Informační technologie v bankovnictví

Information Technology In Banking

Bc. Martina Koryčanská

Diplomová práce
2020

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

Ústav elektroniky a měření

Akademický rok: 2019/2020

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Martina Koryčanská**
Osobní číslo:	**A18744**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**Kombinovaná**
Téma práce:	**Informační technologie v bankovnictví**
Téma práce anglicky:	**Information Technology In Banking**

Zásady pro vypracování

1. Zpracujte rešerši literatury a pramenů k tématu.
2. Vymezte zkoumanou oblast – fenomenologie, etiologie
3. Analyzujte aktuální trendy a postupy užívané v bankovním sektoru proti vnitřním a vnějším hrozbám.
4. Analyzujte preventivní opatření v oblasti informačních technologií, využívání outsourcingu.
5. Výstupy z praktické části aplikujte ve vlastních návrzích a opatřeních, získaná data prezentujte v grafické podobě.

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

Seznam doporučené literatury:

1. KOCH, Miloš a ONDRÁK, Viktor. *Informační systémy a technologie.* Brno, VUT AN CERM 2008. ISBN – 9788021437326.
2. MAIULA, Jan. *Informační management.* Opava, Slezská univerzita 2017. ISBN - 9788075102645.
3. HAAG, Stephen a CUMMINGS, Maeve a PHLLIPS, Amy. *Management Information systems for the information age.* Boston, McGraw-Hill/Irwin, 2007. ISBN - 9780073052236.
4. GÁLA, Libor a POUR, Jan a ŠEDIVÁ Zuzana. *Podniková informatika.* Praha, Grada Publishing, 2015. ISBN – 9788024754574.
5. DOHNAL, Jan a POUR Jan. *IT v řízení podniku MBI.* Praha : Professional Publishing, 2016. ISBN – 9788074311604.

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

Datum zadání diplomové práce: **9. prosince 2019**
Termín odevzdání diplomové práce: **29. května 2020**

L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Milan Navrátil, Ph.D.
ředitel ústavu

Ve Zlíně dne 9. prosince 2019

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové 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 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 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 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 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 práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

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

Ve Zlíně, dne 12. 8. 2020

Martina Koryčanská, v. r.
podpis diplomanta

ABSTRAKT

Cílem práce je posouzení informačních technologií užívaných v bankovní sféře, možné hrozby a útoky, které tyto technologie ohrožují. Úvod práce je věnován informační bezpečnosti a vymezení pojmů. Práce dále specifikuje právní legislativu a navazuje na nejčastější hrozby a využívané metody ohrožující bezpečnost v bankovním sektoru. Závěr teoretické části jsem věnovala outsourcingu a jeho využití v bankovnictví. V praktické části se práce zabývá analýzou zabezpečení internetového bankovnictví významných bank v České republice. Závěr je zaměřen na nový návrh autentizace a autorizace s využitím biometrických identifikačních systémů.

Klíčová slova: informační technologie, informační systémy, bankovnictví, bezpečnost, hrozby, internetbanking, platební karty, smartbanking, autentizace, autorizace, identifikace

ABSTRACT

The aim of this thesis is to assess information technologies used in the banking sector, possible threats and attacks that threaten these technologies. The introductory section deals with information security and definitions. Further on, the thesis specifies the legislation and describes the most common threats and methods used to threaten security in the banking sector. The last chapter of the theoretical part deals with outsourcing and its use in banking. The practical part contains the analysis of Internet banking security of major banks in the Czech Republic. The conclusion is focused on new suggestions of authentication and authorization using biometric identification systems.

Keywords: information technology, information systems, banking, security, threats, internetbanking, payment cards, smartbanking, authentication, authorization, identification

Poděkování

Ráda bych na tomto místě poděkovala mému vedoucímu PhDr. Mgr. Stanislavu Zelinkovi za odborné vedení, praktické rady a vstřícnost při zpracování diplomové práce. Poděkování patří i mé rodině za neustálou podporu a motivaci po celou dobu studia.

Motto

„Když všichni mluví o nemožnostech, hledej možnosti.“

Tomáš Baťa

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

OBSAH

ÚVOD

V současnosti se nacházíme v době intenzivního rozvoje informačních a komunikačních systémů a technologií. Každou chvíli můžeme sledovat vývoj nových produktů, případně zdokonalovaní produktů a technologií již existujících. Tento neustálý vývoj informačních systémů má dopad na náš každodenní život, kdy si jen stěží dokážeme představit člověka, který nevlastní mobilní telefon, tablet, či jiné elektronické komunikační zařízení. Není proto vůbec překvapující, že provázanost rozvoje informačních technologií a bankovnictví je zřejmá a dnes už nikoho nepřekvapí.

Celá oblast bankovního sektoru je velmi důležitá pro ekonomické prostředí, které se transformací a inovací finančních produktů přizpůsobilo technickému vývoji moderních technologií a požadavkům klientů volajících po pohodlnosti. Komunikace mezi klientem a bankou doznala velkých změn, které umožňují klientovi ovládat bankovní úkony z pohodlí domova a prostřednictvím chytrých mobilních telefonů vlastně odkudkoliv, aniž by musel navštívit banku. Velký vliv na komunikační vývoj mezi klientem a bankou má internet, který bankovní sféru bezpochyby nejvíce ovlivnil. Rozšířil velké možnosti a přínosy informačních technologií a zvláště celých informačních systémů, které jsou technologickým základem revolučních společenských změn vedoucích ke společnosti nového typu, tzv. informatické společnosti.

Využívání moderních informačních a komunikačních technologií má řadu výhod, jak pro banku, tak pro klienta. U obou stran je to hlavně úspora času, který v dnešní uspěchané době hraje velkou úlohu. Vývoj a kvalita informačního systému tak přímo ovlivňuje kvalitu služeb banky. Nemalým problémem však zůstává komunikační bezpečnost mezi klientem a bankou, která se týká přenosu osobních a důvěrných informací o klientovi, jeho osobním účtu a riziko s tím spojené. Pro útočníky a narušitele se jedná o velmi zajímavou oblast. Forma útoků na bankovní data a finanční prostředky klientů se stále zvyšuje, proto i vývoj této oblasti, týkající se komunikační bezpečnosti zůstává neustále střežen, jak v rovině praktické, tak v rovině právní.

Cílem diplomové práce je zpracovat problematiku informačních technologií v bankovnictví. Využitím analýzy stávajících trendů se pokusím představit a ukázat pravidla, která by měla zamezit vzniku příchozích rizik. Tato rizika mohou ohrozit jak banku, tak i její klienty.

Diplomovou práci tvoří několik kapitol. V první kapitole jsou popsány a vymezeny základní pojmy, které popisují informační bezpečnost, systém spolu s procesem a na závěr šifrování. Druhá a třetí kapitola je zaměřena na právní rámec bezpečnosti a vývoj moderního bankovnictví v porovnání s minulostí. Dále popisuje zabezpečení osobních dat a informací, kde se zaměřuji na pojem autentizace a způsob identifikace v elektronickém bankovnictví.

Následující čtvrtá kapitola popisuje programovou bezpečnost informačních systémů a programy, které tuto bezpečnost mohou narušovat. V páté kapitole jsou vymezeny pravidla bezpečnosti v síti internet. Šestá kapitola se zabývá outsourcingem a jeho využití v bankovním sektoru.

Praktická část je zaměřena na analýzu bezpečnosti internetového bankovnictví v pěti nejznámějších bankách v Česku. Sdílnost jednotlivých bankovních institutů, na které jsem rozeslala písemnou prosbu o sdělení informací, které se týkaly bezpečnostních prvků zabezpečení přihlašovací stránky dané banky, nebyla na moc vstřícné úrovni, což je asi pochopitelné stanovisko ze strany banky. Přesto se mě podařilo zpracovat analýzu zabezpečení komunikace prostřednictvím testu certifikační autority na stránce *Qualys SSL Labs* a pro ověření správnosti získaných informací ještě na stránce *ImmuniWeb security*. Závěr praktické části je zaměřen na nové návrhy a opatření v oblasti bankovních informačních technologií.

I. TEORETICKÁ ČÁST

1 INFORMAČNÍ TECHNOLOGIE A INFORMAČNÍ BEZPEČNOST

Společnost je stále více odkázána na použití informačních technologií. Informační systémy a informační a komunikační technologie se stávají páteří v mnoha odvětvích. Tento proces je pro dnešní moderní dobu nevyhnutelný. Vývoj a nabídka možností v oblasti informačních technologií neustále roste a tím vzrůstá i množství nástrah, které nás při cestě k jejich ovládnutí čekají. Žádná organizace užívající informační a komunikační technologie jako součást svého informačního systému se dnes neobejde bez bezpečnostních opatření. V každém případě je výhodné řešit problémy bezpečnosti informačního systému komplexně s ohledem na všechny jeho složky. Nestačí bezpečnostní politiku vytvořit, je potřebné dostat ji do povědomí zaměstnanců, aby se bezpečnostní chování stalo samozřejmostí. [1]

1.1 Informační technologie

Informační technologie v posledních dekádách nabyly tak široké uplatnění, že jejich vývoj podmiňuje rozvoj moderní společnosti. Samotný rozvoj informačních technologií v posledních letech je vyvoláván stále rostoucí potřebou společnosti po informacích a po neustále dokonalejším informačním zabezpečení těchto informací.

Při praktickém využívání informatiky pro všechny operace s daty se používají technické a programové prostředky. Souhrn těchto prostředků a postupů se označuje jako informační technologie.

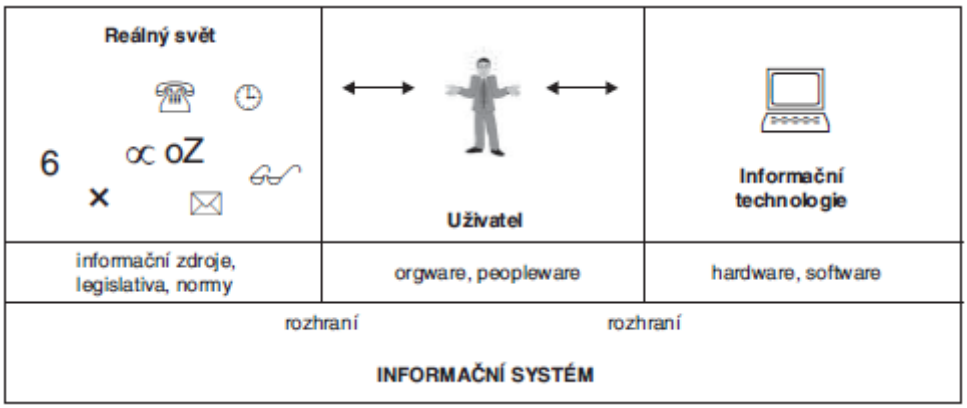
V současnosti neexistuje odvětví lidské činnosti, které by nebylo charakterizováno aktivním využíváním informací a informačních technologií. Komunikační možnosti se stávají základní vlastností současných automatizovaných systémů řízení. [2]

Jako definice pro pojem informační technologie je uváděno, že *„**Informační technologie** představují množinu prostředků a metod používaných na práci s údaji a informacemi. Je to široce definovaný pojem informačních technologií, který zahrnuje různé techniky a technologie sběru, přenosu, zpracovávání, uchovávání, distribuování a prezentace informací.“* [2]

Jedná se o jakýkoliv elektronický přístroj, který je schopen zpracovat určité informace. Tento přístroj musí umět přijmout vstupní data, ta následně zpracovat (tj. ukládat a uchovávat) a vytvořit z nich příslušná výstupní data. Mluvíme-li o informačních technologiích, máme na mysli hardwarové a softwarové vybavení.

Hardware – je označení pro širokou škálu různých zařízení (počítače, počítačové systémy a další stroje včetně příslušenství), doplněné o potřebné periferní jednotky, které jsou v případě potřeby propojeny prostřednictvím počítačové sítě a napojeny na paměťový subsystém pro práci s velkými objemy dat.

Software – je označení pro informační technologie, tvořené systémovými programy, řídícími chod počítače, efektivní práci s daty a komunikaci počítačového systému s reálným světem. Může se jednat o aplikační programy, řešící určité třídy úloh určitých tříd uživatelů. [3]



Obrázek 1 Prvky informačního systému [1]

1.2 Informační bezpečnost

Pojem ***„bezpečnost“*** obecně, si každý z nás může vyložit jinak. Záleží na tom, jakou bezpečnost má na mysli. Dokážeme se ale shodnout, že bezpečnost nám zaručuje určitý druh jistoty a zmenšuje lidem vlastní pocit možného ohrožení. Každý se chce cítit bezpečně po celý svůj život. Existují tři skupiny, do kterých můžeme zařadit bezpečnost, resp. ochranu:

- život, zdraví,
- majetek (hmotný i nehmotný, každý majetek, který má určitý vztah k předmětům),
- informace, data, znalosti.

Tyto skupiny spolu v řadě případů úzce souvisejí (např. takové porušení bezpečnosti informace, případně její ztráta může vést ke ztrátám na majetku) a často se i prolínají, zejména v případě ochrany nehmotných statků a informací a znalostí na informacích založených.

Poznatky a znalosti získané na základě informací tvoří zvláštní skupinu. Nejedná se tedy o veškeré informace, které jsou běžně dostupné, ale jen o informace, které mají určitou (často velmi významnou) hodnotu pro jejich nositele a pro určitý okruh subjektů v případě, že by tuto informaci (znalost) získaly. Subjektem ochrany jsou všichni uživatelé informačních systémů. [4]

Lidé si myslí, že když používají dostatečně silná hesla, tak to stačí pro zajištění informačních systémů. Důležité je zajistit systém jako jeden celek. Vnější a vnitřní ohrožení je přímo úměrné kvalitě, která je prováděna bezpečnostní politikou každého státu. Bezpečnostní politiku si můžeme vysvětlit, jako analýzu bezpečnostních hrozeb a rizik, jejich výběr a efektivita a v poslední řadě protiopatření k jejich snížení. Každý stát se snaží reagovat na dynamický, ale i dramatický vývoj bezpečnostního prostředí v uplynulém období.

Zvyšování rychlosti a kvality informačního procesu má na starosti rychlé rozšíření informačních a komunikačních technologií. Proto je velmi nutné, aby se dbalo na pozornost a dostatečnou ochranu dat a informací v informačních systémech. Nesmíme zapomínat ani na útočníky, kteří se také snaží a hledají nové způsoby a cesty útoků na informační systémy za účelem zničení, změny nebo snahy dostat se do těchto systémů.

- *Mezi vnější* okolnosti náleží zejména existence hrozeb a míra rizika s jakou se hrozby mohou uskutečnit.
- *Mezi vnitřní* okolnosti náleží například ekonomické možnosti subjektu realizovat nutná protiopatření.

V současné době se jedná o trestnou činnost, která se nazývá kybernetická kriminalita. Tato kriminalita ohrožuje důležité pojmy, jako jsou důvěrnost, integrita a dostupnost počítačových systémů. Nejedná se jen o tyto, ale spadá sem i bezpečnost rozhodující o kritických infrastrukturách státu. Při rychlosti, jakou se vyvíjejí dnešní technologie, vznikají různé druhy problémů, které vyplývají z kybernetické kriminality a odrážejí rozdíly ve znalostech. Nastávají zde složité forenzní problémy, kterým musí vyšetřovatelé a státní zástupci čelit. Je to kvůli tomu, že digitální procesy vznikly s nehmotnou a přechodnou povahou digitálních důkazů. Kromě toho je nutné smysluplné vyšetřování a stíhání kybernetické kriminality, časté sledování kriminálních aktivit, které mohou vycházet i za hranice státu, což dále komplikuje situaci a vedení k otázkám týkajících se pravomocí.

Informační bezpečnost je označení pro aktivitu, která směřuje k ochraně informací. Jde o ochranu informací a dat před negativními událostmi. Jedná se o ztrátu, únik, odcizení, zneužití, zničení, změny nebo narušení celistvosti, důvěrnosti a dostupnosti. Chráněné informace mohou mít různou podobu, např. může jít o elektronickou, tištěnou, ale existují i takové informace, které lze odpozorovat z logistických procesů.

Zneužití informace hrozí nejen z vnějšího prostředí, ale ve větší míře sem spadá i vnitřní prostředí (organizace). Informace jsou pro organizaci klíčovým zdrojem. Pokud bychom o ně přišli, nebo pokud by se informace dostaly do rukou konkurence, dalo by se to nazvat jako konec fungování a podnikání.

O informace můžeme přijít na svém počítači, na serveru nebo počítačové síti. Informační bezpečnost lze označit jako celkový pohled na organizaci, která pomáhá poznávat a chránit si svá data. Snaží se nasměrovat k praktickým opatřením a k eliminaci snížení škod, při mimořádných událostech. Informační bezpečnost chrání informace jako celek.

Je třeba vytyčit a pochopit, jaké informace daná organizace má a jaká je jejich hodnota. Součástí informační bezpečnosti je řízení bezpečnosti. Je třeba promyslet fungování organizace a na základě toho navrhnout fungující a efektivní systém řízení informační bezpečnosti. Dalším faktorem je i dlouhodobá funkčnost a rozvoj systému, který bude reagovat na změny organizace a jejího okolí. Pomocí zavedení dobře fungujícího systému je možné minimalizovat rizika patřící k úniku informací. Dále tento systém pomáhá snižovat náklady na informační a komunikační technologie a následnou efektivitu procesů. Velkou roli hraje i při rozhodovacích procesech. Tyto systémy řízení, by měly zlepšit situaci v interních službách a procesů, a navíc procesů a služeb pro klienty organizace nebo státní instituce. [5]

Okruhy činností řízení informační bezpečnosti v organizaci.

- Potřeba stanovit si pravidla zacházení s informacemi – kdo, kdy, jak, proč má přístup k datům nebo informacím.
- Stanovení řízení přístupu k datům a informacím – třeba vědět, kdo a k jakým informacím může a kdo nesmí. Vědět, zda existuje ochrana proti podvodům.
- Řešit bezpečnost zařízení proti ztrátě a odcizení – např. pracovník ztratí nebo mu byl ukraden počítač – je třeba vědět, co se stane. Byla data zálohována? Je disk šifrován?

- Ochrana proti napadení nebo odcizení informací – řeší otázku o dostatečném zabezpečení sítě proti kybernetickým útokům.
- Uložená data z pohledu havárie – ochrana proti haváriím, zničení serverů (požár, kolaps disku), schopnost obnovit data.

Celkovou odpovědnost za řízení bezpečnosti ve velkých a středních organizacích má manažer bezpečnosti. V řadě velkých organizací existuje profese manažera informační bezpečnosti zaměřená výhradně na informační a komunikační bezpečnost. Velké organizace nebo organizace podnikající v rizikovém prostředí (například banky, pojišťovny) mohou mít ještě další určené specialisty řízení bezpečnosti. [6]

1.3 Základní pojmy informační bezpečnosti

Do informační bezpečnosti zasahuje mnoho nových pojmů a definic, proto je třeba si tyto definice vysvětlit, a hlavně správně pochopit danou problematiku. Informační systémy jsou ohrožovány větším množstvím hrozeb a je třeba předem vědět, že jim hrozí nebezpečí. Pokud dojde k poškození, které bylo způsobeno přírodními vlivy, dokážeme ho rychle zjistit a vyhodnotit. Pokud by došlo k nelegálnímu úniku informací, nebo dat, tak velmi těžko by se tento únik dokazoval. V případě, že k úniku dojde, tak majitel informačního systému nechce o tom komunikovat, protože se zkreslují informace a z dané situace vyplyne, že o nic nejde. Útoky proto bývají neodhalené, a pokud se i podaří část útoků odhalit, tak se nikdy nedostanou k veřejnosti, aby ten, kdo se postaral o únik informací, nevěděl, k jakému úspěchu se dopracoval. Pokud jde o uživatele, tak ten nechce ztratit svou dobrou pověst.

Celá problematika informační bezpečnosti je velmi rozsáhlá a závažná a lze ji definovat jako *„**Informační bezpečnos**t je ochrana informací během jejich vzniku, zpracování, ukládání, přenosů a likvidace prostřednictvím logických, technických, fyzických a organizačních opatření, která musí působit proti ztrátě důvěrnosti, integrity a dostupnosti těchto hodnot.“* [7]

Bezpečný informační systém pak definujeme *„jako systém, který chrání informace během jejich vstupu, zpracování, uložení, přenosu a výstupu proti ztrátě dostupnosti, integrity a důvěrnosti a při jejich likvidaci proti ztrátě důvěrnosti.“* [7]

1.3.1 Aktivum

Mezi aktiva se zařazují všechny hmotné, ale i nehmotné majetky, vše, co má pro majitele určitou hodnotu. Pro člověka a majitele organizace jsou největší hodnotou data a informace. Pokud by o ně přišel, nebo by byly zneužity pro jiné účely, dané osobě nebo majiteli by způsobily obrovské škody. Proto by mělo být každé aktivum vhodným způsobem chráněno. Aktiva se rozdělují na hmotná a nehmotná.

Hmotná aktiva vznikají za pomoci výpočetní techniky a komunikačními technologiemi (počítače, diskové pole, servery, aktivní síťové prvky). Pokud by majitel potřeboval zjistit hodnotu těchto aktiv, zjistí to jednoduše, a to podle jejich pořizovací ceny.

Mezi *nehmotná aktiva* se zařazují data a programové vybavení. Nejsou to žádné věci fyzické povahy. Jsou to např. operační systémy, patenty, ochranné známky, programové nástroje pro řízení informačního systému a v neposlední řadě aplikační programy. Důležitou součástí nehmotných aktiv je datová základna.

Hodnot aktiva může být jeho cena, ale může to být také ocenění důležitosti a významu pro majitele, které se často ani konkrétní finanční hodnotou vyjádřit nedá. Každý tento chráněný objekt má proto svoji cenu, která může být rozdílná jak pro majitele, tak pro útočníka. [7]

1.3.2 Bezpečnost

Obecně pojmenovává stav, kdy při provádění běžné práce nezpůsobuje újmu. V případě možné újmy je tato minimalizovaná a tudíž akceptovatelná. *„Bezpečnost proto chápeme jako vlastnost objektu nebo subjektu (v našem případě informačního systému, nebo informační technologie), která určí stupeň, míru jeho ochrany proti škodám a hrozbám (ztrátě, zneužití, nebo zničení), které mohou vzniknout“*. [5]

1.3.3 Hrozba

Hrozbu lze pojmenovat jako skutečnost, událost, sílu, nebo osobu (osoby), která může svou činností způsobovat narušení důvěrnosti, hodnotu aktiva nebo integritu. Hrozba často poukazuje na objektivní jev, který je identifikovatelný a reálně začíná působit destrukčně. Hrozby mohou spouštět jak lidé, tak i vliv techniky (porucha zařízení, hacker, zaměstnanec aj.) nebo přírodní jevy (voda, oheň). Mezi lidské hrozby patří teroristé, zločinci (jednotlivci, skupina) a nadšenci do počítačových systémů. [5]

1.3.4 Riziko

Riziko je pojem, kterým se dá vyjádřit, zda hrozba zneužije zranitelnost a může způsobit narušení integrity. Stejně může způsobit nedostupnost aktiv. Jde o výraz, s jakou pravděpodobností bude aktivum poškozeno nebo zničeno díky působení konkrétní hrozby. Výsledek je často jiný, než byl očekáván. [5]

1.3.5 Ocenění rizik

Při ocenění rizik se vyhodnocují hrozby, které mohou určitým způsobem napadat informační systém. Pokud by hrozilo, že systém bude reálně vystaven určitému riziku, musí dokázat definovat úroveň rizika, které může nastat a včas ho minimalizovat nebo úplně eliminovat. Hlavním cílem ocenění rizik je zjišťování, zda zavedená bezpečnostní opatření vyhovují a jsou dostatečně silná na to, aby uměla zredukovat pravděpodobnost vzniku škody. [5]

1.3.6 Zranitelnost

V každém systému existuje daná zranitelnost, která určuje slabou část celého bezpečnostního systému. Nemusí jít vždy o celý bezpečnostní systém, ale může jít jen o jeho část. Pokud dojde k poškození, v horším případě zničení hodnot nebo aktiva, můžeme určit, že slabá část bezpečnostního systému byla zneužita hrozbou. V každém informačním systému existují zranitelná místa – prvky, která jsou využitelné pro útočníka k útoku na data, nebo celý systém. Mohou to být slabiny softwaru, aplikace, ale i lidské (úmyslné i neúmyslné) chyby, neznalost, podcenění bezpečnosti. [5]

1.3.7 Útok

Útokem rozumíme úmyslné využití zranitelného místa ke způsobení škod/ztrát na aktivech informačního systému, nebo neúmyslné uskutečnění akce, jejímž výsledkem je škoda na aktivech. Analýzou možných forem útoků na informační technologie je třeba řešit problémy typu:

- jak se projevuje počítačová kriminalita,
- jaké jsou možné formy útoků, kdo útočí,
- jaká rizika souvisí s používáním informačních technologií,
- jak se před útoky chránit.

Útočit se může přerušením, odposlechy, změnou či přidáním hodnoty k datu. [5]

1.4 Informační systém

Je soubor lidí, zdrojů a uživatelů zaměřených na technické prostředky a metody, které zajišťují přenos a zpracování dat. Jejich účelem je tvorba informací. Systémy nás denně obklopují, aniž si to výrazným způsobem uvědomujeme. Označuje se jako určitá abstrakce reálného objektu. Tuto abstrakci lze definovat při respektování vytyčeného cíle určitými prvky a vazbami mezi nimi. Za společné znaky se dají označit prvky systému, které mohou být současně systémem nižšího řádu, ale i systémy, které mohou být současným prvkem systému vyššího řádu.

U informačního systému, ale také u jakéhokoli jiného systému, rozlišujeme dvě základní vlastnosti:

- struktura systému,
- fungování systému. [5]

Strukturu systému lze chápat jako způsob uspořádání jednotlivých prvků systému a vazeb mezi nimi. Čili nejde jen o náhodný, libovolný chaoticky rozházený souhrn prvků, ale každý prvek má přesné vymezení místa, zejména jeho funkční vztahy k ostatním prvkům (nadřazenost, nebo podřízenost, osobní vztahy, organizační pravidla, právní normy aj.).

Fungování systému lze chápat jako závislost mezi podněty a reakcemi. Podněty na systémy nemusejí pocházet přímo z okolního prostředí. Jejich zdrojem může být sám systém. Pokud jde o tyto podněty, mluvíme o podnětech vnitřních, kterými je systém ovlivňován a může na ně odlišně reagovat. Informační systém se nám může zdát velmi jednoduchý a dokážeme si ho sami ovládat bez jakéhokoli složitého technického vybavení. Po čase nám budou informace a data přibývat a na jejich zpracování a ukládání je třeba najít výkonnější informační technologie. Zjistíme, že takový přístup nám nemůže stačit.

Každý informační systém by měl v sobě obsahovat alespoň základní tvorbu databází, která je na systémové úrovni. V ní mají soubory definovány své struktury. Tyto databáze musejí být chráněny, aby se k nim nedostala neoprávněná osoba, která by mohla obsah databází změnit.

Další důležitou věcí informačního systému je systém, který chrání integritu dat. Například pokud jde o transakci, musí být dokončena i pokud by došlo k výpadku elektřiny nebo při poruše počítače. [5].

1.5 Informační proces

Pojem ***„informační proces“*** zahrnuje řadu dílčích procesů k možnému využívání informací. Jde o uzavřený cyklus od vzniku informace až k jejímu použití. Pomocí informačního systému je zajišťován informační proces, kam patří operace s daty a informacemi, které obsahují určité kroky:

- získávání informací,
- přenos informací (od zdroje do místa zpracování),
- určitou registraci, na kterém místě byly zpracovány,
- ukládání informací pro práci do budoucna,
- zpracování informací, kam spadá třídění a posuzování kvality vlastností, ale i vyhledávání doplňkových informací a tvorba nových informací,
- využívání informací. [5]

1.6 Šifrování

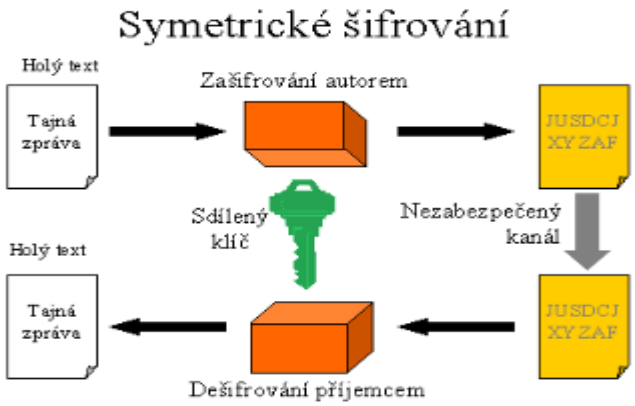
Šifrovací techniky je možné použít pro citlivé údaje a data. Tímto se výrazným způsobem docílí snížení rizika anebo dokonce jeho odstranění. V případě, že útočník získá citlivá data, nebude díky šifrování možné tato data vyzradit. Existuje zde šifrovací algoritmus, který umožní zasílaná data zašifrovat pomocí šifrovacích klíčů. Znamená to, že je pak nelze přečíst a jsou pro nás bez znalosti dešifrovacího klíče nesrozumitelné. V jednoduchém případě to může být jen heslo, v opačném případě se může jednat o posloupnost numerických znaků apod. *„Šifrovací algoritmus je proces transformace, která převede otevřený text (plain-text) na šifrovaný text (cipher-text) a naopak.“* [5]

Využívání šifer má své dávné historické kořeny. Až donedávna bylo výsadou organizací, jako jsou diplomatické služby, armáda či zpravodajské centrály. Rozsáhlé nasazování informačních a komunikačních technologií tuto situaci zásadně mění. Počítače dnes umožňují realizovat i ty nejsložitější šifrovací algoritmy. Kryptografie poskytuje neocenitelné služby při přenosu informací na větší vzdálenosti, zejména telekomunikační kanály, kdy je přenos informací úplně mimo kontrolu běžného uživatele. Postupným pronikáním moderních informačních a komunikačních technologií do všech oblastí života moderní společnosti se bez kryptografie nelze obejít. Kromě přenosu informací na velké

vzdálenosti se kryptografie využívá v bankách při peněžních transakcích a operacích. Většina organizací používá k šifrování počítačů, které jsou propojeny přes speciální linky a data jsou po celé délce přenosu šifrována. [5]

1.6.1 Symetrické šifrování

Pokud se použije k zašifrování a dešifrování zprávy symetrické šifrování je třeba, aby odesílatel i příjemce zprávy použili stejný tajný klíč. Zabezpečení přenosu doručení klíče je velmi podstatné, aby se klíč nedostal do nepovoleného vlastnictví.



Obrázek 2 Symetrické šifrování. [13]

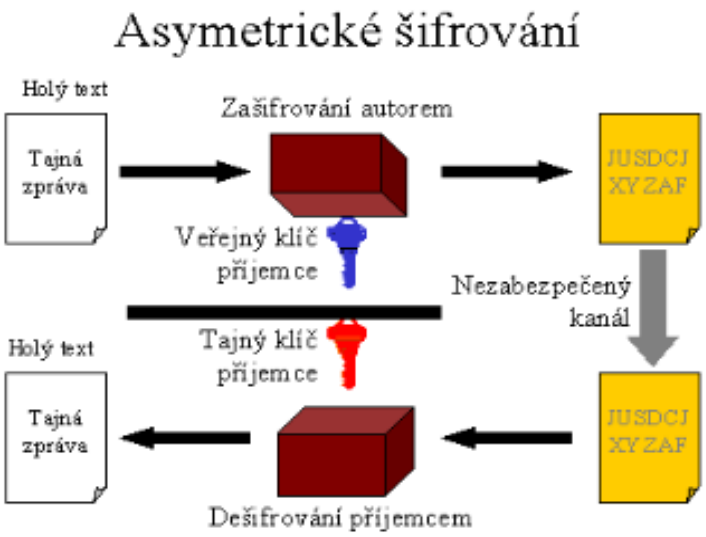
K známým a nejčastěji používaným symetrickým metodám patří šifrovací algoritmy:

- AES - *Advenced Encryption standard* (Pokročilý šifrovací standard), šifruje bloky o délce 128, 192 a 256 bitů a podporuje délky klíčů 128, 192 a 256 bitů. V současné době není možný útok hrubou silou ani na 128 bitový klíč.
- BlowFish - používá bloky dlouhé 64 bitů a proměnlivou délku klíče od 32 až po 256 bitů
- IDEA - šifruje bloky dlouhé 64 bitů, s délkou klíče 128 bitů
- RC4 - *Rivest Cipher 4* šifruje bloky dlouhé 64 bitů, a délkou klíče 40-128 bitů
- 3DES - šifruje bloky dlouhé 64 bitů, a délkou klíče 128 nebo 192 bitů
- DES - využíval délku klíče 56 bitů, kterou se podařilo prolomit

Doporučuje se používat RC4 nebo AES, které mají délku klíče 128-256 bitů. Výhodou je jejich rychlost a nenáročnost na výpočetní techniku a možnost zpracování velkého objemu dat. Nevýhodou je zasílání šifrovacích tajných klíčů, v případě tajné komunikace. [5]

1.6.2 Asymetrické šifrování

Při asymetrickém šifrování se používá jeden klíč pro zašifrování a druhý pro dešifrování dokumentů. Zpráva se zašifruje veřejným klíčem a dešifruje se pomocí soukromého klíče. Pokud chce uživatel dostat zašifrovanou zprávu, musí nejprve poskytnout svůj veřejný klíč. Ten odesílatel použije k zašifrování zprávy a kód odešle. Pro dešifrování potřebuje mít příjemce druhý klíč z páru - svůj vlastní soukromý klíč, kterým zprávu dešifruje. Výhodou oproti symetrickým metodám je, že není třeba posílat soukromý klíč a nedojde tak k jeho prozrazení.



Obrázek 3 Asymetrické šifrování. [13]

Asymetrické algoritmy jsou velmi pomalé a prakticky nepoužitelné pro šifrování velkého objemu dat. V praxi se často obě metody kombinují: vlastní data se zašifrují pomocí symetrického algoritmu AES a použitý jednorázový klíč (který je dosti malý) se zašifruje pomocí asymetrického algoritmu RSA (iniciály autorů Rivest, Shamir, Adleman) šifra s veřejným klíčem. RSA algoritmus je použitelný jak pro šifrování, tak pro podepisování dokumentů.

„Hlavní výhodou je to, že není třeba nikam posílat soukromý klíč a tak nemůže dojít k jejímu vyzrazení. Naproti tomu veřejný klíč je možné dát k dispozici všem. Je třeba méně klíčů než u symetrických metod. Nevýhodou je malá rychlost oproti symetrickým metodám. Další nevýhodou je ověření pravosti klíče.“ [5]

2 PRÁVNÍ RÁMEC BEZPEČNOSTI

Ochrana dat v informačních systémech musí mít jednotný právní rámec. Pokud by zákony jasně nedefinovaly vztahy mezi chráněnými údaji, jejich majitele nebo útočníků, nebylo by možné ani stíhání. Současný právní řád České republiky obsahuje právní normy, které řeší dílčí problémy, ale právní předpis pro informační bezpečnost v české legislativě chybí. Vzhledem k absenci právního předpisu, který by řešil informační bezpečnost se ochrana informačních a komunikačních systémů řídí různými právními předpisy. Výsledkem je nedostatečná úroveň ochrany informačních a komunikačních technologií.

Legislativa informační bezpečnosti:

- Zákon č. 21/1992 Sb. Zákon o bankách
- Vyhláška č. 163/2014 Sb. Vyhláška o výkonu činnosti bank, spořitelních a úvěrních družstev a obchodníků s cennými papíry
- Zákon č. 634/1992 Sb. Zákon o ochraně spotřebitele
- Zákon č. 89/1995 Sb. Zákon o státní statistické službě
- Zákon č. 106/1999 Sb. Zákon o svobodném přístupu k informacím
- Zákon č. 365/2000 Sb. Zákon o informačních systémech veřejné správy a o změně některých dalších zákonů
- Zákon č. 412/2005 Sb. Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti
- Zákon č. 297/2016 Sb. Zákon o službách vytvářejících důvěru pro elektronické transakce
- Zákon č. 110/2019 Sb. Zákon o zpracování osobních údajů
- Zákon č. 311/2019 Sb. Zákon, kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů
- Zákon č. 40/2009 Sb. trestní zákoník
- Zákon č. 89/2012 Sb. občanský zákoník

3 INFORMAČNÍ TECHNOLOGIE 21 STOLETÍ

Nástupem 21. století přišla doba nových technologií. Přinesla s sebou moderní komunikace, znalosti a výpočty v oblasti informační bezpečnosti. Změnilo to způsob života, kterým lidé dosud žili a který se bude neustále dále měnit. Radikálně se změní způsob práce a lidské přemýšlení dostane jiný rozměr. V dnešní době, při rychlém nárůstu vysokorychlostních sítí, je už možné používat aplikace, které v minulosti nepřipadaly v úvahu. Výhodou je, že klesají nároky na výpočetní výkony a stávají se tak cenově dostupnější. Přenášet data, obrázky nebo jiné digitální soubory dokážeme během několika sekund a to po celém světě. Tato nová technologie celkově mění způsob bankovního sektoru.

V minulosti šlo vše papírovou formou, ale dnes tuto komunikaci změnily digitalizované soubory. Bankovní sektory se změnily na digitalizované a síťové bankovní služby. Tato změna rovněž změnila vnitřní účetnictví a management systému banky. Došlo k zásadní změně v komunikaci mezi bankou a klienty. Banky po celém světě neustále čelí novým výzvám měnícího se prostředí, proto musí usilovat o správném nalezení technologických řešení. S určitou pravděpodobností se dá říci, že s nástupem nových technologií se navždy změní postupy a celkově celý bankovní sektor. Banky po celém světě, které mají schopnost investovat nebo integrovat informační technologie, se díky tomu stanou bankami, které se svou dominancí budou okupovat vysoké místo na konkurenčním globálním trhu. Management každé banky si je vědom, že investice do informačních technologií jsou v dnešní době rozhodující pro zvyšování jak konkurenceschopnosti, tak poskytovanou rychlost a kvalitu jednotlivých služeb klientům banky. [8]

3.1 Technologie a transformace bank

Počítačová technika a samotné počítače se dnes pro běžného člověka dají brát jako složitá technologie. Každým rokem stoupají nároky na počítačovou gramotnost a stávají se stále komplikovanějšími. Počítačová technika nabídla mnohým bankám velký potenciál a svým bankovním klientům dala obrovské očekávání. Zaměstnanci bank, úředníci i klienti se museli přizpůsobit těmto novým změnám přicházejícím do bankovnictví. Banky, které prošly velkým vývojem a investovaly do moderních technologií, umožňují mnohem pohodlnější poskytování bankovních služeb svým klientům. V budoucnu se budou úspěšné banky od sebe rozlišovat rychlým přístupem k důležitým informacím a schopností rychlého a efektivního řízení. [8]

3.2 Zabezpečení osobních dat a informací

K zabezpečení osobních dat a informací se uplatnila kombinace šifrování citlivých údajů a dostatečná autentizace. Tato kombinace se doporučuje pro uživatele, kteří chtějí mít svá data a komunikaci řádně zabezpečenou.

3.2.1 Autentizace

Autentizací se dá označit proces, pomocí kterého se poskytuje jistá záruka identity sloužící k jednoznačnému určení uživatele, který přistupuje k systému. Ve zkratce řečeno, jde o ujištění se, že daná osoba nebo uživatel je právě ten, za koho se vydává.

Ověřování uživatele se provádí prostřednictvím vnitřních mechanizmů systému, zpravidla prostřednictvím databázového serveru, kde je vytvořena databáze uživatelů s nastavenými hesly. Tato hesla jsou navíc zašifrována.

Existují tři možné způsoby identifikace:

- autentizace pomocí uživatelského jména a hesla,
- autentizace pomocí tokenu nebo čipové karty s certifikátem.
- autentizace pomocí biometrie (otisky prstů),

Pro zvýšení bezpečnosti je možná kombinace všech tří způsobů. Pokud jde o autentizaci pomocí uživatelského jména a hesla, je třeba zadat správně jméno a heslo, které vlastní daný uživatel. Jde o nejvíce využívané přihlašování do systému. Problém, který se zde může naskytnout, je zapomenutí hesla nebo zvolení hesla slabého. [4]

Autentizace prostřednictvím jména a hesla: doporučené zásady týkající se vytváření a používání hesel.

- Nejdůležitější je ochrana hesla. Heslo nikomu neprozrazovat a držet je v tajnosti. Jednoduché a účinné pravidlo.
- Složitost hesla je důležitá. Jednoduchá hesla a klasická jmenná hesla (Petr, Jan) se nedoporučují, protože jsou snadno uhodnutelná.
- Použitá hesla by měla odolávat slovníkovému útoku. Na internetu existují programy, které obsahují slovník slov z různých jazyků. Stačí tento program spustit a v případě jednoduchého hesla dokáže tento program za krátkou dobu heslo odhalit.

- Heslo by se mělo měnit v určitých intervalech. Změna hesla může zaskočit i útočníka, který získá informace pouze během doby platnosti hesla, než si uživatel heslo změní.
- Použití starých hesel se nedoporučuje, mohlo by dojít k opětovnému prolomení.
- Dodržovat délku hesla. Heslo se považuje za dostatečně bezpečné, pokud jeho délka obsahuje minimálně 14 znaků obsahující písmena, čísla i znaky. Za bezpečně silné heslo lze považovat: "Mt47 & UHWx # 50wK".
- Takový tvar hesla může být pro některé lidi těžko zapamatovatelný, je důležité nepsat heslo na papír jako pomůcku nebo ho dokonce lepit na monitor. To by výrazným způsobem usnadnilo práci útočníkovi.
- Nepoužívat stejné heslo ve více aplikacích. [4]

Autentizace prostřednictvím tokenu - tokeny jsou, zjednodušeně řečeno, zařízení, která mohou uživatelé nosit neustále s sebou, aby se mohli autentizovat do systém. Mají buď specifické fyzické vlastnosti (tvar, elektrický odpor, elektrickou kapacitu, atd.), nebo obsahují specifické tajné informace (např. kvalitní heslo nebo kryptografický klíč), nebo jsou dokonce schopny provádět specifické (obvykle kryptografické) výpočty.

Nejčastějším autentizačním tokenem současnosti jsou karty. Uživatelé vlastnící tyto karty jsou vázáni na zadání čísla, tzv. PIN kódu, čímž se minimalizuje riziko spojené s jejich ztrátou či krádeží. Úplně nejjednodušší jsou karty s magnetickým proužkem (obsahují obvykle neměnnou informaci, kterou lze ale kdykoliv přepsat), složitějšími a dražšími jsou pak čipové karty (dokáží provádět nad uloženými/zaslanými daty různé operace). Téměř každý, kdo má bankovní účet, tak vlastní alespoň jednu platební kartu. [9]

***Autentizace prostřednictvím biomet*rie**, což je metoda, která snímá jedinečné fyzické znaky osob. Biometrických technologií existuje mnoho a jsou založeny na měření fyziologických vlastností lidského těla (např. otisk prstu, geometrie ruky, nebo snímek oční duhovky) nebo chování člověka (např. dynamika podpisu nebo vzorek hlasu). Tato metoda je však náročnější jak na hardware, tak i na software. V minulosti tyto systémy nebyly ve větší míře využívány, protože technologie byly příliš drahé a nespolehlivé. Teprve v poslední době se vývoj těchto identifikačních zařízení znatelněji rozbíhá a můžeme se setkat i s jejich aplikacemi do rozsáhlejších technologických celků. [9]

Nejúčinnější metodou ochrany dat a informací je kombinace více složek. Může jít o heslo, šifrování a hardwarové klíče. Úspěšný útok je přímo neproveditelný a úspěšnost útoku je minimální. Šifrování má druhotný krok ochrany. Pokud by měl útočník přístup do počítače, snadno získá potřebné soubory, ale jejich obsah bude nečitelný. Jediné co může udělat, je zničit data, ale obsah nikdy nemůže zneužít. [4]

3.2.2 Autorizace

„Autorizace je proces ověření přístupových oprávnění uživatele vstupujícího do informačního systému.“ [10] Tento proces ve většině případů navazuje na proces autentizace. Podstatou autorizace je ověřit na základě seznamu oprávnění, zda daný uživatel má přístupová práva k souborům, adresářům, či přístup k prostředkům v počítači a je mu umožněno provést příslušnou akci, například vložení nového záznamu do seznamu dodavatelů apod. [10]

4 PROGRAMOVÁ BEZPEČNOST INFORMAČNÍCH SYSTÉMŮ

Ochranné mechanismy informačních systémů realizují ochranu hodnot tak, že se snaží minimalizovat jejich slabé stránky, nebo rizika působení hrozeb, přičemž účinnost mechanismů musí být vůči možným hrozbám přiměřená. Při zavádění ochranných mechanismů musíme brát v úvahu řadu ovlivňujících faktorů. Konkrétně se jedná o cenu bezpečnostních mechanismů a nákladů v poměru k jejich bezpečnostnímu efektu. Cyklus zavádění informační bezpečnosti je vlastně neustálý proces, který periodicky kontroluje úroveň bezpečnostních opatření a podle potřeby je aktualizuje, nebo vylepšuje a inovuje. Konkrétní realizace informační bezpečnosti je závislá na mnoha faktorech a vlivech jako je velikost systému, citlivost informací, dostupnost technologií, finanční možnosti či personální obsazení. Žádný bezpečnostní mechanismus zatím nedokáže pokrýt celý rozsah požadavků na ochranu, a proto se požadované bezpečnostní úrovně dosahuje kombinací více nástrojů a metod. [7]

Programová bezpečnost je oblast informačního systému, která se týká aplikačních programů, které by mohly poškodit či zcela zničit data, způsobit kompromitaci utajovaných skutečností, omezit a případně vyloučit funkčnost celého systému. K nejčastějším útokům na data a informace dochází ze strany zaměstnanců dané organizace. Jejich počátečním spouštěčem může být oznámené propuštění z firmy. Tento útok berou jako pomstu vůči zaměstnavateli a mohou svým následným jednáním způsobit organizaci obrovské škody jako např. vynášením citlivých informací, které následně mohou poskytnout konkurenci. [5]

4.1 Programy ohrožující bezpečnost, integritu a utajení dat

Existují programy, které jsou určeny k tomu, aby určitým způsobem zničily data, nebo se snaží poškodit důležité operační systémy a nakonec i aplikační vybavení. V případě úspěšného použití programu mohou omezit celý fungující systém a napáchat nemalé škody v informačním systému celé organizace. Místem nejčastějšího útoku na operační systém je útok na jeho mechanismus zpracování vstupně-výstupních operací. Takový postup je nebezpečný a může vést k haváriím operačního systému.

4.1.1 Zadní vrátka (Trap Door)

Jedná se o metodu, díky které je možné obejít autentizaci. Může se jednat jak o softwarový tak i hardwarový skrytý program. Tento mechanismus často využívají programátoři, kteří vyvíjejí určitou aplikaci a záměrně vloží do jejího kódu proceduru, která vykonává některé

nepožadované operace. Při vývoji jim usnadňuje zdokonalovat program při jeho ladění, avšak po dokončení vývoje programu musí být tyto sekvence odstraněny, aby nenarušovaly celkovou funkčnost aplikace. V opačném případě mohou programátoři Trapdoors ponechat a v pozdější době je záměrně využívat pro získání neoprávněného přístupu a získat tak neoprávněný prospěch k citlivým datům. [5]

4.1.2 Salámový útok (Salami Attack)

Nastává-li velmi velké množství finančních operací, může při této technice podvodu dojít ke vzniku velkých finančních škod. Tato metoda využívá chyby při číselném matematickém zaokrouhlování na hranici přesnosti. Pokud se jedná o bankovní aplikaci lze touto metodou posílat programátorovi na jeho účet malé peněžní částky. Pokud tedy při několikanásobném zaslání financí na účet nastane chyba v zaokrouhlování, může z malých hodnot najednou vzniknout poměrně velká částka. Tento útok nezpůsobuje viditelné chyby, to znamená, že útok se dá těžko odhalit. Pokud dojde k odhalení, jedná se ve většině případů o náhodu. [5]

4.1.3 Skrytý kanál (Covert Channel)

Tyto kanály se zneužívají k nepovolenému přenosu informací. Vzniká zde způsob komunikace, který porušuje bezpečnostní politiku daného informačního systému. Tato komunikace probíhá mezi jednotlivými procesy operačního systému, a pokud se objeví chyba v operačním systému, hrozí zde únik informací. Vznikají jednak chybou v operačním systému, nebo činností trojského koně, který tento kanál vytvoří. K informačním kanálům se dá těžko dostat, ale existuje možnost odhalení v případě, kdy se vyskytne konkrétní chyba ve výpisech, nebo se objevují či naopak chybí specifické soubory, nebo vzniknou jisté systémové události. [5]

4.1.4 Nenasytné programy (Greedy Programs)

Jedná se o programy, které ke své činnosti vyžadují velkou část výkonu systému. V praxi to znamená, že v počítačích běží programy, které mají nastavenou malou prioritu, ale vytvářejí zdlouhavé až nekonečné funkce a pomalu zatěžují procesor a paměť a tím se jeho činnost postupně zpomaluje, až nastane kolaps. V jiném případě programy běží v nekonečném cyklu. Operační systémy často obsahují obranné mechanizmy, které násilně tyto programy ukončí. [5]

4.1.5 Počítačové viry

Počítačové viry trápí většinu lidí a každý z nás se s nimi již alespoň jednou setkal. Dělají nám značné starosti, a dokonce poškozují i naše data. Jedná se o programy, které dokáží napadat jiné programy. Viry nahrazují část kódu programu, na který se připojily a tuto část kódu mění, aby obelstily detekci. Pokud se spustí daný program, nejprve se provede část nahrazeného kódu a ten se nainstaluje do paměti systému nebo změní funkce systému.

Pokud je nákaza již v systému, záleží na škodlivosti viru. Může jít např. o jednoduché iniciace multimediálních obrazových efektů se zvukem, které nejsou až tak škodlivé jako ty, které dokáží zničit naše data a programy. Většina těchto virů se nachází v programech volně šiřitelných po internetu. Získat se dají stahováním nelegálního softwaru nebo se mohou nacházet již v počítačích - např. v internetové kavárně a jiných volně používaných počítačích. Ochranou před virem může být antivirový program, poučení pracovníků firmy nebo rozdělení dat do oddílů, které budou dostatečně oddělené. [5]

4.1.6 Červi (Worms)

Červi jsou podobní virům, které se šíří především pomocí komunikačních linek z počítače do počítače. Červi se umí šířit sami. Oproti virům je tedy jejich šíření daleko rychlejší, a tedy i škody jsou mnohem větší. Ochranou před nimi je opět jako u virů používání ověřených programů a rozdělení sítě na jednotlivé domény, mezi nimiž je přenos informací minimální. Největší červ, jaký kdy existoval, napadl v roce 1988 přes 6000 počítačových stanic na internetu a škody byly vyčísleny na 100 milionů amerických dolarů. Tento červ je připisován 23 letému Robertu T. Morrisovi. [7]

4.1.7 Trojské koně (Trojan Horse)

Trojský kůň bývá často ukrytý v bezplatných aplikacích, nebo se také často šíří infikovanými emailovými přílohami. Některé trojské koně se distribuují na nezabezpečených webových stránkách prostřednictvím vyskakovací reklamy. Trojský kůň dokáže provádět skryté akce, jejichž příčina je zaměřena k ničení systému (zvýšená zátěž procesoru a tím způsobené zpomalení prováděných operací, krádeže dat případně k úplnému zablokování). Trojský kůň se do systému instaluje ihned po vniknutí, nebo po uplynutí určitého času, na který byl nastaven. Od červa se liší tak, že neinfikuje ostatní programy. [5]

5 JAK SE CHOVAT V SÍTI INTERNET

Surfování po síti internetu není nijak komplikované a může se ho naučit téměř každý, avšak ne všichni uživatelé surfují za stejným účelem. Existuje skupina lidí, uživatelů, kteří využívají internetovou síť, aby škodili, podváděli, ničili a dopouštěli se protiprávních přestupků a zločinů. Proto jsou v internetové síti doporučena určitá pravidla, která je třeba dodržovat a která uživatelům pomáhají, jak se mají chovat z pohledu bezpečnosti informací, uchovávání osobních dat atd. Každý uživatel, který bude používat informační a komunikační zdroje, by se měl řídit standardními pravidly:

- nezveřejňovat své osobní údaje pokud to není nutné,
- v elektronické poště poskytovat pouze základní informace a údaje,
- chránit své přihlašovací údaje jako jsou hesla a autorizační PINkódy,
- nevyužívat elektronickou poštu na rozesílání textů a souborů, které jsou přísně zakázané, a porušoval by se jimi zákon, např. může jít o rasovou a politickou nesnášenlivost apod.,
- s velkou obezřetností využívat cizí WI-FI připojení, vyvarovat se platebních transakcí apod.,
- v případě použití sítě, která se nachází v jiné lokalitě, je třeba dodržovat pravidla vyžadovaná v dané oblasti. [7]

5.1 Bezpečné síťové rozhraní

K útokům na informační systémy, které jsou připojeny k síti internetu, dochází většinou zvenčí. Takový informační systém napadají útočníci, kteří se technicky dobře orientují, jejich znalosti jsou na požadované úrovni a navíc mají dostatek volného času na připravovaný útok. Proto je důležité, aby do vnitřní privátní sítě nebyl umožněn případný neoprávněný přístup. Útokům, které směřují zvenku, se dá bránit několika způsoby. Jako první způsob je možné fyzické oddělení lokální sítě. Tím se vyloučí elektronický přenos informací, mimo okruh interního kabelového rozvodu.

Nevýhodou tohoto použitého způsobu je, že se jedná o drastické a nejméně funkční řešení, ale pokud bychom měli posuzovat cenovou kalkulaci, tak se řadí k nejlevnějším. Druhým způsobem je použití bezpečné oddělovací technologie. Tato technologie dokáže spojit

privátní síť s okolním světem a zároveň kontroluje oboustrannou komunikaci na základě bezpečnostních pravidel. Tímto způsobem dokáže zabránit nebezpečné komunikaci. Pro správné fungování je důležité použít vhodně promyšlené bezpečnostní zásady. [7]

5.1.1 Galvanické oddělení podsítě

Síť je galvanicky oddělena od privátní sítě tzn., že jsou zde vytvořeny dvě sítě. Privátní síť, která slouží pro vnitřní chod dané firmy a druhá, která je oddělená od privátní sítě, a je zároveň připojena k internetu. Toto řešení nabízí vysokou bezpečnost. Nevýhodou jsou jak vysoké náklady, tak i to, že omezuje funkčnost celého systému. Uživatel musí neustále přecházet z jedné sítě na druhou. [7]

5.1.2 Bezpečnostní brána - firewall

V případě napojování lokálních sítí k veřejným komunikačním platformám, především k internetu, je nutným požadavkem zachovat bezpečnost lokální sítě a neomezit funkcionalitu propojení. U této kombinace se často uvádí pojem bezpečnostní brána, která znamená realizaci spojovacího bodu mezi veřejnou a lokální sítí při zachování bezpečnosti. Způsob tohoto spojení se nazývá firewall.

- Firewall

  Firewall doslovně přeloženo „ohnivzdorná zeď“, dokáže zabránit neautorizovanému přístupu uživatele z vnější sítě ke zdrojům lokální sítě. Firewall nutí síťové propojení, aby využívalo kontrolní systém, kde se analyzuje vzájemná komunikace. Výsledek analýzy určí, zda vnější síť získá povolení nebo zákaz propojení. Úkolem firewallu není ochraňovat vnější svět sítě, ale ochránit lokální síť před vnějším světem. Firewall, ale neochrání před viry, odposlechem nebo před zničením dat při přenosu po síti. *„Firewall je především implementace bezpečnostní politiky, která definuje povolené služby a možnosti přístupu pomocí technických prostředků, které jsou umístěny v bodě napojení informačního systému k vnější nechráněné a implicitně nebezpečné síti.“* [7]

  Základní typy firewallu:

  - Paketový firewall,
  - Aplikační brány,
  - Stavové paketové firewally,

- Stavové paketové firewally s kontrolou protokolů a IDS (Intrusion Detection Systems – systémy pro detekci útoků). [7]

Paketový firewall se vyznačuje vysokou rychlostí, ale nízkou úrovní zabezpečení. Jeho funkce spočívá v tom, že přesně určuje, z jaké adresy a portu a na jakou adresu a port může být doručen procházející paket. Paketový firewall není schopen upozornit na podezřelé aktivity.

Při použití aplikačních bran probíhá komunikace pomocí dvou spojení. Klient (iniciátor spojení) se připojí na aplikační bránu proxy[1], a ta toto spojení zpracuje. Na základě požadavku klienta otevře nové spojení k serveru, kde klientem je aplikační brána. Aplikační brány jsou podstatně bezpečnější než paketové filtry avšak omezují uživatele na úzce vymezený okruh služeb. Pro každou další službu napsat tzv. proxy, neboli aplikaci, která bude dalším rozhraním mezi chráněnou lokální sítí a nedůvěryhodnou sítí a kontroluje pakety pro nastavenou službu.

Stavové paketové filtry fungují jako výše jmenované paketové filtry, ale navíc si ukládají informaci o povolených spojeních, kterou mohou později využít při rozhodování, zda procházející paket patří do povoleného spojení a může být propuštěn, nebo musí projít rozhodovacím procesem. Stavové firewally umožňují analýzu paketů, kdy zaznamenávají informace o konkrétním spojení jako je např. IP adresa a čísla portů. Dynamické filtrování paketů pak může realizovat mnohem vyšší míru zabezpečení. Každý nově přijatý paket je porovnáván se stavovou tabulkou firewallu, která určuje stav paketu, zda není v rozporu s očekávaným stavem. [7]

Firewall s kontrolou protokolů a IDS jsou schopny kontrolovat procházející spojení až na úroveň korektnosti procházejících dat známých protokolů i aplikací. Mohou zakázat průchodu spojení, v němž se objeví indikátory, že se nejedná o požadavek na spojení s WWW serverem, ale tunelování jiného protokolu. Výhodou systému je vysoká úroveň bezpečnosti procházejících protokolů. Naopak nevýhodou je zejména složitost kontrolního systému. Zvyšuje se pravděpodobnost, že v některé části jejich kódu bude zneužitelná chyba. [7]

[1] ***Proxy server*** je důležitý počítačový program, který plní funkci komunikačního prostředníka mezi klientem a cílovým serverem. Proxy server překládá požadavky klienta vůči serveru, přebírá jeho odpověď, kterou zdárně doručuje zpět klientovi. Dostupné z: https://www.sprava-site.eu/proxy-server/

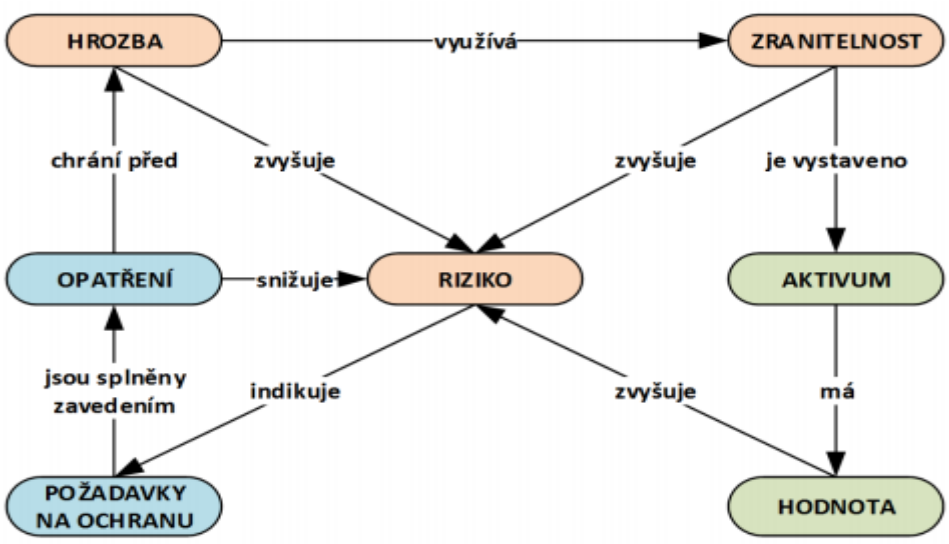
6 HROZBY A RIZIKA

Informační bezpečnost je nedílnou součástí budování informačních systémů. Součástí informačního systému jsou zákonitě místa, která jsou zranitelná, jejichž existence způsobuje, že některé vlivy prostředí, ve kterém se informační systém provozuje, představují pro něj hrozby. V porovnání ostatních subjektů finančního trhu má bankovní sektor více propracovaný systém ovládání rizik.

Hrozby a rizika v informačním systému můžeme rozdělit podle různých hledisek:

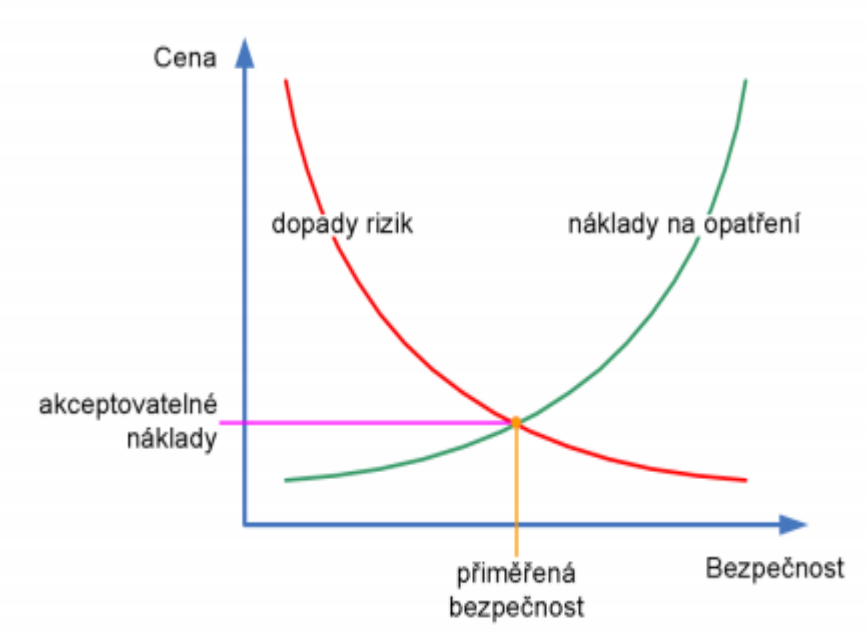
- *Objektivní* – sem spadají hrozby přírodní, fyzické, technické a je většinou důležité zaměřit se na jejich minimalizaci a pro případnou potřebu vytvořit havarijní plán.
- *Subjektivní* – hrozby, které vznikají neúmyslně nebo záměrně z důvodu působení lidského faktoru. V případě neúmyslné hrozby může být viníkem nekvalifikovaný pracovník informačního systému. Do úmyslných hrozeb zařazujeme vnější, ale i vnitřní útočníky. Vnitřním útočníkem se většinou stávají naštvaní, propuštění zaměstnanci, kteří představují přibližně 80 % všech útoků. Cílem těchto útoků bývají finanční zisky, pomsta nebo dosažení konkurenční výhody. [5]

Dalšími hrozbami může být používání neautorizovaných zdrojů, kde dochází k odcizení softwarových, ale i hardwarových produktů a následně jejich zneužití. Hrozba může vzniknout i agregací citlivých informací z méně citlivých dílčích informací.



Obrázek 4 Přehledové schéma - řízení rizik. [11]

Náklady na bezpečnostní opatření by však měly být vždy přiměřené a neměly by převýšit náklady spojené s následky realizace rizika. Toto ilustruje následující schéma.



Obrázek 5 Akceptovatelné náklady. [12]

6.1 Zabezpečení internetového bankovnictví

V dnešní době je internetové bankovnictví základní službou každé banky. Klientům umožňuje rychlou a pohodlnou správu finančních prostředků, avšak vedle nesporných pozitiv obsahuje tento způsob komunikace i nemalá rizika. Banky proto musí dbát na to, aby co nejvíce snížily možnost napadnutí a prolomení bezpečnosti tohoto komunikačního systému. Tato služba je zabezpečena na několika úrovních a jednotlivé úrovně zabezpečení se navzájem doplňují. Systém ochrany zabezpečení se skládá ze tří na sobě nezávislých bezpečnostních prvků:

- identifikace banky
- identifikace klienta
- zabezpečení přenosu dat

Banky navíc dávají klientovi na výběr, jaké riziko je ochoten přijmout a kterou metodu zabezpečení si zvolí. Zájem klientů o nadstandardní zabezpečení není až tak velký. Zabezpečení ze strany banky je tedy dostatečné a k prolomení ochrany dochází nejčastěji v důsledku neopatrnosti klientů, které útočník nemá problém využít ve svůj prospěch. [14]

6.1.1 Identifikace banky

Identifikace banky je velmi důležitá, ať už ze strany banky nebo klienta. Banka musí vědět, že právě komunikuje se správnou osobou, která má oprávnění spravovat účet. Stejně i klient musí vědět, že se nachází na stránce banky, se kterou může bezpečně komunikovat. V případě ověření identity banky jde o zajištění toho, aby předávaná citlivá osobní data klienta byla nasměrována správnému subjektu. *„Identita banky je ověřována certifikátem, který vydává nezávislá instituce (nejčastěji VeriSign, nebo I.CA). Klient má tak jistotu, že stránky, jejichž prostřednictvím komunikuje s bankou, patří skutečně jí. Přenos dat je ve všech bankách řešen SSL šifrováním na vysoké úrovni a lze jej považovat za dostatečně bezpečný.“* [14]

6.1.2 Identifikace klienta

Je třeba si vysvětlit pojmy, jako jsou identifikace a autentizace klienta. V praxi to znamená rozpoznání a ověření totožnosti klienta. Banky se musí ujistit, že danou manipulaci a bankovní operaci provádí skutečný majitel účtu. Nesmí se stát, že by se za skutečného majitele účtu vydával jiný člověk. Proto banky věnují velkou pozornost úrovni zabezpečení a snaží se používat co nejvíce ověřovacích prvků, aby nedošlo k nepovoleným operacím. Ovšem díky velkému počtu ověřovacích prvků má zajištění také nevýhody. Například z hlediska uživatelské pohodlnosti klienta, kdy je nutné pro přístup do internetového bankovnictví, aby si klient pamatoval své heslo, případně PIN kód. Některé banky volí různé úrovně zabezpečení s ohledem na to, jaký typ operace byl zvolen.

Aktivní operace	Pasivní operace
Zadání příkazu k úhradě	Zjištění zůstatku na účtu
Zadání příkazu k inkasu	Zjištění pohybů na účtu
Zřízení trvalého příkazu	Informace o produktech a službách banky
Zahraniční platební styk	Informace o aktuálních úrokových sazbách
Obsluha termínovaných účtů	Informace o aktuálních kurzech cizích měn

Tabulka 1 Přehled aktivních a pasivních operací. Zdroj vlastní

Bankovní operace se dají rozdělit na pasivní a aktivní viz tabulka 1. Při pasivních operacích se nemění zůstatek na účtu. Příkladem takové operace je například zjištění pohybů na účtu. Aktivní operace slouží k využití finančních prostředků (příkaz k úhradě). Pokud použijeme pasivní operaci, banka od nás bude vyžadovat základní způsob autentizace. Autentizace probíhá pomocí jména a hesla. Po úspěšné autentizaci je možné vytvářet uživatelské operace jako je zjišťování zůstatku na účtu apod. Systém ale nedovolí vytvářet příkazy k úhradě, k inkasu, převody finančních prostředků atd. [7]

Pokud by uživatel chtěl tyto operace provádět, bude od něho vyžadována další úroveň autentizace. Například:

- ***SMS klíč***, kdy kód je po zadání aktivního úkonu vygenerován bankou a odeslán SMS zprávou na telefon klienta. Transakce je provedena až poté, co tento potvrzovací kód opíšete do systému banky. Vyšší míru zabezpečení poskytují banky, které autorizaci SMS kódem požadují pro každou aktivní transakci. [16]
- ***Autorizační kalkulátor*** je drobné elektronické zařízení, které dokáže generovat jednorázová hesla pro potvrzení operací. Kalkulačka tedy funguje na podobném principu jako SMS klíč. Kalkulačka je přenosná a je chráněna čtyřmístným heslem. Po zadání hesla a stisknutí příslušného tlačítka vygeneruje šestimístný kód, který klient aplikuje pro vstup do internetbankingu. Pro každou aktivní transakci musí být vygenerováno nové číslo. [16]
- ***Elektronický certifikát,*** který je vydáván pro komunikaci s použitím elektronického podpisu vydávaný autorizovanou certifikační autoritou, jehož vystavení vám zprostředkuje banka. Vedle komerčních certifikátů existují také tzv. kvalifikované certifikáty, které zároveň slouží ke komunikaci se státní správou či zdravotní pojišťovnou. [16]

6.1.3 Zabezpečení přenosu dat

Datový tok citlivých informací, který probíhá mezi klientem a bankou prochází několika uzly, kde by bylo možné tyto data zachytit, odposlechnout, případně přečíst a zneužít. Proto jsou data proudící oběma směry šifrována pomocí tzv. veřejného šifrovacího klíče, který je během úvodního představování předán klientovi a ten ho poté předává zpět bance. Od okamžiku předání klíče jsou veškerá data na straně odesílatele šifrována klíčem druhé strany a pro následné použití opět dešifrována. Šifrování procházejících dat zajišťuje webový

prohlížeč a přesvědčit se o tom můžeme pohledem na horní stavovou lištu, kde by v levém rohu měla svítit žlutá ikona visacího zámku. Uživateli je tím oznámeno, že komunikace s bankou je šifrovaná a SSL certifikát je platný. Z pohledu rizika se tak jedná o kvalitní zabezpečení internetového bankovnictví. [15]

„Vysoký standard zabezpečení představuje klientský certifikát na čipové kartě. V čipové kartě je bezpečně uložen tajný osobní klíč klienta a každá zpráva od klienta bance je tímto klíčem přímo v kartě podepsána (tedy doplněna o unikátní kód, který je odvozen z obsahu zprávy a tajného klíče). Tajný osobní klíč klienta nelze z karty nijak získat ani uhodnout, proto bez této karty není možné elektronický podpis klienta padělat. Banka přijme zprávu od klienta jen po ověření elektronického podpisu podle certifikátu, který klientovi ke kartě vydala.“ [17]

Obrázek 6 Identifikační prvky internetového bankovnictví GE Money bank. [18]

6.2 Nejznámější způsoby prolomení bezpečnosti

Neustálým vývojem nových informačních technologií a konkurence bank přinášejí větší počet bankovních služeb. Díky rychlému vývoji vznikají i nová rizika, které se týkají zabezpečení účtů a k neoprávněným transakcím jinou osobou.

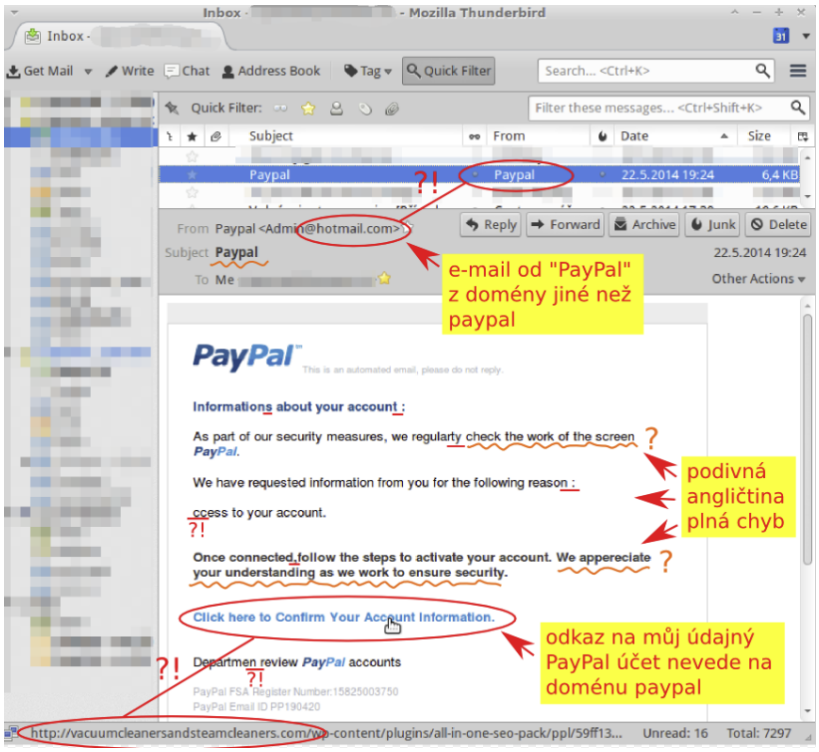
Nejčastěji využívané formy zneužití jsou:

- phishing
- pharming
- vishing
- skimming
- spying
- tabnabbing

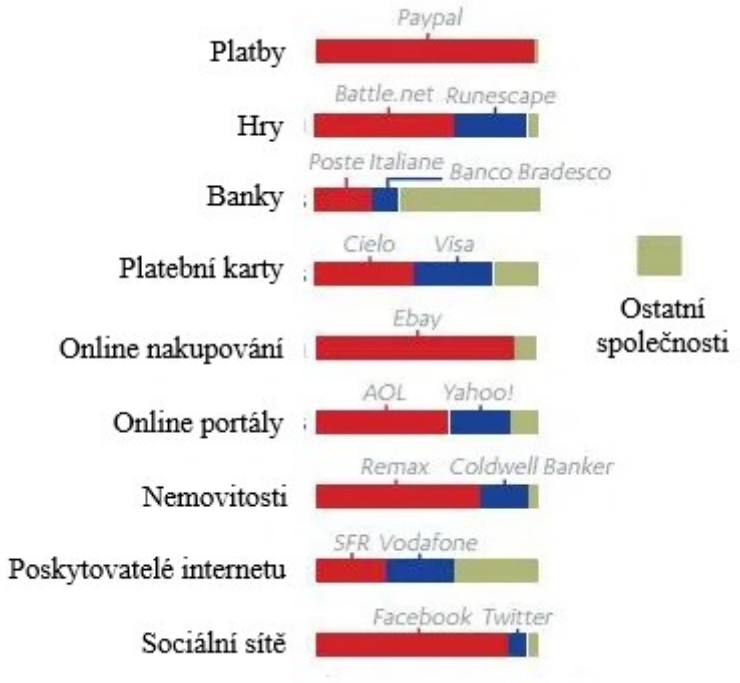
6.2.1 Phishing

Password Harvest Fishing což v překladu znamená sbírání hesel rybařením. Jde o velmi známý a jeden z nejstarších způsobů, jak oklamat uživatele a získat citlivé údaje. *„Využívá se zde sociální inženýrství. Je to metoda, kde útočník manipuluje s osobou, od níž získá citlivé údaje a pomocí nich je může zneužít k určité činnosti.“* [19]

Jedná se o podvodné zprávy, které útočníci rozešlou prostřednictvím e-mailu. Cílem podvodného e-mailu může být získání přihlašovacích údajů k internetovému bankovnictví, PIN kódů platebních karet nebo dalších bezpečnostních údajů a jejich následné zneužití. Principem zprávy je věrohodné napodobení oficiální žádosti banky nebo podobné instituce. Zpráva může být psána špatnou češtinou, případně je v angličtině. Podobně se mohou podvodníci snažit získat přístupové údaje k elektronickým peněženkám pro obchodování na internetu jako je PayPal, eBay, Paysec. Na první pohled jde o obdobu stránky internetového bankovnictví, která se na první pohled nikterak neliší, avšak po důkladném prohlédnutí můžeme zjistit, že adresa stránky je jiná a začíná nezajištěným protokolem (http: //). [19]



Obrázek 7 Ukázka typického phishing e-mailu s vysvětlením. [20]



Obrázek 8 Světové společnosti, které jsou nejvíce napadány phishingovými útoky. [21]

6.2.2 Pharming

Pharming neboli farmaření je útok založený na složitějším a důmyslnějším podvodném jednání, než jaké představuje phishing. Pod tímto pojmem se rozumí kybernetický útok, jehož cílem je, nasměrovat klienta na falešnou webovou stránku, která má stejný vzhled a přibližně stejné funkce, jako je přihlašovací stránka jeho banky. Klienta pak požádají o zadání příslušných hesel a kódů. *„Princip takového útoku využívá speciální počítačové programy, které umí napadnout DNS (doménový server) a přepsat IP adresu.“* [22]

V případě pharmingu založeném na škodlivém malwaru může dojít prostřednictvím e-mailu k vyzvednutí trojského koně, nebo jiného viru. Pokud se klient přihlašuje na stránku své banky, tento malware klienta tajně přesměruje na falešný web vytvořený a kontrolovaný podvodníky. Problém je v tom, že před otevřením odkazu si uživatel neuvědomí, zda odkaz, který právě otevřel, vede na stránku skutečnou, nebo falešnou. [23]

6.2.3 Vishing

Skládá se ze zkratky slov voice-over phishing. V překladu to znamená, lovení hesel přes telefon. Forma sociálního inženýrství, namísto používání podvodných e-mailů, se zde jedná o pravidelné podvodné telefonní hovory přes VoIP (Voice over Internet Protocol), což je

služba, která využívá pro volání prostředí internetu. Útočník se představuje jako zaměstnanec banky, aby navodil důvěryhodnou atmosféru, a emotivně manipuluje s klientem a cílí tak na získání jeho citlivých informací. Vishing je poměrně úspěšná kyberkriminální metoda. [24]

6.2.4 Skimming

Výraz je odvozen od slova to skim, což znamená sbírat, stahovat. Jde o trestnou činnost, která je spojena s bankovními kartami. Útočníci pomocí speciálního zařízení nasazeného na bankomat kopírují data z magnetického proužku. Po získání těchto dat vytvářejí nové falešné karty. Důležitým údajem je PIN kód, který je potřebný k přístupu k účtu. Ten útočníci získávají pomocí bankomatových kamer, mobilních telefonů nebo mají speciální klávesnici, kterou umístí místo původní klávesnice nebo ji dají rovnou na ni [25].

Obrázek 9 Skimming platební karty [25]

6.2.5 Spying

Spying je metoda, při které se špehuje pomocí škodlivého softwaru a to spyware. Ve většině případů, si jej stáhneme do počítače při pouhém surfování po internetu. Spyware pracuje tak, že odesílá informace o surfování na internetu na své webové stránky a tak sleduje uživatele, získává autorizační údaje a čísla kreditních karet. Samotný uživatel si nemusí být vědom, že má něco v počítači. Na odhalení se používají různé antispywarové programy. [26]

6.2.6 Tabnabbing

Metoda phishing je založena na tom, že útočník podstrčí oběti zamaskovanou URL[2] adresu v odkazu, který zasílá e-mailem s historkou, proč by se měl dotyčný přihlásit prostřednictvím tohoto podstrčeného odkazu na falešnou stránku své banky, případně PayPalu. Útočník spoléhá na to, že vystrašený uživatel přehlédne, že adresa stránky je jiná než adresa domovské stránky jeho banky. Útočníkovi tak zadáním poskytne své přihlašovací údaje.

Tabnabbing vychází ze stejného předpokladu, kdy rovněž využívá nepozornosti uživatele, ale podstata získání osobních údajů je založena na jiném principu. Uživatel pracuje se svým internetovým prohlížečem a v záložkách má otevřeno několik stránek, které postupně prohlíží a hledá třeba nějaký výrobek a pořád otevírá další a další odkazy. Při prohlížení jednotlivých stránek a jejich ukončování narazí na stránku, kde je přihlašovací formulář k Gmailu, uživatel zazmatkuje a přihlásí se a vůbec nepostřehne, že se přihlásil na falešnou stránku a poskytl tak údaje útočníkovy. Uživatel v tomto případě narazil na stránku, která provozuje Tabnabbing. Na první pohled je stránka naprosto nenápadná a může to být i reálná webová stránka, napadená skriptovým Trojanem, tak že spouští Tabnabbingový skript. Jakmile se uživatel přepne na jinou záložku, napadená stránka po určitém čase změní ikonu v záložce a obsah stránky tak aby vypadal třeba jako přihlašovací stránka do Gmailu (může to být přihlašovací stránka banky nebo PayPalu). Adresa URL je jiná, ale nepozorný uživatel si toho ani nevšimne a dojde k odeslání údajů útočníkovi. Proto je vždy nutné zkontrolovat si vždy adresu URL, než napíšeme přihlašovací údaje. [27]

[2] **URL** (Uniform Resource Locator) je soubor znaků, který slouží k identifikaci přesného umístění informací na internetu. URL definuje doménovou adresu serveru, umístění zdroje na server a protokol. Dostupné z: https://www.antstudio.cz/slovnik/co-je-url.htm

7 OUTSOURCING

Jednou z podmínek úspěšného podnikání je být v dlouhodobém horizontu schopen zaměřit úsilí a zdroje na hlavní podnikové činnosti. To znamená neztrácet čas s činnostmi, které nejsou přímo spojené s hlavním zaměřením společnosti, ale které jsou nezbytné pro její fungování. Jednou z efektivních forem řízení vedlejších činností je outsourcing.

Nejen v podnikatelském sektoru hraje outsourcing velkou úlohu, ale i v bankovním sektoru má své nemalé uplatnění což se týká zajištění plynulého a bezproblémového fungování jednotlivých procesů v bance. Bezpečnost všeobecně a zejména bezpečnost informačních technologií má mezi lidmi značné povědomí. S rostoucím objemem dat a využíváním nových komunikačních kanálů se zvýšila četnost zveřejněných bezpečnostních incidentů.

„Využití outsourcingu se stává v globálním světě nezbytné, mají-li si banky zachovat konkurenceschopnost. V oblasti bankovnictví v České republice je outsourcing ovlivněn nejen zákonem o bankách, ale i zákonem na ochranu osobních údajů a dalšími předpisy. Podrobnější podmínky stanovuje Česká národní banka ve svých sděleních a vyhlášce upravující řízení rizik a vnitřní kontrolní prostředí. Pokud chtějí bankovní subjekty outsourcovat některé aktivity, musí připravit detailní analýzu rizik spojených s danou aktivitou, stanovit způsob, jakým budou riziko řídit, monitorovat a eliminovat, což významným způsobem snižuje výsledné úspory.“ [28]

7.1 Historie vzniku outsourcingu

Vznik outsourcingu by se mohl datovat již od ideje dělby práce, kde se jednotlivé složky navzájem různě podporovaly a na sebe navazovaly. Většina zdrojů však jako začátek jeho masového používání považuje outsourcing informačního systému firmou Kodak v roce 1989, někdy se dokonce mluví o éře "před Kodakem" a o éře "po Kodaku". Masovost outsourcingu tedy začíná vytěsnění informačního systému.

Pátráme-li, ale po vzniku poskytovatelských podniků, pak zjistíme, že velcí poskytovatelé služeb v nějaké funkční oblasti, jejichž původní výrobní zaměření je jiné, ale ve kterých jistá funkční oblast dosáhla tak vysoké úrovně, že se rozhodly poskytovat ji jako službu. Příkladem může být společnost American Airlines a jejich rezervační systém letenek. [29]

Průkopníkem outsourcingu v ČR byl na počátku 90. let benešovský podnikatel Miroslav Švarc. Propustil zaměstnance a ti si zřídili živnostenské oprávnění a začali pro něj pracovat jako dodavatelé. Takto dosáhl významných úspor na odvodech státu. Po roce 1989 se forma

outsourcingu začala vytvářet v odvětvích stravování pro zaměstnance větších firem, které využívaly outsourcingových společností jako je např. Sodexho a Eurest. I když se v té době nejednalo o širší využívání outsourcingu, začalo se toto vytěsňování neprosperujících služeb a činností rozvíjet.

V oblasti informačních technologií využívají outsourcing společnosti, které poznaly, že vlastní vývoj a údržba svého informačního systému je pro ně z ekonomického hlediska nevýhodná. Využívají služeb specializovaných počítačových firem, neboli poskytovatelů outsourcingu, kterým předají odpovědnost za návrh, budování a správu jejich informačního systému. [30]

7.2 Definice outsourcingu

Pojem outsourcing vznikl z anglického "Outside Resource Using", což v doslovném překladu znamená ***používání vnějších zdrojů***. V literatuře se však setkáváme s dalšími definicemi outsourcingu. Ačkoliv je pojem outsourcing v dnešní době široce používán, velmi často dochází k jeho nesprávné interpretaci. [31]

Podle zdroje [31], „O*utsourcing představuje rozhodování mezi dvěma strategiemi "vyrob nebo kup" (z anglického "make or buy"). Slovo outsourcing je možné chápat i jako sloučeniny dvou částí – out a sourcing. Jedná se tedy o přemístění (provedení, vytěsnění) jedné nebo více aktivit, které dosud organizace realizovala výhradně ve vlastní režii, na externí organizaci, od které výsledky těchto aktivit (výrobky a služby) nakupuje.“* [31]

Jiný pohled na vymezení outsourcingu poskytuje zdroj [32] když uvádí, že termín *„**outsourcing** nelze ztotožňovat s rozhodnutím "vyrobit nebo koupit", nebo s dodáním jakéhokoliv zboží, nebo služby od dodavatele. Zásadním rozdílem mezi outsourcingem a nákupem určité služby nebo zboží je dlouhodobost vztahu mezi klientem a poskytovatelem outsourcingu, kdy poskytovatel je plně zodpovědný za výsledky outsourcované činnosti.“*

Teorii outsourcingu se věnuje mnoho odborných publikací. Jednu z ucelených definic outsourcingu také poskytuje zdroj [33] *"Outsourcing je krok společnosti, při kterém dochází k transferu některých vedlejších interních, často se opakujících aktivit a rozhodovacích pravomocí podniku na externího dodavatele. S vedlejšími činnostmi přecházejí na externí společnost i ostatní tzv. produkční faktory potřebné k poskytování outsourcovaných aktivit."* Produkčními faktory jsou lidé, kapacity, zařízení, služby, technologie a jiná aktiva.

Výraznou změnu, kterou přináší využívání outsourcingu v podnicích, vyjadřuje definice, která uvádí, že *"Outsourcing není revoluce, ale evoluce změn v obchodních organizacích a způsob, jakým vykonávat podnikatelskou činnost."* [34]

Na jedné straně vidíme společnosti, které využitím outsourcingu dosahují růst, snížení nákladů, diverzifikaci rizik nebo zvýšení kvality výrobků či služeb. Na druhé straně, existuje mnoho společností, u nichž využití outsourcingu vedlo ke vzniku škod, ztratily kontrolu nad procesy nebo ztratily zákazníky. [34]

Nejdůležitějším rozhodnutím, které přijímá vrcholové vedení podniku v souvislosti s outsourcingem je, které činnosti vyčlení z podniku a které bude nadále provádět ve vlastní režii.

Při rozhodování o tom, co vyčlenit a co ne, se používají následující kritéria:

- z podniku by se neměly vyčleňovat takové funkce, jejichž význam pro úspěch podniku je značný a jsou reprezentovány kritickými faktory úspěchu,
- v podniku musí zůstat i strategické plánování a kontrola,
- vyčleňují se činnosti spojené s velkými investicemi. [35]

7.3 Důvody pro využívání outsourcingu

K důvodům pro využívání outsourcingu patří snížení a kontrola provozních nákladů, přístup k novému know-how, nedostupnost potřebných zdrojů, snížení investičních nákladů, transfer rizika, zlepšení kvality procesů v podniku, zlepšení cash-flow, uvolnění kapacity na "core business"[3], získání hotovosti z prodeje zařízení poskytovateli a uvolnění interních zdrojů pro jiné aktivity. [36]

Outsourcing vybraných podnikových činností umožňuje podniku rozšířit investice v oblasti, na kterou je podnik specializován a která nabízí největší konkurenční výhodu. Vyčlenění přesně vybrané oblasti a převedení odpovědnosti za oblast na externího dodavatele by tak mělo přinést provozní úspory. V případě oblasti informačních technologií je vhodný výběr a zajištění externího dodavatele. [37]

[3] ***Core business*** – jádro (hlavní předmět) podnikání, původní smysl existence dané firmy. Slovník Magdalena Čevelová, zdroj: https://www.cevelova.cz/slovnicek/core-business/

7.3.1 Základní důvody proč přistoupit k outsourcingu informačních technologií

- finanční náklady resp. přínosy (cena),
- jasná definice měřitelnosti předávaných služeb (kvalita),
- škálovatelnost služeb,
- sdílení rizik.

Mezi tato hlavní kritéria lze zahrnout i další parametry, jako je stabilita poskytovatele, rozvoj know-how, inovační potenciál, technologie, podniková kultura, predikovatelnost, schopnost reakce na změny, kompetentnost, zlepšování finančních a nefinančních ukazatelů firmy. Jednotlivá kritéria mají pro zákazníky různou váhu a mezi sebou jsou navzájem provázána. Neznamená však, že zlepšení v jedné oblasti nemůže znamenat zhoršení nebo zvýšení nákladů ve druhé oblasti. Můžeme to demonstrovat na příkladu ceny a sdílení rizik, kdy dodavatel musí vytvářet opravné položky pro pokrytí případných rizik. Podobně zvýšení kvalitativních parametrů poskytovaných služeb zpravidla vede ke zvýšení ceny za danou službu. [38]

7.3.1.1 Finanční náklady – přínosy.

Základní otázka pro dané kritérium poskytovateli outsourcingu je – o kolik bude služba levnější než vlastní provozování informačních systémů ve vlastní režii. V tomto případě lze vycházet z údajů o nákladech za informační technologie v minulých letech a provést určité porovnání do budoucna. Podrobnou analýzou je tak možné jednotlivé náklady přiřadit konkrétním službám. Vyčleněním majetku oddělení informačních technologií u nějaké obchodní organizace může znamenat relativně významnou část majetku firmy, kdežto u hutí nebo energetických podniků se toto vyčlenění na majetku a od něho odvozených ukazatelů projeví nepatrně. [38]

7.3.1.2 Jasná definice a měřitelnost předávaných služeb.

V tomto kritériu je výhodná definice jednotlivých služeb pomocí SLA (Service Level Agreement)[4], což nutí zákazníka k diskuzi, zda danou službu potřebuje a zda je ochoten, nebo schopen danou cenu zaplatit. Vhodným řešením je vytvořit katalog

[4] ***SLA*** Service Level Agreement, je dohoda o úrovni poskytovaných služeb. SLA představuje formalizovaný popis služby, kterou poskytuje dodavatel zákazníkovi. SLA definuje rozsah, úroveň a kvalitu služby. Zdroj: https://managementmania.com/cs/service-level-agreement

služeb popsaných v samostatných SLD (Service Level Description)[5]. V jednotlivých SLD je možné nastavit celou řadu kvalitativních a kvantitativních parametrů a tak vytvořit požadovanou komplexní službu. [38]

7.3.1.3 Škálovatelnost

Do této oblasti patří rozvoj znalostí a dovedností lidí. Provozování současných informačních technologií vyžaduje stále komplexnější a rozsáhlejší know-how, což je podmíněno rozsáhlými a drahými školeními pracovníků. Zajištění nepřetržitého provozu pro jednoho zákazníka je nákladnou záležitostí. Pokud je však možné zajistit servis pro více zákazníků nepřetržitým provozováním systémů, lze dosáhnou finančních úspor. V oblasti škálovatelnosti platí pozitivní zpětné vazby typu *"čím lépe - tím lépe"* nebo *"čím hůře - tím hůře"*. Pokud si poskytovatel outsourcingových služeb vybuduje kvalitní infrastrukturu pro několik zákazníků včetně dohledových středisek, systémů pro zálohování a zajištění provozu i po živelné katastrofě, je efektivnější do takovéto infrastruktury připojovat další zákazníky. Takovýto poskytovatel může pak nabízet mnohem komplexnější služby za výhodnější ceny. [38]

7.3.1.4 Sdílení rizik.

„Při definici outsourcingové smlouvy je možné velmi přesně definovat rozsah jednotlivých rizik a určit jejich rozdělení mezi poskytovatele a zákazníka.“ [38] V případě několikadenního výpadku služeb informačních technologií může být pro celou řadu organizací velmi kritický. V režimu sdílení rizik, je ale nutné vzít do úvahy smluvní vztah mezi poskytovatelem a zákazníkem. Zákazník si musí uvědomit, která rizika je ochoten nést sám a která rizika chce přenést na poskytovatele služeb outsourcingu a kolik je ochoten za toto přenesení rizika zaplatit. [38]

7.3.1.5 Důvěra - základní stavební kámen outsourcingu

Výše uvedená kritéria se dají více nebo méně objektivně změřit nebo definovat. *„Při vlastních úvahách o outsourcingu hraje významnou roli důvěra zákazníka v poskytovatele outsourcingu. Toto jediné kritérium, které je velmi obtížně měřitelné, může významně posílit,*

[5] **SLD** Service Level Description, je popis úrovně služby pro fyzickou podporu informační technologie. Zdroj: https://www2.physics.ox.ac.uk/it-services/service-level-description-sld-for-physics-it-support

nebo naopak převážit ostatní čtyři kritéria. Vyčlenění oblasti informačních technologií mimo vlastní organizaci je dlouhodobý proces a není možné na něj aplikovat metodu pokusu a omylu. Zákazník si musí být 100% jist, že rozhodnutí pro daného poskytovatele služeb outsourcingu, které učinil, je správné. K získání této jistoty ve většině případů nestačí pouze přinést dokonalé studie a poskytnout záruky ve smlouvách. Tato důvěra se musí vybudovat dlouhodobým vzájemným vztahem postaveným na společných projektech a spolupráci. V Čechách je poměrně častým jevem, že významný podnik vyčlení své oddělení informatiky jako samostatnou organizaci, která mu bude poskytovat služby týkající se informačních systémů a očekává, že se tato skupina lidí na trhu uchytí a bude své mateřské firmě místo nákladů generovat zisk. Existuje jen několik organizací, kterým se tento proces podařilo dokončit, a staly se z nich významní hráči na trhu outsourcing informačních technologií." [38]

7.3.2 Výhody a nevýhody outsourcingu

Dosud bylo v práci uvedeno, co konkrétně znamená samotný pojem outsourcing podle několika významných autorů. Stejně byla přiblížena i historie, která vedla k vzniku outsourcingu. Nyní je důležité vysvětlit, v čem spočívají výhody a nevýhody této metody. Vždy je však velkou nutností si důkladně zvážit zda je vůbec nutné k outsourcingu určitého procesu přistupovat a hodnotit jednotlivé vytěsňované oblasti odděleně. Nesmíme však opomenout skutečnost, že nákladová stránka věci nemusí být vždy rozhodujícím elementem rozhodování o outsourcingu, spíše kritériem pro výběr partnera. [31]

7.3.2.1 Výhody outsourcingu

Outsourcing je moderní způsob přesunu některých činností podniku na jiný subjekt. Mezi nejčastější činnosti, které se provádějí formou outsourcingu lze zařadit, také účetnictví, nebo správu informačních technologií.

Mezi hlavní výhody outsourcingu informačních technologií v bankovním sektoru patří:

- **Možnost zaměření se na hlavní činnost**

  Činnost banky, která se bude soustředit pouze na hlavní činnost, bude vykazovat větší flexibilitu a operativnost při řízení. To se nakonec projeví i ve vyšší kvalitě poskytovaných služeb, neboť si může hlídat kvalitu a provádění jedné hlavní činnosti což je poskytování bankovních služeb.

- **Časové výhody**

  Vytěsněním některých podpůrných činností na externího dodavatele je možné rychlejší zavádění nejmodernějších technologií díky odborné specializaci externího dodavatele. Banky tak mohou vytvářet kvalitní prostředí pro své klienty.

- **Zlepšení operativního řízení**

  Tato výhoda úzce souvisí se zaměřením na hlavní činnost. Zaměřením pozornosti na menší objem činností vede zákonitě k operativnějšímu stylu řízení a celkovému zefektivnění řízení celkových služeb.

- **Snížení rizika v delším horizontu**

  Přestože je outsourcing považován obecně za rizikový krok, může jím být zároveň riziko sníženo, a to v tom případě, že podnik přenese riziko možného investování či změn v technologiích na dodavatele technologií.

- **Snížení nákladů**

  V případě, že poskytovatel outsourcingu poskytuje stejné služby více odběratelům, dosahuje tím vyšší efektivnosti, což je prostředek ke snížení nákladů. Dále lze snížit náklady lepším know-how, kdy lze předpokládat, že podnik specializující se na určitou oblast v ní bude mít rovněž lepší technologie a odborníky. Také přístup k lepší infrastruktuře dodavatele může vést ke snížení nákladů.

- **Převedení fixních nákladů na variabilní**

  Tím, že banka přenechá některé činnosti externím dodavatelům, sníží se jí fixní náklady (aktiva), které by jinak musela držet k zajištění této činnosti. Outsourcingem jsou tyto fixní náklady vyvedeny mimo banku a následně nakupovány jako meziprodukty a služby ve formě variabilních nákladů. Oproti fixním nákladům mají variabilní tu výhodu, že vznikají v takovém čase a v takovém objemu, v jakém jsou nutné pro zajištění objednávaných služeb. [39]

7.3.2.2 Nevýhody outsourcingu

Tak jako každá činnost i outsourcing má své nevýhody, které je nutné si uvědomit, než se banka rozhodne pro outsourcingové řešení. Jak byly v předchozí části práce zmíněny výhody outsourcingu, stejným způsobem lze popsat i nevýhody této poskytované externí služby.

- **Úspory nákladů nemusí splnit očekávání**

  Banky od této externí služby očekávají především snížení nákladů, ať již jako hlavní cíl, nebo doprovodný cíl. Pokud však nebude outsourcingový vztah fungovat tak, jak by měl, může naopak dojít ke zvýšení nákladů, zejména pak v oblasti nákladů transakčních.

- **Náklady na změnu kontraktu**

  V případě, že outsourcingový kontrakt nebude splňovat očekávání outsourcera, může být velmi nákladné tento kontrakt změnit. Podmínky kontraktu v době uzavření akceptovaly obě strany a v případě požadavku od outsourcera na změnu, nemusí to být výhodné pro dodavatele. V takovém případě nezbývá outsourcerovi než pokračovat ve vztahu podle smluvních podmínek, nebo se pokusit z outsourcingového vztahu „vycouvat“, což však pro něj může být velice riskantní, neboť na dodavatele většinou přechází vlastnictví potřebného majetku či infrastruktury.

- **Snížení kvality služeb**

  Přes všechny předpoklady vyplývající z přenechání činnosti specializovanému dodavateli může dojít ke snížení kvality nakupovaných služeb. Může se to týkat i opožděné reakci na obměnu nových informačních technologií, což může banku dostat do nežádoucí konkurenceschopnosti.

- **Riziko změny dodavatele**

  Podobné riziko jako byla změna kontraktu, je i samotná změna dodavatele, což bude v každém případě znamenat vysoké výdaje za právní služby. Musí nalézt (v dostatečně krátkém čase) nového a přitom kvalitnějšího dodavatele, který bude muset nakoupit zařízení, technologii, případně najmout zaměstnance, kteří byli předtím převedeni na dodavatele v rámci outsourcingového kontraktu.

- **Náklady na samotný outsourcing**

  Rozhodnutí zvolit outsourcing je vždy vedle určitého rizika spojeno s vysokými počátečními transakčními náklady. Pro banku to znamená zejména čas, který musí outsourcingu věnovat její management, náklady na případné poradce, možné omezení efektivnosti výroby v době, kdy se potenciální dodavatelé seznamují

s provozem, případné dopravní náklady, náklady na zpracování kontraktů a tak podobně.

- **Riziko úniku citlivých informací**

  Outsourcing je postaven na intenzívní spolupráci dodavatele a outsourcera. Tato oblast snad představuje největší riziko pro outsourcera. Při takto těsném kontaktu, kdy často dodavatel provádí některé své činnosti přímo v podniku outsourcera, se dostává dodavatel i k různým citlivým informacím. V případě selhání vztahu s dodavatelem může dojít k vyzrazení těchto informací. [39]

7.3.3 Outsourcing v bankovním sektoru

Mají-li si banky zachovat konkurenceschopnost, je využití outsourcingu v globálním světě nezbytné. V oblasti bankovnictví v České republice je outsourcing ovlivněn nejen platnou *Vyhláškou č. 163/2014 Sb. Vyhláška o výkonu činnosti bank, spořitelních a úvěrních družstev a obchodníků s cennými papíry*, ale i *Zákonem č. 110/2019 Sb. Zákon o zpracování osobních údajů* a dalšími předpisy. Podrobnější podmínky stanovuje Česká národní banka ve svých sděleních a vyhlášce upravující řízení rizik a vnitřní kontrolní prostředí. Pokud chtějí bankovní subjekty outsourcovat některé aktivity, musí připravit detailní analýzu rizik spojených s danou aktivitou, stanovit způsob, jakým budou riziko řídit, monitorovat a eliminovat, což významným způsobem snižuje výsledné úspory. [28]

V současné době lze u mnoha menších a středních bankovních domů, které jsou sice součástí globálních bankovních skupin, vysledovat trend tzv. interního outsourcingu, zejména v oblasti informačních technologií, ale i v oblasti podpůrných funkcí jako je vedení účetnictví, daňová evidence, řízení financí a finančních zdrojů, zpracování dokladů, nebo fakturace.

V tomto případě se jedná o jakési vytváření center sdílených služeb pro danou funkci v rámci celé skupiny či regionu. Hlavním přínosem takových center je určitě zvýšení rychlosti a efektivnosti v oblasti řízení informačních technologií a jeho provozu. Hlavním přínosem interního outsourcingu je zvýšení efektivity řízení změn informačních technologií, což ve svém důsledku snižuje riziko bezpečnostních rizik.

Pomineme-li lokální problémy, skutečné využívání outsourcingu ve finančních institucích je často limitováno nízkou důvěrou ve schopnost třetích stran zajistit právě výše jmenovanou dostatečnou bezpečnost a důvěrnost zpracovávaných informací. S rostoucím objemem dat

a využíváním nových komunikačních kanálů se zvýšila i četnost zveřejněných bezpečnostních incidentů. [28]

V roce 2019 vydal Evropský orgán pro bankovnictví (dále jen EBA) nové a přísnější pokyny k outsourcingu, které dopadnou na všechny subjekty podléhající jeho dohledu, včetně platebních institucí a institucí elektronických peněz. Pokyny EBA vznikají především v reakci na digitalizaci finančního sektoru, v důsledku, kde se hojně objevují nová a komplexnější fintechová[6] outsourcingová uspořádání [41].

České banky zatím outsourcing informačních technologií v plném rozsahu nevyužívají. Některé banky si zajišťují u externích zdrojů například vývoj aplikací či zprávu části hardwaru. Pro kompletní provoz a rozvoj technologické infrastruktury se však zatím nerozhodla ani jedna finanční instituce, ačkoli v českém průmyslu si už outsourcing své místo našel. Informační technologie však mají pro kvalitu poskytovaných produktů v bance obvykle větší význam než například ve výrobním podniku. Finanční instituce v současnosti získávají nebo ztrácejí konkurenční výhodu často díky vyšší nebo nižší kvalitě těch služeb, které jsou přímo závislé na kvalitě řešení a provozu informačních systémů. Zvýšení kvality a spolehlivosti informačních technologií se přitom považuje za jeden z hlavních přínosů outsourcingu. [42]

Při zaměření pouze na Českou republiku v ohledu na outsourcing IT služeb vydal Doupal [43] článek, kde uvedl *„Mezi státy střední a východní Evropy jsou Česká republika společně s Polskem nejvyspělejšími a nejoblíbenějšími destinacemi pro outsourcing v oblasti IT. Zahraniční firmy si u nás cení především vyspělosti právního systému, politické stability, infrastruktury, vzdělávacího systému a datové bezpečnosti“.* Z čehož vyplývá pozitivní vliv outsourcingu informačních technologií mezi, které patří také bankovnictví.

[6] ***Spojení slov*** „finance“ a „technologie“ představuje pojem, vyjadřující fúzi těchto dvou širokých oblastí, přičemž jejich společným průsečíkem je inovace, pokrok, progres. Dostupné z: https://www.epravo.cz/top/clanky/fintech-cast-i-definice-a-subjekty-106711.html

II. PRAKTICKÁ ČÁST

8 ANALÝZA - INFORMAČNÍ TECHNOLOGIE V BANKOVNICTVÍ

Informační bezpečnost se stává významným faktorem dlouhodobého úspěchu či naopak neúspěchu organizace. Aby organizace přežila, musí určitá rizika přijmout a tyto do jisté míry řídit. Míra rizika je pak dána velikostí negativního dopadu. Abychom mohli zjistit jaká rizika, a hrozby informačním systémům hrozí, je nutné provádět jejich analýzu. Cílem analýzy rizik je, aby případné hrozby a rizika identifikovala. Výsledkem analýzy je pak pravděpodobnost rizika, které může vzniknout. Analýza je klíčovou aktivitou v procesu řešení bezpečnosti pro určení jaká informační aktiva je třeba chránit, jaká pro ně existují ohrožení a s jakou pravděpodobností mohou nastat. V oblasti týkající se bezpečnosti informačních systémů vytváří analýza rizik účinný systém ochrany k identifikaci a vyhodnocování určitých hrozeb, kterými jsou informační systémy ohrožovány a jejím úkolem je vybrat správné ochranné opatření. [5]

Tato kapitola analyzuje pět nejznámějších bank v České republice a poukazuje na jejich bezpečnost a zabezpečení internetového bankovnictví. Postupně popisuji jejich vzhled, náročnost, přehled a orientace na internetových stránkách dané banky. Dále jsem se zaměřila na poskytování a dostupnost informací ve vybraných bankovních portálech a jaké bezpečnostní prvky využívají.

Postupně jsem narážela na problémy, které se týkaly získávání informací zaměřených na bezpečnost a zabezpečení internetového bankovnictví od konkrétních bank. Nedá se to nazvat o nechtění podání konkrétních informací, ale jednalo by se o zveřejnění interních předpisů dotyčné banky. Pro banky jsou tyto informace interní a důvěrné, proto pro obyčejného člověka, který nemá s dotyčnou bankou pracovní poměr, nemohou banky poskytovat informace ohledně bezpečnosti a zabezpečení internetového bankovnictví. Pokud by tyto informace veřejně sdílely, samy by tím ohrožovaly svou vlastní bezpečnost. Z vlastní zkušenosti mohu říci, že tento systém tak funguje, když jsem se snažila získat tyto informace. Do každé banky jsem poslala přes informační centrum banky požadavek o poskytnutí podrobnějších informací o bezpečnostních prvcích a používaného zabezpečení elektronické komunikace mezi bankou a klientem. Odpovědi se mě dostalo od každé banky s tím, že informace, které můžou poskytnout, najdu na jejich domovských stránkách.

Zkoušela jsem to i přes známého, který pracuje jako vývojář v dané bance, ale oznámil mě, že tyto informace nemůže poskytnout z důvodu utajení informací a pokud by porušil tato pravidla, banka by musela vyvodit důsledky. Takže po těchto negativních událostech mě

nezbývalo nic jiného než získávat informace, které byly dostupné na internetových stránkách banky a prostřednictvím stránek, které umožňují test zabezpečení protokolu SSL/TLS.[7]

8.1 Výběr pěti nejznámějších bank v České republice

V České republice je velké množství bank, zaměřila jsem se však na ty nejvíce využívané. Vybrala jsem pět nejznámějších bank v České republice a na nich budu postupně analyzovat a hodnotit bezpečnost internetového bankovnictví.

Pro mou práci jsem si vybrala banky:

- Komerční banka,
- Česká spořitelna,
- Československá obchodní banka (ČSOB),
- Air Bank,
- MONETA Money Bank.

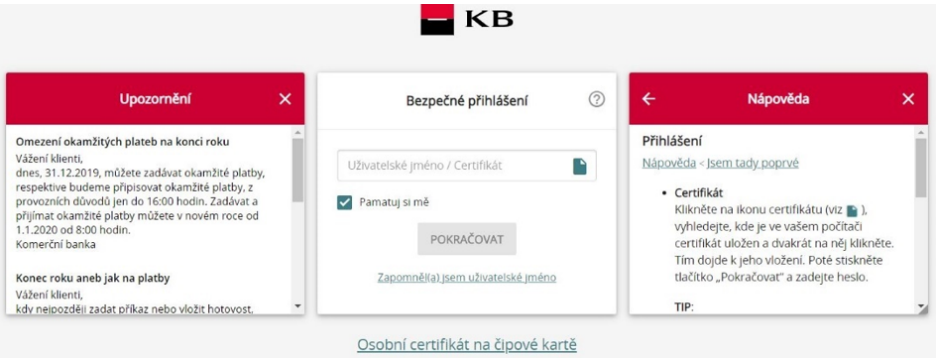
8.1.1 Komerční banka

Komerční banka (dále jen KB) je přední bankovní instituce v České republice se širokou škálou nabízených bankovních služeb. KB je mateřskou společností Skupiny komerčních bank a součástí mezinárodní skupiny Société Générale[8]. Obsluhuje 1,67 milionů klientů v České republice s rozmístěním 776 bankomatů a 365 poboček. Přístup do internetového bankovnictví KB, je přes úvodní stránku a rozklikávací políčko, které je umístěno v pravé horní části. Po rozkliknutí internetbankingu se zobrazí pole pro přihlášení ke službě ***Mojebanka***, do nějž je třeba zadat přidělený osobní certifikát. Dále se zde nachází informace ohledně hrozeb a varování, které mají zákazníky poučit. Velmi dopodrobna se věnují bezpečnosti, což je velmi pozitivní. Pravidla bezpečnosti poukazují na to, jak pracovat s internetem, vše je doprovázeno i grafickým znázorněním. Na stránce se nacházejí návody k bezpečnostním předmětům, které by mohly být viditelnější.

[7] ***SSL/TLS*** (Secure Sockets Layer/ Transport Layer Security) jsou kryptografické protokoly poskytující možnost zabezpečené komunikace na Internetu. Dostupné z: https://www.ssls.cz/slovnik/tls.html

[8] ***Société Générale*** je francouzská obchodní banka s centrálou v Paříži. Patří ke třem nejstarším bankám ve Francii. Od roku 2001 je majitelem české Komerční banky. Dostupné z: https://cs.wikipedia.org/wiki/Soci%C3%A9t%C3%A9_G%C3%A9n%C3%A9rale

Jak na svých stránkách KB uvádí, spustila nový způsob přihlašování do internetového bankovnictví prostřednictvím zabezpečené aplikace v chytrém telefonu tzv. KB Klíč. Klienti banky tak mohou nahradit bezpečnostní certifikát internetového bankovnictví aplikací v chytrém telefonu, a získat tak přístup ke svému účtu z jakéhokoliv zařízení.



Obrázek 10 Stránka internetového bankovnictví Komerční banky. [44]

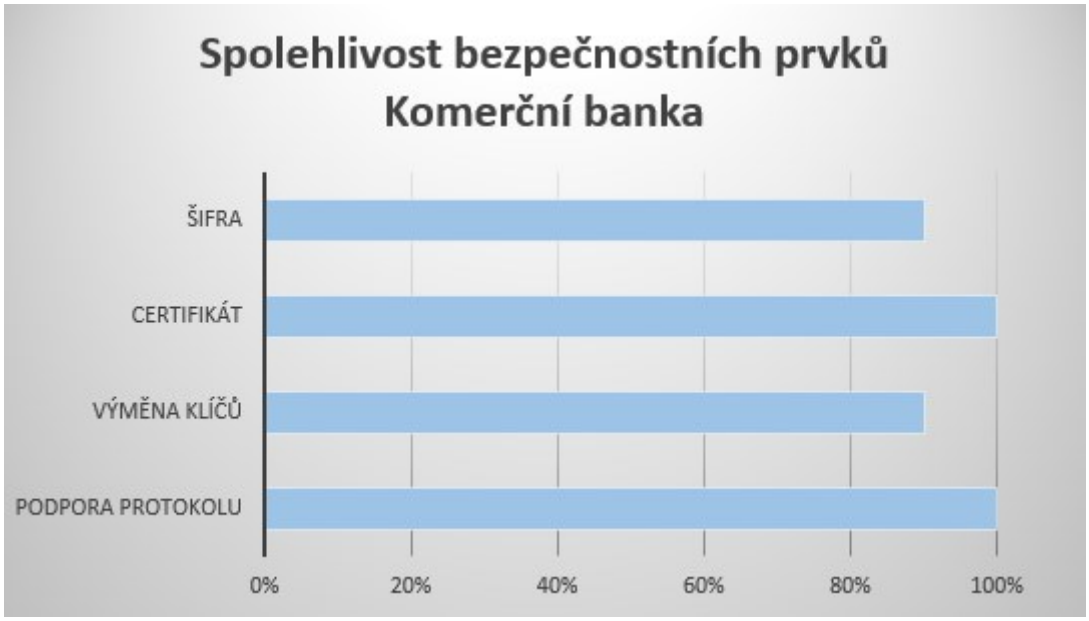
Bezpečnostní prvky používané k zabezpečení komunikace mezi bankou a klientem, které jsou využívané KB, jsou uvedeny v tabulce 2.

Tabulka 2 Bezpečnostní nástroje a algoritmy Komerční banky [45]

Idetifikace	Autorizace	Asymetrické šifrování	Transformační algoritmus	Certifikační autorita	Algoritmus podpisu
Přihlašovací jméno	Jednorázové heslo	Algoritmus RSA	SHA256RSA	DigiCert SHA2 Extendet Validation Server CA	SHA256 s RSA
Heslo	Elektronický token	Délka kliče 2048 Bitů			
	SMS kód				
	Vyšší úroveň zabezpečení: digitální podpis, certifikát na čipové kartě				

Informace uvedené v tabulce jsem získala jednak přímo na domovských stránkách KB a jednak na stránce ***Qualys SSL Labs*** – test pro ověření instalace certifikátu, uvedeno na adrese *(https://www.ssllabs.com/ssltest/analyze.html?d=www.kb.cz&latest)*. Pro ověření správnosti získaných informací na stránce Qualys SSL Labs, jsem provedla kontrolu certifikátu ještě na stránce ***ImmuniWeb, SSL Security Test,*** uvedeno na adrese *(https://www.immuniweb.com/ssl/?id=k86u4UF7)*. Hodnoty a informace získané testem certifikátu zabezpečení přihlašovací stránky o bezpečnostním certifikátu KB se shodují ve všech uvedených algoritmech a bezpečnostních prvcích.

Grafické znázornění spolehlivosti jednotlivých bezpečnostních prvků komunikace je vyobrazeno v grafu č. 1. Graf jsem vytvořila na základě získaných hodnot ze zdroje [45] po ukončení testovaného certifikátu zabezpečení stránky pro přístup do internetového bankovnictví KB. Po dokončení testu jsou na stránce vyhodnoceny jednotlivé oblasti zabezpečení.



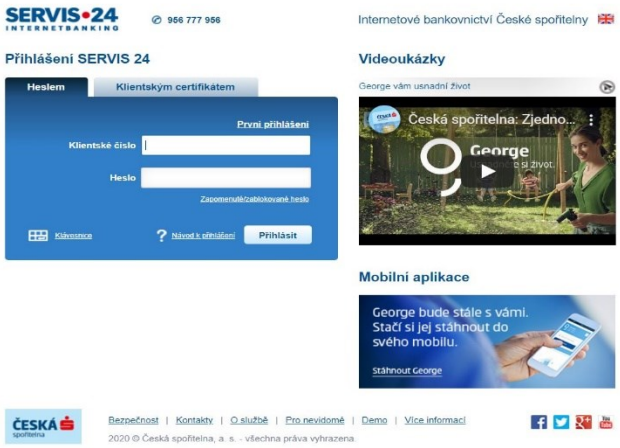
Graf 1 Bezpečnostní prvky komunikace Komerční banky. Zdroj: vlastní

8.1.2 Česká spořitelna

Česká spořitelna je další v řadě analyzovaných bankovních společností. Je to banka s nejdelší tradicí na českém trhu. Česká spořitelna je od roku 2000 součástí silné středoevropské Skupiny Erste.[9] Obsluhuje 4,6 mil. klientů, 483 poboček a 1800 bankomatů. Česká spořitelna má podobný přihlašovací design jako Komerční banka. Jedná se o moderní, poměrně přehledné uspořádání hlavního okna pro přihlášení do internetového bankovnictví uvedeného jako ***Servis 24***. Na úvodní stránce se nacházejí navigační panely, ve kterých se ale velmi těžko orientuje, potřebné informace se proto zdlouhavě hledají. Na pravé straně se nachází políčko pro vstup na přihlašovací stránku. Po přesměrování se stránka změní na velmi jednoduchou a přehlednou. Nenacházejí se zde žádná upozornění a rady pro

[9] ***Erste Group Bank AG*** je rakouská obchodní banka se sídlem ve Vídni, sdružuje celou skupinu bankovních institucí ve střední a východní Evropě. Zdroj: https://www.csas.cz/cs/korporace/o-nas/erste-group

zákazníky, což může být drobná nevýhoda. Navíc je tu panel s informacemi o mobilních aplikacích, které se dnes již využívají na mobilních smartphonech.



Obrázek 11 Stránka internetového bankovnictví ČS. [46]

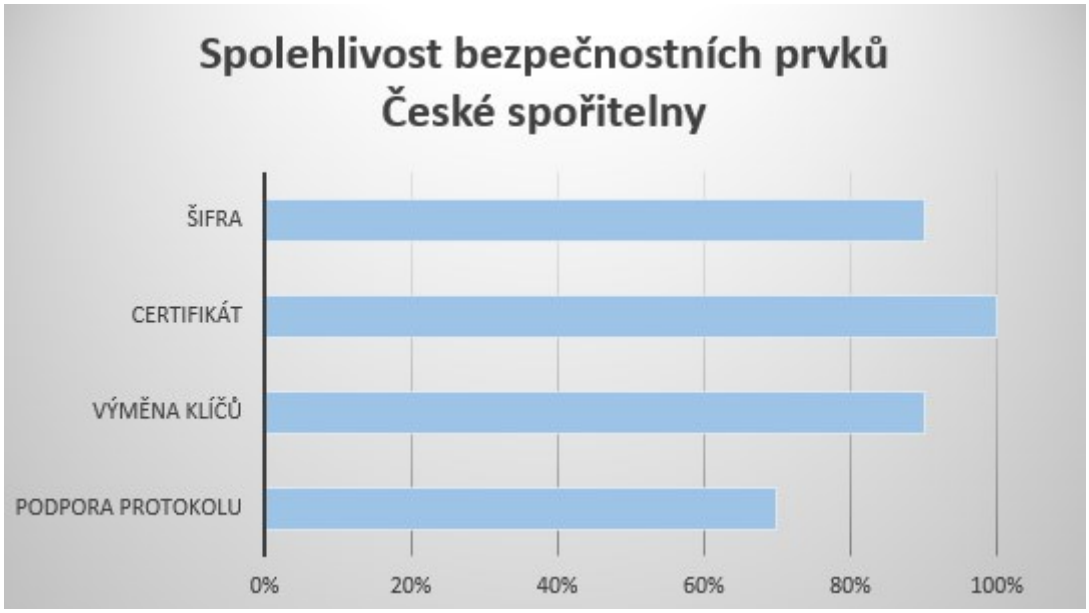
Bezpečnostní prvky používané k zabezpečení komunikace mezi bankou a klientem, které jsou využívané Českou spořitelnou, jsou uvedeny v tabulce 3.

Tabulka 3 Bezpečnostní nástroje a algoritmy České spořitelny [47]

Identifikace	Autorizace	Asymetrické šifrování	Transformační algoritmus	Certifikační autorita	Algoritmus podpisu
Klientské číslo	PIN kód	Algoritmus RSA	SHA256RSA	DigiCert SHA2 Global CA G2	SHA256 s RSA
Heslo	SMS kód doplňuje heslo	Délka kliče 2048 Bitů			
	SMS kód doplňuje heslo nadlimitní transakce				
	Vyšší úroveň zabezpečení: autentizační kalkulátor, certifikát na čipové kartě				

Tak jako u Komerční banky jsem provedla test používaného certifikátu Českou spořitelnou na stránkách poskytující test kontroly zabezpečení (Qualys SSL Labs a ImmuniWeb). Výsledné informace o bezpečnostním certifikátu České spořitelny se shodují ve všech uvedených algoritmech a bezpečnostních prvcích.

Grafické znázornění spolehlivosti jednotlivých bezpečnostních prvků komunikace. Graf jsem vytvořila na základě získaných hodnot ze zdroje [47] po ukončení testovaného certifikátu zabezpečení stránky pro přístup do internetového bankovnictví České spořitelny.



Graf 2 Bezpečnostní prvky komunikace ČS Zdroj: vlastní

8.1.3 Československá obchodní banka (ČSOB)

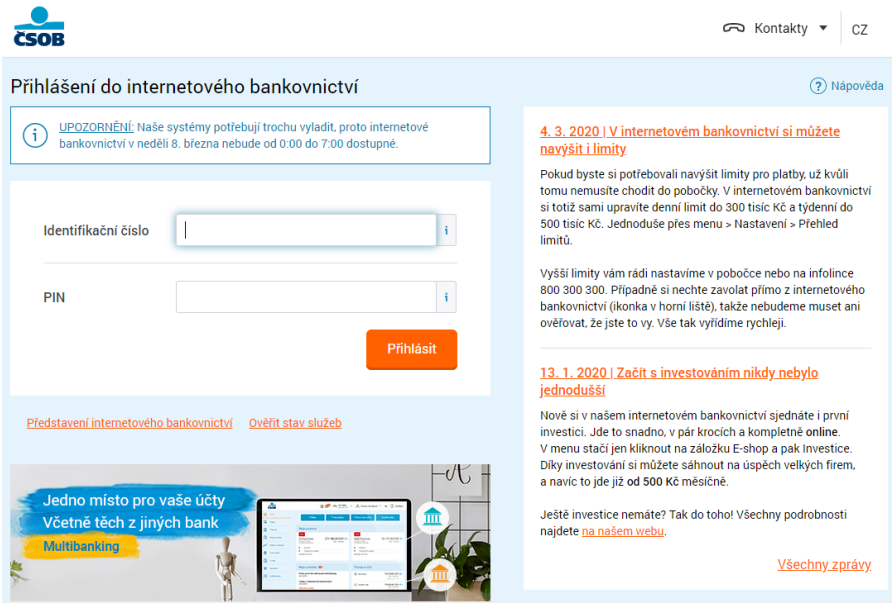
Československá obchodní banka je třetí analyzovanou bankou, která patří rovněž mezi velké bankovní instituce. Obsluhuje 3,6 mil. klientů na 235 pobočkách s 1063 bankomaty.

Československá obchodní banka má svou internetovou stránku méně přehlednou. Nachází se zde více navigačních panelů. Panely jsou nahrazeny velkým množstvím informací, které svou malou velikostí působí velmi špatně a klienty mohou zmást. Na pravé straně se nachází políčko nazvané elektronické bankovnictví. Po rozkliknutí se otevře nabídka služeb jako je smartbanking, smart klíč nebo internetbanking 24.

Můžeme si všimnout, že do internetového bankovnictví se můžeme přihlásit pomocí identifikačního čísla a hesla, pomocí elektronického podpisu z čipové karty s certifikátem, nebo čtečky čipových karet. Karty komunikují pomocí softwaru, např. CryptoPlus.[10] Informace týkající se zabezpečení se hledají hůře kvůli nepřehlednému designu. Banka se

[10] ***CryptoPlus***™ - osobní elektronická identita na čipové kartě. Je to čipová karta, která dokáže především spolehlivě identifikovat a bezpečně komunikovat. Dostupné z: https://www.cryptoplus.cz/

snaží hned na své úvodní přihlašovací stránce informovat klienty o možných hrozbách, uživatel je tedy s tímto upozorněním v kontaktu při každém přihlašování do internetového bankovnictví.



Obrázek 12 Stránka internetového bankovnictví ČSOB. [48]

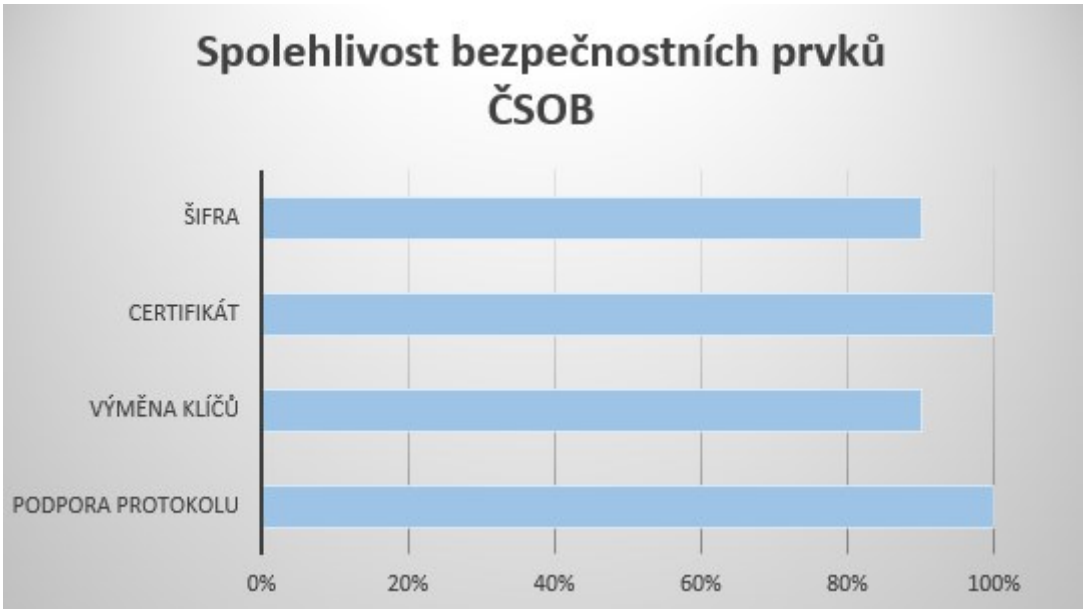
Bezpečnostní prvky používané k zabezpečení komunikace mezi bankou a klientem, které jsou využívané bankou ČSOB, jsou uvedeny v tabulce 4.

Tabulka 4 Bezpečnostní nástroje a algoritmy ČSOB banky [49]

Identifikace	Autorizace	Asymetrické šifrování	Transformační algoritmus	Certifikační autorita	Algoritmus podpisu
Čipová karta	Identifikační číslo	Algoritmus RSA	SHA256RSA	DigiCert SHA 2 Global CA G2	SHA256 s RSA
Certifikát	PIN kód	Délka klíče 2048 Bitů			
	SMS kód				
	Smart klíč				

Tak jako v předchozích případech jsem provedla test používaného certifikátu banky ČSOB na stránkách poskytující test kontroly zabezpečení (Qualys SSL Labs a ImmuniWeb). Informace o bezpečnostním certifikátu ČSOB se shodují ve všech uvedených algoritmech a bezpečnostních prvcích.

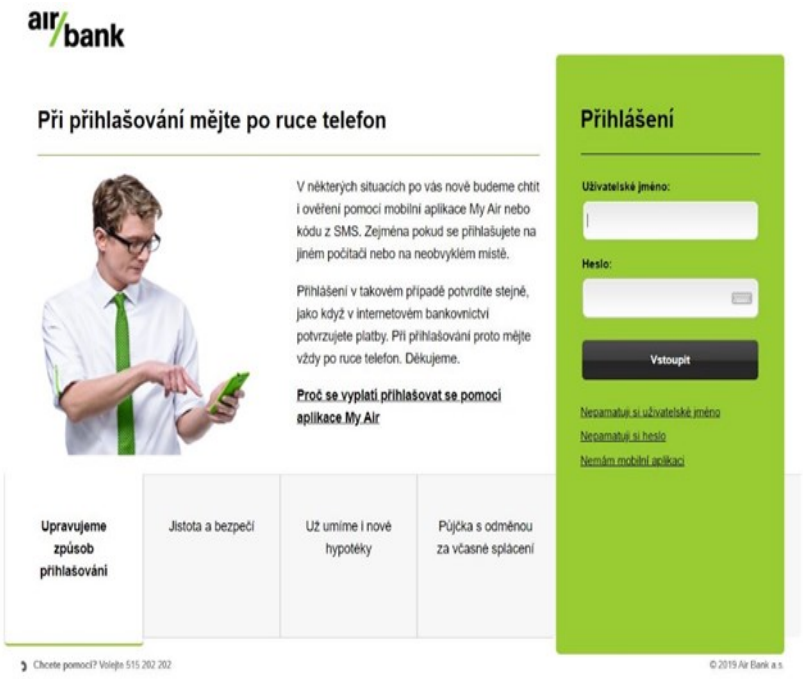
Grafické znázornění spolehlivosti jednotlivých bezpečnostních prvků komunikace. Graf jsem vytvořila na základě získaných hodnot ze zdroje [49] po ukončení testovaného certifikátu zabezpečení stránky pro přístup do internetového bankovnictví ČSOB.



Graf 3 Bezpečnostní prvky komunikace ČSOB. Zdroj: vlastní

8.1.4 Air Bank

Následující analýzu zabezpečení komunikace jsem provedla na bankovní společnosti Air Bank. Jedná se o menší bankovní společnost, která obsluhuje téměř 800 000 klientů. Air Bank musí designem svých stránek zaujmout každého návštěvníka. Jde o velmi jednoduchou, ale stylovou prezentaci. Velmi dobrá přehlednost stránky pomáhá uživatelům, kteří hledají informace o poskytovaných službách. Web má jednoduchý navigační panel, na kterém najdeme vše potřebné. Co se týče bezpečnosti, Air Bank jako první přišla s kartou a čtečkou, která slouží k autorizaci platby. Panel pro vstup do internetbankingu je rovněž jednoduchý. Nachází se zde také další panel s užitečnými informacemi.



Obrázek 13 Stránka internetového bankovnictví Air Bank. [50]

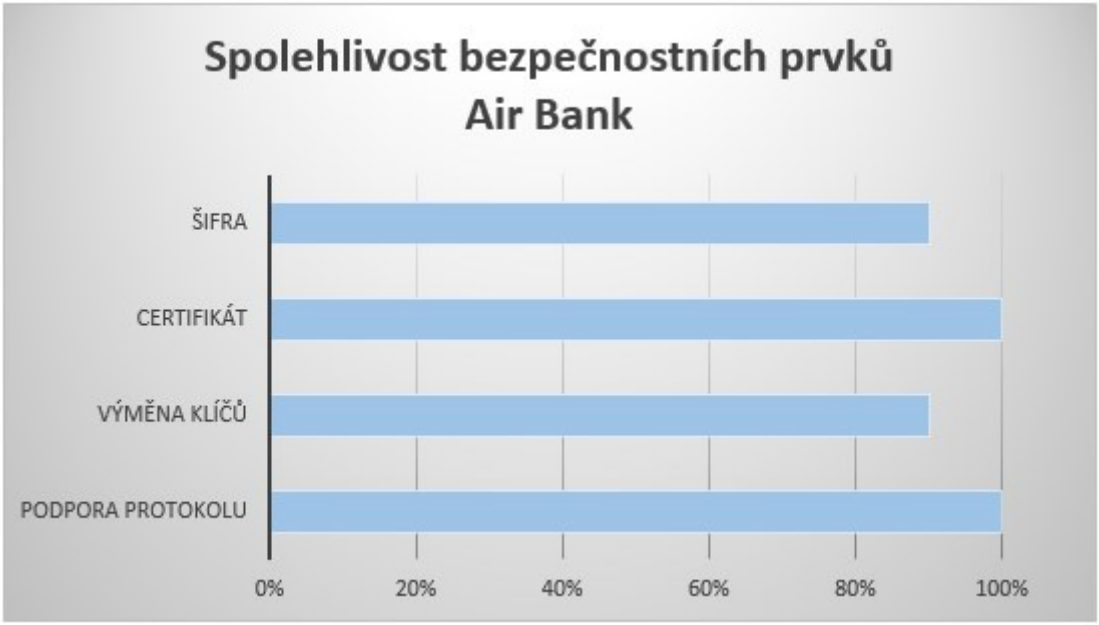
Bezpečnostní prvky a algoritmy používané k zabezpečení komunikace mezi bankou a klientem, jsou uvedeny v tabulce 5.

Tak jako v předchozích případech jsem provedla test používaného certifikátu Air Banky na stránkách poskytující test kontroly zabezpečení (Qualys SSL Labs a ImmuniWeb). Informace o bezpečnostním certifikátu Air Banky se shodují ve všech uvedených algoritmech a bezpečnostních prvcích.

Tabulka 5 Bezpečnostní nástroje a algoritmy Air Bank [51]

Identifikace	Autorizace	Asymetrické šifrování	Transformační algoritmus	Certifikační autorita	Algoritmus podpisu
Přihlašovací jméno	Jednorázové heslo	Algoritmus RSA	SHA256RSA	DigiCert SHA2 Extendet Validation Server CA	SHA256 s RSA
Heslo	Mobilní aplikace potvrzení	Délka kliče 2048 Bitů			
	SMS kód				
	Bezpečnostní otázky				

Grafické znázornění spolehlivosti jednotlivých bezpečnostních prvků komunikace. Graf jsem vytvořila na základě získaných hodnot ze zdroje [51] po ukončení testovaného certifikátu zabezpečení stránky pro přístup do internetového bankovnictví Air Bank.



Graf 4 Bezpečnostní prvky komunikace Air Bank. Zdroj: vlastní

8.1.5 MONETA Money Bank

Poslední analyzovanou bankou je bankovní institut MONETA Money Bank, což je čtvrtá největší banka v České republice, která obsluhuje 1mil. klientů na 180 pobočkách s více než 630 bankomaty. Internetové stránky MONETA Money Bank prošly před několika měsíci inovací a došlo zároveň k jejich přejmenování. Nový design působí zpočátku oproti původnímu složitě a nepřehledně, vše je však o zvyku a po čase zjišťujeme, že nový design je velmi zjednodušený a veškeré informace mají své místo a člení se podle příslušných kategorií. V pravé horní části se nachází políčko k přihlášení do internetového bankovnictví. Toto políčko nás přesměruje na stránku, kde je třeba správně zadat identifikační číslo a heslo, čímž se dostaneme ke svému účtu. Při prvním přihlášení je nutné však vygenerovat autorizační SSL certifikát a podpisový certifikát. Na úvodní stránce pro přihlášení si můžeme všimnout navigačních panelů, které poskytují informace klientovi. Ve spodní části se nacházejí důležitá bezpečnostní upozornění, která poukazují na výskyt phishingu a nabádají klienty, aby na tento druh útoku nenaletěli. Dále zde nalezneme tipy, jak se před útoky chránit. Díky přehlednému designu se informace o bezpečnostních předmětech hledají

vcelku rychle, ačkoliv je třeba rozkliknout několik odkazů, které uživatele postupně přesměrují na požadovanou pozici.

Obrázek 14 Přihlašovací okno do Monety Money bank. [52]

Bezpečnostní prvky a algoritmy používané k zabezpečení komunikace mezi bankou a klientem jsou uvedeny v tabulce 6.

Tabulka 6 Bezpečnostní nástroje a algoritmy MONETA Money Bank. [53]

Identifikace	Autorizace	Asymetrické šifrování	Transformační algoritmus	Certifikační autorita	Algoritmus podpisu
Přihlašovací jméno	Digitální certifikát	Algoritmus RSA	SHA256RSA	DigiCert SHA2 Global CA G2	SHA256 s RSA
Heslo	SSL certifikát	Délka klíče 2048 Bitů			
	Podpisový certifikát				

Tak jako v předchozích případech jsem provedla test používaného certifikátu banky Moneta na stránkách poskytující test kontroly zabezpečení (Qualys, SSL Labs a ImmuniWeb). Informace o bezpečnostním certifikátu banky MONETA se shodují ve všech uvedených algoritmech a bezpečnostních prvcích.

Grafické znázornění spolehlivosti jednotlivých bezpečnostních prvků komunikace. Graf jsem vytvořila na základě získaných hodnot ze zdroje [53] po ukončení testovaného certifikátu zabezpečení stránky pro přístup do internetového bankovnictví MONETA Money Bank.

Graf 5 Bezpečnostní prvky komunikace Moneta Money Bank. Zdroj: vlastní

8.1.6 Vyhodnocení analýzy

Provedenou analýzou bylo zjištěno, že dnešní banky mají poměrně dobře zabezpečené internetové bankovnictví díky moderním šifrovacím algoritmům a délce klíče. Banky splňují moderní standardy, využívají k zajištění komunikace asymetrické šifrovací algoritmy RSA, s využitím kryptografických hashovacích funkcí SHA 2

SHA 2 (Secure Hash Algorithm) – jedná se o jednosměrné funkce, které musí splňovat přesně definované podmínky. Základní hashovací funkce mapují řetězec libovolné délky (zpráva, datový soubor) na řetězec konstantní délky o velikosti SHA224, SHA256, SHA384, SHA512 bitů a vytvářejí tak otisk vstupního řetězce. Výsledný otisk se označuje jako výtah, hash, fingerprint nebo miniatura a je závislý na všech bitech vstupního řetězce. Tyto funkce slouží ke kontrole integrity dat, k porovnání dvojice zpráv, k vyhledávání, indexování a využívají se pro tvorbu digitálních podpisů. [54]

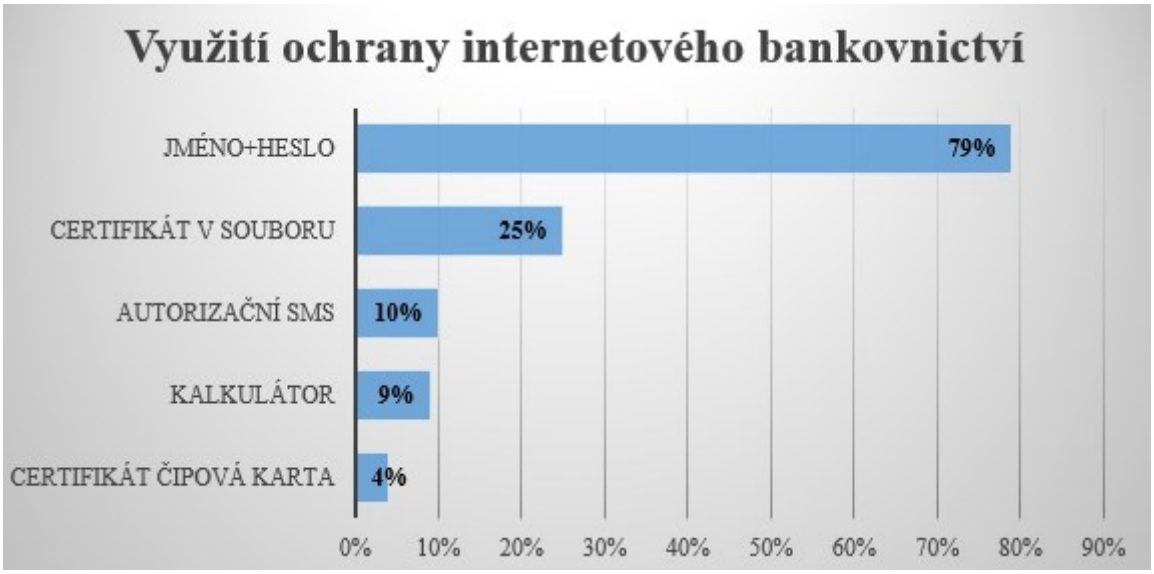
Na základě provedeného testu přihlašovací stránky jednotlivých bank do elektronického bankovnictví prostřednictvím testovacích stránek ***Qualys, SSL Labs a ImmuniWeb*** jsem zjistila jejich údaje o používaných šifrovacích algoritmech. Výše jmenované banky, jak jsem se již zmínila, používají asymetrický šifrovací algoritmus RSA s délkou šifrovacího klíče 2048 bitů, v kombinaci hashovací funkce SHA 256 bitů, což je transformační algoritmus převodu komunikace. Jelikož šifrovací algoritmus RSA je využíván jak k šifrování, tak k podepisování zpráv, je tato kombinace RSA s SHA256 využívána i k vytvoření algoritmu podpisu.

Jako Certifikační autoritu používají jmenované banky certifikáty vydané společností ***CA DigiCert***, která nabízí v oblasti šifrování komplexní bezpečnostní řešení. Její nabídka zahrnuje všechny druhy serverových SSL/TLS certifikátů, co do typu ověření i technických funkcí. [40]

Česká spořitelna, Československá obchodní banka a banka MONETA Money Bank používají globální certifikát ***DigiCert SHA2 Global CA G2***. Komerční banka a banka Air Bank používají certifikát s rozšířeným ověřováním serveru ***DigiCert SHA2 Extendet Validation Server CA***.

Základní bezpečnostní úkony, které se týkají klientů, pro vstup do internetového bankovnictví jsou k identifikaci klienta v největší míře využívány přihlašovací jméno a heslo (PIN). V případě banky ČSOB se k identifikaci využívá čipová karta a certifikát. Jako autorizace, resp. potvrzování různých úkonů a pokynů k platbě se využívají u každé banky různé způsoby autorizace, jako je identifikační číslo, PIN kód, SMS kód, smart klíč, mobilní aplikace, digitální certifikát, podpisový certifikát, elektronický token. V případě klientem požadované vyšší úrovně zabezpečení internetového bankovnictví se využívá digitální podpis nebo certifikát na čipové kartě, případně autentizační kalkulátor.

Na grafu č. 6 můžeme vidět ***využívání bezpečnostních prvků*** internetového bankovnictví z roku 2006. Procenta ukazují, kolik bank využívalo tyto prvky a jak je vidět, nejvíce využívaným způsobem zabezpečení byla identifikace klienta pomocí jména a hesla, která platí i v současnosti.



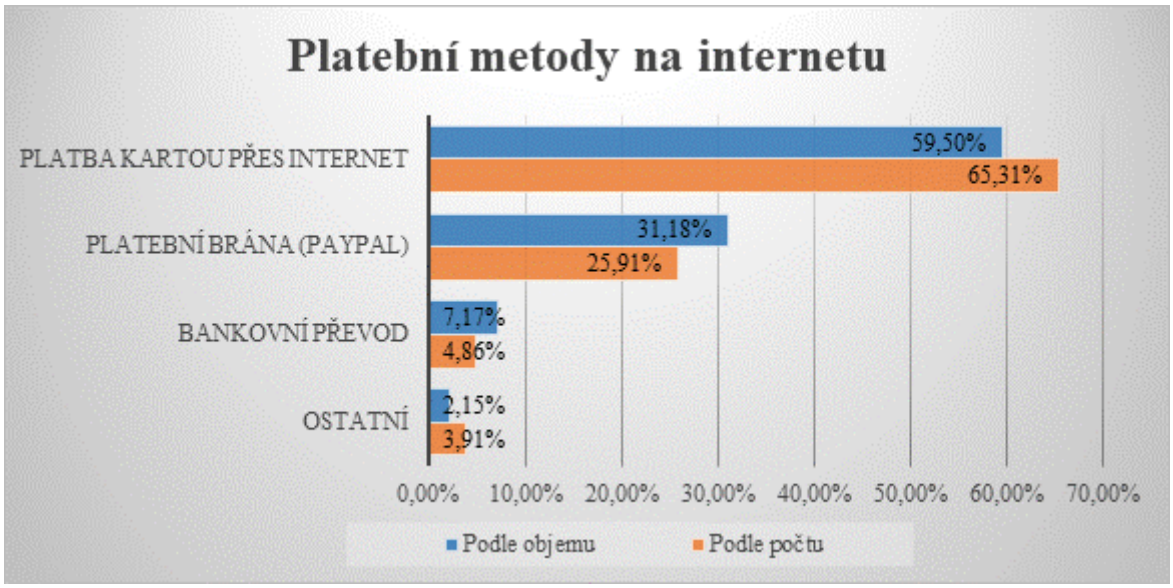
Graf 6 Využití ochrany internetového bankovnictví na českém trhu [14]

Mezi moderní technologie internetového bankovnictví patří i využívání různých platebních metod. Zatímco v kamenných obchodech platíme hotově, nebo kartou, platby na internetu nabízejí ještě několik dalších možností.

- ***Platba kartou přes internet*** (plastovou, nebo virtuální). Platební metoda spočívá v opsání čísla karty, její datum expirace (datum platnosti karty) a bezpečnostní kód, který je uveden na opačné straně karty. Jako bezpečnostní prvek platební metody kartou je využívána zaslaná SMS k přístupu na stránky banky, která kartu vydala.
- ***Platební brána (PayPa***l). Tato metoda je kombinací platby kartou a virtuální peněženkou. Ve vytvořeném PayPal účtu jsou zadány údaje platební karty a vytvořené konto s určitým množstvím finančních prostředků převedených z jiného účtu. Při platbě touto metodou je zadáván jenom email klienta, jako přihlašovací jméno a heslo. Pokud není ve virtuální peněžence dostatek finančních prostředků, provede služba úhradu z platební karty.
- ***Bankovní převod*** je další metoda internetového bankovnictví, kdy prostřednictvím jednorázového příkazu k úhradě dojde k převodu finančních prostředků na účet obchodníka. Nevýhodou této, i když oblíbené platební metody, je její zpracování pouze v úředních hodinách banky.

- ***Ostatní*** platební metody, mezi které může patřit platba online bankovním tlačítkem, mobilní platby, kupónové platby, nebo platby v bitcoinech.

V grafu jsou znázorněny oblíbené platební metody využívané k placení na internetu. Platby jsou rozděleny co do množství provedených plateb a co do objemu převáděných finančních prostředků. Údaje jsem zpracovala na základě získaných informací ze zdroje. [56]



Graf 7 Nejpoužívanější platební metody na internetu. Zdroj: vlastní

Využívání bezpečnostních nástrojů je dnes již na velmi vysoké úrovni. Zvyšováním konkurence při tvorbě internetových stránek stoupají i nároky na ně. Můžeme si všimnout, že každá banka má stránky velmi propracované. Některé jsou kvůli nadužívání designových vylepšení a nadměrnému množství textu až nepřehledné. Svým způsobem však poskytují uživatelům potřebné informace o možných hrozbách, ukazují různé návody a tipy, jak se před nimi chránit.

9 NÁVRHY A OPATŘENÍ INFORMAČNÍCH TECHNOLOGIÍ ELEKTRONICKÉHO BANKOVNICTVÍ

Elektronické bankovnictví má v současnosti v oblibě stále více lidí, a proto se na technologie elektronického bankovnictví v této kapitole zaměřím. Vymezím nové návrhy na jeho zabezpečení do budoucnosti. Nejtěžším úkolem pro banky bylo přesvědčit své klienty, aby začali elektronické bankovnictví využívat. S touto velkou výzvou se však banky dokázaly poprat a postupně si u svých klientů získaly důvěru a ukázaly jim, jaké výhody elektronické bankovnictví přináší. Proto si myslím, že budoucnost elektronického bankovnictví je velmi důležitá. Pro každého z nás je jednodušší využívat místo osobních návštěv poboček elektronické služby, které nám šetří čas.

V dnešní době jde o velký fenomén a nárůst využívání elektronických služeb je opravdu vysoký. Nicméně je zde ještě skupina lidí, kteří tyto služby nevyužívají, ale znají je od svých známých apod. Banky se proto musí nadále snažit informovat své klienty o výhodách, které elektronické bankovnictví přináší, aby tak přesvědčily i tuto skupinu lidí k využívání elektronických služeb. Tím se zvýší celkový podíl využívání elektronického bankovnictví. Pro mladé lidi je použití elektronického bankovnictví velmi jednoduché. Musíme však brát ohled i na starší generaci lidí, pro které se zdají být tyto nové služby komplikované a obtížně pochopitelné. Důvodem je to, že neměli možnost získat ve školách počítačovou gramotnost na takové úrovni, jakou disponuje v současné době mladší generace.

V předešlé kapitole jsou vymezeny bezpečnostní nástroje jednotlivých bank, které jsou využívány k autentizaci a autorizaci. Cílem této části bude tedy návrh nového modelu autentizace a autorizace. V teoretické části je zmíněna autorizace pomocí biometrických systémů, které se dnes stále více a více využívají, proto budou zakomponovány i do nového modelu. Provedenou analýzou bylo také zjištěno, že na autentizaci a autorizaci se využívá několik metod, které banky kombinují. Dnes je velkým fenoménem elektronické bankovnictví, které i samotné banky rády prosazují mezi své klienty.

Proto se zaměřím na technologie:

- Internetové bankovnictví (Internetbanking),
- Mobilní bankovnictví (Smartbanking),
- Bezkontaktní platební karty,
- Bankomaty.

9.1 Internetbanking

Pokud se chceme přihlásit do internetbankingu, je od nás požadováno, abychom zadali své přihlašovací jméno a heslo. Jak vyplývá z analýzy, každá z bank má jiný typ autentizace a autorizace. Dalším krokem je autorizace úkonů (jako platba, zadání trvalého příkazu atd.) pomocí dalšího bezpečnostního prvku. Může se jednat o SMS autorizaci. Dnes však už systém dokáže vyhodnotit riziko a posoudí, zda je třeba zadávat SMS autorizaci, nebo je přihlášení bezpečné a není třeba zadávat druhý krok. Pokud by systém vyhodnotil, že je při přihlašování možné riziko, bude vyžadovat, abyste zadali bezpečnostní kód, který Vám přijde jako SMS zpráva, případně se může jednat o použití tokenu, či autorizační kalkulačky. V případě využití autorizace SMS zprávou je třeba mít mobilní telefon.

Výhoda: výhodou tohoto způsobu je jeho dnešní masivní využívání. Pro banku to znamená snížení množství pracovníků, kteří by se starali o klienty. Stejně i bezpečnost je vysoká, pokud klient nenaletí na podvodné typy útoků, např. phishing, který byl rozebírán v teoretické části. Pro uživatele je tento způsob využití bankovních služeb velmi jednoduchý, poměrně rychlý a dnes už k němu lze využít i smartphone.

Nevýhoda: každý systém má i své nevýhody a stejně je tomu i v tomto případě. Banky čelí phishingovým útokům, kterých v současnosti neustále přibývá, a tyto útoky ohrožují uživatelské účty. Většinou jsou ohroženi starší klienti, kteří tomuto typu útoku naletí a útočníkovi poskytnou své citlivé údaje. Tito lidé se pak domnívají, že banky mají slabě zabezpečený systém a dále už internetovému bankovnictví nevěří, chyba však nastala na straně uživatele. Je nutné, aby si uživatel pamatoval své identifikační číslo, které bývá většinou příliš dlouhé, a rovněž heslo. V případě, že je nutná SMS autorizace a mobilní telefon nemá signál, není možné využívat tuto funkci.

9.1.1 Nový model systému v internetbankingu

Jak bylo zmíněno, do nového modelu budou zakomponovány biometrické systémy, které budou využívány k autentizaci. Tu by uživatelé prováděli pomocí otisku prstu, případně celé dlaně, nebo prostřednictvím naskenování obličeje, či oční duhovky. Celý systém bude fungovat velmi jednoduše. Uživatel bude při vstupu do internetového bankovnictví vyzván, aby provedl test na otisk prstu, nebo na jiný autentizační úkon. Otisk bude porovnán s otiskem, který je již v databázi, a po úspěšném porovnání bude uživatel vyzván k druhému kroku,

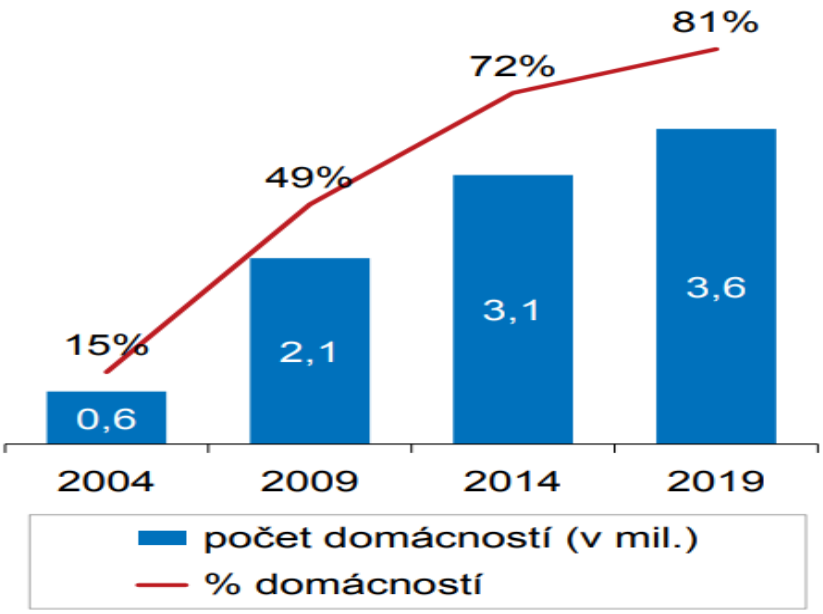
a to k zadání svého hesla. Pokud se vše bude shodovat, bude mu povolen vstup do

internetbankingu. Dvojitá ochrana s použitím biometrie je dostačující, avšak pro ještě bezpečnější přihlášení je možné využití i trojité ochrany přidáním skenování oční duhovky.

Výhoda: tento model systému je velmi bezpečný. Útočníkům by dalo velkou práci takové zabezpečení obejít. Pro uživatele by tento systém nebyl komplikovaný a obsluhovat by ho dokázali i starší lidé.

Nevýhoda: za nevýhodu se označuje nutnost vlastnit systém, který uživateli sejme otisk prstu. Banky by musely udělat vlastní databázi otisků prstů všech svých klientů, která by musela být dostatečně zajištěna proti útočníkům, kteří by usilovali o odcizení databáze, na jejímž následném prodeji by mohli vydělat nemalé finanční částky.

Pokud si banky mají udržet své klienty, musí se vydat cestou spolupráce a inovací s technologickými společnostmi a využívat nejmodernější informační technologie, které budou přispívat jak na zjednodušení komunikace s klientem, tak zvýšené bezpečnosti této komunikace. Přesto obliba internetového bankovnictví a využívání internetu k online nakupování mezi Čechy stále roste, viz graf níže. V českých domácnostech přibývá počet uživatelů využívajících počítač. Roste velká obliba využívání přenosných počítačů, tedy notebooku nebo tabletu. Přibývá více počítačové gramotnosti mezi seniory, podle zprávy českého statistického úřadu za rok 2019 *„využívá internetové bankovnictví, více než 5,5 milionu Čechů, z nichž je již 39% osob starších 65 let“*. [40]



Graf 8 Počet domácností s připojením na internet. [40]

9.2 Smartbanking

V dnešní době se ze smartbankingu stává velký hit, především pro mladší generaci lidí. Nicméně stále není užíván na takové úrovni jako bankomaty či platební karty. Nelze opomenout, že i tato služba musí být kvalitně a dostatečně zabezpečena, a co se týče autentizace a autorizace, neměly by tyto služby být příliš zdlouhavé a komplikované. Prozatím se vývojářům nepodařilo najít způsob, jak vyřešit jednoduché mobilní bankovnictví. V současnosti tento systém funguje tak, že pokud se potřebujeme přihlásit do mobilního bankovnictví, je třeba přihlašovací jméno spolu s PIN kódem. To však není vše, vzápětí na mobilní telefon přijde SMS zpráva s našim autorizačním kódem, který je třeba zadat do dvou kroků. Jedním je přihlašovací aplikace a dalším samotná autorizace k přihlášení.

Jde o velmi zdlouhavý cyklus, který by se dal vyřešit efektivnějším způsobem. Stejně jako u internetbankingu, i zde by bylo možno použít biometrické systémy jako nový modelový návrh. Zavedení biometrických systémů jako způsobu autentizace a autorizace se v dnešní době s nástupem nových smartphonů přímo nabízí.

Dnes už každý nový smartphone dokáže při dobrém nastavení vzít otisk prstu, tím majiteli zpřístupní odblokování telefonu a následně povolí přístup k jeho ovládání. Objevily se už i různé aplikace na snímání obličeje, ale větší využití získal otisk prstu. Proto je možné, že biometrické systémy budou do budoucna využity na autentizaci a autorizaci mobilního bankovnictví. Nové technologie nabízejí smartphonům široké rozhraní a zjednodušení přístupu a je zřejmé, že v budoucnosti je toto dobrá cesta k rozvoji.

Výhoda: pokud vlastníme mobilní telefon, který podporuje tento druh aplikace, velmi pomáhá, zjednodušuje a urychluje užití mobilního bankovnictví. Aplikace je rychlá, nezasekává se a rychle si na ni dokážou zvyknout i starší lidé. V případě, že bychom ztratili mobilní telefon nebo by byl odcizen, pachatel tuto aplikaci nedokáže využít ve svůj prospěch, protože nezná přihlašovací jméno a heslo uživatele. Další výhodou je, že za aplikaci nemusíme platit. Uživateli je zpřístupněna zdarma, pouze je třeba mít telefon, který tuto aplikaci podporuje. Stačí, když máme v telefonu aktivní internet, a dokážeme se na mobilní bankovnictví připojit z kteréhokoliv místa na Zemi.

Nevýhoda: hlavní nevýhodou je nutnost vlastnit smartphone. Pokud vlastníme obyčejné mobilní telefony, které nepodporují tuto aplikaci, nemůžeme využívat mobilní bankovnictví. Pro mladou generaci je dnes vlastnictví smartphonů samozřejmostí,

horší je to u starší generace lidí, kteří jsou zvyklí na obyčejné mobilní telefony. Další nevýhodou jsou i dlouhé přihlašovací údaje, které jsou hůře zapamatovatelné.

9.2.1 Nový model systému v smartbankingu

S nástupem nových technologií přicházejí i nové možnosti – dnes již existují smartphony, které dokáží pomocí snímání otisku prstu odblokovat telefon. Proto jako nový návrh jsou využity biometrické systémy do nových aplikací v smartbankingu. Jedná se o snímání otisku prstu a následného zadání PIN kódu. Systém by pracoval na dvojité ochraně. Bylo by to velmi pohodlné a rychlé a nevyžadovalo by to žádné přihlašovací údaje. Nemuseli bychom dostávat zbytečné SMS zprávy s autorizačním kódem. Po spuštění aplikace do smartbankingu bude od uživatele vyžadován otisk prstu spolu s PIN kódem pro správné přihlášení. Aplikace porovná otisk s databází, a pokud se bude shodovat, uživateli se zpřístupní cesta k jeho účtu.

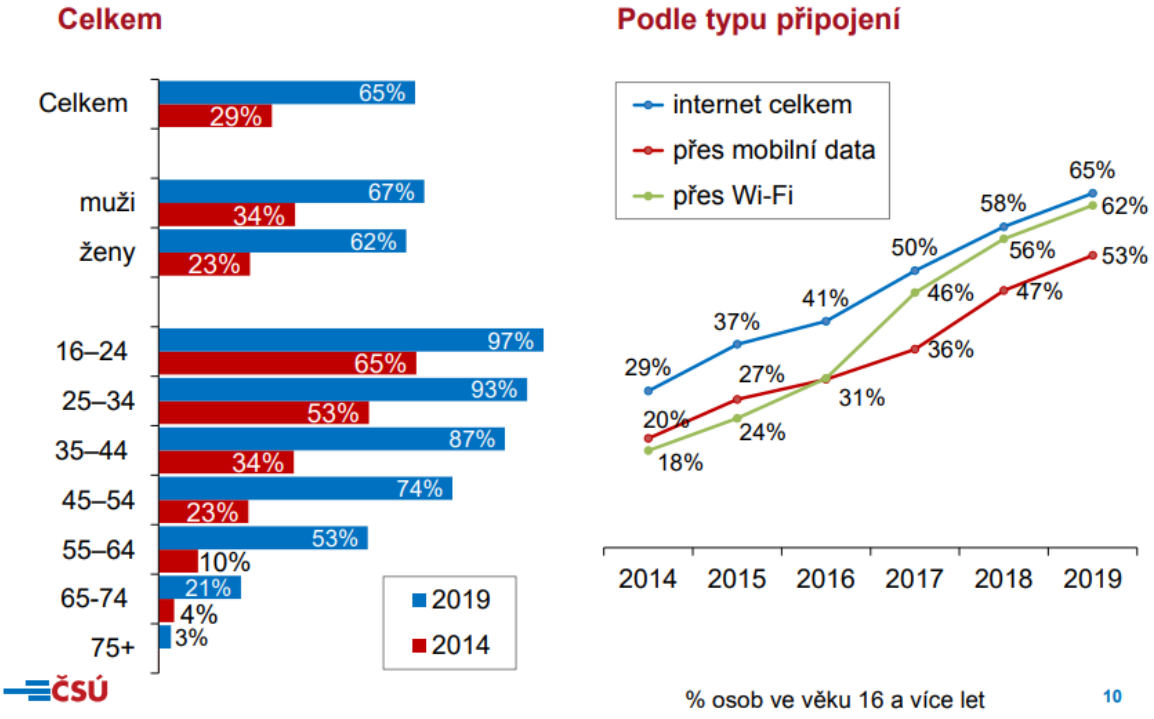
Pokud by se otisk nepodařilo identifikovat a třikrát by se tento cyklus opakoval nesprávně, uživateli by se účet uzamkl. Jako doporučení je před vstupem do aplikace vloženo výstražné okno, které by oznamovalo uživateli, zda má nainstalovanou antivirovou aplikaci na zachycování škodlivých virů. Takto by byl ochráněn mobilní telefon před různými hrozbami, zahrnujícími i možné sledování otisku prstu a hesla.

Výhoda: mezi výhody se řadí vysoká bezpečnost mobilního bankovnictví. Jednalo by se o rychlou autentizaci a autorizaci a tento způsob by si lidé i banky rychle oblíbili. Výhodou je i to, že není třeba si pamatovat zbytečně dlouhé přihlašovací údaje.

Nevýhoda: velká nevýhoda tohoto systému je nutnost vlastnit mobilní telefon podporující tuto aplikaci. Telefon by v sobě musel také obsahovat funkci otisku prstu. Další nevýhodou je potřeba vytvořit novou aplikaci, která by v sobě měla databázi otisků prstů uživatelů. Pro některé lidi to může být nepříjemné, aby své otisky někomu zveřejňovali, ale jsou k tomuto kroku potřebné.

Na grafu je znázorněn průzkum Českého statistického úřadu, který se týká statistiky, kolik lidí využívá internet na mobilním telefonu. Průzkum je vytvořen za období 2014 – 2019 a podle celkového hodnocení se jedná o nárůst o více jak o polovinu. V případě věkových

kategorií jsou na tom hůř senioři starší 65 a více let. Nejsilnější věková skupina využívání internetu na mobilním telefonu je 16 – 44 let.



Graf 9 Využívání internetu na mobilním telefonu [40]

9.3 Bezkontaktní platební karty

Velkým přínosem jsou dnes bezkontaktní platební karty. Lidé si je rychle oblíbili, protože jejich použití je velmi jednoduché. Uživatel při platbě jednoduše položí kartu na terminál a po pípnutí je vše hotovo. Bezkontaktní platby lze použít u částky, která nepřesáhne 500,- Kč. Co se týče bezpečnosti, zařazuje se tato služba do průměru.

Výhoda: rychlost a jednoduchost používání. Při platbě do 500,- Kč není třeba si pamatovat PIN kód. Není nutné kartu vsouvat do terminálu nebo ji podávat obsluze, která by ji vložila do terminálu.

Nevýhoda: v současnosti ještě existují obchody, které nenabízejí možnost používání bezkontaktních karet. Obrovskou nevýhodou je ochrana karty, kdy v případě ztráty karty může nálezce kartu využít k platbě, dokud nebude zablokována. To nastává až při nahlášení ztráty a do té doby pomocí ní mohou být prováděny neoprávněné platby. Protože není třeba znát PIN kód, pachateli to zjednodušuje zneužití karty.

9.3.1 Nový model systému pro bezkontaktní platební karty

Celý systém bude fungovat na stejné úrovni jako v současnosti, ale místo zadávání PIN kódu bych navrhovala skenování otisku prstu. Po přiložení bezkontaktní karty k terminálu bude v případě nadlimitní platby vyžadován otisk prstu. Ten se porovná s databází, systém provede srovnání a v případě shody bude platba realizována.

Výhoda: jednoduchost, větší bezpečnost. Uživateli odpadne starost – nemusí si pamatovat svůj PIN kód pro provedení nadlimitní platby. Kartu může využívat pouze osoba, která vlastní tuto platební kartu.

Nevýhoda: finanční náklady spojené s instalací zařízení na otisk prstu.

9.4 Bankomaty

Každý z nás jistě dobře zná zařízení nazývaná bankomaty. Nacházejí se v každém městě a poskytují lidem rychlé vydání peněz z bankovního účtu. Nemusíme u sebe nosit velké množství finanční hotovosti, v případě potřeby zajdeme k bankomatu a vybereme si určitou částku. Banky se snaží stále rozšiřovat síť svých bankomatů, aby umožnily svým klientů co nejširší dostupnost ke své hotovosti. V minulosti, ale i dnes, se však vyskytují případy, kdy byly tyto bankomaty vyloupeny. Využívají se techniky jako je skimming, nebo je pachatelé jednoduše fyzicky zničí. Jejich ochrana musí být dnes co nejvyšší, aby se předešlo možným hrozbám. Bankomaty a jejich autorizace fungují na dvojitém zabezpečení. Jedná se o bankomatovou kartu platnou na určité období, kterou vydává samotná banka do rukou svého klienta, a příslušný PIN kód.

Pro správné použití této služby je nutné, aby uživatel vložil svou bankomatovou kartu do bankomatu, následně je vyzván, aby zadal svůj PIN kód. Po úspěšném ověření může využívat svůj účet. Klient si však musí dávat pozor, aby bankomatovou kartu neztratil, a také aby jej nesledovala jiná osoba (skimming) za účelem zjištění PIN kódu při jeho zadávání. V blízkosti bankomatu se mohou nacházet nainstalované skryté kamery pro zjišťování PIN kódů apod. Konstrukce bankomatů je na dobré úrovni, ale pokud se jedná o autorizaci a autentizaci, je možné vidět jisté mezery.

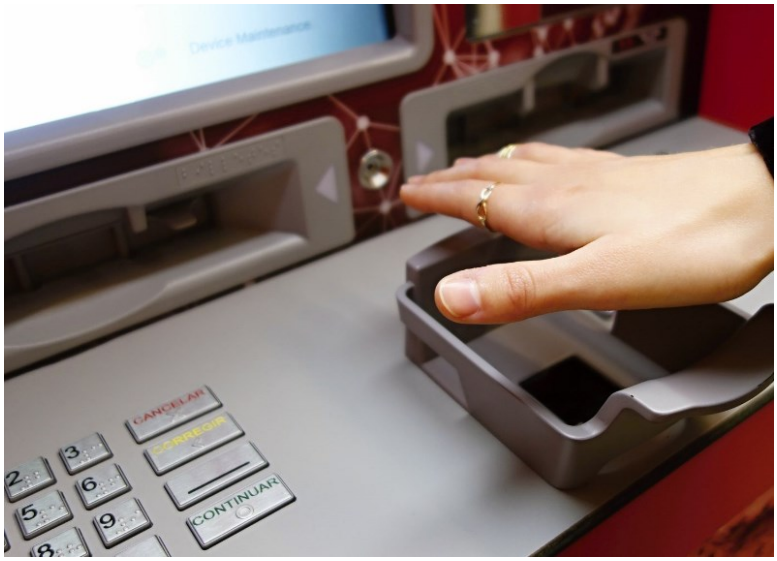
Výhoda: rozmístění bankomatů je dnes už na vysoké početní úrovni, proto v případě potřeby vybrání peněz nemusíme jezdit daleko do větších měst. Jedná se o rychlý a jednoduchý

systém. Menší poplatky za výběr z bankomatu než u samotné banky. Stejně i výběr v případě, pokud se nacházíte v zahraničí.

Nevýhoda: velkou nevýhodou těchto bankomatů je atraktivita pro útočníky, kteří vidí snadnou cestu k získání peněz. Pro banky to znamená velké ztráty ať už z finančního hlediska nebo v podobě odchodu zákazníků. Další nevýhodou je nutnost správy bankomatů – jejich provoz, poškození, opravy. Dalším úkonem navíc je, pokud si chce uživatel vybrat peníze, musí mít u sebe platební kartu. Bez ní se ke svému účtu nedostane. Stejně je to i s množstvím vlastněných platebních karet, bankomatových karet a jejich různých přístupových PIN kódů, které se z hlediska bezpečnosti od sebe liší.

9.4.1 Nový model systému bankomatů

V tomto novém návrhu bych opět chtěla doporučit a využít biometrické systémy, kde je použito na autorizaci a autentizaci skenování oční duhovky nebo klasický otisk prstu, případně rozpoznání uživatele podle krevního řečiště dlaně. Celý systém bude fungovat na dvojité ochraně. Rovněž se využívá i dnes a splňuje své požadavky. Na bankomatu bude nainstalováno zařízení, které bude sloužit ke skenování krevního řečiště dlaně, viz Obrázek 15.



Obrázek 15 Bankomat s biometrickým zabezpečením. [55]

Bankomatový systém bude v sobě obsahovat databázi, kde se budou nacházet jednotlivé naskenované uživatelské parametry. Tuto databázi bude potřeba velmi dobře zajistit, např.

využitím šifrovací metody, pro případ, že by se k těmto citlivým údajům dostal útočník, aby neměl možnost je zneužít.

Celý systém bude fungovat na základě bezpečných metod biometrické autentizace. Následně po úspěšném biometrickém ověření osoby, systém potvrdí shodu a uživatel bude vyzván, aby provedl druhý stupeň ochrany, a to zadání svého PIN kódu. Pokud splní i tento požadavek, bude mu zpřístupněn jeho účet a může začít volit příslušné funkce prostřednictvím bankomatu. Využitím některé výše jmenované biometrické metody autentizace, by přihlášení přes bankomat bylo pro uživatele jednodušší a pohodlnější. Uživatel bude mít tři možné pokusy pro zadání správného PIN kódu. Pokud by došlo k opakování nesprávného PIN kódu, systém vyhodnotí riziko a přístup zablokuje.

Bankomaty by byly pro všechny banky stejné. Změna by byla jen v systému, kdy by uživatel na začátku vybral z možností, kterou banku chce využít. Takto by se zabránilo možnému chaosu databází, aby systém věděl, kterou z nich má v daném okamžiku na srovnání využít.

Výhoda: velkou výhodou pro uživatele by bylo to, že by odpadla nutnost využívat bankomatové karty, a tak by zmizel strach z jejich ztráty nebo odcizení. Bankomaty by se sjednotily a postupně by mohlo dojít i ke snížení jejich počtu, přičemž uživatel by si mohl peníze vybírat kdekoliv. V podstatě je toto možné i dnes, ale pokud klient využije jiný bankomat, než náleží jeho bance, bude mu započítán poplatek z výběru. Další výhodou je samozřejmě zvýšení bezpečnosti proti neoprávněným vstupům. Stejně tak by banky nemusely řešit každoroční vydávání nových bankomatových karet a náklady na ně by mohly využít do zavedení nových systémů.

Nevýhoda: pro banky by to byl nárůst finančních prostředků na zavedení nových systémů do všech bankomatů. Následně by banky musely vytvořit databázi skenování očních duhovek, otisku prstu apod. Nastává zde také možnost neochoty využívat tuto službu ze strany uživatele. Uživateli může být nepříjemné skenování oční duhovky, ale pokud se jedná o bezpečnost, měl by udělat výjimku.

9.5 Shrnutí všech typů informačních technologií

Nové modely byly postaveny na biometrických systémech, konkrétně skenování otisků prstu, krevního řečiště a skenování oční duhovky, které by byly využívány ve všech typech autentizace a autorizace. Mají své výhody, ale i nevýhody, s nimiž je třeba počítat. Tyto systémy by poskytovaly vysokou ochranu, došlo by ke zvýšení bezpečnosti a zjednodušení využívání všech typů služeb. Pokud by systémy využívaly jen jednu ochranu, např. kdyby šlo jen o skenování a srovnání otisku bez zadání hesla, PIN kódu, bezpečnost by byla podprůměrná. Získat otisk prstu by bylo velmi jednoduché, např. ze sklenice. Útočník by si udělal odlitek ve vosku a takto by ho mohl zneužít.

Pokud jde např. o využívání skenování oční duhovky, může být toto pro uživatele nepříjemné, proto by určitou dobu trvalo, než by si lidé na takový systém zvykli. Pro bankovnictví by nové systémy přinesly novou ochranu, ale na vývoj a realizaci by musely být poskytnuty nemalé finanční prostředky. Současné technologie a jejich vývoj jsou na vysoké úrovni, a pokud si vezmeme, že nové smartphony už v sobě obsahují funkci na snímání otisku prstu, tak ve smartbankingu, ale i v jiných typech služeb, by to byl dobrý krok vpřed.

V této podkapitole se chci dále zamyslet nad možným budoucím vývojem a rozvojem v oblasti bezpečnosti v internetovém bankovnictví. Trendem budoucnosti je využívání biometrické identifikace osob, tedy rozpoznávání obličeje (sítnice), hlasu a otisků prstů. V dnešní době je více než jisté, že každý člověk preferuje rychlost, přehlednost, jednoduchost a hlavně bezpečnost bankovních aplikací. Zadávat heslo při každém přihlášení do bankovní aplikace v mobilním telefonu nebo v jiném zařízení lidi jen zdržuje. Přesto to všichni dělají, protože nechtějí, aby se k citlivým datům dostal i někdo jiný.

Se vzrůstajícím počtem elektronických služeb je neustálé vyplňování údajů náročné, a to z hlediska času i paměti. Různé průzkumy také ukázaly, že až 50 % respondentů, kteří využívají bankovní aplikace, má své přihlašovací údaje zapsané buď někde na papíře, nebo přímo ve svém zařízení. Zde však hrozí, že se k údajům snadno dostane i další osoba. Právě díky těmto zjištěním bych ráda navrhla bezpečnostní funkci, která by nahradila hesla do jednotlivých bankovních aplikací. Jde o metodu, kterou by mohli využívat všichni majitelé smartphonů. Inspiraci mi poskytnul mobilní telefon iPhone 5s od Apple, který představil jako první funkci Touch ID. Jde o metodu využití snímače otisku prstu pro odemknutí zařízení. Jde o senzor zabudovaný v zařízení, který snímá otisk prstu. Otisk je přímo uložen

v hardwaru telefonu a není tak distribuován mimo zařízení. Jde o jedinečný údaj, který si každý z nás přináší na tento svět. Od 4. měsíce po narození se otisky jedince nemění.

Samozřejmě, že i při těchto technologiích mohou vzniknout různé otázky a možnosti, jak je překonat, ale zatím jde o to nejbezpečnější a nejpřirozenější řešení, jak uchránit naše peníze. Využití biometrických funkcí by se mělo podle mého stát základem jednoduchého, efektivního a bezpečného bankingu v 21. století, a to nejen v oblasti internet bankingu, ale i v osobním styku s bankou.

V budoucnu je možné, že otisky prstů nebudou využívány pouze v počítačích a telefonech, ale i v bankomatech či terminálech po celém světě. Předělání klasických bankomatů, které jsou používány v dnešní době, na ty se snímačem biometrických údajů, bude určitě velkým přínosem pro spokojeného klienta.

V některých obchodních sítích v USA je běžnou realitou, že zákazníci s sebou nemusí nosit žádnou hotovost ani platební kartu a stačí, když přiloží svůj prst na displej terminálového zařízení. Zákazník musí být však předem zaregistrován a po identifikaci z otisku se zobrazí na displeji platební karty, které vlastní, a sám si může zvolit tu, s níž zaplatí. Klientovi to ušetří čas u pokladny a navíc s sebou nemusí nosit žádné karty. Obchodníci tento způsob placení také ocení, a to proto, že nemusí následně platit poplatky bankovním firmám.

ZÁVĚR

Nástup nových informačních technologií lidem zjednodušuje život a šetří čas. Avšak je třeba brát také v úvahu, že s nimi přicházejí i rizika, na která nesmíme zapomínat. Elektronické bankovnictví je forma, díky níž komunikuje banka a klient, aniž by se museli osobně setkat. Komunikace probíhá ve virtuální formě, proto musíme dbát na to, aby byla dostatečně zajištěna její bezpečnost.

Práce se zabývala druhy informačních technologií zaměřených na bankovní sektor. Mezi velkou internetovou hrozbu se řadí sociální inženýrství, které se do povědomí lidí dostává v malé míře. Hlavními podvodnými technikami, které útočníci v současnosti využívají, jsou phishing, pharming, spying, skimming, vishing, tabnabbing apod. Proto byly rozebrány tyto typy útoků, a jakou techniku útočníci praktikují. V současnosti je elektronické bankovnictví velmi využíváno, proto je třeba mít alespoň minimální znalosti o těchto technikách.

Byla popsána technologická opatření bezpečnosti, která by měla banka splňovat a dodržovat. Tímto, banka zajistí nejvyšší úroveň ochrany před možnými útoky. V praktické části byla zpracována analýza bezpečnosti vybraných bank. Popisuje vzhled a dostupnost bezpečnostních informací, ke kterým má klient možnost přístupu. Patří sem autentizační a autorizační nástroje a dále způsoby šifrování, které banky využívají. Autentizace a autorizace byla zaměřena na internetové bankovnictví, smartbanking, bezkontaktní platební karty a bankomaty. Byly popsány současné autorizace, jejich výhody a nevýhody, a následně byly vytvořeny nové návrhy pro bezpečnostní autorizaci a autentizaci, které využívají biometrické systémy. Většinou by se jednalo o otisk prstu, který je pro všechny typy velmi výhodný, ale např. u bankomatů by mohlo být využito i skenování oční duhovky. I u těchto nových návrhů byly popsány jejich výhody a nevýhody, a to na straně banky i klienta.

Předpokládá se, že těchto typů útoků bude neustále přibývat, a banky by měly celé problematice věnovat dostatečnou pozornost. I přes úsilí ze strany bank, které se snaží o silné zabezpečení nelze každé hrozbě zabránit, jelikož nejslabším článkem celého zabezpečení je samotný klient.

SEZNAM POUŽITÉ LITERATURY

[1] TVRDÍKOVÁ, Milena. *Aplikace moderních informačních technologií v řízení firmy: Nástroje ke zvyšování kvality informačních systémů*. Praha: Grada, 2008. ISBN 978-80-247-6298-2.

[2] KOKLES, Mojmír a Anita ROMANOVÁ. *Informatika*. Druhé vyd. Bratislava: Sprint 2, 2018. ISBN 978-80-89710-40-9.

[3] GÁLA, Libor, Jan POUR a Zuzana ŠEDIVÁ. *Podniková informatika: Počítačové aplikace v podnikové a mezipodnikové praxi*. 3. akt. vyd. Praha: Grada, 2015. ISBN 978-80-247-5457-4.

[4] 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

[5] POŽÁR, Josef. Informační bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. s. 75 Vysokoškolské učebnice. ISBN 8086898385

[6] SEKERA, Tomas. Řízení bezpečnosti (Security Management). *ManagementMania.com* [online]. Wilmington (DE), 2011-2020 [cit. 2020-02-12]. Dostupné z: https://managementmania.com/cs/rizeni-bezpecnosti

[7] LUBOŠ, Dobda. *Ochrana dat v informačních systémech*. Praha: Grada Publishing 288 s, 1998. ISBN 80-7169-479-7.

[8] Informační technologie v bankovním sektoru. *: Příležitosti, hrozby a strategie.* [online]. Postgraduální škola podnikání a managementu, Americká univerzita, 1998 [cit. 2020-02-12]. Dostupné z: https://almashriq.hiof.no/ddc/projects/business/it-banking.html

[9] KRHOVJÁK, Jan a Václav MATYÁŠ. Autentizace a identifikace uživatelů. *ÚVT MU* [online]. Brno: MUNI ISSN 1212-0901, 2007 [cit. 2020-02-12]. Dostupné z: http://webserver.ics.muni.cz/zpravodaj/articles/560.html

[10] Autentizace a autorizace. *TRISUL s.r.o.* [online]. Brno: 2005_2020 [cit. 2020-02-12]. Dostupné z: http://www.trisul.cz/bezpecnost-autentizace-autorizace/

[11] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 4. aktualizované vyd. Praha: Grada, 2013. ISBN 978-80-247-4644-9. Dostupné z: https://www.govcert.cz/download/kii-vis/2019_01_04_metodika_k_varov%C3%A1n%C3%AD_z_17-12-2018_v1.0.pdf

[12] ONDÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4. Dostupné z: https://www.govcert.cz/download/kii-vis/2019_01_04_metodika_k_varov%C3%A1n%C3%AD_z_17-12-2018_v1.0.pdf

[13] Elektronický podpis. *Sandbox.cz* [online]. [cit. 2020-02-16]. Dostupné z: http://sandbox.cz/~varvara/El_podpis/index.html

[14] NYKODÝMOVÁ, Helena. Jak je to s bezpečností internetového bankovnictví? *LUPA.cz* [online]. 2006 [cit. 2020-02-16]. Dostupné z: https://www.lupa.cz/clanky/jak-je-to-s-bezpecnosti-internetoveho-bankovnictvi/

[15] ANTOŠ, Ondřej. Představuje přímé bankovnictví riziko pro vaše peníze?: Zabezpečení přenosu dat a identifikace banky. *Měšec.cz* [online]. 2005 [cit. 2020-06-22]. Dostupné z: https://www.mesec.cz/clanky/rizikove-prime-bankovnictvi/

[16] BOUŠOVÁ, Kateřina. *Peníze.cz* [online]. 2006 [cit. 2020-02-16]. Dostupné z: https://www.penize.cz/bezne-ucty/18366-internetove-bankovnictvi-jsou-vase-penize-v-bezpeci ISSN 1213-2217

[17] Vyšší typy zabezpečení. *Bezpečný internet.cz* [online]. [cit. 2020-02-17]. Dostupné z: http://www.bezpecnyinternet.cz/pokrocily/internetove-bankovnictvi/vyssi-typy-zabezpeceni.aspx

[18] Pravidla bezpečného užívání Internet Banky. In: *GE Money Bank* [online]. Praha [cit. 2020-02-17]. Dostupné z: https://legacy.moneta.cz/documents/cz/primebankovnictvi/pravidla-bezpecneho-uzivani-ib.pdf

[19] PROTIVINSKÝ, Miroslav. Bankovní loupeže. Praha: Armex, 2001. ISBN 80-862-4421-0.

[20] Phishing. Wikipedia [online]. 2006 [cit. 2020-02-17]. Dostupné z: https://cs.wikipedia.org/wiki/Phishing#/media/Soubor:Jak_snadno_poznat_phishing.png

[21] PAGANINI, Pierluigi. Techniky sociálního inženýrství. *Security Affairs* [online]. 2013 [cit. 2020-02-25]. Dostupné z: http://securityaffairs.co/wordpress/18883/cybercrime/complex-fishing-poste-italiane.html

[22] Pharming. *IT Slovník.cz* [online]. [cit. 2020-02-25]. Dostupné z: https://it-slovnik.cz/pojem/pharming

[23] GRACE, Alison. Co je pharming a jak se chránit. *Norton* [online]. [cit. 2020-02-25]. Dostupné z: https://us.norton.com/internetsecurity-online-scams-what-is-pharming.html

[24] Vishing. *FraudWatch International* [online]. 2019 [cit. 2020-02-25]. Dostupné z: https://fraudwatchinternational.com/vishing/what-is-vishing/

[25] Skimming. *PC REVUE* [online]. 2015 [cit. 2020-02-25]. Dostupné z: https://www.pcrevue.sk/a/Skimming-platobnej-karty-este-skor--ako-ju-vlozite-do-bankomatu

[26] Spyware. *PCMag.com* [online]. [cit. 2020-02-25]. Dostupné z: http://www.pcmag.com/encyclopedia/term/51898/spyware

[27] MALÝ, Martin. TabNabbing krade přihlašovací údaje nepozorným: Jak vypadá TabNabbing. *ROOT.CZ* [online]. 2010 [cit. 2020-06-23]. Dostupné z: https://www.root.cz/clanky/tabnabbing-krade-prihlasovaci-udaje-nepozornym/

[28] HAMŘÍK, Antonín a Jan BRÁZDIL. Banky a bezpečnostní trendy IT. *Bankovní poplatky* [online]. Copyright (2010) ČTK a The Associated Press (AP), 2008 [cit. 2020-02-26]. Dostupné z: https://www.bankovnipoplatky.cz/clanky/reportaz/banky-a-bezpecnostni-trendy-it-4731.html

[29] BRUCKNER, Tomáš a Jiří VOŘÍŠEK. *Outsourcing informačních systémů*. Praha: EKOPRESS, 1998. ISBN 80-86119-07-6.

[30] KANDLEROVÁ, Kateřina. Outsourcing a jeho využití v praxi. *Portál.POHODA.cz* [online]. 2014 [cit. 2020-02-28]. Dostupné z: https://portal.pohoda.cz/pro-podnikatele/uz-podnikam/outsourcing-a-jeho-vyuziti-v-praxi/

[31] DVOŘÁČEK, Jiří a Ladislav TYLL. *Outsourcing a offshoring podnikatelských činností*. Praha: C. H. Beck, 2010. ISBN 978-80-7400-010-2.

[32] MILECOVÁ, Miroslava, Miroslav GRZNÁR a Ľuboslav SZABO. Outsourcing: rozhodovanie o vyčlenení podnikovej aktivity a riadenie outsourcingového projektu. *AGRIC* [online]. AGRIC. ECON. -CZECH, 2010 [cit. 2020-02-26]. Dostupné z: https://www.agriculturejournals.cz/publicFiles/87_2010-AGRICECON.pdf

[33] MAISNER, Martin a Jiří ČERNÝ. *Právní aspekty outsourcingu*. Praha: Wolters Kluwer, 2012. ISBN 978-80-7357-746-9.

[34] MIKUŠOVÁ-MERIČKOVÁ, Beáta a Petr FANTA. *Optimalizace outsourcingu ve veřejném sektoru*. Praha: Wolters Kluwer, 2012. ISBN 978-80-7357-990-6.

[35] ŘEZÁČ, Jaromír. *Moderní management: Manažer pro 21. století*. Brno: Computer Press, 2009. ISBN 978-80-251-1959-4.

[36] RYDVALOVÁ, Petra a Jiří RYDVAL. *Outsourcing ve firmě*. Brno: Computer Press, 2007. ISBN 978-80- 251-1807-8.

[37] ZAHRADNÍK, Jaroslav. Finanční dopady outsourcování služeb v průmyslovém podniku. *MMspektrum* [online]. Praha: MM publishing, 2004 [cit. 2020-03-01]. Dostupné z: https://www.mmspektrum.com/clanek/financni-dopady-outsourcovani-sluzeb-v-prumyslovem-podniku.html

[38] MERVART, Petr. S přehledem ve světě informačních technologií. Cesty k outsourcingu Petr Mervart.: IT SYSTEM 4/2004. *SystemOnLine* [online]. Praha, 2004 [cit. 2020-03-01]. Dostupné z: https://www.systemonline.cz/clanky/cesty-k-outsourcingu.htm, ISSN 1802-615X

[39] FANTA, Petr. *Outsourcing*. Praha, 2004. Autoreferát k doktorské disertační práci. Vysoká škola ekonomická v Praze, Fakulta podnikohospodářská. Vedoucí práce Prof. Ing. Eva Kislingerová, CSc., Dostupné z: https://webhosting.vse.cz/ekisl/prace/Fanta.pdf

[40] MANA, Martin a Lenka WEICHETOVÁ. Internetové bankovnictví: Tisková zpráva. *Český statistický úřad* [online]. Praha: ČESKÝ STATISTICKÝ ÚŘAD, 2019 [cit. 2020-03-19]. Dostupné z: https://www.czso.cz/csu/czso/internetove-bankovnictvi-vyuziva-55-milionu-cechu

[41] HORÁK, Filip a Kristýna TUPÁ. Outsourcing ve finančních službách-nově a přísněji. *Daňové a právní aktuality* [online]. 2019 [cit. 2020-03-02]. Dostupné z: https://danovky.cz/cs/outsourcing-ve-financnich-sluzbach-nove-a-prisneji

[42] PAVELKA, František. Outsourcing – nástroj zvýšení konkurenceschopnosti Českých bank. In: PALÁN, Josef F. *Socioekonomické a humanitní studie 2/2011*. 2011. ISSN 1804-6797. Dostupné z: http://sehs.educast.cz/subdom/sehs/wp-content/uploads/2017/09/2-2011.pdf

[43] DOUPAL, František. Česko je nejoblíbenější destinací pro outsourcing IT služeb mezi zeměmi střední a východní Evropy. *Reseller Magazine OnLine: Web o businessu v informačních technologiích* [online]. Praha: DCD Publishing, 2018 [cit. 2020-03-03]. Dostupné z: https://www.rmol.cz/novinky/cesko-je-nejoblibenejsi-destinaci-pro-outsourcing-it-sluzeb-mezi-zememi-stredni-vychodni

[44] MojeBanka login. *Komerční banka* [online]. 2020 [cit. 2020-03-05]. Dostupné z: https://login.kb.cz/login?sso=MB

[45] SSL Report: login.kb.cz: Certificate: RSA 2048 bits (SHA256withRSA). *Qualys SSL Labs* [online]. 2020 [cit. 2020-03-11]. Dostupné z: https://www.ssllabs.com/ssltest/analyze.html?d=login.kb.cz&s=194.50.226.52&latest

[46] Servis 24. *Česká spořitelna* [online]. Česká spořitelna, 2020 [cit. 2020-03-05]. Dostupné z: https://www.servis24.cz/ebanking-s24/ib/base/usr/aut/login?execution=e1s1

[47] SSL Report: www.servis24.cz: Certificate: RSA 2048 bits (SHA256withRSA). *Qualys SSL Labs* [online]. 2020 [cit. 2020-03-11]. Dostupné z: https://www.ssllabs.com/ssltest/analyze.html?d=www.servis24.cz

[48] Přihlášení do Vaší Internet Banky. *ČSOB* [online]. 2020 [cit. 2020-03-11]. Dostupné z: https://ib.csob.cz/prihlaseni

[49] SSL Report: ib.csob.cz: Certificate: RSA 2048 bits (SHA256withRSA). *Qualys SSL Labs* [online]. 2020 [cit. 2020-03-11]. Dostupné z: https://www.ssllabs.com/ssltest/analyze.html?d=ib.csob.cz

[50] Přihlášení do Vaší Internet Banky. *AirBank* [online]. 2020 [cit. 2020-03-11]. Dostupné z: https://ib.airbank.cz/

[51] SSL Report: www.airbank.cz: Certificate: RSA 2048 bits (SHA256withRSA). *Qualys SSL Labs* [online]. 2020 [cit. 2020-03-11]. Dostupné z: https://www.ssllabs.com/ssltest/analyze.html?d=www.airbank.cz

[52] Přihlášení do Vaší Internet Banky. *MONETA Money Bank* [online]. 2020 [cit. 2020-03-11]. Dostupné z: https://ibs.internetbanka.cz/ibs/ControllerServlet

[53] SSL Report: ibs.internetbanka.cz: Certificate: RSA 2048 bits (SHA256withRSA). *Qualys SSL Labs* [online]. 2020 [cit. 2020-03-11]. Dostupné z: https://www.ssllabs.com/ssltest/analyze.html?d=ibs.internetbanka.cz

[54] Hashovací funkce: Elektronické studijní materiály. *Mendelova univerzita v Brně* [online]. [cit. 2020-03-11]. Dostupné z: https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=7029

[55] NÝVLT, Václav. Nový bankomat vydá peníze i bez karty a PIN. *IDNES.cz* [online]. 2016 [cit. 2020-04-04]. Dostupné z: https://www.idnes.cz/technet/technika/bankomat-biometricky-senzor.A161120_104301_tec_technika_nyv

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AES	Advanced Encryption Standard, symetrická šifra dat v informatice
ČS	Česká spořitelna
ČSOB	Československá obchodní banka
DES	Data Encryption Standard – symetrický šifrovací algoritmus (starší verze)
DNS	Domain Name Systém protokol, který zajišťuje překlad názvů domén webových stránek
EBA	Evropský orgán pro bankovnictví
HTTP	HyperText Transfer Protocol internetový protokol, původně určený k výměně hypertextových dokumentů mezi serverem a prohlížečem
IDEA	Symetrická šifra, nazývaná konvenční, je takový šifrovací algoritmus, který používá k šifrování i dešifrování jediný klíč
IDS	Intrusion Detection Systems – systémy pro detekci útoků
IP	Internet Protocol - adresa, která slouží jako primární identifikátor každého počítače, který je připojen v počítačové síti
IS	Informační systém
IT	Informační technologie
KB	Komerční banka
PayPal	Platební brána
PIN	Personal identification number, což znamená osobní identifikační číslo
RC4	V informatice název kryptografického algoritmu
RSA	Iniciály autorů Rivest, Shamir, Adleman, asymetrická šifra, která je založena na Eulerově větě, a která je použitelná jak pro šifrování, tak pro podepisování dokumentů.
SHA	Secure Hash Algorithm, název pro rodinu rozšířených kryptografických hašovacích algoritmům

SLA	Service Level Agreement, dohoda o úrovni poskytovaných služeb. SLA představuje formalizovaný popis služby, kterou poskytuje dodavatel zákazníkovi.
SLD	Service Level Description, popis úrovně služby (SLD) pro fyzickou informační technologickou podporu
SMS	Short message service je název pro službu dostupnou na většině digitálních mobilních telefonů, zprávu lze posílat mezi mobilními telefony, jinými zařízeními, na pevné telefony nebo přes internet
SSL	Secure Sockets Layer, je protokol, který mezi vrstvu transportní (TCP/IP) a vsrtvu aplikační (HTTPS) vloží další vrstvu, která poskytuje zabezpečení komunikace šifrováním a umožní autentizaci
TCP	Transmission Control Protocol, je nejpoužívanějším protokolem transportní vrstvy v sadě protokolů TCP/IP používaných v síti Internet, použitím TCP mohou aplikace na počítačích propojených do sítě vytvořit mezi sebou spojení, přes které mohou obousměrně přenášet data.
TLS	Transport Layer Security, kryptografický protokol, který je nástupcem protokolu SSL
URL	(Uniform Resource Locator) je soubor znaků, který slouží k identifikaci přesného umístění informací na internetu. URL definuje doménovou adresu serveru, umístění zdroje na server a protokol.
VoIP	Voice over Internet Protocol, služba, která využívá pro volání prostředí internetu

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM GRAFŮ