieľom ocenenia rizík je zisťovanie, či zavedené bezpečnostné opatrenia vyhovujú a sú dostatočne silné nato, aby vedeli zredukovať pravdepodobnosť vzniku škody, ktorá bude v daný okamih prijateľná [5].

1.1.5 Riziko

Riziko je pojem, ktorým sa dá označiť, že hrozba zneužije zraniteľnosť a môže spôsobiť narušenie integrity. Rovnako môže spôsobiť dostupnosť aktív. Ide o výraz, akou pravdepodobnosťou bude aktívum poškodené alebo zničené vďaka pôsobením konkrétnej hrozby a výsledok je často rozdielny ako bol očakávaný.

1.1.6 Zraniteľnosť

V každom systéme existuje daná zraniteľnosť, ktorá určuje slabú časť celého bezpečnostného systému. Nemusí ísť vždy len o celý bezpečnostný systém, ale môže ísť len o jeho časť. Ak dôjde k poškodeniu, v horšom prípade zničeniu hodnôt alebo aktíva, môžeme určiť, že slabá časť bezpečnostného systému bola zneužitá hrozbou.

1.2 Informačný systém

Je to súbor ľudí, zdrojov, užívateľov zameraných na technické prostriedky a metódy , ktoré zabezpečujú prenos a spracovanie dát. Ich účelom je tvorba informácií. Systémy nás dennodenne obklopujú bez toho, aby sme si to výrazným spôsobom uvedomili. Označuje sa ako určitou abstrakciou reálneho objektu. Táto abstrakcia sa dá definovať pri rešpektovaní vytýčeného cieľa prvkami a väzbami medzi nimi. Za spoločné znaky sa dajú nazvať prvky systému, ktoré môžu byť súčasne systémom nižšieho radu, ale aj systémy, ktoré môžu byť súčasným prvkom systému vyššieho radu. Nielen v informačnom systéme, ale aj u akéhokoľvek iného systému rozlišujeme dve základné vlastnosti:

1. Štruktúru systému,
2. Fungovanie systému [2].

Štruktúru systému je možné chápať ako spôsob usporiadania jednotlivých prvkov systému a väzieb medzi nimi. Čiže nejde len o náhodný, ľubovoľný chaoticky rozhádzaný súhrn prvkov. Každý prvok má presné vymedzenie miesta (nadriadenosť alebo podriadenosť). Fungovanie systému sa dá rozumieť ako závislosť medzi podnetmi a reakciami. Podnety na systémy nemusia pochádzať priamo z okolitého prostredia. Ich zdrojom môže byť sám systém. Pokiaľ ide o tieto podnety, hovoríme o podnetoch vnútorných, ktorými je systém ovplyvňovaný a môže naň odlišne reagovať. Informačný systém sa nám môže zdať veľmi jednoduchý. Dokážeme si ho sami ovládať bez akéhokoľvek zložitého technického vybavenia. Po čase nám budú informácie a dáta pribúdať a na ich spracovanie, ukladanie je potrebné nájsť výkonnejšie informačné technológie. Zistíme, že takýto prístup nám nemôže stačiť. Každý informačný systém by mal v sebe obsahovať aspoň základnú tvorbu databáze, ktorá je na systémovej úrovni. V nej majú súbory definované svoje štruktúry. Tieto databázy musia byť chránené, aby sa k nim nedostala neoprávnená osoba, ktorá by mohla obsah databáz zmeniť. Ďalšou dôležitou vecou informačného systému je systém, ktorý chráni integritu údajov. Napríklad ak ide o transakciu, musí byť dokončená aj v prípade, ak by došlo k výpadku elektriny alebo pri poruche počítača. Väčšinou viacerí užívatelia pracujú so súbormi v rovnakom čase, preto je potrebné, aby systém obsahoval zdieľaný prístup k údajom. Systém musí vedieť odstraňovať prebytočnosti a to docieli tým, že sa budú vytvárať zložitejšie hierarchické dátové štruktúry na základe prepájania údajov z viacerých súborov [2].

1.3 Informačný proces

Pod týmto procesom sa vykonávajú pracovné činnosti s informáciami. Menia sa tu procesy, činnosti a chovanie celej organizácie. Ide o uzavretý cyklus, kde informácie vznikajú až ku svojmu použitiu. Pomocou informačného systému je zabezpečovaný informačný proces, kde patrí sled operácií s dátami a informáciami, ktoré obsahujú určité kroky:

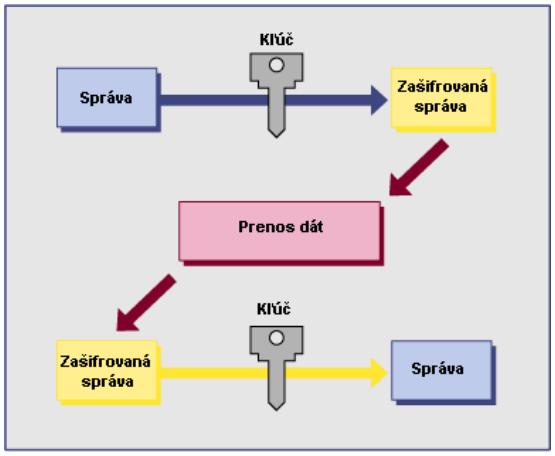
- Zisk informácií,
- Prenos informácií (od zdroja po miesto spracovania),
- Určitú registráciu, na ktorom mieste boli spracované,
- Ukladanie informácií pre prácu do budúcnosti,
- Spracovanie informácií, kam spadá triedenie a posudzovanie kvality vlastností, ale aj vyhľadávanie doplnkových informácií a tvorba nových informácií,
- Využívanie informácií [2].

1.4 Šifrovanie

Šifrovacie techniky je možné použiť pri citlivých údajoch, dátach. Týmto sa výrazným spôsobom docieli zníženie rizika a alebo jeho odstránenie. V prípade, že útočník získa citlivé dáta, informácie vďaka šifrovaniu nebude možné tieto dáta vyzradiť. Čiže nastáva tu šifrovací algoritmus, ktorý utajuje dáta pomocou šifrovacích kľúčov tzn., že ich potom nejde prečítať a následne sú pre nás nezrozumiteľné.

1.4.1 Symetrické šifrovanie

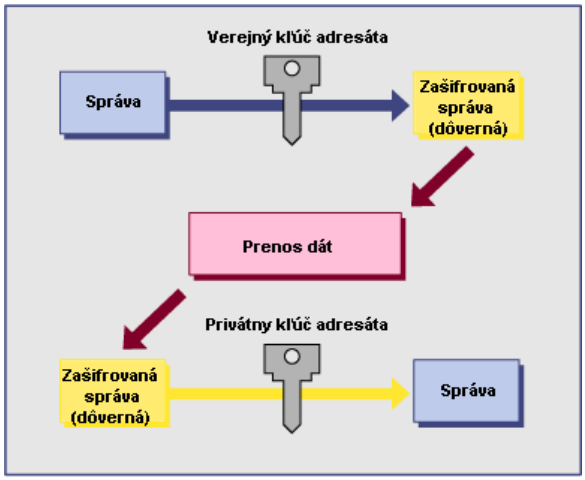
Ak sa použije na zašifrovanie a dešifrovanie správy symetrické šifrovanie je potrebné, aby ten kto odosielal správu a následne ten kto ju prijme použili rovnaký tajný kľúč. Zabezpečenie prenosu doručenia kľúča je veľmi podstatné, aby sa kľúč nedostal do nepovoleného vlastníctva. K známym symetrickým metódam patrí napr. algoritmus DES, 3DES, Blowfish, IDEA, RC4. Odporúča sa používať RC4 alebo AES, ktoré majú dĺžku kľúča 128-256 bitov. Výhodou je ich rýchlosť a nenáročnosť na výpočtovú techniku. Nevýhodou je zasielanie tajných kľúčov, v prípade tajnej komunikácií [2].



Obr. 1. Šifrovanie symetrickou šifrou [29]

1.4.2 Asymetrické šifrovanie

Pri asymetrickom šifrovaní sa používa jeden kľúč pre zašifrovanie a druhý pre dešifrovanie dokumentov. Správa sa zašifruje verejným kľúčom a dešifruje sa pomocou súkromného kľúča. Pokiaľ chce užívateľ, aby dostal zašifrovanú správu, musí najprv poskytnúť tento svoj verejný kľúč. Ten odosielateľ použije na zašifrovanie správy a kód odošle. Pre dešifrovanie príjemca potrebuje mať druhý kľúč z páru, svoj vlastný súkromný kľúč, ktorým dešifruje správu. Výhodou oproti symetrickým je, že nie je potrebné posielať súkromný kľúč a tak nedôjde k jeho prezradeniu. A verejný kľúč je možné dať verejnosti. Nevýhodou je ich rýchlosť oproti symetrickým. Ďalšou nevýhodou je overenie pravosti kľúča. Patria sem známe metódy ako sú RSA (Rivest-Shamir Adleman), DH (Diffie-Hellman) [2].



Obr. 2. Šifrovanie asymetrickou šifrou [29]

2 PRÁVNY RÁMEC BEZPEČNOSTI

Ochrana dát v informačných systémoch musí mať jednotný právny rámec. Pokiaľ by zákony jasne nedefinovali vzťahy medzi chránenými údajmi, ich majiteľov alebo útočníkov nebolo by možné ani trestné stíhanie. Na Slovensku zatiaľ nie je v primeranej miere premietnutý do legislatívy. Súčasný právny poriadok Slovenskej republiky obsahuje právne normy, ktoré riešia čiastkové problémy, ale právny predpis pre informačnú bezpečnosť v slovenskej legislatíve chýba. Vďaka neúplným právnym rámcom informačnej bezpečnosti sa ochrana informačných a komunikačných systémov riadi rôznymi právnymi predpismi. Výsledkom je nedostatočná úroveň ochrany informačných a komunikačných technológií [28].

2.1 Legislatívny rámec informačnej bezpečnosti

- *zákon č. 211/2000 Z. z. o slobodnom prístupe k informáciám a zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov,*
- *zákon č. 483/2001 Z. z. o bankách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,*
- *zákon č. 540/2001 Z. z. o štátnej štatistike v znení neskorších predpisov,*
- *zákon č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,*
- *zákon č. 395/2002 Z. z. o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov,*
- *zákon č. 428/2002 Z. z. o ochrane osobných údajov v znení neskorších predpisov,*
- *zákon č. 610/2003 Z. z. o elektronických komunikáciách v znení neskorších predpisov,*
- *zákon č. 618/2003 Z. z. o autorskom práve a právach súvisiacich s autorským právom v znení neskorších predpisov,*
- *zákon č. 22/2004 Z. z. o elektronickom obchode a o zmene a doplnení zákona č. 128/2002 Z. z. o štátnej kontrole vnútorného trhu vo veciach ochrany spotrebiteľa a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,*
- *zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,*
- *zákon č. 300/2005 Z. z. trestný zákon v znení neskorších predpisov,*

- *ústavný zákon č. 254/2006 Z. z. o zriadení a činnosti výboru Národnej rady Slovenskej republiky na preskúmavanie rozhodnutí Národného bezpečnostného úradu,*
- *zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,*
- *nariadenie vlády Slovenskej republiky č. 216/2004 Z. z., ktorým sa ustanovujú oblasti utajovaných skutočností,*
- *metodické usmernenie Úseku bankového dohľadu Národnej banky Slovenska č. 7/2004 k overeniu bezpečnosti informačného systému banky a pobočky zahraničnej banky*
- *výnos Ministerstva financií Slovenskej republiky z 8. septembra 2008 č. MF/013261/2008-132 o štandardoch pre informačné systémy verejnej správy, ktorý obsahuje aj bezpečnostné štandardy [28].*

Elektronický obchod upravuje zákon č. 22/2004 Z. z. o elektronickom obchode a o zmene a doplnení zákona č. 128/2002 Z. z. o štátnej kontrole vnútorného trhu vo veciach ochrany spotrebiteľa a o zmene a doplnení niektorých zákonov v znení neskorších predpisov [28].

Počítačovú kriminalitu upravuje § 247 zákona č. 300/2005 Z. z. trestný zákon v znení neskorších predpisov, do ktorého sú premietnuté princípy Dohovoru o kybernetickom zločine CETS č. 185/2001, vydanom Radou Európy [28].

2.2 Nová éra

Nástupom 21. storočia prišla doba nových technológií. Priniesla so sebou moderné komunikácie, znalosti a výpočty v oblasti informačnej bezpečnosti. Zmenilo to spôsob života, ktorým ľudia doteraz žili a neustále sa bude meniť. Radikálne sa zmení spôsob práce a ľudské premýšľanie dostane iný rozmer. V dnešnej dobe pri rýchlom náraste vysokorýchlostných sietí už je možné používať aplikácie, ktoré v minulosti nepripadali do úvahy. Výhodou je, že klesajú nároky na výpočtové výkony a s nimi aj cenová dostupnosť. Prenášať dáta, obrázky alebo iné digitálne súbory dokážeme behom niekoľkých sekúnd a to po celom svete. Táto nová technológia celkovo mení spôsob bankového sektora. V minulosti všetko išlo cez papiere, no dnes to už zmenili digitalizované súbory, čiže bankové sektory sa zmenili na digitalizované a sieťové bankové služby. Táto zmena taktiež zmenila vnútorné účtovníctvo a manažmentu systému banky. Momentálne to zásadne zmenilo doručovací systém bánk pre komunikáciu s ich zákazníkmi. Banky po celom svete

neustále čelia novým výzvam meniaceho sa prostredia, preto sa musia usilovať pre správne nájdenie technologických riešení, aby mohli prijímať stále nové výzvy. S určitou pravdepodobnosťou sa dá povedať, že s nástupom nových technológií navždy zmenia postupy a celkovo celý bankový sektor. Banky po celom svete, ktoré majú schopnosť investovať alebo integrovať informačné technológie sa vďaka tomu z nich stanú banky, ktoré so svojou dominanciou budú okupovať vysoké miesto v konkurenčnom globálnom trhu. Pracovníci bánk sú si vedomí, že investície do informačných technológií je v dnešnej dobe kritické. Investícia do informačných technológií bude mať veľmi veľký dôsledok na bankový sektor.

2.3 Technológia a transformácia bánk

Počítačová technika a samotné počítače sa dajú dnes brať ako zložitá technológia pre bežného človeka. Každým rokom stúpajú nároky na počítačovú gramotnosť a stávajú sa stále komplikovanejšími. Počítačová technika ponúkla mnohým bankám veľký potenciál a svojím bankovým klientom dala obrovské očakávania. Zamestnanci bánk, úradníci, klienti sa museli rovnako prispôsobiť týmto novým zmenám prinášajúce do bankovníctva. Moderné technológie, ktoré prešli veľkým pokrokom, umožňujú omnoho pohodlnejšie poskytovanie svojich bankových služieb svojim klientom, ako to bolo pred niekoľkými rokmi. V budúcnosti sa budú úspešné banky od seba rozlišovať rýchlym prístupom k dôležitým informáciám a schopnosťou rýchleho a efektívneho konania. Tým, že má banka priamy marketing a zodpovedné služby. Vďaka využívaniu priameho marketingu a ponúknutie zodpovedných služieb svojim klientom banky týmto získavajú konkurenčnú výhodu [6].

2.4 Zabezpečenie osobných dát a informácií

Na zabezpečenie osobných dát a informácií sa uplatnila kombinácia šifrovania citlivých údajov a dostatočná autentizácia. Táto kombinácia sa odporúča pre ľudí, ktorí chcú mať svoje dáta a komunikáciu dostatočne zabezpečenú.

2.4.1 Autentizácia

Autentizáciou sa dá označiť ako proces, pomocou ktorého sa poskytuje istá záruka identity subjektu alebo objektu. V skratke povedané, uistenie sa, že daná osoba, užívateľ je práve

ten, za koho sa vydáva. Za najlepší spôsob autentizácie sa považuje pomocou hesla. Existujú tri spôsoby identifikácie:

- Autentizácia pomocou užívateľského mena a hesla,
- Autentizácia pomocou biometrie (odtlačok prstov),
- Autentizácia pomocou tokenu alebo čipovej karty s certifikátom,
- Kombináciou všetkých spôsobov [1].

Ak ide o autentizáciu pomocou užívateľského mena a hesla, je potrebné zadať správne meno a heslo, ktoré vlastní daný užívateľ. Ide o najviac používaný systém, problém ktorý sa tu môže naskytnúť, je zabudnutie hesla alebo o zvolenie slabého hesla. Odporúčaná práca s heslom a zaobchádzanie s ním:

- Medzi hlavnú úlohu patrí ochrana hesla. Heslo nikomu neprezradiť, držať ho v tajnosti. Jednoduché účinné pravidlo,
- Zložitosť hesla je dôležitá. Jednoduché heslá a klasické menné heslá (Peter, Jano) sa neodporúčajú, pretože sú ľahko uhádnuteľné,
- Použité heslá by mali odolávať slovníkovému útoku., tzn. že na internete existujú programy, ktoré obsahujú slovník slov z rozličných jazykov. Stačí tento program spustiť a v prípade jednoduchého hesla dokáže za krátku dobu heslo odhaliť,
- Heslo by sa malo meniť v rozumných intervaloch. Menenie hesla môže zaskočiť aj útočníka, ktorý získa informácie len počas doby, kedy si užívateľ zmenil heslo. Použitie starých hesiel sa neodporúča, aby nedošlo k opätovnému prelomeniu. Útoky prebiehajú dekryptáciou zo zachytených hash hodnôt,
- Dodržovať dĺžku hesla. Heslo sa považuje za dostatočne bezpečné, ak jeho dĺžka obsahuje minimálne 14 znakov obsahujúce aj čísla. Za bezpečne silné heslo možno považovať:„Mt47&UHWx#50wK",
- Pri takomto tvare hesla pre niektorých ľudí môže byť ťažko zapamätateľné, je dôležité, aby sa heslo nenapísalo na papier ako pomôcku a prilepili ho k monitoru, čo by výrazným spôsobom uľahčilo prácu útočníkovi,
- Rovnaké heslo nepoužívať na rôznych stránkach, programoch [1].

Autentizácia pomocou biometrie je metóda, ktorá sníma jedinečné fyzické znaky ľudí. Táto metóda je však náročnejšia čo sa týka hardwaru tak aj softwaru. V minulosti tieto systémy neboli vo väčšej miere využívané, pretože technológie boli príliš drahé a

nespoľahlivé. Dnes je tomu opak, sú často využívané v rôznych organizáciách vo väčšom množstve.

Využívanie čipových kariet, magnetických kariet alebo tokenov je ďalšia možnosť autentizácie. Ide o veľmi jednoduchú autentizáciu a vyniká svojou presnosťou. Užívatelia vlastnia tieto karty a sú viazané na zadanie čísla a PIN kódu [1].

Najúčinnejšou metódou ochrany dát a informácií je ich kombinácia viacerých zložiek. Môže ísť o heslo, šifrovanie. Úspešný útok je priam nezrealizovateľný a úspešnosť útoku je minimálna. Šifrovanie má druhotný krok ochrany. Ak by mal útočník prístup do počítača, ľahko získa potrebné súbory, no ale ich obsah bude nečitateľný. Jediný spôsob, ktorý môže spraviť, je zničiť dáta, ale obsah nikdy nemôže zneužiť [1].

2.5 Útoky a úniky dát a informácií

K najčastejším útokom na dáta a informácie dochádza zo strany zamestnancov danej organizácie. Ich začiatočným spúšťačom môže byť prepustenie z firmy a tento útok berú ako pomstu a neznášanlivosť k zamestnávateľovi. Týmito útokmi môžu pre organizáciu spôsobiť obrovské škody, vynášanie citlivých informácií a následne prechod ku konkurencií. K zisku informácií sa často využívajú podplatení zamestnanci, ktorí donášajú citlivé informácie konkurencii. Ťažko sa dá vopred zistiť, že daný zamestnanec pracuje v inej organizácii. Niekedy daný zamestnanec nemá na výber a musí túto ponuku prijať a vyskytuje sa tu vydieranie. Najľahšou formou úniku dát je prostá krádež. Či už v noci vylúpením sa do firmy alebo jednoducho cez deň, pomocou technických prístrojov na odpočúvanie, tvorbu fotografií až po tie náročné drahé prístroje. Ak organizácia hľadá na dôležitý post nového zamestnanca, pri prijatí by si mala overiť, či daný človek nepracoval v minulosti u svojej konkurencií alebo náhodou jeho rodinný známy nepracuje u konkurencie, čo by mohlo ohroziť únik dát a informácií. Existujú ľudia, ktorí schválne menia zamestnanie za cieľom odnášania citlivých informácií. K technickým prostriedkom na využívanie zisku informácií sa najviac využíva mobilný telefón, ktorý sa dá jednoducho napojiť na danú linku. Obľúbené sú aj skryté mikrofóny, dosah nie je veľký, ale svoju úlohu si dokáže splniť [2].

2.5.1 Využívané programy na ohrozenie bezpečnosti

Sú to programy, ktoré sú určené nato, aby určitým spôsobom zničili dáta alebo sa snažia poškodiť dôležité operačné systémy a nakoniec aj aplikačné vybavenie. V prípade

úspešného využitia programu môžu obmedziť celý fungujúci systém a napáchať obrovské škody v organizácií.

2.5.1.1 Zadné vrátka (Trap Door)

Jedná sa o metódu, vďaka ktorej je možnosť obísť autentifikáciu, ktorá slúži aby neoprávnená osoba nemohla využívať informačné systémy. Môže sa jednať o softwarový tak aj hardwarový skrytý program. Tento mechanizmus často využívajú programátori, ktorí vyvíjajú určitú aplikáciu využívanú v bankovníctve. Ten im uľahčuje prácu pri vývoji a zdokonaľovaní programu. Preto musia byť veľmi opatrní, aby svoje pomocné kódy (príkazy) odstránili z ich kódov po dokončení [4].

2.5.1.2 Salámový útok (Salami attack)

Ak nastávajú veľmi veľké množstvá finančných operácií, tak pri tejto technike podvodu môže dôjsť k vzniku veľkým finančným škodám. Táto metóda využíva chyby pri číselných matematických zaokrúhľovaniach na hranici presnosti. Ak sa jedná o bankovú aplikáciu, tak tá posiela peniaze programátorovi na jeho účet malé peňažné hodnoty. Takže ak pri niekoľkonásobnom zaslaní financií na účet nastane chyba v zaokrúhľovaní, tak z malých hodnôt zrazu vznikne veľká čiastka. Tento útok nespôsobuje viditeľné chyby, tzn., že útok sa dá ťažko odhaliť. Ak aj dôjde k odhaleniu, tak vo väčšine prípadov sa jedná o náhodu [2] [4].

2.5.1.3 Skryté kanály (Covert channels)

Tieto kanály vytvárajú možnosť prenosu informácií a dochádza tu ku komunikácií, ktorá by nemala byť sprístupnená. Komunikácia prebieha medzi procesmi operačného systému. Hrozí tu možný únik informácií, ak je chyba v operačnom systéme, ale aj trójskym koňom vďaka ktorému je vytváraný tento skrytý kanál. Opäť k týmto kanálom sa dá ťažko dopátrať, no existujú spôsoby, že sa vyskytne určitá chyba vo výpisoch alebo príde k strate súborov [2].

2.5.1.4 Nenásytné programy (Greedy programs)

K činnosti týchto programov je zbytočne potrebný vysoký výkon systému. V praxi to znamená, že v počítačoch bežia programy, ktoré majú nastavenú malú prioritu a vytvárajú zdĺhavé až nekonečné funkcie a pomaly zaťažujú procesor a pamäť. Toto dokáže zahltiť celý systém [2].

2.5.1.5 Počítačové víry (Virus)

Počítačové víry trápia väčšinu ľudí a každý z nás sa s nimi už aspoň raz stretol. Robia nám starosti a dokonca aj poškodia naše dáta. Jedná sa o program, ktorý dokáže napadnúť ďalšie programy. Víry nahradzujú časť kódu do programu, na ktorý sa pripojili a túto časť kódu dokážu meniť, čo slúži na anti-detekciu. Ak sa spustí daný program, najprv sa vykoná časť nahradeného kódu, nainštaluje sa do pamäti systému alebo zmení funkcie systému. Ak už je nákaza v systéme, môže ísť napr. o jednoduché multimediálne obrazové efekty so zvukom, ktoré nie sú až tak škodlivé ako tie, ktoré dokážu zničiť naše dáta a programy. Väčšina týchto vírov sa nachádza v programoch voľne šírených po internete. Získať sa ich dá aj sťahovaním nelegálnych softwarov alebo môžu sa nachádzať už v počítačoch napr. v kaviarni a iných voľne použiteľných počítačoch. Ochranou pred vírom môže byť antivírusový program, poučenie pracovníkov vo firme alebo rozdeliť dáta do oddielov, ktoré budú dostatočne oddelené.

2.5.1.6 Červy (Worms)

Červy sú podobné vírom, ktoré sa dokážu šíriť pomocou komunikačných liniek z počítača do počítača. Červy sa dokážu samé šíriť, čiže oproti vírom je šírenie ďaleko rýchlejšie a aj škody sú teda väčšie. Ochranou pred nimi je opäť ako u vírusov používanie overených programov a sieť rozdeliť na domény, kde prenos informácií je minimálny. Najväčší červ aký bol, tak napadol v roku 1988 cez 6000 počítačových staníc internetu a škody boli vyčíslené na 100 miliónov amerických dolárov. Tento červ sa pripisuje k 23 ročnému Robertovi T.Morrisovi, ktorý dokazoval otcovi, že siete systému UNIX sú nenapadnuteľné [4].

2.5.1.7 Trójske kone (Trojan horse)

Trójsky kôň dokáže ešte navyše vykonávať skryté akcie na ničenie systému. Trójsky kôň sa nainštaluje do systému až keď dosiahne určitý čas, kedy bol naprogramovaný. Od červa sa líši tak, že neinfikuje ostatné programy.

2.6 Ako sa správať v sieti Internet

V sieti internet sú vymedzené určité pravidlá, ktoré je potrebné dodržiavať a ukazujú užívateľom ako sa majú správať z pohľadu bezpečnosti informácií, dát atď. Každý

užívateľ, ktorý bude používať informačné a komunikačné zdroje, mal by sa riadiť týmito pravidlami:

- Pri posielaní dát pomocou elektronickej pošty dbať na veľkosť prenášaných súborov a zbytočne tak nepreťažovať sieť,
- Poskytovať v elektronickej pošte len základné informácie, údaje. Zbytočne nepísať citlivé informácie, ktoré tam nepatria,
- Pri písaní správ sa vyjadrovať slušne, nepoužívať vulgárne a urážlivé slová,
- Pred odoslaním správy sa kladie dôraz, aby užívatelia vyplňovali kolónku tzv. „Predmet" správy,
- Nevyužívať elektronickú poštu na rozosielanie textov, súborov, ktoré sú prísne zakázané a porušoval by sa pri nich zákon. Môže ísť o rasovú neznášanlivosť, politickú a pod.,
- V prípade použitia siete, ktorá sa nachádza v inej lokalite dodržiavať pravidlá využívané v danej oblasti [4].

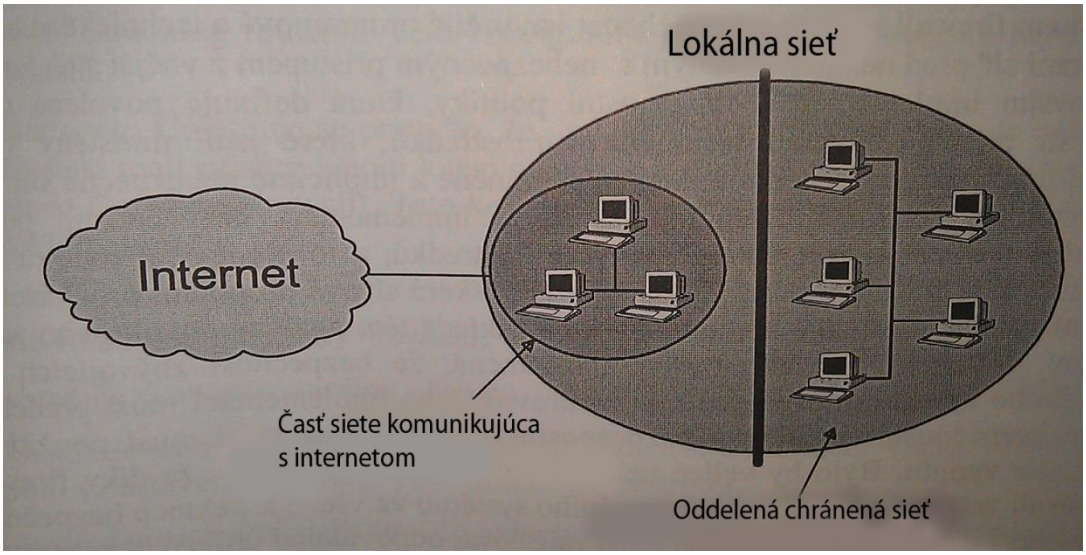
2.7 Bezpečné sieťové rozhranie

Väčšinou dochádza k útokom z vonku na systémy, ktoré sú pripojené na internet. Takýto informačný systém napádajú útočníci, ktorí sa dobre orientujú v technickom smere a ich znalosti sú na dobrej úrovni rovnako aj ich voľný čas pre kvalitný útok. Preto je dôležité, aby do vnútornej privátnej siete bol zabránený prípadný neoprávnený prístup. Útokom smerujúce z vonku sa dá brániť niekoľkými spôsobmi. Ako prvý spôsob je možné oddeliť fyzickú lokálnu sieť. Elektronický prenos informácií, ktorý nezasahuje do okruhu interného káblového rozvodu nepripadá do úvahy. Nevýhodou tohto použitého spôsobu je, že je najmenej funkčný, ale ak by sme mali pozerať na cenovú kalkuláciu tak sa zaraďuje k najlacnejším. Druhým spôsobom je použiť bezpečnú oddeľovaciu technológiu. Táto technológia dokáže spojiť privátnu sieť s okolitým svetom a kontroluje obojstrannú komunikáciu na základe bezpečnostných pravidiel. Týmto spôsobom sa dokáže zabrániť k dochádzaniu nebezpečnej komunikácií. Pre správne fungovanie je dôležité použiť vhodne premyslené bezpečnostné zásady [4].

2.7.1 Galvanické oddelenie podsiete

Sieť je galvanicky oddelená od privátnej siete tzn., že sú tu vytvorené dve siete. Privátna sieť, ktorá slúži pre vnútorný chod danej firmy a druhá oddelená privátna sieť pripojená k

internetu. Pre užívateľa to znamená, že neustále prechádza medzi týmito sieťami. Toto riešenie ponúka vysokú bezpečnosť no nevýhodou sú jak vysoké náklady, tak aj funkčnosť systému [4].



Obr. 3. Galvanicky oddelená podsieť [4]

2.7.2 Firewall

Firewall alebo inak povedané bezpečnostná brána dokáže zabrániť neautorizovaný prístup užívateľa z vonkajšej siete k zdrojom lokálnej sieti. Firewall prinucuje, aby sieťové prepojenia išli cez kontrolný systém, kde sa analyzujú komunikácie a výsledok analýzy určí povolenie alebo zákaz prepojenia. Úlohou firewallu nie je ochraňovať vonkajší svet lokálnej siete, ale ochrániť lokálnu sieť pred vonkajším svetom. Firewall nechráni pred vírmi a odposluchom alebo pri zničení dát pri prenosu po sieti. Základné typy firewallu:

- Paketový firewall,
- Aplikačné brány,
- Stavové paketové firewally,
- Stavové paketové firewally s kontrolou protokolov a IDS [2] [4].

Paketový firewall je najjednoduchší, spočíva v tom, že presne sa uvádza z akej adresy a portu na akú adresu a port môže byť doručený prechádzajúci paket. Pri aplikačných bránach komunikácia prebieha pomocou dvoch spojení. Klient (iniciátor spojenia) sa pripojí na aplikačnú bránu (proxy), tá toto spojenie spracuje a na základe požiadavku klienta otvorí nové spojenie k serveru, kde klientom je aplikačná brána. Stavové paketové filtre sú ako obyčajné paketové, ale navyše si uložia informáciu o povolených spojeniach,

ktoré sa neskôr môžu využiť pri rozhodovaní, či prechádzajúci paket patrí do povoleného spojenia a môže byť prepustený alebo musí prejsť rozhodovacím procesom. Pri posledných firewalloch s kontrolou protokolov a IDS sú tieto firewally schopné kontrolovať prechádzajúce spojenie až na úroveň korektnosti. Môžu zablokovať prechod "http" spojenia, ak sa nejedná o požiadavku na www server.

3 HROZBY A RIZIKÁ

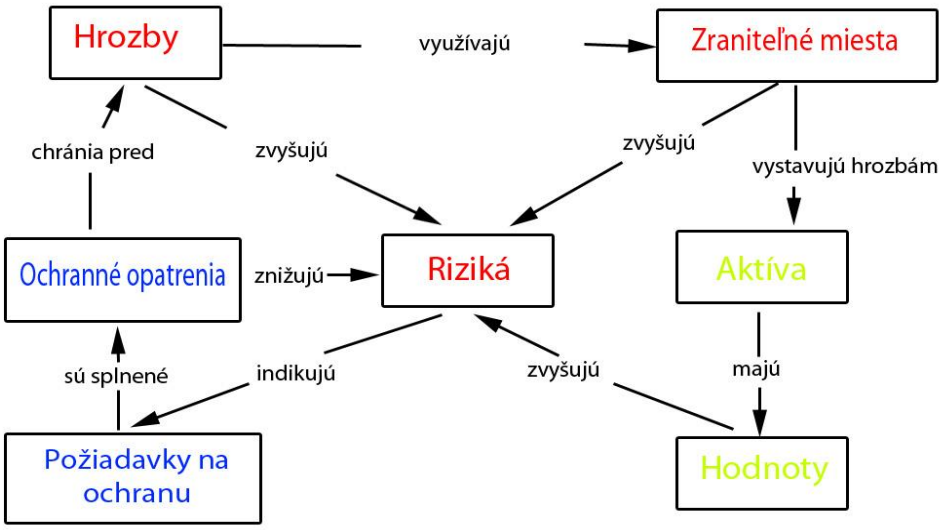
Hrozby v informačnom systéme môžeme deliť z rôznych hľadísk:

- Objektívne – sem spadajú hrozby prírodné, fyzické, technické a skôr sa zamerať na ich minimalizáciu a v prípade potreby vytvoriť havarijný plán.
- Subjektívne – hrozby, ktoré vychádzajú neúmyselne alebo úmyselne z ľudského faktora. V prípade neúmyselnej hrozby môže dochádzať pri nezaškolenom pracovníkovi informačného systému. Do úmyselných hrozieb sa zaraďujú vonkajší, ale i vnútorní útočníci. Vnútorným útočníkom sa väčšinou stávajú nahnevaní, prepustení zamestnanci, ktorí predstavujú približne 80% útokov. Cieľom týchto útokov bývajú finančné zisky alebo dosiahnutie konkurenčnej výhody [2].

Ďalšími hrozbami môže byť používanie neautorizovaných zdrojov, kde dochádza k odcudzeniu softwarových ale i hardwarových produktov a následne ich využívanie.

3.1 Analýza rizík

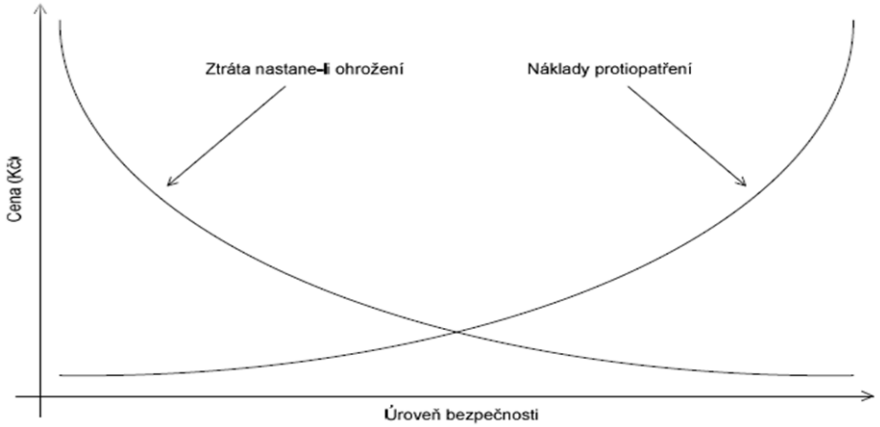
Cieľom tejto analýzy je, aby identifikovala dané hrozby a prípadné riziká. Je potrebné, aby sa tieto hrozby a riziká akceptovali a usmerňovali a výsledkom bývajú pravdepodobné riziká, ktoré môžu ohrozovať aktíva. Ak je dôležité predísť týmto rizikám, vytvárajú sa analýzy aktív, hrozieb a zraniteľností. Cieľom analýzy rizík je identifikovať riziko, postarať sa o jeho zvládnutie a následného odstránenia a tak minimalizovať nežiaduce vplyvy na aktíva. Ďalej musí odhadnúť škody, ktoré dochádzajú pri vzniku útoku, vybrať prospešné opatrenia a stanoviť približné finančné prostriedky na odstránenie alebo minimalizáciu daného rizika. V oblasti týkajúcej sa bezpečnosti informačných systémov analýza rizík vytvára efektívny systém ochrany na identifikovanie a ohodnocovanie určitým hrozbám, ktorými sú informačné systémy ohrozované a úlohou je vybrať správne ochranné opatrenie.



Obr. 4. Vzťahy medzi prvkami

3.2 Zabezpečenie internetového bankovníctva

Medzi klientom a bankou prebieha komunikácia vzdialene cez celosvetovú počítačovú sieť. Je potrebné, aby klient mal dostupný osobný počítač, internetové pripojenie a v poslednom rade musí mať aktivované samotné internetové bankovníctvo. Jedná sa teda o službu, ktorá sa dá využívať po celom svete, takže je tu možnosť, že tento systém je možné zneužiť kdekoľvek vo svete. Banky musia čeliť týmto hrozbám a preto sú nútené zavádzať bezpečnostné prvky, ktoré majú za úlohu takejto hrozbe predísť a zabrániť jej [7].



Obr. 5. Analýza nákladov a prínosov [2]

3.2.1 Zabezpečenie prenosu dát

Dátový tok nevyužíva len jeden komunikačný uzol. Je to zásadný problém, pretože pripojenie prechádza niekoľkými komunikačnými uzlami a je možné ich odpočúvať. Tomuto výrazu sa hovorí tzv. sniffing. Pri bezdrôtovej komunikácii býva zraniteľné miesto medzi počítačom klienta a pripojovacím bodom. V skratke povedané, neodporúča sa používať pripojenie, ktoré má otvorené bezdrôtové siete, pretože takýto prenos nie je šifrovaný a ľahko sa dá zachytiť iným počítačom. Toto však nestačí dodržiavať a k vaším dátam sa môže dostať technicky skúsenejší človek, ktorý prelomí staré, no dnes ešte používané WEP šifrovanie. Preto z týchto dôvodov banky pre komunikáciu s klientom používajú zvlášť šifrovanú technológiu SSL. Táto technológia funguje na princípe asymetrickej šifry [8] [9].

„Prenos citlivých dát je vo všetkých bankách riešený SSL šifrovaním (obvykle ikona žltého visiaceho zámku na stavovej lište) na vysokej úrovni a dá sa ju považovať za dostatočne bezpečnú“ [10].

Z pohľadu rizika na ohrozenú časť internetového bankovníctva je vďaka SSL šifrovaniu minimálne. Treba brať do úvahy, že ak sa využívajú dobre zabezpečené technológie pre komunikáciu, tak to neznamená, že bankovníctvo je dobre zabezpečené ako celok.

3.2.2 Identifikácia klienta

Je potrebné si vysvetliť pojmy ako sú identifikácia a autentizácia klienta. V praxi to znamená rozpoznanie a overenie totožnosti klienta. Banky sa musia uistiť, že dané manipulácie a bankové operácie vykonáva skutočný majiteľ účtu. Nesmie sa stať, že by sa iný človek vydával za skutočného majiteľa účtu. Preto banky dávajú do pozornosti toto zabezpečenie. Banky sa snažia používať čo najviac overovacích prvkov, aby nedošlo k nepovoleným operáciám. Z veľkého počtu overovacích prvkov prichádzajú aj nevýhody. Napríklad zo strany užívateľskej prívetivosti a úrovne zabezpečenia. Tieto problémy sa riešia viacúrovňovým zabezpečením s ohľadom nato, aký typ operácie bol prevedený. Delia sa na pasívne a aktívne operácie. Pri pasívnych operáciách sa nemení zostatok na účte. Príkladom tejto operácie môže byť zistenie pohybov na účte. Pomocou aktívnych operácií sa využívajú peňažné prostriedky (príkaz k úhrade).

Tab. 1. Prehľad aktívnych a pasívnych operácií

Aktívne operácie	**Pasívne operácie**
Zadanie príkazu k úhrade	Zistenie zostatku na účte
Zadanie príkazu k inkasu	Zistenie pohybov na účte
Zriadenie trvalého príkazu	Informácie o produktoch a službách banky
Zahraničný platobný styk	Informácie o aktuálnych úrokových sadzbách
Obsluha termínovaných účtov	Informácie o aktuálnych kurzoch cudzích mien

Pokiaľ využijeme pasívnu operáciu, banka od nás bude vyžadovať základný spôsob autentizácie. Autentizácia prebieha pomocou mena a hesla. Po úspešnej autentizácií je možné vytvárať užívateľské operácie. Zisťovanie zostatku na účte a pod. Systém mu ale nedovolí vytvárať príkazy k úhrade, inkasu. Pokiaľ by chcel tieto operácie vykonávať, bude od neho žiadaná ďalšia úroveň autentizácie. Napríklad SMS kľúč, elektronický certifikát atď.

3.2.2.1 Meno a heslo

Využívanie mena a hesla ako spôsob autentizácie v súčasnosti využívajú mnohé banky. Zároveň ide aj o najmenej bezpečný spôsob autentizácie klienta pri pasívnych operáciách. Údaje väčšinou banky posielajú v špeciálnych obálkach poštou. Po prvom prihlásení klienta do prostredia internetového bankovníctva systém vyzve klienta k zmene hesla, ktoré má byť dostatočne silné, aby sa zabránilo k prelomeniu hesla pomocou softwaru. Heslo musí obsahovať minimálne 8 znakov, skladať sa aspoň z jedného veľkého písmena a musí obsahovať číslicu. Aj napriek silnému heslu je tento spôsob identifikácie klienta veľmi zraniteľný. Využíva sa škodlivý software napríklad tzv. keylogger, ktorý má za úlohu sledovať prácu s klávesnicou, inak povedané odpočúvať ju. Ďalej to môžu byť phishingové útoky, ktoré sú v súčasnosti veľmi využívané a menej zručný užívateľ môže tomuto útoku ľahko podľahnúť bez toho, aby si niečoho podozrivého všimol [11].

3.2.2.2 SMS kľúč

Táto metóda je dnes veľmi rozšírená. Funguje na princípe odosielania SMS správy s autorizačným kľúčom. Tento kľúč je vyžadovaný pri rôznych operáciách ako bolo spomenuté v tabuľke č. 1 (napr. zadanie príkazu k inkasu). Využívanie tejto metódy internetového bankovníctva však vyžaduje, aby klient mal funkčný mobilný telefón. GSM komunikácia je šifrovaná, jediná možnosť ako obísť túto metódu je ukradnutie SIM karty, ktorá je viazaná na daný účet [12].

3.2.2.3 Elektronický kalkulátor

Z hľadiska bezpečnosti ide o veľmi silný prvok. Elektronický kalkulátor je známy ako token, ktorý generuje unikátne číselné kódy. Bez týchto kódov nie je možné sa dostať do aktívnych bankových operácií. Token je chránený štvormiestnym kódom PIN, ktorý slúži na ochranu proti odcudzeniu [11].

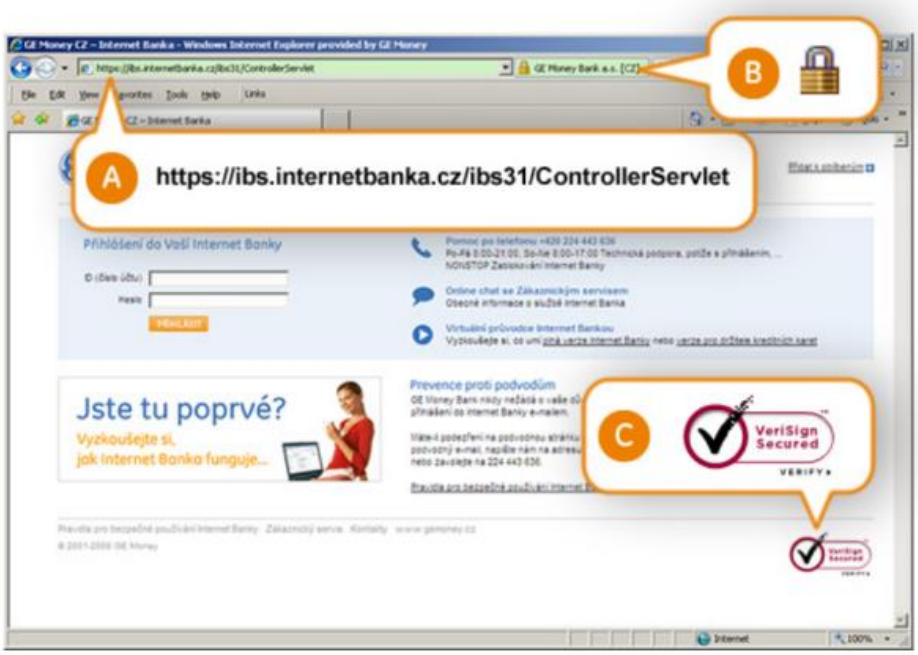
3.2.2.4 Elektronický certifikát

Slúži k autentizácií klienta a obsahuje jedinečný súbor. Vydanie elektronického certifikátu sprostredkováva samotná banka. Platnosť certifikátu nie je doživotná, preto je potrebné po uplynutí doby požiadať o vydanie nového certifikátu. Tento certifikát by sme nemali ukladať na disk počítača, ktorý denne využívame,, ale lepšie ho uchovávať na USB kľúči. Dôvodom je, že certifikát obsahuje súborový charakter tzn. môže dôjsť k duplicite. K jeho použitiu je potrebné vedieť heslo. Existuje aj elektronický certifikát uložený na čipovej karte [11].

3.2.3 Identifikácia banky

Identifikácia banky je veľmi dôležitá či už zo strany banky alebo klienta. Banka musí vedieť, že práve komunikuje so správnou osobou, ktorá má oprávnenie spravovať účet. Rovnako aj klient musí vedieť, že sa nachádza na stránke banky s ktorou komunikuje. Klient si dokáže overiť adresu pobočky, firemné logá apod. V súčasnosti by nikoho nenapadlo otvárať falošnú pobočku banky, ale objavili sa už aj také problémy, kedy banka bola falošná a jej cieľom bolo získanie citlivých údajov od klienta. Veľmi častá metóda je označovaná ako phishing. Útočníci rozošlú e-mailové správy, ktoré na prvý pohľad vyzerajú dôveryhodne, avšak jedná sa o podvodnú stránku. Vďaka rýchlemu vývoju informačných a komunikačných technológií klienti nemajú dostatočné znalosti k identifikovaniu banky, čo využívajú útočníci. Väčšinou ide o staršiu generáciu ľudí, ktorá

na školách počítačovú gramotnosť nezískala. Tým pádom sú odkázaní na sebavzdelávanie. To je však nedostatočné a na tomto základe sú na nich prevádzané útoky, pri ktorých klienti dobrovoľne odovzdávajú citlivé údaje o kreditných kartách alebo svojich prihlasovacích údajoch v domnienke, že komunikujú so svojou pravou bankou. Banky sa usilujú o silné zabezpečenie no predovšetkým najslabším článkom celého zabezpečenia je samotný klient. Niektoré z bánk ponúkajú klientom rôzne odporúčania, rady ako sa týmto problémom vyhnúť, no samotný klient nemá o to záujem. Domnieva sa, že banky za neho všetko vyriešia a bude v bezpečí. Dokonca majú aj príručky ako pomôcť svojím klientom v ktorých sú presne dopodrobna napísané návody k vyhnutiu sa hrozbe.



Obr. 6. Identifikačné prvky internetového bankovníctva GE Money bank [13]

3.3 Najznámejšie spôsoby prelomu bezpečnosti

Neustálym vývojom nových informačných technológií a konkurencií bánk prinášajú väčší počet bankových služieb. Vďaka rýchlemu vývoju vznikajú aj nové riziká, ktoré sa týkajú zabezpečenia účtov a k neoprávneným transakciám inou osobou.

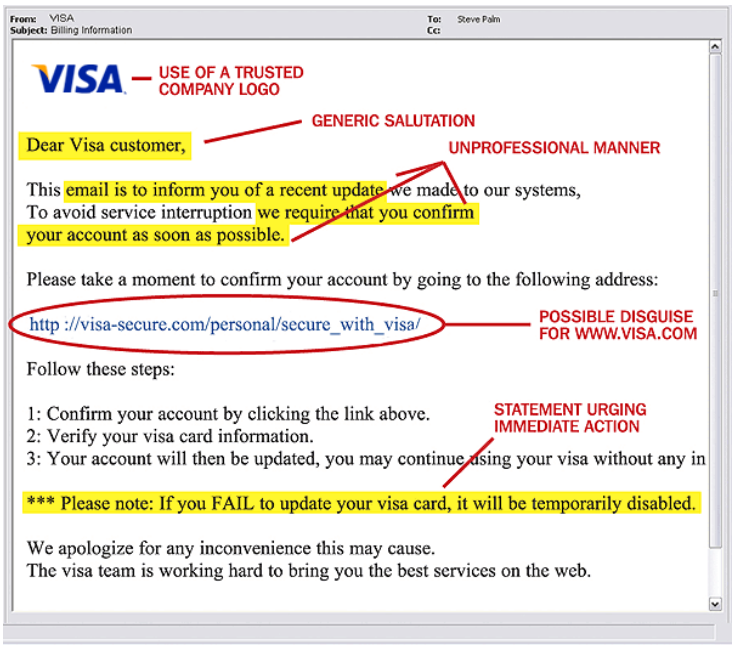
Najčastejšie využívané formy zneužitia sú:

- phishing
- pharming
- vishing

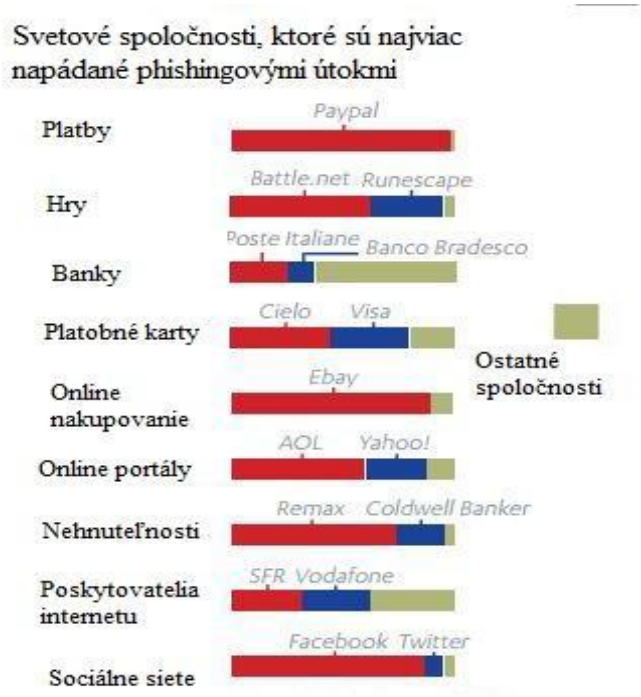
- skimming
- spying
- tabnabbing

3.3.1 Phishing

Password Harvest Fishing čo znamená v preklade zbieranie hesiel rybárčením. Ide o veľmi známy a jeden z najstarších spôsobov ako oklamať užívateľa a získať citlivé údaje. Využíva sa tu sociálne inžinierstvo. Je to metóda, kde útočník manipuluje s osobou od ktorej získa jeho údaje a pomocou nich ich môže zmanipulovať k určitej činnosti. Jedná sa o podvodné správy, ktoré útočníci rozošlú pomocou e-mailu. Po rozoslaní správ prídu užívateľom falošné emaily, ktoré na prvý pohľad vyzerajú ako pravé z banky, no realita je iná. Príkladom týchto emailov môže byť napr. PayPal, eBay apod. V emaily býva väčšinou oznámenie o neprevedení platobného príkazu a oznámenie k zmene prihlasovacích údajov. Vo vnútri tele správy sa nachádza odkaz, adresa, ktorá by nás mala presmerovať na originálnu stránku, ale reálne nás presmeruje na falošnú stránku. Na prvý pohľad ide o rovnakú stránku ako vyzerá originálna, ničím sa nelíši. Po dôkladnom obzretí môžeme zistiť, že adresa stránky je iná a začína nezabezpečeným protokolom (http://) [14].



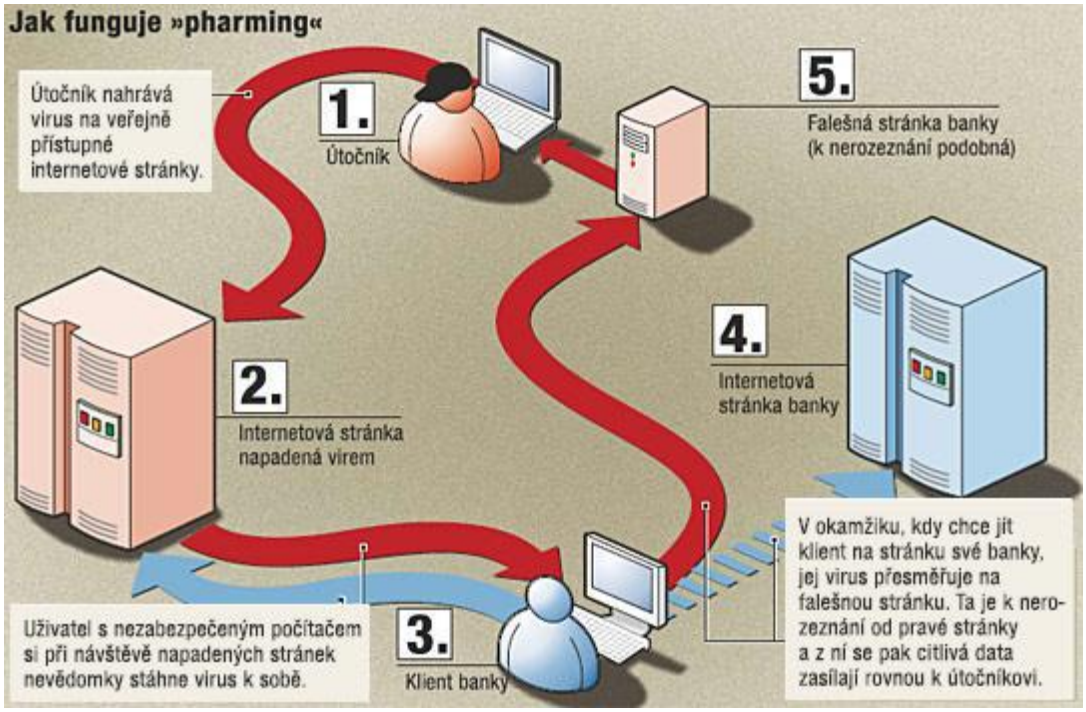
Obr. 7. Príklad phishingového emailu [15]



Obr. 8. Najviac napádané spoločnosti phishingovými útokmi [17]

3.3.2 Pharming

Jedná sa o automatizovanú formu phishingu. Nespadá pod sociálne inžinierstvo. Útočníci, ktorý využívajú túto metódu, tak napádajú DNS servery alebo počítače. Ak dôjde k zle zabezpečeným DNS serverov je to veľký problém. Užívatelia, ktorý využívajú toto pripojenie môžu zadávať správnu adresu, ale sú presmerovaní na inú stránku. Útočníci väčšinou napádajú počítače s operačným systémom Windows, ktoré v sebe obsahujú host súbory, ktoré fungujú rovnako ako DNS server. Stačí, ak útočník zapíše do tohto súboru adresu ktorú potrebuje (podvodná stránka) a princíp je rovnaký ako pri DNS serveroch [11].



Obr. 9. Vysvetlenie pharmingu [18]

3.3.3 Vishing

Skladá sa zo skratky slov voice-over a phishing. V preklade lovenie hesiel cez telefón. Spadá pod sociálne inžinierstvo. Pomocou telefónneho rozhovoru dokážu útočníci získať od klienta informácie o prístupe k internetbankingu. A to všetko pomocou jediného malwaru získajú autorizačné údaje. Po získaní údajov sa dokáže prihlásiť do internetbankingu, ale ešte je požadovaný autorizačný kód, ktorý veľmi ľahko získajú. Pošle klientovi varovnú SMS v zmysle: *„Dobrý deň, evidujeme podvodnú transakciu no Vašom účte. V nasledujúcich hodinách Vás bude pracovník banky kontaktovať z telefónneho čísla xxxx. S pozdravom Vaša banka xxxx."* Útočník ihneď zavolá klientovi, povie mu základné údaje napr. meno apod., aby získal dôveru od klienta. Vypýta si od neho transakčný kód a po tomto môže jednoducho manipulovať s účtom [19].

3.3.4 Skimming

Výraz je odvodený od slova to skim, čo znamená zbierať, sťahovať. Ide o trestnú činnosť, ktorá je spojená s bankomatovými kartami. Útočníci pomocou špeciálneho zariadenia nasadeného na bankomat kopírujú dáta z magnetického prúžku. Po získaní týchto dát vytvárajú nové falošné karty. Dôležitým údajom a to PIN kód je potrebný k účtu. Ten

získavajú pomocou bankomatových kamier, mobilných telefónov alebo majú špeciálnu klávesnicu, ktorú umiestnia miesto pôvodnej klávesnice alebo ju dajú rovno na ňu [20].

3.3.5 Spying

Je to metóda, pri ktorej sa špehuje pomocou škodlivého programu a to spyware. V 99% prípadoch si ho stiahneme do počítača pri obyčajnom surfovaní po internete. Spyware pracuje tak, že sleduje užívateľov, získava autorizačné údaje a čísla kreditných kariet. Následne sa údaje odosielajú útočníkovi. Samotný užívateľ si nemusí byť vedomý, že má niečo v počítači. Na odhalenie sa používajú rôzne antispywarové programy [21].

3.3.6 Tabnabbing

Ide o sofistikovanejšiu formu phishingu. Manipuluje so záložkami, ktoré má užívateľ vo webovom prehliadači a nepozornosť užívateľa internetu. Princíp je jednoduchý. Užívateľ má pri kúpe tovaru na internete otvorených viacero záložiek a vyhľadáva ich na viacerých stránkach a porovnáva. Tovar si chce kúpiť cez internetové bankovníctvo. Nevšimne si a otvorí stránku, ktorá je napadnutá skriptovým trojským koňom tak, že spúšťa TabNabbingový skript. Voľným okom je to nerozpoznateľné, žiadne zvláštne veci nie je vidno, ale keď sa prepne na inú stránku, zmení sa ikona v záložke a stránka zrazu vyzerá ako stránka internetového bankovníctva. Pri väčšom otvorení stánok, ktoré si prezeral a vyberal tovar si bude myslieť, že stránku s internetovým bankovníctvom si otvoril sám a do podvrhnutej stránky napíše svoje prihlasovacie údaje. Pri internetovom bankovníctve je potrebné vedieť viac ako je meno a heslo, preto útočníci túto metódu využívajú na získavanie prístupu do sociálnych sietí. Príkladom môžu byť aj stránky ako sú Paypal alebo eBay, ktoré majú priamy prístup k účtom [4].

II. PRAKTICKÁ ČASŤ

4 ANALÝZA BEZPEČNOSTI INTERNETOVÉHO BANKOVNÍCTVA VO VYBRANÝCH BANKÁCH

Táto kapitola zobrazuje výber bánk na Slovensku, poukazuje na ich bezpečnosť a zabezpečenie internetového bankovníctva. Postupne opisujem ich vzhľad, náročnosť, prehľad a orientácia na internetových stránkach. Ďalej som sa zameral na poskytovanie a dostupnosť informácií vo vybraných bankových portáloch a aké bezpečnostné prvky využívajú. Postupne som narážal na problémy, ktoré sa týkali získavania informácií zameraných na bezpečnosť a zabezpečenie internetového bankovníctva od konkrétnych bánk. Nedá sa to nazvať o nechcení podania konkrétnych informácií, ale z miestnych predpisov. Pre banky sú tieto informácie utajené a dôverné, preto pre obyčajného človeka, ktorý nemá s dotyčnou bankou pracovný pomer nemôžu banky poskytovať informácie ohľadom bezpečnosti a zabezpečenia internetového bankovníctva. Pokiaľ by tieto informácie verejne zdieľali, sami by si ohrozovali svoju vlastnú bezpečnosť. Banky majú zavedený systém a zaučených pracovníkov v prípade o informovanosti ľudí, aby ich odkázali na ich internetovú stránku, kde sa dozvedia všetky dôležité informácie a tak sa vyhnú priamemu kontaktu s pracovníkom banky.

Z vlastnej skúsenosti môžem povedať, že tento systém tak funguje, v snahe keď som sa snažil získať tieto informácie. Ak by ste sa snažili tento systém obísť a to pomocou zavolania na infolinku banky, rovnako Vás odkážu na internetovú stránku banky. Skúšal som to aj cez známeho, ktorý pracuje ako vývojár v danej banke, no oznámil mi, že tieto informácie mi nemôže poskytnúť z dôvodu utajenia informácií a ak by porušil tieto pravidlá, banka by musela vyvodiť následky a to vyhodením daného pracovníka. Takže po týchto negatívnych udalostiach mi neostávalo nič iné ako získavať informácie, ktoré boli dostupné na internetových stránkach banky.

4.1 Výber piatich najznámejších bánk na Slovensku

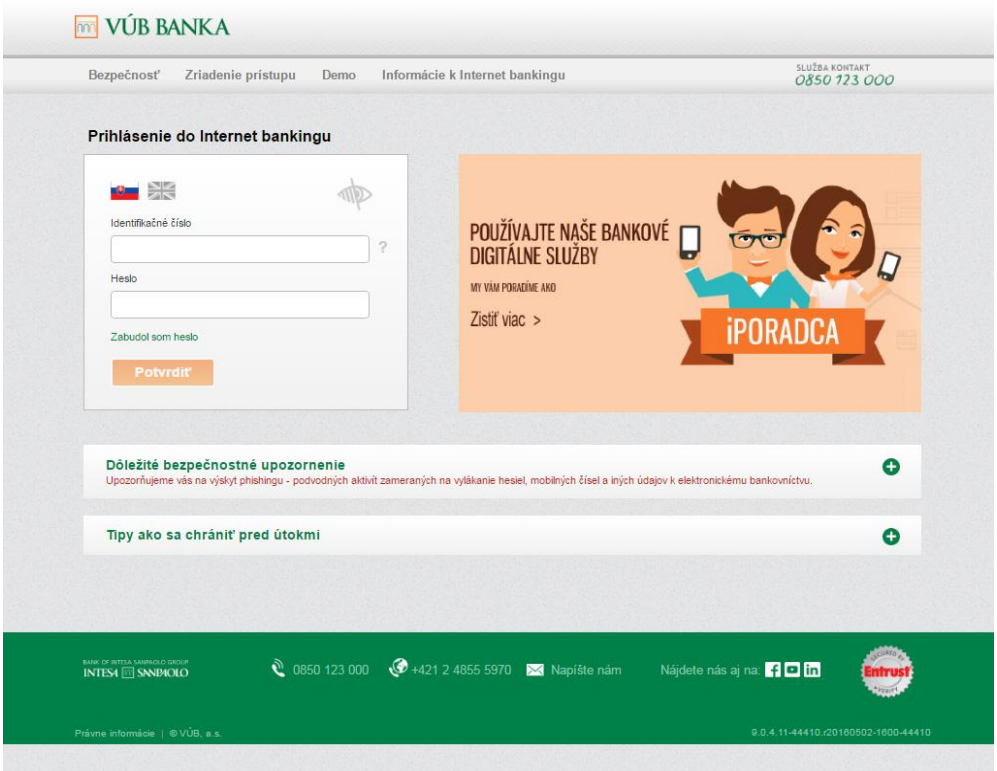
Samozrejme, že na Slovensku je tých bánk o niekoľkokrát viac, no zameral som sa na tie najviac využívané a známe. Vybral som teda päť najznámejších bánk na Slovensku a na týchto bankách budem postupne analyzovať a hodnotiť bezpečnosť internetového bankovníctva. Konkrétne sa jedná o :

1. Všeobecná úverová banka (VÚB),
2. Československá obchodná banka (ČSOB),

3. Slovenská sporiteľňa (SLSP),
4. Tatra banka,
5. Poštová banka.

4.1.1 Všeobecná úverová banka (VÚB)

Internetová stránka Všeobecnej úverovej banky prebehla pred niekoľkými mesiacmi novým dizajnom, ktorý zo začiatku pôsobí zložito a neprehľadne oproti starému. No všetko je to len o zvyku a po čase zisťujeme, že nový dizajn je veľmi zjednodušený a všetky informácie majú svoje miesto a členia sa podľa rôznych kategórií. V pravej hornej časti je políčko na prihlásenie sa do internetbankingu. To nás presmeruje na stránku, kde po správnom zadaní identifikačného čísla a hesla sa dostaneme do nášho internetbankingu. Môžeme si tu všimnúť navigačné panely, ktoré poskytujú informácie klientovi. V spodnej časti sa nachádzajú dôležité bezpečnostné upozornenia, ktoré poukazujú na výskyt phishingu a upozorňujú svojich klientov, aby na tento druh útoku nenaleteli. Ďalej sa tu nachádzajú tipy ako sa pred útokmi chrániť. Vďaka prehľadnému dizajnu sa informácie o bezpečnostných predmetoch hľadajú vcelku rýchlo, no je potrebné k tomu rozklikať niekoľko odkazov, ktoré Vás postupne presmerujú na požadovanú pozíciu.



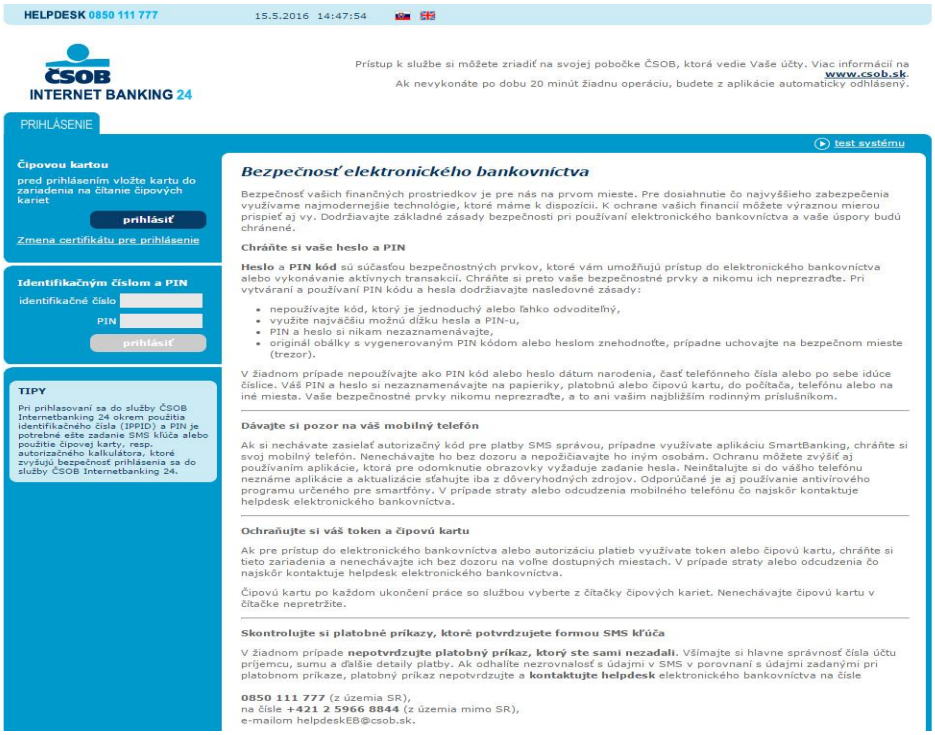
Obr. 10. Prihlasovacie okno do VÚB banky [22]

Tab. 2. Bezpečnostné nástroje a algoritmy VÚB banky [22]

Autentifikačné nástroje	Autorizačné nástroje	Symetrické šifrovanie	Asymetrické šifrovanie	Hašovací algoritmus	Certifikačná autorita
Identifikačné číslo	SMS kód	Algoritmus (RC4)	Algoritmus (RSA)	SHA-1	Entrust
PIN	Token	Dĺžka kľúča (128 bitov)	Dĺžka kľúča (2048 bitov)		
Heslo	Mobilný PIN				

4.1.2 Československá obchodná banka (ČSOB)

Československá obchodná banka má svoju internetovú stránku menej prehľadnú. Nachádza sa tu viac navigačných panelov. Panely sú nahradené veľkým množstvom informácií, ktoré svojou malou veľkosťou pôsobia veľmi zle a klientov môžu zmiasť. Na ľavej strane sa nachádzajú políčka na prihlásenie sa do internetbankingu. Môžeme si všimnúť, že do internetbankingu sa môžeme prihlásiť pomocou identifikačného čísla a hesla a aj pomocou elektronického podpisu z čipovej karty s certifikátom a čítačky čipových kariet. Karty komunikujú pomocou softvéru napr. CryptoPlus. Informácie ohľadom zabezpečenia sa hľadajú o trochu pomalšie kvôli neprehľadnému dizajnu. Banka sa snaží hneď na svojej úvodnej stránke v internetbankingu informovať klientov o možných hrozbách a užívateľ je neustále s týmto upozornením v kontakte pri prihlasovaní do internetbankingu.



Obr. 11. Stránka internetového bankovníctva ČSOB [23]

Tab. 3. Bezpečnostné nástroje a algoritmy ČSOB banky [23]

Autentifikačné nástroje	Autorizačné nástroje	Symetrické šifrovanie	Asymetrické šifrovanie	Hašovací algoritmus	Certifikačná autorita
Identifikačné číslo	Elektronický podpis	Algoritmus (RC4)	Algoritmus (RSA)	SHA-1	GlobalSign
PIN	SMS kód	Dĺžka kľúča (128 bitov)	Dĺžka kľúča (2048 bitov)		
SMS kód					
Čipová karta a čítačka					

4.1.3 Slovenská sporiteľňa (SLSP)

Slovenská sporiteľňa má pomerne rovnaký dizajn ako už spomínané banky. Jedná sa o moderný, pomerne prehľadný dizajn. Na úvodnej stránke sa nachádzajú navigačné panely v ktorých sa ale veľmi ťažko orientuje a potrebné informácie sa zdĺhavo hľadajú. Na pravej

strane sa nachádza políčko internetbanking. Po presmerovaní sa dizajn zmení na veľmi jednoduchý. Nenachádzajú sa tu žiadne upozornenia a rady pre zákazníkov, čo môže byť drobná nevýhoda. Navyše je tu panel o informovaní mobilných aplikácií, ktoré sa dnes už využívajú na mobilných smartfónoch.

Obr. 12. Stránka internetového bankovníctva SLSP [24]

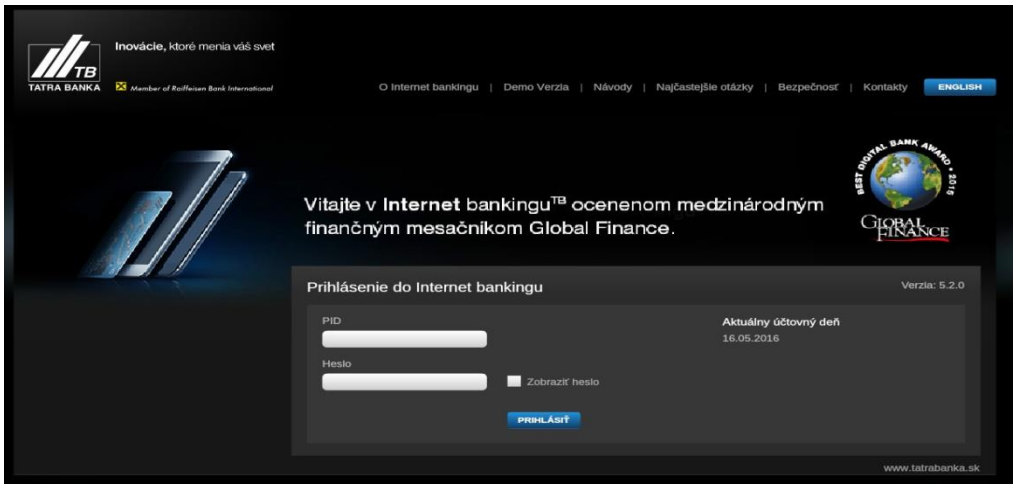
Tab. 4. Bezpečnostné nástroje a algoritmy SLSP banky [24]

Autentifikačné nástroje	Autorizačné nástroje	Symetrické šifrovanie	Asymetrické šifrovanie	Hašovací algoritmus	Certifikačná autorita
Prihlasovacie meno	GRID karta	Algoritmus (RC4)	Algoritmus (RSA)	SHA-1	VeriSign
Heslo	SMS kód	Dĺžka kľúča (128 bitov)	Dĺžka kľúča (2048 bitov)		
Elektronický token	Elektronický token				

4.1.4 Tatra banka

Tatra banka svojím dizajnom stránky musí zaujať každého návštevníka. Ide o veľmi jednoduchú, ale štýlovú stránku. Veľmi dobrá prehľadnosť stránky pomáha užívateľom,

ktorí hľadajú informácie a kráti čas pri vyhľadávaní. Má jednoduchý navigačný panel, na ktorom nájdeme všetko potrebné. Čo sa týka bezpečnosti, ako prvá prišla s kartou a čítačkou, ktorá slúži na autorizáciu platby. Panel do internetbankingu je rovnako jednoduchý v ktorom sa nachádza ďalší panel s informáciami.



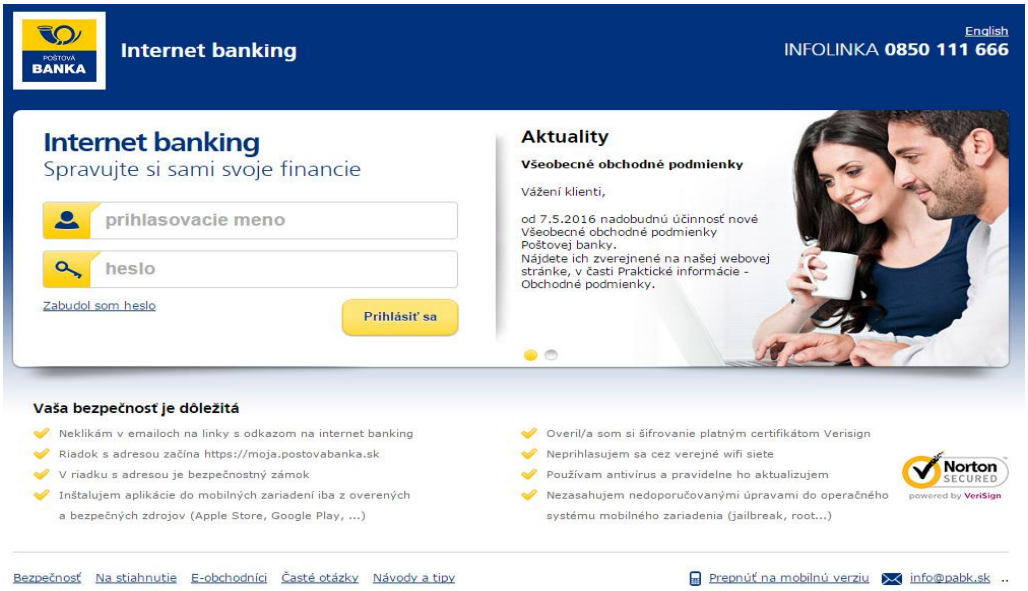
Obr. 13. Stránka internetového bankovníctva Tatra banky [25]

Tab. 5. Bezpečnostné nástroje a algoritmy Tatra banky [25]

Autentifikačné nástroje	Autorizačné nástroje	Symetrické šifrovanie	Asymetrické šifrovanie	Hašovací algoritmus	Certifikačná autorita
PID užívateľa	GRID karta	Algoritmus (AES)	Algoritmus (RSA)	SHA-1	VeriSign
Heslo	SMS kód	Dĺžka kľúča (128 bitov)	Dĺžka kľúča (2048 bitov)		
Karta a čítačka	Karta a čítačka				
	i:key				
	Secure ID karta				

4.1.5 Poštová banka

Čo sa týka poštovej banky a dizajn stránky, ani ona nezaostáva za poprednými bankami. Rovnaký typ dizajnu a navigačných polí. Po rozkliknutí internetbankingu sa zobrazia polia na prihlásenie. Ďalej sa tu nachádzajú informácie ohľadom hrozieb a upozornenia, ktoré poučujú svojich zákazníkov. Veľmi dopodrobna sa venujú bezpečnosti, čo je veľmi pozitívne. Pravidlá bezpečnosti poukazujú ako pracovať s internetom, dopodrobna graficky poukázané pojmy. Na stránke sa nachádzajú návody k bezpečnostným predmetom, ktoré by mohli byť viditeľnejšie.

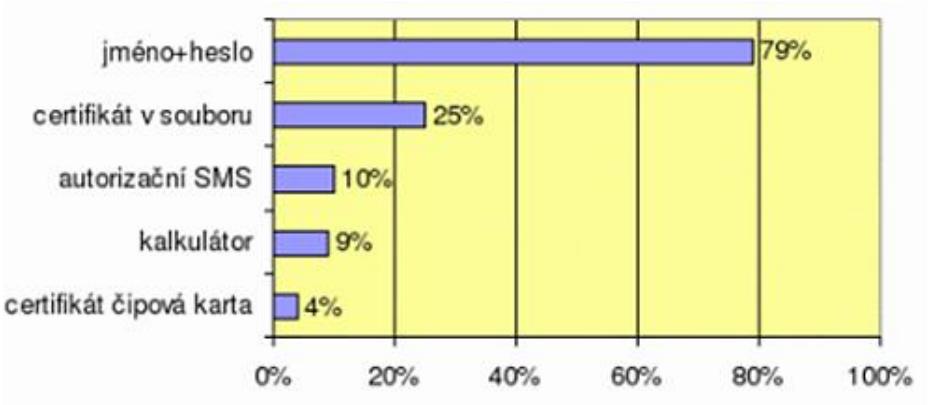


Obr. 14. Stránka internetového bankovníctva Poštovej banky [26]

Tab. 6. Bezpečnostné nástroje a algoritmy Poštovej banky [26]

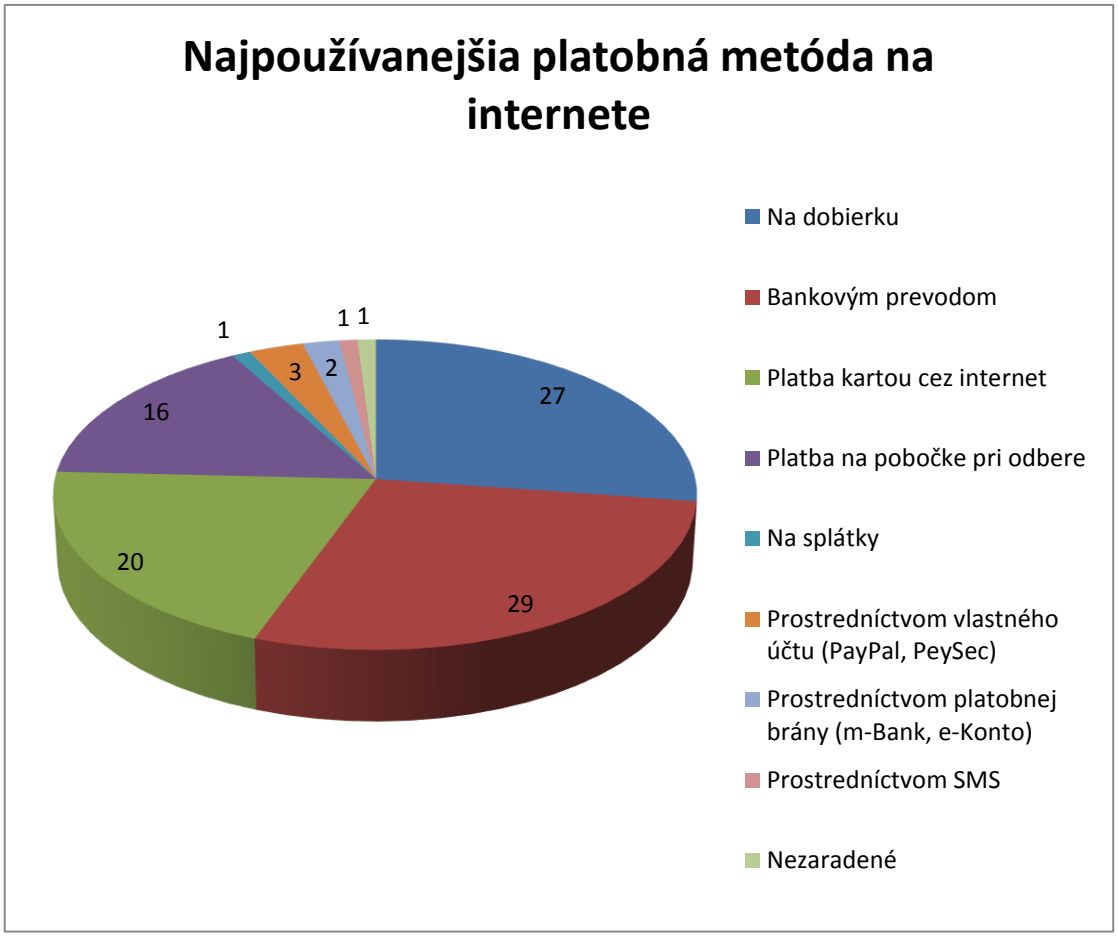
Autentifikačné nástroje	Autorizačné nástroje	Symetrické šifrovanie	Asymetrické šifrovanie	Hašovací algoritmus	Certifikačná autorita
Prihlasovacie meno	Jednorazové heslo	Algoritmus (RC4)	Algoritmus (RSA)	SHA-1	VeriSign
Heslo	Elektronický token	Dĺžka kľúča (128 bitov)	Dĺžka kľúča (2048 bitov)		
	SMS kód				

Po tejto analýze nám vychádza, že dnešné banky majú pomerne dobre zabezpečené internetové bankovníctvo vďaka šifrovacím algoritmom a dĺžke kľúča. Banky spĺňajú moderné štandardy, využívajú na zabezpečenie komunikácie symetrické algoritmy AES, ktoré majú dĺžku kľúča 256 bitov. Niektoré z bánk využívajú asymetrické šifrovanie, kde je použitý algoritmus RSA s dĺžkou kľúča 2048 bitov. Banky, ktoré využívajú symetrický algoritmus RC4, kde dĺžka kľúča je 128 bitov sú mierne pozadu ale je to postačujúce. Každá jedna banka používa hašovací algoritmus SHA-1 a certifikáty SSL (šifrovacia vrstva). Využívanie bezpečnostných nástrojov je dnes už na veľmi vysokej úrovni. Zvyšovanie konkurencie pri tvorbe internetových stránok stúpajú aj nároky a môžeme si všimnúť, že pri každej banke sú stránky veľmi prepracované. Niektoré sú až neprehľadné z nadpriemeru dizajnových vylepšení a nadmerného textu. Avšak svojim spôsobom poskytujú užívateľom potrebné informácie a informujú o možných hrozbách, ukazujú rôzne návody a tipy ako sa pred nimi chrániť. Jedným z nových návrhov by sme navrhli pre banky, aby na svoje internetové stránky pridali odkazy na antivírusové balíky, ktoré by si užívatelia mohli vo verzií beta vyskúšať v prípade, ak ešte nevlastnia žiadny z týchto systémov a možnosti vyhnúť sa tak možnej hrozbe.



Graf 1. Využitie ochrany internetového bankovníctva na českom trhu [16]

Na tomto grafe môžeme vidieť využívanie bezpečnostných prvkov internetového bankovníctva z roku 2006. Percentá ukazujú, koľko bánk využívalo tieto prvky a ako je vidieť, najviac využívaným spôsobom bola autentizácia pomocou mena a hesla, ktorá platí aj v súčasnosti.



Graf 2. Najpoužívanejšia platobná metóda na internete [30]

Graf poukazuje na spôsoby platobnej metódy využívanej na internete. Ľudia si najviac obľubujú platbu pomocou bankového prevodu a platbu kartou. Ak je ľuďom poskytnutá táto metóda, radi ju využijú. Platby sú rýchle a nie sú zložité.

5 NÁVRHY A OPATRENIA ELEKTRONICKÉHO BANKOVNÍCTVA

Elektronické bankovníctvo v súčasnosti obľubuje čo viac ľudí a preto sa naň v tejto kapitole zameriame a popíšeme jeho nové návrhy zabezpečenia do budúcnosti. Najťažšou úlohou pre banky bolo presvedčiť svojich klientov a ľudí a naviesť ich na elektronické bankovníctvo. Pre banky to bola veľká výzva s ktorou sa museli popasovať. Postupne si banky u svojich klientov získali svoju dôveru a ukázali im, aké výhody elektronické bankovníctvo prináša. Preto si myslíme, že budúcnosť elektronického bankovníctva je veľmi dôležitá. Pre každého z nás je jednoduchšie využívať elektronické služby, ktoré nám šetria čas. Dnes je to veľký fenomén, vďaka ktorému je tento nárast využívania elektronických služieb tak vysoký. Avšak je tu ešte skupina ľudí, ktorí tieto služby nevyužívajú, ale poznajú ich od svojich známych a pod. Banky musia byť preto v strehu a svojich klientov neustále informovať o výhodách, ktoré elektronické bankovníctvo prináša. Týmto si banky zaručia istotu, že presvedčia klientov a nasmerujú ich na tieto služby a zvýši sa tak celkový počet využívania elektronického bankovníctva. Pre mladých ľudí využívanie elektronického bankovníctva je veľmi jednoduché. No musíme brať ohľad aj na staršiu generáciu ľudí, pre ktorých sa zdajú byť tieto nové služby komplikované a ťažké. Je to tým, že nemali možnosť získať na školách počítačovú gramotnosť na takej úrovni, aká disponuje v súčasnej dobe. V predošlej kapitole sú ukázané bezpečnostné nástroje jednotlivých bánk, ktoré využívajú na autentizáciu a autorizáciu. Cieľom tejto časti bude teda návrh nového modelu autentizácie a autorizácie. V teoretickej časti je spomenutá autorizácia pomocou biometrických systémov, ktoré sa dnes stále viac a viac využívajú, preto budú zakomponované aj do nového modelu.

Po analýze som zistil, že na autentizáciu a autorizáciu sa využíva viacero metód, ktoré banky kombinujú. Dnes je veľkým fenoménom elektronické bankovníctvo, ktoré aj samotné banky rady presadzujú medzi svojich klientov. Preto sa zameriam na:

1. Internetové bankovníctvo,
2. Smartbanking,
3. Bezkontaktné platobné karty,
4. Bankomaty.

5.1 Internetbanking

Pokiaľ sa chceme prihlásiť do internetbankingu, tak je od nás požadované, aby sme zadali svoje prihlasovacie meno a heslo. Každá z bánk má iný typ autorizácie a autentizácie, napr. vo Všeobecnej úverovej banke, kde je od nás potrebné zadať identifikačné číslo a heslo. Ďalším krokom je autorizovanie pomocou bezpečnostného prvku. Môže sa jednať o SMS autorizáciu. Dnes však už systém dokáže vyhodnotiť riziko a posúdi, či je potrebné zadávať SMS autorizáciu, alebo systém vyhodnotí, že prihlásenie je bezpečné a nie je potrebné zadávať druhy krok. Pokiaľ by systém toto prihlásenie vyhodnotil, že je možné riziko pri prihlasovaní, systém bude vyžadovať, aby ste zadali bezpečnostný kód, ktorý Vám príde ako SMS správa alebo sa môže jednať o token. Pri tomto spôsobe prihlásenia je potrebné mať mobilný telefón, v prípade nutnosti zadania druhého kroku.

Výhoda: výhodou tohto spôsobu je dnešné masívne využívanie a pre banku to znamená zníženie pracovníkov, ktorí by sa starali o klientov. Rovnako aj bezpečnosť je vysoká, pokiaľ klient nenaletí na podvodné typy útokov, napr. phishing atď., ktorý bol rozoberaný v teoretickej časti. Pre užívateľa je tento spôsob veľmi jednoduchý, pomerne rýchly a dnes už nato môže využiť aj svoj smartfón.

Nevýhoda: každý systém má aj svoje nevýhody a rovnako je to aj pri tomto. Banky neustále čelia phishingovým útokom, ktoré v súčasnosti neustále pribúdajú a tým ohrozujú užívateľské kontá. Väčšinou sa jedná o staršiu generáciu, ktorá týmto typom útokom naletí a útočníkovi poskytne svoje citlivé údaje. Takto si ľudia myslia, že banky majú slabo zabezpečený systém a ďalej už neveria bankám, no chyba bola na strane užívateľa. Je potrebné, aby si užívateľ pamätal svoje identifikačné číslo, ktoré býva väčšinou príliš dlhé a heslo. V prípade, ak je potrebná SMS autorizácia a mobilný telefón nemá signál, nie je možné využívať túto funkciu.

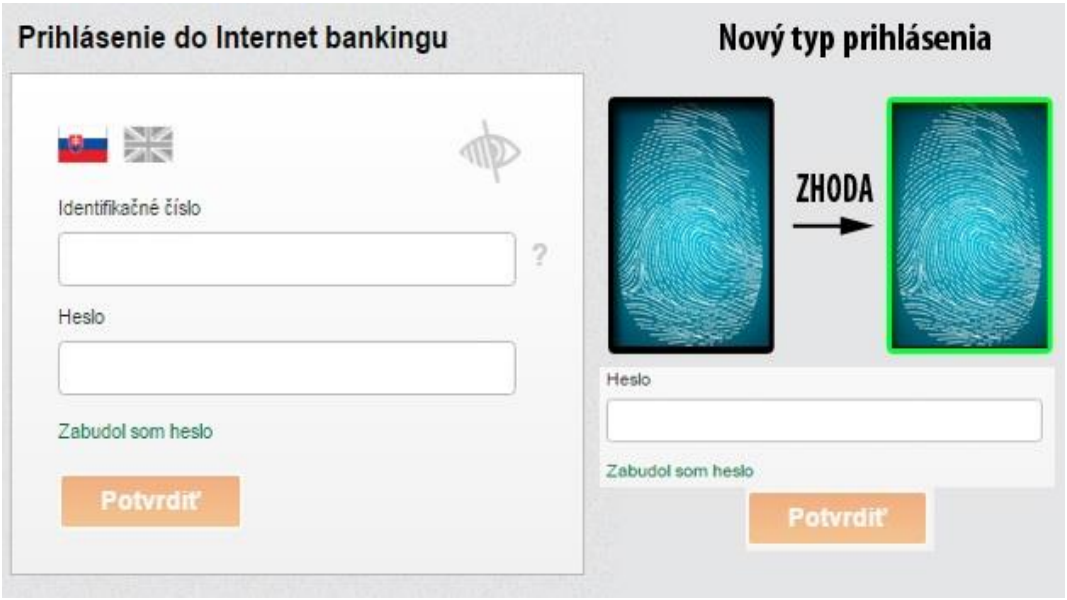
5.1.1 Nový model systému v internetbankingu

Ako bolo spomenuté, do nového modelu budú zakomponované biometrické systémy, ktoré budú využívané na autentizáciu. Tú by užívatelia vykonávali pomocou odtlačku prsta alebo pomocou krvného riečiska. Celý systém bude fungovať veľmi jednoducho. Užívateľ pri vstupe do internetového bankovníctva bude vyzvaný, aby vykonal test na odtlačok prsta. Odtlačok by sa porovnal s odtlačkom, ktorý je už v databáze a po úspešnom porovnaní testu odtlačku bude užívateľ vyzvaný k druhému kroku a to k zadaniu svojho hesla. Ak sa

všetko zhoduje, bude mu povolený vstup do internetbankingu. Dvojitá ochrana k autorizovaniu je postačujúca, no je tu možnosť aj trojitej ochrany.

Výhoda: za výhodu sa považuje tento model systému veľmi bezpečný. Útočníkom by zabralo veľkú námahu ako tento systém obísť. Pre užívateľa by tento systém nebol komplikovaný a obsluhovať by ho dokázali aj starší ľudia.

Nevýhoda: za nevýhodu sa označuje nutnosť vlastniť systém, ktorý vám zosníma odtlačok prsta. Banky by museli spraviť vlastnú databázu odtlačkov prstov všetkých svojich klientov, ktorá by musela byť dostatočne zabezpečená od strany útočníkov, ktorí by sa ihneď usilovali o odcudzenie databázy a na následnom predaji by mohli zarobiť nemalé finančné odmeny.



Obr. 15. Staré a nové prihlásenie do internet bankingu

5.2 Smartbanking

V dnešnej dobe sa postupne zo smartbankingu stáva dennodenný hit, ktorý si obľubuje mladšia generácia ľudí. Avšak stále nie je na tej úrovni ako sú bankomaty či platobné karty. Netreba zabúdať, že aj tento využívaný spôsob musí byť kvalitne a dostatočne zabezpečený a čo sa týka autentizácie a autorizácie nemala by byť príliš zdĺhavá a komplikovaná. No zatiaľ sa vývojárom nepodarilo nájsť spôsob, ako vyriešiť jednoduché mobilné bankovníctvo. V súčasnosti tento systém funguje tak, že ak sa potrebujeme prihlásiť do mobilného bankovníctva je potrebné prihlasovacie meno spolu s PIN kódom. To však nie je všetko, vzápätí na mobilný telefón príde SMS správa, kde sa nachádza náš

autorizačný kód. Tento kód je potrebné zadať do dvoch krokov. Jedným je prihlasovacia aplikácia a ďalším krokom s tým istým autorizačným kódom k prihláseniu. Ide o veľmi zdĺhavý cyklus a dalo by sa to vyriešiť efektívnejším spôsobom. Rovnako ako u internetbankingu tak aj tu sú použité biometrické systémy ako nový modelový návrh. Zavedenie biometrických systémov ako spôsob autentizácie a autorizácie je v dnešnej dobe s nástupom nových smartfónov priam dokonalé. Dnes už každý nový smartfón dokáže pri dobrom nastavení zosnímať odtlačok prsta a tým majiteľovi sprístupní odblokovanie telefónu a následne povolí prístup k ovládaniu mobilného telefónu. Objavili sa už aj rôzne aplikácie na zosnímanie tváre, no väčšiu šancu získal odtlačok prsta. Preto je možné. že biometrické systémy sa budú do budúcna využívať na autentizáciu a autorizáciu mobilného bankovníctva, pretože nové technológie ponúkajú smartfónom široké rozhranie a zjednodušenie prístupu a v budúcnosti je zrejmé, že toto je dobrá cesta k rozvoju.

Výhoda: pokiaľ vlastníme mobilný telefón, ktorý podporuje tento druh aplikácie, veľmi pomáha, zjednodušuje a urýchľuje spôsob mobilného bankovníctva. Aplikácia je rýchla, nezasekáva sa a rýchlo si na ňu dokážu zvyknúť aj starší ľudia. V prípade, ak by sme stratili mobilný telefón alebo by bol odcudzený, páchateľ túto aplikáciu nedokáže využiť vo svoj prospech, pretože nepozná prihlasovacie meno a heslo užívateľa. Ďalšou výhodou je, že za aplikáciu nemusíme platiť. Užívateľovi je sprístupnená zadarmo, no je potrebné mať telefón podporujúci túto aplikáciu. Stačí, ak máme v telefóne aktívny internet, dokážeme sa na mobilné bankovníctvo pripojiť z ktoréhokoľvek miesta na zemi.

Nevýhoda: hlavnou nevýhodou je nutnosť vlastniť smartfón. Pokiaľ vlastníme obyčajné mobilné telefóny, ktoré nepodporujú túto aplikáciu, nemôžeme využívať mobilné bankovníctvo. Preto je potrebné vlastniť tento smartfón, aby sme si aplikáciu stiahli. Pre mladú generáciu je to dnes už nepredstaviteľné, aby nevlastnili jeden zo smartfónov. Horšie je to u staršej generácie ľudí, ktorí sú zvyknutí na starú klasiku. Ďalšou nevýhodou sú aj dlhé prihlasovacie údaje, ktoré sú ťažšie zapamätateľné.

5.2.1 Nový model systému v smartbankingu

S nástupom nových technológií prichádzajú aj nové možnosti a to smartbanking. Dnes už existujú smartfóny, ktoré dokážu pomocou zosnímania odtlačku prsta odblokovať telefón. Preto ako nový návrh sú využité biometrické systémy do nových aplikácií v smartbankingu. Jedná sa o zosnímanie odtlačku prsta a následného zadania PIN kódu. Systém by pracoval na dvojitej ochrane. Bolo by to veľmi pohodlné a rýchle a

nevyžadovalo by to žiadne prihlasovacie údaje. Nemuseli by sme dostávať zbytočné SMS správy s autorizačným kódom. Po spustení aplikácie do smartbankingu bude od užívateľa vyžiadaný odtlačok prsta spolu s PIN kódom pre správne prihlásenie. Aplikácia porovná odtlačok s databázou a pokiaľ sa zhodujú, užívateľovi sa sprístupní cesta k svojmu účtu. Ak by sa odtlačok nepodarilo identifikovať a trikrát by tento cyklus opakoval nesprávne, užívateľovi by sa jeho účet uzamkol na dobu 15 minút. Ako odporučenie je pred vstupom do aplikácie vložené výstražné okno, ktoré by oznamovalo užívateľovi, či má nainštalovanú antivírusovú aplikáciu na zachytávanie škodlivých vírusov. Takto bude ochránený mobilný telefón pred hrozbami, ktoré by ohrozovali telefón a možné sledovanie odtlačku prsta a hesla.

Výhoda: medzi výhody sa považuje vysoká bezpečnosť mobilného bankovníctva. Išlo by o rýchlu autentizáciu a autorizáciu a tento spôsob by si ľudia, ale aj banky rýchlo obľúbili. Výhodou je aj to, že nie je potrebné si pamätať zbytočne dlhé prihlasovacie údaje.

Nevýhoda: veľká nevýhoda tohto systému je nutnosť vlastniť mobilný telefón podporujúci túto aplikáciu a aby aj telefón v sebe obsahoval funkciu odtlačku prsta. Ďalšou nevýhodou je potrebné vytvoriť novú aplikáciu, ktorá by v sebe mala databázu odtlačkov prstov užívateľov. Pre niektorých ľudí to môže byť nepríjemné, aby svoje odtlačky niekomu zverejňovali, no sú potrebné k tomuto kroku.

5.3 Bezkontaktné platobné karty

Veľkým fenoménom sa dnes stávajú bezkontaktné platobné karty. Ľudia si ich rýchlo obľubujú, pretože ich použitie je veľmi jednoduché. Užívateľ pri platbe jednoducho položí kartu na terminál a po pípnutí je všetko hotové. Bezkontaktné platby môže využívať pri platbe, ak platba nepresiahne 20 eur. No čo sa týka bezpečnosti, zaraďuje sa na taký priemer.

Výhoda: rýchlosť a jednoduchosť používania. Pri platbe do 20 eur nie je potrebné si pamätať PIN kód. Nie je nutné kartu vsúvať do terminálu alebo ju podávať obsluhe, ktorá ju vloží do terminálu.

Nevýhoda: v súčasnosti existujú ešte obchody, ktoré neponúkajú možnosť používania bezkontaktných kariet. Obrovskou nevýhodou je jej ochrana a v prípade neúmyselného stratenia karty môže páchateľ túto kartu využiť k platbe, kým bude zablokovaná.

To nastáva až pri nahlásení straty a dovtedy pomocou nej môže byť vykonávaná neoprávnená platba. Pretože nie je potrebné poznať PIN kód, páchateľovi to zjednodušuje cestu.

5.3.1 Nový model systému pre bezkontaktné platobné karty

Celý systém bude fungovať na rovnakej úrovni ako v súčasnosti, ale namiesto zadávania PIN kódu bude skenovanie odtlačku prsta. Čiže po priložení bezkontaktnej karty k terminálu v prípade platby nad 20 eur bude vyžadovaný odtlačok prsta. Ten sa porovná s databázou, systém vykoná porovnanie a v prípade zhody bude platba realizovateľná.

Výhoda: jednoduchosť, väčšia bezpečnosť. Užívateľovi odpadne starosť a nemusí si pamätať svoj PIN kód pre vykonanie platby. Kartu môže využívať len osoba, ktorá vlastní túto platobnú kartu.

Nevýhoda: finančné náklady spojené s inštalovaním zariadení na odtlačok prsta.

5.4 Bankomaty

Každý z nás určite dobre pozná zariadenia nazývané bankomaty. Nachádzajú sa v každom meste a poskytujú ľuďom rýchle vydanie peňazí z bankomatového účtu. Čiže nemusíme pri sebe nosiť veľké množstvo peňazí, v prípade potreby zájdeme k bankomatu a vytiahneme si určitú sumu. Banky investovali do inštalácie bankomatov množstvo peňazí, čo bol dobrý krok vpred. V minulosti ale aj dnes sa vyskytujú určité prípady, kedy boli tieto bankomaty vylúpené. Využívajú sa techniky ako je skimming alebo ich jednoducho fyzicky zničia. Ich ochrana musí byť dnes čo najvyššia, aby sa predišlo možným hrozbám. Bankomaty a ich autorizácia funguje na dvojitom zabezpečení. Jedná sa o bankomatovú kartu platnú na určité obdobie, ktorú vydáva samotná banka do rúk svojho klienta a príslušný PIN kód. Pre správne použitie tejto služby je, aby užívateľ vložil svoju bankomatovú kartu do bankomatu, je vyzvaný aby zadal svoj PIN kód a po úspešnom overení môže využívať svoj účet. Musí si však dávať pozor, aby bankomatovú kartu nestratil, aby ho iná osoba nesledovala za cieľom zistenia jeho PIN kódu pri jeho zadávaní. Môžu sa nachádzať blízko bankomatu nainštalované skryté kamery na zisťovanie PIN kódov apod. Konštrukcia bankomatov je na dobrej úrovni, no ak sa jedná o autorizáciu a autentizáciu, je tam možné vidieť isté medzery.

Výhoda: umiestnenie bankomatov dnes už je na veľkej úrovni, preto v prípade potreby vyberania peňazí nemusíme jazdiť ďaleko do väčších miest. Jedná sa o rýchly a

jednoduchý systém. Menšie poplatky za výber z bankomatu ako u samotnej banky. Rovnako aj výber v prípade ak sa nachádzate v zahraničí.

Nevýhoda: veľkou nevýhodou týchto bankomatov je atraktivita pre útočníkov, ktorí vidia jednoduchú cestu k získaniu peňazí. Pre banky to znamená veľké straty či už z finančnej straty alebo straty zákazníkov. Ďalšou nevýhodou je ich prevoz, poškodenia, opravy. Ak si chce užívateľ vybrať peniaze, musí mať pri sebe bankomatovú kartu. Bez nej sa k jeho účtu nedostane. Rovnako je to aj s množstvom vlastnenia platobných kariet, bankomatových kariet a ich rôzne prístupové PIN kódy, ktoré z hľadiska bezpečnosti sa od seba líšia.

5.4.1 Nový model systému bankomatov

V tomto novom návrhu sú opäť využité biometrické systémy, kde je použité na autorizáciu a autentizáciu skenovanie očnej dúhovky alebo klasický odtlačok prsta prípadne využitie krvného riečiska. Celý systém bude fungovať na dvojitej ochrane. Rovnako sa využíva aj dnes a spĺňa svoje požiadavky. Na bankomate bude nainštalované zariadenie, ktoré bude slúžiť na skenovanie očnej dúhovky. Bankomatový systém bude v sebe obsahovať databázu, kde sa budú nachádzať zoskenované jednotlivé užívateľské parametre. Túto databázu bude potrebné veľmi dobre zabezpečiť napr. využiť šifrovacie metódy, v prípade, ak by sa k týmto citlivým údajom dostal útočník, aby nemal možnosť ich použiť. Celý systém bude fungovať jednoducho. Ak užívateľ bude chcieť vybrať peniaze, príde k bankomatu, postaví sa na určité vyhradené miesto, aby prebehlo úspešné zoskenovanie očnej dúhovky. Následne po úspešnom overení osoby z databázy momentálneho skenovania systém potvrdí zhodu a užívateľ bude vyzvaný, aby vykonal druhý stupeň ochrany a to zadanie svojho PIN kódu. Ak splní aj túto požiadavku, bude mu sprístupnený jeho účet a môže začať voliť prístupné funkcie. Rovnako by systém fungoval aj v prípade využitia odtlačku prsta, kde by sa vykonávalo namiesto skenovania očnej dúhovky skenovanie odtlačku prsta. Pre užívateľa by to bolo jednoduchšie a pohodlnejšie. Užívateľ bude mať tri možné pokusy pre zadanie správneho PIN kódu. Ak by došlo k opakovaniu nesprávneho PIN kódu, systém mu účet zablokuje na určitú dobu. Táto doba sa bude zdvojnásobovať po opakovanom neúspešnom zadaní kódu. Bankomaty by boli pre jednotlivé banky všetky rovnaké. Zmena by bola len v systéme, kde by na začiatku užívateľ vybral z možností, ktorú banku chce využiť. Takto by sa zabránilo možnému

chaosu databáz, aby systém vedel, ktorú databázu má v danom momente na porovnanie využiť.

Obr. 16. Bankomat so skenovaním očnej dúhovky

Obr. 17. Bankomat s biometrickým systémom odtlačku prsta [27]

Výhoda: veľkou výhodou pre užívateľa by nebolo nutné využívať bankomatové karty a tak by aj zmizol strach a obavy z ich nevedomého stratenia alebo odcudzenia karty. Z rôznych druhov bankomatov by sa obmedzil na určitý počet a postupne by sa prechádzalo na menší počet bankomatov, čo by pre užívateľa bolo výhodou, že si peniaze môže vyberať kdekoľvek. V podstate je to skoro možné aj dnes, no ak sa využije iný bankomat ako má

užívateľ banku, bude mu zarátaný poplatok z výberu. Ďalšou výhodou je samozrejmé zvýšenie bezpečnosti proti neoprávneným vstupom. Rovnako aj banky by nemuseli riešiť každoročné vydávanie nových bankomatových kariet a náklady na ne by mohli využiť do zavedenia nových systémov.

Nevýhoda: pre banky by to bol nárast finančných prostriedkov na zavedenie nových systémov do všetkých bankomatov. Následne by banky museli vytvoriť databázu skenovania očných dúhoviek, odtlačku prsta a nastáva tu možnosť neochoty zo strany užívateľa. Užívateľovi môže byť nepríjemné skenovanie očnej dúhovky, no ak sa jedná o bezpečnosť, mali by spraviť výnimku.

5.5 Zhrnutie všetkých typov

Nové modely systémov boli postavené na biometrických systémoch, konkrétne odtlačkov prsta, krvného riečiska a skenovanie očnej dúhovky, ktoré by boli využívané vo všetkých typoch autentizácie a autorizácie. Majú svoje výhody, ale aj nevýhody s ktorými treba počítať. Tieto systémy by poskytovali vysokú ochranu, zvýšenie bezpečnosti a zjednodušenie využívania všetkých typov. Pokiaľ by systémy využívali len jednu ochranu, napr., ak by išlo len o skenovanie a porovnanie odtlačku bez zadania hesla, PIN kódu, bezpečnosť by bola podpriemerná. Získať odtlačok prsta by bolo veľmi jednoduché napr. z pohára. Útočník si spraví odliatok vo vosku a takto by ho mohol zneužiť. V prípade využívania skenovania očnej dúhovky môže byť pre užívateľov nepríjemné, preto by určitú dobu trvalo, aby si ľudia na takýto systém zvykli. Pre bankovníctvo by nové systémy priniesli novú ochranu, no museli by na vývoj a realizáciu poskytnúť nemalé finančné prostriedky. Súčasné technológie a ich vývoj je na vysokej úrovni a ak si zoberieme, že nové smartfóny už v sebe obsahujú funkciu na odtlačok prsta, tak v smartbankingu, ale aj v inom type by to bol dobrý krok vpred.

ZÁVER

S nástupom nových informačných technológií ľuďom zjednodušujú a šetria čas. Avšak treba brať aj do úvahy, že s nimi prišli aj riziká, na ktoré nesmieme zabúdať. Elektronické bankovníctvo je forma, kde komunikuje banka a klient bez toho, aby sa nemuseli osobne stretnúť. Komunikácia prebieha vo virtuálnej forme. Preto musíme dbať nato, aby bola dostatočne zabezpečená.

Bakalárska práca sa zaoberala druhmi elektronických krádeží zameraný na bankový sektor. Medzi veľkú internetovú hrozbu sa zaraďuje sociálne inžinierstvo, ktoré sa do povedomia ľudí dostáva v malej miere. Hlavnými podvodnými technikami, ktoré útočníci v súčasnosti využívajú sú phishing, pharming, spying, skimming, vishing a tabnabbing apod. Preto boli rozobrané tieto typy útokov a akú techniku útočníci praktizujú. V súčasnosti sú elektronické bankovníctva veľmi využívané, preto je potrebné mať aspoň minimálne znalosti o týchto technikách. Boli opísané technologické opatrenia bezpečnosti, ktoré by mala banka spĺňať a dodržiavať ich. Týmto banka zabezpečí najvyššiu úroveň ochrany pred možnými útokmi. V praktickej časti bola spracovaná analýza bezpečnosti vybraných bánk. Popisovala vzhľad, dostupnosť bezpečnostných informácií, ku ktorým má klient možnosť prístupu. Patrili sem autorizačné a autentifikačné nástroje a aký spôsob šifrovania banky využívajú. Autorizácia a autentizácia bola zameraná na internetové bankovníctvo, smartbanking, bezkontaktné platobné karty a bankomaty. Boli opísané súčasné autorizácie, ich výhody a nevýhody a následne vytvorené nové návrhy pre bezpečnostnú autorizáciu a autentizáciu, kde boli využité biometrické systémy. Väčšinou sa využíval odtlačok prsta, ktorý bol pre všetky typy veľmi výhodný, ale napr. pri bankomatoch bolo využité skenovanie očnej dúhovky. Aj pri tomto novom návrhu boli popísané ich výhody a nevýhody či už zo strany banky alebo klienta.

Predpokladá sa, že tieto typy útokov budú neustále pribúdať a banky by mali tejto problematike venovať dostatočnú pozornosť. Aj napriek úsiliu zo strany bánk o silné zabezpečenie sa nedá každej hrozbe zabrániť, keď najslabším článkom celého zabezpečenia je samotný klient.

Bakalárska práca by mala čitateľa zoznámiť s problematikou bezpečnosti internetového bankovníctva a aby bol poučený a oboznámený s možnými hrozbami.

ZOZNAM POUŽITEJ LITERATÚRY

[1] JAŠEK, Roman a David MALANÍK. Bezpečnost informačních systémů. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013. ISBN 978-80-7454-312-8. Dostupné také z: http://hdl.handle.net/10563/25821

[2] POŽÁR, Josef. Informační bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. Vysokoškolské učebnice. ISBN 8086898385

[3] Informační bezpečnost. Managementmania [online]. 2015 [cit. 2016-04-03]. Dostupné z: https://managementmania.com/cs/informacni-bezpecnost

[4] DOBDA, Luboš. Ochrana dat v informačních systémech. Praha: Grada Publishing, 1998. ISBN 80-7169-479-7

[5] POŽÁR, Josef. Manažerská informatika. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2010. ISBN 978-80-7380-276-9

[6] Information technology in the banking sector : opportunities, threats and strategies. American University of Beirut [online]. Norway, 1998 [cit. 2016-04-03]. Dostupné z: http://ddc.aub.edu.lb/projects/business/it-banking.html

[7] Novinky.cz [online]. 2006 [cit. 2016-04-09]. Důvěra v zabezpečení internetového bankovnictví stála ženu 20 tisíc. Dostupné z www: http://www.novinky.cz/ekonomika/99752-duvera-v-zabezpeceni-internetoveho-bankovnictvi-stala-zenu-20-tisic.html

[8] OBR, Jiří. ItBiz.cz [online]. 2009 [cit. 2016-04-09]. Sniffing: Odposlech datové komunikace. Dostupné z www: http://www.itbiz.cz/sniffing-odposlech-datove-komunikace

[9] Petr. Root.cz [online]. 2008 [cit. 2016-04-09]. Jak prolomit WEP šifrování za pět minut. Dostupné z www: http://www.root.cz/zpravicky/jak-prolomit-wep-sifrovani-za-pet-minut/

[10] BOUŠOVÁ, Kateřina. Penize.cz [online]. 2006 [cit. 2016-04-09]. Internetové bankovnictví: jsou vaše peníze v bezpečí?. Dostupné z www: http://www.penize.cz/bezne-ucty/18366-internetove-bankovnictvi-jsou-vase-penize-v-bezpeci/

[11] KOLÁŘ, Jan. MOŽNÁ OHROŽENÍ ELEKTRONICKÉHO BANKOVNICTVÍ [online]. Brno, 2011 [cit. 2016-04-10]. Dostupné z: http://is.muni.cz/th/251357/esf_b/

[12] HOUSER, Pavel. SecurityWorld.cz [online]. 2010 [cit. 2016-04-10]. Vědci prolomili další šifru GSM. Dostupné z www: http://securityworld.cz/securityworld/vedci-prolomili-dalsi-sifru-gsm-2234

[13] Pravidla bezpečného užívání Internet Banky. Gemoney.cz [online]. [cit. 2016-04-10]. Dostupné z: https://www.gemoney.cz/documents/cz/primebankovnictvi/pravidla-bezpecneho-uzivani-ib.pdf

[14] PROTIVINSKÝ, Miroslav. Bankovní loupeže. Vyd. 1. Praha: Armex, 2001, 279 s. ISBN 80-862-4421-0

[15] Secure with Visa. Visa.ca [online]. 2016 [cit. 2016-04-10]. Dostupné z: http://www.visa.ca/en/personal/securewithvisa/phishing.jsp

[16] Jak je to s bezpečností internetového bankovnictví? Lupa.cz [online]. 2006 [cit. 2016-04-10]. Dostupné z: http://www.lupa.cz/clanky/jak-je-to-s-bezpecnosti-internetoveho-bankovnictvi/

[17] Original fishing scheme against Poste Italiane. Security Affairs [online]. 2013[cit. 2016-04-10]. Dostupné z: http://securityaffairs.co/wordpress/18883/cyber-crime/complex-fishing-poste-italiane.html

[18] Gamee.cz. Phishing aneb rhybaření [online]. 2008 [cit. 2016-04-10]. Dostupné z: http://www.gamee.cz/blogosfera/13063-phishing-aneb-rhybareni

[19] Nový typ podvodu v internetbankingu - „vishing“. [online]. 2010 [cit. 2016-04-10]. Dostupné z: http://www.sbaonline.sk/sk/presscentrum/tlacove-spravy-sba/novy-typ-podvodu-v-internetbankingu-vishing.html

[20] Dajte si pozor na skimming! Viete rozpoznať sfalšovaný bankomat?. [online]. 2013 [cit. 2016-04-10]. Dostupné z: http://www.itnews.sk/spravy/bezpecnost/2013- 03-04/c154590-dajte-si-pozor-na-skimming-viete-rozpoznat-sfalsovany-bankomat

[21] Pcmag.com: cyber espionage [online]. 2016 [cit. 2016-04-10]. Dostupné z: http://www.pcmag.com/encyclopedia/term/64376/cyber-espionage

[22] Vub.sk. Všeobecná úverová banka: Internet banking [online]. 2016 [cit. 2016-05-15]. Dostupné z: https://ib.vub.sk/ibr/login?sc=1

[23] Csob.sk Československá obchodná banka [online]. 2016 [cit. 2011-05-15]. InternetBanking 24. Dostupné z: http://www.csob.sk/internet-banking24

[24] Slsp.sk Slovenská sporiteľňa [online]. 2016 [cit. 2016-05-15]. Bezpečnostné predmety. Dostupné z: http://slsp.sk/podnikatelia-a-firmy/podnikatelia-a-malefirmy/elektronicke-bankovnictvo/internetbanking/bezpecnostsluzby/5618/bezpecnostne-predmety.html

[25] Tatrabanka.sk [online]. 2011b [cit. 2016-05-15]. Internet banking. Dostupné z http://www.tatrabanka.sk/cms/page/sk/fyzicke_osoby/elektronicke_bankovnictvo/internet_banking.html

[26] Ibpb.pabk.sk Poštová banka [online]. 2016 [cit. 2016-05-15]. Uţívateľská príručka Internet bankingu. Dostupné z: http://ibpb.pabk.sk/prirucky.aspx

[27] Biometric ATMs, the future?. [online]. 2005 [cit. 2016-05-15]. Dostupné z: http://www.rediff.com/money/2005/oct/11atm.htm

[28] Informatizácia - Informačná bezpečnosť. Informatizacia.sk [online]. 2014 [cit. 2016-05-15]. Dostupné z: http://informatizacia.sk/informacna-bezpecnost/2999s

[29] Oskole.sk. Symetrická šifra [online]. 2016 [cit. 2016-05-15]. Dostupné z: http://www.oskole.sk/?id_cat=1008&clanok=16677

[30] Shopsys.cz. *Nová platební metoda AGMO* [online]. 2012 [cit. 2016-05-16]. Dostupné z: https://www.shopsys.cz/clanky/nova-platebni-metoda-agmo/

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

PIN	Osobné identifikačné číslo
IDS	Systém pre odhalenie prieniku
SSL	Vrstva bezpečných socketov
WEP	Šifrovanie bezdrôtového protokolu
SMS	Krátka textová správa
GSM	Globálny systém mobilných komunikácií
SIM	Identifikačná karta v mobilnej sieti
USB	Univerzálna sériová zbernica
HTTP	Hypertextový prenosový protokol
DNS	Systém názvov domén
WWW	Celosvetová sieť

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK

ZOZNAM GRAFOV