Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Zabezpečení webových aplikací bankovních institucí

Jaroslav Tesař

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jaroslav Tesař

Informatika

Název práce

Zabezpečení webových aplikací bankovních institucí

Název anglicky

Web Application Security of Banking Institutions

Cíle práce

Cílem práce je analyzovat jednotlivé internetové aplikace českých bankovních institucí, provést komparaci z hlediska použitých protokolů a odolnosti proti různým typům webových útoků a vyvodit závěry o jejich bezpečnosti.

Metodika

Teoretické části práce bude dosaženo prostřednictvím analýzy a syntézy vědeckých a odborných zdrojů a komparace případových studií, které jsou zaměřeny na typy internetových protokolů a typy útoků.

Praktická část bude realizována srovnáním ochrany webových aplikací českých bankovních institucí. Srovnání bude založeno na použitých protokolech, které jsou na těchto stránkách používány a dalších dostupných informacích o tom, proti jakým typům útoků jsou tyto stránky odolné.

Doporučený rozsah práce

30 – 40 stran

Klíčová slova

zabezpečení, internetové stránky, online prostředí, protokoly, útoky

---

Doporučené zdroje informací

KABELOVÁ, Alena a Libor DOSTÁLEK. Velký průvodce protokoly TCP/IP a systémem DNS. Brno: Computer Press, 2008. ISBN 978-80-251-2236-5.

MATEJKA, J. Internet jako objekt práva: hledání rovnováhy autonomie a soukromí. Praha: CZ.NIC, 2013. ISBN 978-80-904248-7-6.

MCCLURE, Stuart, Saumil SHAH a Shreeraj SHAH. Web Hacking: Útoky a obrana. Praha: SoftPress, c2003. ISBN 80-86497-53-4.

SATRAPA, Pavel. IPv6: internetový protokol verze 6. 3., aktualiz. a dopl. vyd. Praha: CZ.NIC, c2011. CZ.NIC. ISBN 978-80-904248-4-5.

ZEMÁNEK, Jakub. Stavba a správa sítě, aneb, Cesta do hlubin internetu. Kralice na Hané: Computer Media, 2004. ISBN 80-86686-26-4.

Předběžný termín obhajoby

2017/18 LS – PEF

Vedoucí práce

Ing. Václav Lohr, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 31. 10. 2017

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 1. 11. 2017

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 14. 12. 2017

Čestné prohlášení

Prohlašuji, že jsem svou bakalářskou práci „Zabezpečení internetových aplikací bankovních institucí“ vypracoval samostatně, pod vedením vedoucího bakalářské práce s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a jsou uvedeny v seznamu použitých zdrojů na konci práce. Jako autor výše uvedené práce také prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 15. 3. 2018 _____

Poděkování

Rád bych poděkoval touto cestou vedoucímu práce Ing. Václavu Lohrovi, Ph.D. za odborné konzultace a připomínky k mé bakalářské práci. Velké poděkování patří také mojí rodině za neustálou podporu v průběhu mého celého studia.

Zabezpečení webových aplikací bankovních institucí

Abstrakt

Cílem této bakalářské práce je analyzovat jednotlivé internetové aplikace českých bankovních institucí, provést komparaci z hlediska použitých protokolů a odolnosti proti různým typům webových útoků a vyvodit závěry o bezpečnosti těchto aplikací. Práce je zaměřena na bankovní aplikace českých bank a zabývá se protokoly těchto aplikací a jejich odolností vůči webovým útokům.

Rešeršní část práce se zabývá elektronickým bankovnictvím, jeho historií v naší zemi, jeho druhy, možnostmi zabezpečení a bezpečnostními riziky. Dále popisuje internetové protokoly, jejich druhy, vlastnosti a webové útoky, kterými mohou být webové aplikace nebo stránky napadeny.

Praktická část bude realizována srovnáním ochrany webových aplikací českých bankovních institucí. Srovnání bude založeno na použitých protokolech, které jsou na těchto stránkách používány a dalších dostupných informacích o tom, proti jakým typům útoků jsou tyto stránky odolné.

Klíčová slova: zabezpečení, internetové stránky, online prostředí, protokoly, útoky

Web application security of banking institutions

Abstract

The goal of this thesis is to analyze single web applications of czech banking institutions, to compare from the point of view used protocols and resistence to different types of web attacks and to deduce conclusions about security of these applications. Thesis is mainly focused on web applications of czech banking institutions and is concerned with protocols of these applications and resistence to web attacks.

Theoretical part of this thesis is concerned with electronic banking, its history in our country, its types, possibilities of security and safety risks. Additionally thesis describes internet protocols, its types, attributes and web attacks, which can be web applications or websites assaulted.

Practical part of this thesis will be realized by comparison of security of web applications of czech banking institutions. The comparison will be based on protocols, which are used on these websites and additional informations about, which types of web attacks are websites resistant against.

Key words: security, websites, online environment, protocols, attacks

Obsah

1. Úvod

Tato bakalářská práce se zabývá elektronickým bankovnictvím, internetovými protokoly a webovými útoky, kterými mohou být webové stránky napadány. Dále je zde obsažena komparace bezpečnosti webových aplikací českých bankovních institucí, která je založena na srovnání internetových protokolů jednotlivých stránek a jejich odolnosti proti různým typům webových útoků. Také je zde provedena analýza vybraných českých bankovních institucí. Na konci práce je toto srovnání vyhodnoceno a je zde vyvozen závěr o bezpečnosti konkrétních bankovních aplikací českých bank.

Elektronické bankovnictví vzniklo skoro před dvaceti lety, což je relativně nedávno. Už v době vzniku této služby velká řada potencionálních klientů váhala, jestli ji začnou používat. A to zejména kvůli tomu, že nevěděli, jestli jsou aplikace dobře zabezpečeny. Žádný člověk by samozřejmě nechtěl, aby se k jeho bankovnímu účtu dostal někdo cizí. Takto napadený klient může přijít o velké finanční obnosy, o svou platební kartu nebo také o přístup ke svému účtu úplně. Odcizení peněz je klasifikováno jako trestný čin, i když probíhá přes internet. Tímto způsobem se k odcizení peněz přes internet staví policie i banky samotné. Pokud klient dodrží všechna bezpečnostní pravidla, pak ručí za přístup k účtu banka. Ta má poté povinnost ztrátu uhradit, když se prokáže, že za nedovolený vstup na účet skutečně uživatel nemůže. Ve většině případů si ale klient za krádež peněz nebo přístupových údajů může sám. Stává se tak z mnoha důvodů. Člověk si dostatečně nechrání přístupové údaje k internetovému bankovnictví, má je například napsané a položené na místě, kam mají přístup i jiní lidé nebo je dokonce někomu sám sdělí. Často také lidé naletí na SMS nebo e-mail phishing. Podvodník své oběti pošle e-mail nebo textovou zprávu, kterou vytvoří tak, aby to vypadalo, že zpráva skutečně pochází z bankovní instituce klienta a požaduje přístupové údaje k účtu. Zmatený uživatel jim je pošle a neštěstí je na světě.

Informační technologie a zabezpečení internetového bankovnictví se stále vyvíjí. Banky by se měly snažit, aby jejich aplikace byly chráněny co nejlépe, aby se jejich klienti nemuseli obávat elektronické bankovnictví používat. Na první pohled by se mohlo zdát, že v každé české bance to takhle funguje a aplikace jsou dostatečně chráněné. Ve skutečnosti tomu tak někdy ale není a v zabezpečení jednotlivých bank lze nalézt určité rozdíly. Touto problematikou se bude zabývat praktická část bakalářské práce.

2. Cíl práce a metodika

2.1 Cíl práce

Cílem této bakalářské práce je analyzovat jednotlivé internetové aplikace českých bankovních institucí, provést komparaci z hlediska použitých protokolů a odolnosti proti různým typům webových útoků a vyvodit závěry o bezpečnosti těchto aplikací. Práce je zaměřena na bankovní aplikace českých bank a zabývá se protokoly těchto aplikací a jejich odolností vůči webovým útokům.

2.2 Metodika

Rešeršní část práce se zabývá elektronickým bankovnictvím, historií u nás, jeho druhy, možnostmi zabezpečení a bezpečnostními riziky. Dále popisuje internetové protokoly, jejich druhy, vlastnosti a webové útoky, kterými mohou být webové aplikace nebo stránky napadeny.

Teoretické části práce bude dosaženo prostřednictvím analýzy a syntézy vědeckých a odborných zdrojů a komparace případových studií, které jsou zaměřeny na elektronické bankovnictví, typy internetových protokolů a typy útoků.

Praktická část bude realizována srovnáním ochrany webových aplikací českých bankovních institucí. Srovnání bude založeno na použitých protokolech, které jsou na těchto stránkách používány a dalších dostupných informacích o tom, proti jakým typům útoků jsou tyto stránky odolné.

3. Teoretická východiska

3.1 Elektronické bankovnictví

Jedná se o službu, díky které může klient komunikovat se svojí bankou napřímo prostřednictvím různých komunikačních kanálů a nemusí při tom navštěvovat bankovní pobočku osobně. Službě se také díky výše zmíněnému důvodu přezdívá přímé bankovnictví. Uživatelé mohou realizovat základní bankovní operace (poslat platbu, zadat trvalý příkaz nebo převést peníze z jedné banky do druhé). Všechny tyto úkony lze vyřídit z pohodlí domova a není třeba kvůli tomu docházet na bankovní pobočku. Výše zmíněné operace mohou být prováděny prostřednictvím pevného telefonu, mobilního telefonu, tabletu nebo osobního počítače. (Ceed.cz, 2006)

S rozvojem nových technologií se stále objevují nové produkty v oblasti bankovnictví. Pod přímé bankovnictví řadíme internetové bankovnictví, telefonní bankovnictví, mobilní bankovnictví, domácí bankovnictví, GSM bankovnictví a WAP bankovnictví. Většina těchto služeb umožňuje přístup 24 hodin denně. V dnešní době se nejčastěji používá internetové bankovnictví a mobilní bankovnictví. Je tomu tak především z důvodu přehlednosti, jednoduchosti a pohodlnosti používání těchto služeb. Dnes už provádějí klienti většinu transakcí elektronicky. (Zlatakoruna.cz, 2003)

3.2 Historie elektronického bankovnictví v ČR

První bankou, která u nás založila internetové bankovnictví, byla banka FIO. Jejím klientům bylo umožněno provádět běžné transakce na svém bankovním účtu, a také mít přehled o kompletní historii transakcí. Učinila tak v roce 1998, tedy před devatenácti lety. V tomto roce se k vytvoření internetbankingu postupně přidávaly největší banky v celé Evropě. O další rozvoj internetového bankovnictví se zasloužila Expandia banka (dnes známa pod názvem eBanka). Podle mluvčího eBanky Tomáše Kofroně bylo potřeba klienty přesvědčit, že internetové bankovnictví je skutečně bezpečné, a také je bylo důležité nasměrovat k tomu, že pro provádění běžných bankovních operací není nutné navštěvovat bankovní pobočku osobně. (Tůmová, 2008)

Po eBance se ke zřizování internetového bankovnictví začaly přidávat další české bankovní instituce. Další v pořadí byla v roce 2000 Komerční banka. Nabídla svým klientům běžný internetbanking s názvem služby Moje banka a PC banking ve službě

Profibanka pro podnikovou sféru. V roce 2002 se další dvě velké banky přidaly k novému trendu. Byla to banka ČSOB a Česká spořitelna. ČSOB společně s Poštovní spořitelnou v roce 2003 zavedla autorizaci každé bankovní transakce pomocí SMS kódu. Tento kód bylo nutné zaslat prostřednictvím textové zprávy pro každou bankovní transakci zvlášť. Ostatní banky (nikoli však všechny) začaly toto ověření nabízet svým klientům později. (Tůmová, 2008)

Zpočátku bylo internetové bankovnictví hodně omezené. Toto omezení je myšleno hlavně z technického hlediska. Klienti mohli využívat jen některé operační systémy a pouze vybrané internetové prohlížeče. Například internetové bankovnictví Komerční banky bylo do roku 2007 dostupné pouze v operačním systému Windows a k přihlašování nešel vůbec využít internetový prohlížeč Mozilla Firefox. Nejprve byla k dispozici pouze obsluha běžného účtu, později se k němu přidaly účty spořící, úvěrové, účty stavebního spoření a účty penzijního fondu. Internetové bankovnictví se v Česku i ve světě velmi rychle vyvíjí. Banky oznamují zhruba jednou do měsíce nějaké vylepšení nebo novou službu svého internetbankingu. V dnešní době se klient může připojit na svůj účet pomocí vlastního telefonu, počítače, tablet dokonce i televize. Dají se také on-line nakupovat cestovní pojištění, úvěry nebo cenné papíry. (Kafka, 2006)

3.3 Druhy elektronického bankovnictví

Klienti si mohou vybírat mezi relativně širokým spektrem způsobů, kterými budou svůj bankovní účet obsluhovat. Své rozhodnutí mohou provést na základě toho, jak je pro ně jednotlivá služba pohodlná, dostupná a výhodná.

3.3.1 Internetové bankovnictví (internet banking)

Internetové bankovnictví dovoluje provádět komunikaci klientů se svojí bankou přes internet. Toto spojení může probíhat z jakéhokoliv místa na světě a z každého počítače, který je připojen k internetu. Není samozřejmě úplně vhodné se připojovat k této službě z počítače, na který má přístup široká veřejnost (třeba v internetové kavárně, knihovně, atd.). Nikdy klient nemůže vědět, jestli tento počítač není napaden nějakým virem, zda je chráněn dobrým antivirovým programem nebo jestli není někým monitorován. (Finance.cz, 2012)

Služba funguje celkem jednoduše. V libovolném internetovém prohlížeči klient navštíví adresu svojí bankovní instituce a zvolí přihlášení do internetového bankovnictví. Zde zadá přihlašovací jméno a přístupové heslo k jeho účtu. Tyto údaje přidělí klientovi

banka a obdrží je většinou při zakládání účtu. Poté se dostane do systému internetového bankovnictví dané banky a na tomto místě může provádět široké spektrum operací. Mezi ně patří např. zadávání příkazů k úhradě (v tuzemsku i v zahraničí), vytváření a rušení termínovaných vkladů nebo zadávání a rušení trvalých příkazů k úhradě. Lze zde také dohledat kompletní historii účtu, jeho plateb a toků peněz na účet a z něj pryč. Veškeré tyto úkony jsou realizovány pomocí autorizačního klíče, který zajišťuje zabezpečení osobních údajů k účtu proti potencionálnímu zneužití. (Zlatakoruna.cz, 2003)

3.3.2 Mobilní bankovnictví (smartphone banking)

Tento druh bankovnictví patří k jednomu z nejvyužívanějších mezi veškerými klienty. Dost k tomu přispívá rostoucí popularita chytrých telefonů. Dnes už vlastní chytrý telefon v podstatě každý člověk. Svůj podíl na tom mají také bankovní instituce, které umožňují svým klientům ovládat svůj účet a platby pomocí chytrého telefonu a vyvíjí aplikace, které to umožňují a podstatně zjednodušují. Aby se klient mohl stát uživatelem mobilního bankovnictví, musí vlastnit chytrý telefon a mohou si stáhnout aplikaci, která prováděné operace podstatně ulehčuje. Bankovní instituce obvykle vydávají dvě verze mobilních aplikací, které umožňují přístup do internetového bankovnictví. Jedna verze je pro mobilní telefony od firmy Apple s operačním systémem iOS a druhá verze je určena pro zařízení s operačním systémem Android. (Finance.cz, 2012)

Alternativní možností, jak se přihlásit do internetového bankovnictví z mobilního telefonu, je použití webového prohlížeče a přihlášení se přímo na stránkách konkrétní banky. Bankovní aplikace jsou ale vyvíjeny tak, aby klientům maximálně usnadnily zadávání operací na účtu a ušetřily čas při přihlašování. Proto jsou mobilní aplikace populárnější než přihlašování přes webový prohlížeč v chytrých telefonech. (Finance.cz, 2012)

3.3.3 Telefonní bankovnictví (telebanking, phonebanking)

Telefonní bankovnictví je dostupné pomocí pevného telefonu (tzv. pevné linky) nebo mobilního telefonu. Klient zavolá na linku, která zprostředkovává telefonní bankovnictví v jeho bance. U většiny bank se za volání na toto číslo neplatí žádný finanční poplatek a klientům je umožněno na linku volat také z mobilního telefonu. Až se uživatel na linku dovolá, tak musí operátorovi sdělit své identifikační číslo a heslo. Tento druh bankovnictví je dostupný ve dvou verzích. První verze spočívá v tom, že klient

komunikuje s automatickým hlasovým systémem. Ten mu může dát informaci o současném zůstatku na účtu, jestli klient může zadávat trvalé příkazy nebo provádět konverzi měn. Při komunikaci s automatem je nezbytné, aby klient vlastnil telefon s tónovou volbou. (Finance.cz, 2012)

Druhá verze tohoto typu bankovnictví je rozdílná v tom, že klient se dovolá reálnému člověku (telefonnímu bankéři), který může realizovat stejné operace jako pracovník na přepážce v běžné bankovní pobočce. Drobnou nevýhodou je, že když bude klient chtít něco vyřídit mimo pracovní dobu, tak bude nucen komunikovat pouze s hlasovým systémem. Člověk za přepážkou nebude k dispozici, když je v bance zavřeno. V současné době není tento způsob internetového bankovnictví příliš využíván, jelikož internetové nebo mobilní bankovnictví nabízí stejné služby a je mnohem jednodušší a pohodlnější. (Zlatakoruna.cz, 2003)

3.3.4 Domácí bankovnictví (home banking)

Tato služba svým klientům dovoluje obsluhovat bankovní účet pomocí počítače z pohodlí jejich domova. Stroj musí být připojen k internetu a je nutné mít k dispozici speciální program, který je vydáván bankovní institucí. Zařízení klienta je propojeno s počítačem v bance pomocí datové sítě. Toto připojení je obvykle realizováno prostřednictvím modemu (telefonní spojení) nebo připojením k internetu prostřednictvím síťového adaptéru. (Zlatakoruna.cz, 2003)

Hlavní výhodou je kompatibilita s účetními programy, které využijí hlavně menší firmy, které potřebují denně provést mnoho transakcí. Nevýhodou je, že se klient může připojit pouze z počítače, na kterém je nainstalován speciální program produkovaný bankou. Toto bankovnictví je využíváno především firmami, ale je možnost ho používat i jako soukromý subjekt. (Finance.cz, 2012)

3.3.5 GSM bankovnictví (GSM banking)

Této služby existují dva typy. Jeden se nazývá SIM Toolkit, kdy bankovní instituce nainstaluje na SIM kartu klienta svou aplikaci, kterou poté může ve svém mobilu využívat. V průběhu instalace programu do telefonu je SIM karta zablokována a nelze z ní získat žádné údaje. To platí i v případě krádeže zařízení. Přístup do bankovní aplikace je bezpečnostně ošetřen speciálním PIN kódem, kterému se říká BPIN. Poté, co se do aplikace klient dostane, může provádět běžné operace na svém bankovním účtu. O průběhu

operace dostane informaci ve formě SMS nebo e-mailu. V České republice poskytují tuto službu tři operátoři. Jedná se o operátory O2, T-Mobile a Vodafone. (Zlatakoruna.cz, 2003)

Další variantou této služby je tzv. SMS banking. Přednost této varianty služby spočívá v tom, že je úplně jedno, jakého má klient mobilního operátora. Komunikace s klientem je zprostředkována textovými zprávami. Toto řešení by se mohlo zdát trochu rizikové z hlediska bezpečnosti, jelikož SMS zprávy nejsou nijak zvlášť chráněny proti zneužití. Banka má sice možnost vygenerovat ověřovací kód, ale není to její povinností. Tento kód poté musí uživatel zadat do každé zprávy, kterou prostřednictvím této služby odesílá. Nevýhodou tohoto způsobu komunikace s bankou je, že zprávy mají přesně daný formát, který musí uživatel dodržet. Při psaní takové zprávy si musí dát klient bedlivě soustředit, aby se někde při psaní zprávy nepřeklepl. Formát zprávy může vypadat například takto: „*Částka účet_debet účet_kredit splatnost [Vvar_symbol] [Kkonst_symbol] [Sspec_symbol] [MAC]*“. (Finance.cz, 2012)

3.3.6 WAP bankovnictví (WAP banking)

Tento druh internetového bankovnictví je v dnešní době již překonaným. Princip spočíval v tom, že uživatel musel mít k dispozici mobilní telefon s technologií WAP (Wireless Application Protocol). Pomocí telefonu s touto technologií se člověk mohl pomocí ověřovacího kódu připojit ke svému účtu a provádět zde běžné bankovní operace. (Zlatakoruna.cz, 2003)

Služba je v dnešní době zcela nahrazena modernějšími technologiemi, a to hlavně mobilním a internetovým bankovnictvím. (Finance.cz, 2012)

3.4 Další zařízení v elektronickém bankovnictví

Klienti nemusí využívat k elektronickému styku se svou bankovní institucí pouze svůj mobil, počítač nebo tablet. Mohou se spojit se svojí bankou i dalšími způsoby, které jim jsou nabízeny na veřejných místech.

3.4.1 Bankomaty

Bankomat je samoobslužný stroj, který umožňuje vlastníkům platebních karet vybírat peníze v hotovosti na určených veřejných místech. Obrovskou výhodou tohoto

zařízení je to, že klient může vybírat peníze mimo pracovní dobu bankovní pobočky. (Banky.cz, 2014)

Dokonce je možné (za určitý hotovostní poplatek) si vybrat peníze z bankomatu, který nepatří přímo bance, u které má klient založený účet. Může tak vybrat peníze z bankomatu Komerční banky, ačkoli má účet zřízen u České spořitelny. Jeden z prvních bankomatů byl zprovozněn v roce 1967 v Londýně. Dnes po celém světě můžeme nalézt přibližně tři miliony bankomatů. (Banky.cz, 2014)

3.4.2 Platební karty

Platební karta je nástroj, který je dnes vyrobený obvykle z plastu. Klient může pomocí této karty platit ve většině obchodů a institucí, které platbu kartou umožňují. Ne každý obchod dovoluje platit svému zákazníkovi kartou, někde může klient platit pouze v hotovosti. (Ministerstvo financí, 2014)

Dále také uživatel může pomocí tohoto nástroje vybírat hotovost z bankomatů a využívat další služby, které bankomaty nabízí. Mezi tyto služby se řadí například dobytí kreditu na mobilní telefon nebo podání platebního příkazu. Podle zákona č. 284/2009 Sb. je platební karta považována za elektronický platební prostředek. (Ministerstvo financí, 2014)

3.5 Zabezpečení elektronického bankovnictví

Vzhledem k tomu, že služba pracuje s penězi svých uživatelů, měla by být bezpečnost na prvním místě. Banky se starají o ochranu svých klientů celkem svědomitě. Velkou roli v zabezpečení hraje sám klient, který by měl své přístupové údaje náležitě tajit a dodržovat bezpečnostní doporučení, která jsou dána bankou.

3.5.1 Obecné zabezpečení

Elektronické bankovnictví je chráněno v několika úrovních, které jsou vzájemně nezávislé. Když jediný prvek neodpovídá, tak nelze provést transakci a ani cokoliv na účtu měnit. Zabezpečení se skládá ze tří základních aspektů. Mezi ně se řadí identifikace banky, identifikace klienta a zabezpečení toku dat. (Bezpečný internet, 2016)

Identifikace klienta banky tvoří rozhraní, do kterého se klient přihlašuje, aby mohl elektronické bankovnictví používat. Většinou je přístup klienta řešen unikátním jménem a heslem. Tyto údaje jsou obvykle přidělovány klientům bankou. Přihlašování lze řešit i bezpečnějšími metodami, například autentizačním kalkulátorem. Tyto služby jsou ale

brány jako nadstandardní a jsou za ně vyžadovány celkem vysoké poplatky. Klienti obecně upřednostňují nižší úroveň zabezpečení s vyšším uživatelským komfortem, protože obecně platí, že čím vyšší je bezpečnost přístupu, tím méně je přihlašování pohodlné. (Nykodýmová, 2006)

Přenos dat mezi klientem a bankou je nejčastěji realizován šifrováním dat, které je na velmi vysoké úrovni. Z tohoto hlediska lze považovat zabezpečení toku dat za dostatečně bezpečné. Šifrování zajišťuje webový prohlížeč. (Zámečník, a další, 2005)

Na následujícím obrázku lze vidět délku šifrovacího klíče jednotlivých českých bank a podpisovou autoritu, kterou používají.

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

Obrázek 1 - Přehled šifrování

Zdroj: ZÁMEČNÍK, Petr, KRČMÁŘ, Petr, 2005. *Analýza zabezpečení internetového bankovnictví v České republice.* [online]. [cit. 2017-12-27]. Dostupné z WWW: http://i.iinfo.cz/urs-att/Mesec.cz-studie_int.bankovnictvi-112002647608700.pdf

3.5.2 Uživatelské jméno a heslo

Způsob přihlašování klientským jménem (někdy také číslem) je sice pro klienta nejjednodušší a nejpohodlnější, ale také nejvíce rizikový. Potencionálnímu útočníkovi, který by se chtěl na účet klienta dostat, postačuje k tomuto činu znát pouze jméno a heslo k účtu. Zcizení přihlašovacích údajů z počítače, ze kterého se uživatel do elektronického bankovnictví přihlašuje lze provést pomocí programu, který funguje například na principu

keyloggeru. Ten je schopen sledovat, jaké klávesy byly na počítači stisknuty. Takto útočník přihlašovací údaje k účtu snadno získá. (Nykodýmová, 2006)

Klientům, kteří užívají pouze tento způsob zabezpečení je doporučeno, aby používali některé z doplňujících bezpečnostních opatření. Mezi tyto metody se řadí například automatické zasílání textové zprávy při zadání každé transakce nebo nastavení limitu odeslaných peněz na den. Člověk by si měl také pravidelně měnit heslo a jeho heslo by mělo být dostatečně silné. Sílou hesla je míněno, aby obsahovalo velká i malá písmena, číslice a ideálně speciální znaky. (Boušová, 2006)

3.5.3 Autorizace transakce SMS klíčem

Funguje to tak, že když klient chce potvrdit jakoukoliv transakci, tak musí zadat kód, který mu je zaslán prostřednictvím textové zprávy na mobilní telefon. Obrovskou výhodou tohoto způsobu zabezpečení je, že i když se nežádoucí osoba dostane klientovi na účet, tak nemůže provést žádnou transakci, jelikož nezná SMS kód. (Boušová, 2006)

Od roku 2006 kód zavedla eBanka, ČSOB, Česká spořitelna a Komerční banka a to bez ohledu na objem transakcí. U Komerční banky je ale kód vyžadován pouze u první transakce při jednom přihlášení. U dalších transakcí v pořadí už vyžadován není. Ostatní výše zmíněné bankovní instituce mají ke každé transakci kód jedinečný. Klienti Komerční banky jsou tak vystaveni většímu riziku než klienti ostatních bank. (Nykodýmová, 2006)

3.5.4 Elektronický podpis

Klient může využít pro podepisování a potvrzování transakcí elektronický podpis. Tomu se také říká osobní certifikát klienta, který se dá uložit přímo do souboru nebo například na čipovou kartu. Doporučeno je, aby certifikát nebyl ukládán na disk, ale bylo použito jiné externí úložné médium. Pokud bude certifikát uložen přímo v počítači, může ho potencionální útočník přímo ze zařízení odcizit. Může být uložen například na USB disk nebo také na disk CD. (Nykodýmová, 2006)

Klienti by si měli dávat pozor na to, aby úložné zařízení z počítače nezapomněli vyjmout. Pokud zůstane úložiště s certifikátem připojeno, může se za klienta podepisovat někdo úplně jiný a provádět nežádoucí úkony na jeho účtu. Uložení podpisu na čipové kartě je bezpečnější než výše zmíněná média. Výhodou je, že by musela být odcizena čipová karta, aby klientovi byl odcizen osobní certifikát. Opět platí, že klient by měl kartu

ze čtečky čipových karet vždy vyjmout a bezpečně uložit. (Boušová, 2006) Pomocí elektronického podpisu lze také komunikovat se státní správou a je uznáván všemi orgány veřejné moci v České republice. (Postsignum.cz, 2015)

Na obrázku níže je zobrazeno, jaký způsob autorizace transakcí české banky svým klientům v roce 2006 nabízely a které nikoliv.

	Jméno+heslo	Certifikát	Čipová karta	SMS kód	Kalkulátor
Citibank	ano				
Česká spořitelna	ano		ano		ano
ČSOB	ano	ano	ano	ano	
E-banka		ano		ano	ano
GE Money Bank	ano	ano		ano	
HVB Bank					ano
Komerční banka		ano	ano		
Poštovní spořitelna	ano	ano	ano	ano	
Raiffeisenbank	ano				
Volksbank	ano				
Živnostenská banka	ano	ano			

Obrázek 2 – Autorizace transakcí

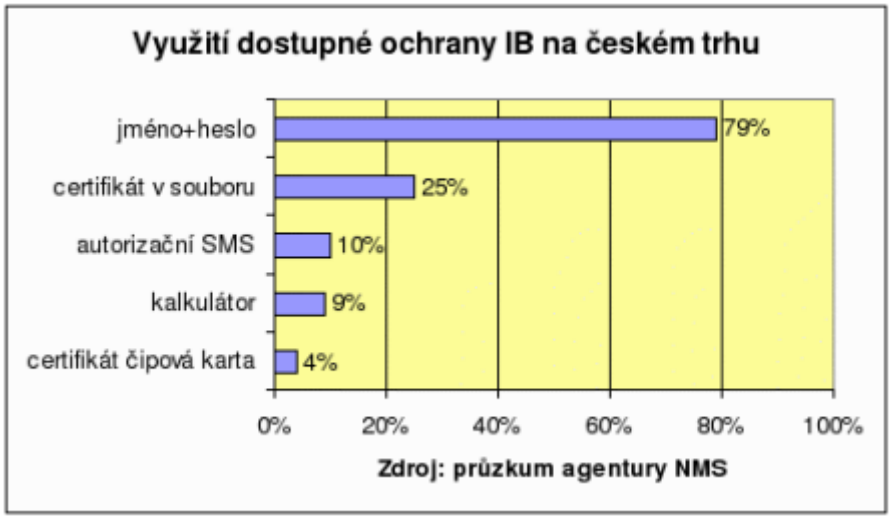
NYKODÝMOVÁ, Helena, 2006. *Jak je to s bezpečností internetového bankovnictví.* [online]. [cit. 2017-12-28]. Dostupné z WWW: https://www.lupa.cz/clanky/jak-je-to-s-bezpecnosti-internetoveho-bankovnictvi/ ISSN: 1213-0702.

3.5.5 Elektronický kalkulátor

Kalkulátory garantují svým klientům jeden z nejlepších způsobů zabezpečení jejich bankovního účtu. Vygenerují kód ke každé prováděné transakci. Uživatel kalkulátoru si sice nemusí nic do svého osobního počítače instalovat, jelikož kalkulátor je externí zařízení, které si lze samostatně zakoupit. (Nykodýmová, 2006)

Je to vlastně taková malá krabička, která se velice podobá běžné kalkulačce. Zařízení je jednoduše přenositelné a je ochráněno čtyřmístným číselným kódem. Po zadání tohoto hesla a zmáčknutí speciálního tlačítka vygeneruje šestimístný kód, kterým klient potvrdí transakci. Pro každý převod peněz se generuje unikátní kód. (Boušová, 2006)

Na obrázku níže je uveden stručný přehled bezpečnostních opatření, které klienti nejčastěji využívali.



Obrázek 3 – Využití ochrany v ČR

NYKODÝMOVÁ, Helena, 2006. *Jak je to s bezpečností internetového bankovnictví.* [online]. [cit. 2017-12-28]. Dostupné z WWW: https://www.lupa.cz/clanky/jak-je-to-s-bezpecnosti-internetoveho-bankovnictvi/ ISSN: 1213-0702.

3.6 Bezpečnostní rizika elektronického bankovnictví

Elektronické bankovnictví se stále vyvíjí a bankovní instituce nabízejí rychle se rozšiřující spektrum služeb. V důsledku toho se samozřejmě i v naší zemi najdou lidé, kteří se pokoušejí tyto služby zneužít. (Cnb.cz, 2014)

Centrální banka (u nás je to Česká národní banka) sleduje, aby ostatní banky pravidelně své klienty informovaly o možných rizicích a snažili se je eliminovat. Bezpečnost účtů nezávisí pouze na zabezpečení, o které se starají samotné banky. Hodně záleží na dodržování bezpečnostních pravidel klientem, jeho zodpovědnosti a pečlivosti. V nemalém množství případů si klient za zneužití svého účtu může sám. (Cnb.cz, 2014)

3.6.1 Používání různých přístupových zařízení

Klienti mohou k přístupu ke svému bankovnímu účtu používat mnoho zařízení. Nejčastěji využívaným nástrojem je osobní počítač, mobilní telefon nebo tablet. Každý člověk zodpovídá za to, jak má své zařízení chráněné. (Cnb.cz, 2014)

Lidé by měli svá zařízení, pomocí kterých se přihlašují do elektronického bankovnictví, pravidelně aktualizovat, jelikož nové verze odstraňují bezpečnostní díry v

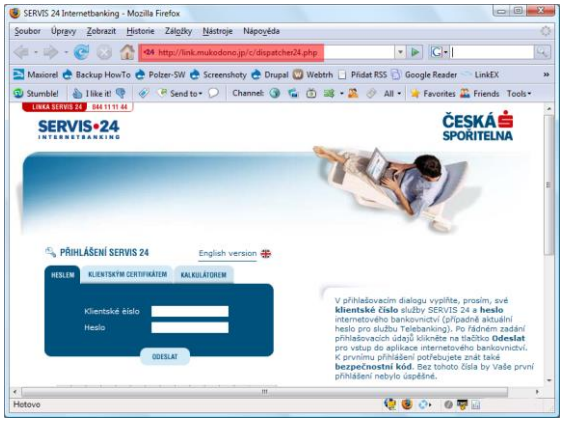
systému. Totéž platí o aktualizaci internetového prohlížeče zařízení. Dále je nutné mít funkční, aktuální a stále aktivní antivirový program, který chrání zařízení před škodlivými programy nebo viry. Ideální je mít také v provozu bránu firewall, která monitoruje komunikaci mezi zařízením a ostatními systémy nebo webovými stránkami. Obecně se také doporučuje instalovat pouze aplikace z důvěryhodných zdrojů, nenavštěvovat pochybné stránky, neklikat na neznámé odkazy a přihlašovat se pouze z důvěryhodných zařízení. (Chip.cz, 2015)

3.6.2 Phishing

Jedná se o metodu, která funguje tak, že klientovi přijde podvodný e-mail, který se z něj snaží vymámit ze smyšlených důvodů přístupové údaje k bankovnímu účtu. Zpráva se přitom zdá být důvěryhodná. Má například stejný (nebo velice podobný) vzhled jako skutečné e-maily, které instituce skutečně svým klientům odesílá. Na phishing se nachytá přibližně pět procent z oslovených lidí. V České republice byly zaznamenány první případy phishingu v roce 2006, kdy se podvodníci zaměřili na klienty banky Citybank. (Slížek, 2006)

Může se stát, že klient informace o přístupech skutečně podvodníkovi odešle nebo klikne na odkaz ve zprávě, který obsahuje link na stránku, která bance nepatří a po zadání přihlašovacích údajů je odešle přímo útočníkovi. V důsledku této skutečnosti banky svým klientům doporučují své přihlašovací údaje nikomu nesdělovat, nereagovat na podezřelé e-maily a neotevírat v nich obsažené přílohy nebo odkazy. (Cnb.cz, 2014)

Na obrázku níže je zobrazen příklad podvodné stránky České spořitelny.



Obrázek 4 - Podvodná stránka

POLZER, Jan, 2008. *Česká spořitelna a phishing – kdy už to skončí?* [online].[cit. 2018-01-09]. Dostupné z WWW: https://www.maxiorel.cz/ceska-sporitelna-phishing-kdy-uz-skonci

3.6.3 Pharming

Tímto pojmem je označován další druh podvodu, který neútočí na klienta přímo, ale snaží se ovládnout internetové stránky banky. Je to v podstatě horší podoba phishingu, jelikož uživatel není atakován přímo a je těžší tuto nežádoucí praktiku odhalit. (Managementmania.com, 2015)

Klient musí spoléhat, že jejich bankovní instituce má stránky dostatečně ochráněné provozovatelem webu. Jedná se totiž o útok, který je směrován přímo na DNS server a přepis IP adresy původní stránky. Klient zadá přístupové údaje do stránky, která vůbec nemusí patřit jeho bance a útočník získaná data zneužije. (Managementmania.com, 2015)

3.7 Internetové protokoly

V informačních technologiích lze internetový protokol definovat jako soubor pravidel, kterým se řídí elektronická komunikace a přenos dat mezi dvěma nebo více koncovými body na internetu. Každému z počítačů je přidělena alespoň jedna specifická IP adresa, která ho odlišuje od ostatních zařízení na internetu. (Rouse, 2008)

Data, která po síti kolují, se dělí na menší části, které nazýváme pakety nebo také datagramy. Každý paket obsahuje IP adresu odesílatele a příjemce. Pakety jsou přenášeny prostřednictvím jejich přepojování a přenos je možný i při výpadku některých spojení v síti. (IT-slovnik.cz, 2012)

3.7.1 Protokol IP (Internet Protocol)

Je to nejdůležitější protokol, který je součástí síťové vrstvy. Jeho hlavní úlohou je doručování dat tam, kam mají být poslána. Zajišťuje sice rychlý a nespojovaný přenos dat mezi uzly. Ten je také méně spolehlivý, ale aplikace si může v případě požadavku spolehlivosti lepší kvalitu přenosu vyžádat. Obsahuje částečné rozpoznávání chyb, které bere v úvahu jen kontrolní součet hlavičky protokolu. Pomáhá také s adresací stanic v síťové vrstvě nebo s definicí a směrováním datových paketů. (Kabelová, a další, 2012)

Protokolu IP existují 2 verze. Verze IPv4 může generovat pouze 32bitové adresy. Není to úplně ideální, jelikož takových adres mohou být vytvořeny pouze čtyři miliardy, což je na současný počet všech zařízení relativně málo. Druhá verze IPv6 tento problém

řeší, protože vytváří 128bitové adresy. Navíc přidává řízení kvality služby, což dělá přenos dat spolehlivějším. (Satrapa, 2011)

3.7.2 Protokoly TCP (Transmission Control Protocol) a UDP (User Datagram Protocol)

Protokol TCP realizuje tok dat mezi jednotlivými body až poté, co si ověří, že oba počítače existují a kontroluje se také dostupnost prvků na cestě přenosu. Až po této proceduře se transport dat mezi počítači zahájí. Příjemce informací posílá zpět zprávu, jestli přijal všechna data v pořádku. Zajišťuje spolehlivý a spojovaný přenos, který je ovšem náročnější na realizaci. (Kejduš, 2012)

UDP zajišťuje nespojovaný a méně spolehlivý přenos dat než protokol TCP. Je používán především aplikacemi, které preferují rychlost přenosu dat před jeho spolehlivostí. Protokol UDP před zahájením toku dat nic nekontroluje a začne například vysílat data, aniž by ověřil existenci koncového počítače. Neprobíhá zde ani žádné řízení toku dat. (Kabelová, a další, 2012)

3.7.3 Protokol TLS (Transport Layer Security)

Tento protokol zajišťuje šifrované spojení mezi odesílatelem dat a jejich příjemcem. Před započetím spojení je realizován tzv. handshake, který zajistí dohodnutí parametrů mezi uzly spojení pomocí výměny několika paketů dat. Protokol realizuje kontrolu identity na straně serveru za pomocí certifikátu serveru. Stejné ověření může být provedeno také za použití certifikátu klienta. (Bouška, 2014)

Klient zde vytvoří tzv. pre-master secret a ten je využitím asymetrického šifrování zašifrován veřejným klíčem serveru a odešle. Tato data to může zpátky rozluštit pouze server a to díky vlastnímu privátnímu klíči. Poté klient společně se serverem z pre-master secretu vytvoří master secret, na který se uplatní předem dohodnutá hashovací funkce. Dále se vytvoří klíč sezení, který je používám k šifrování a dešifrování sezení. Komunikace, která probíhá přes protokol je šifrována symetrickým šifrováním. (Bouška, 2014)

3.7.4 Protokol QUIC (Quick UDP Internet Connections)

Jedná se o relativně nový protokol v oblasti vývoje webových stránek. Web je nyní postaven nad protokolem TCP z důvodu jeho spolehlivosti jako přenosového protokolu. Aby mohlo začít TCP spojení, tak musí být posláno několik paketů, pro tvorbu parametrů spojení. Mimo jiné je třeba dojednat s protokolem TLS vznik zabezpečeného šifrovaného HTTP spojení a k tomu je potřeba odeslat další pakety, aby vše mohlo proběhnout. Důsledkem nutnosti odeslání všech potřebných paketů před započetím spojení je, že vznik nového spojení nabírá na zpoždění. (Geniar, 2016)

QUIC se nachází nad protokolem UDP a je schopen vytvořit spojení a vyřídit vše potřebné s protokolem TLS posláním pouze jednoho nebo dvou paketů dat. Benefitem používání tohoto protokolu je to, že se stráví mnohem méně času schvalováním paketů v síti a vytvářením spojení. To může vyústit v obrovské zrychlení při tvorbě spojení, než při použití jiného protokolu. Protokol kombinuje rychlost přenosu dat samotného UDP protokolu a spolehlivost přenosu protokolem TCP. (Geniar, 2016)

3.7.5 Protokol Telnet

Jedná se o jeden z nejstarších protokolů z rodiny TCP/IP. Dovoluje uživateli přístup ke vzdálenému počítači za pomocí virtuálního terminálu. Tento terminál obsahuje příkazový řádek a umožňuje tak interaktivní přístup k imaginárnímu zařízení. Využívá zejména služeb TCP protokolu. (Kabelová, a další, 2012)

Nedostatkem Telnetu je jeho slabé zabezpečení. Když byl internet nová síť, tak na ní pracovali většinou pouze lidé, kteří působili ve výzkumných odděleních, v počítačových centrech nebo ve vládě. Nebylo tak za potřebí data chránit, aby se k nim nedostal někdo cizí. V případě použití Telnetu dnes, tak je třeba ho externě zabezpečit proti napadení nebo odposlechnutí dat třetí osobou. (Kabelová, a další, 2012)

3.7.6 Protokol DNS (Domain Name System)

Původní funkcí protokolu DNS byl převod doménových jmen na číselné adresy. Doménová jména se daleko lépe pamatují lidem, ale adresy jsou zase mnohem čitelnější pro stroje. Důležitou komponentou systému jsou tzv. DNS servery. V těchto datových úložištích se nachází data o doménách a jejich detailní záznamy. Postupem času se rozšířilo mnoho dalších funkcí protokolu, například elektronická pošta. (Adaptic.cz, 2011)

Protokol pracuje vlastně jako telefonní seznam pro IP adresy. Přiřadí k číselné IP adrese, která je pro lidi těžko zapamatovatelná symbolické doménové jméno, které si člověk může lépe vybavit. Po zadání doménového jména do internetového prohlížeče uživatelem se prohledá seznam doménových jmen. Až se nalezne odpovídající záznam, tak se prohlížeč sám připojí na IP adresu, která konkrétnímu doménovému jménu odpovídá. (Nic.cz, 2007)

3.7.7 Protokol HTTP (Hypertext Transfer Protocol)

Jedná se o standardní síťový protokol, který je používán internetovými prohlížeči a servery ke komunikaci. Je jednoduché rozpoznat, že webová stránky protokol používá, jelikož ho lze nalézt přímo v URL adrese určité stránky. Protokol vznikl v devadesátých letech minulého století a v současnosti je nejčastěji využívaná verze HTTP 2.0. (Mitchell, 2017)

Používá se komunikace klient-server a ta probíhá formou dotaz-odpověď. Domluva mezi klientem a serverem probíhá za pomoci HTTP dotazů a odpovědí, které jsou realizovány formou zpráv. Tři nejčastěji používané zprávy (neboli metody protokolu) jsou GET, POST, HEAD. (Mitchell, 2017)

3.8 Webové útoky

V minulosti se šlo setkat s případy, ve kterých se někteří lidé pokoušeli napadnout stránky nebo servery na internetu a získat z nich informace nebo přístupy, které pak mohli zneužít. Jinak tomu není ani v dnešní době, a proto by všechny stránky a aplikace měly být dostatečně chráněny před různými hrozbami.

Tyto osoby, které provádějí útoky na internetu, provozují počítačovou kriminalitu. Vyznají se velmi dobře v informačních technologiích a programování a vědí, jak vše v počítači a na internetu funguje. K neoprávněnému získávání citlivých informací používají různé druhy útoků, které nějakým způsobem napadnou požadovanou stránku nebo aplikaci.

K napadání webových stránek a serverů je využíváno několik nejrozšířenějších druhů webových útoků. Rozdíly mezi jednotlivými jsou nejčastěji v provedení. Některé útoky modifikují kódy stránek, jiné uživateli pošlou škodlivý skript, který se spustí na jeho počítači a další využívají akcí a práv právě přihlášeného uživatele.

3.9 Útoky DoS (Denial of Service) a DDoS (Distribuated DoS)

Nejprve je třeba znát rozdíl mezi DoS a DDoS útoky. Hrozby DoS používají pouze jeden počítač, ale DDoS jsou realizovány pomocí více než jednoho stroje. V praxi se lze setkat častěji s DDoS útoky, jelikož pomocí více zařízení lze snadněji ochromit požadovanou lokalitu různými způsoby. (Security-portal.cz, 2013)

Existují dvě nejčastěji používané formy těchto útoků. V jedné útočník využívá zahlcování zařízení, serveru, sítě nebo e-mailové schránky pomocí vyčerpání zdrojů, aby dále služba nemohla sloužit svým pravým uživatelům. Druhá forma útoků probíhá obsazením komunikačního kanálu a znemožní komunikaci, která je vyžadována ke správnému fungování služby. (Přibyl, 2006)

Těmito útoky byly v minulosti napadeny také české bankovní instituce. Konkrétně se jednalo o Českou spořitelnu, ČSOB a Komerční banku. Útok lze realizovat pomocí několika výše zmíněných metod. (Security-portal.cz, 2013)

Bránit se před těmito útoky není vůbec jednoduché. Je třeba použít kombinaci komplexních pravidel a doporučení, které spolu zajišťují maximální možnou obranu. (Přibyl, 2006)

Před těmito hrozbami se lze chránit pravidelnou aktualizací bezpečnostních záplat, používáním nejaktuálnějšího softwaru a systému. Tímto uživatel docílí toho, že bude chráněn proti nově nalezeným rizikům. Dalším bodem je nastavení routeru, kde je nutné, aby žádný první paket z libovolné IP adresy nebyl vpuštěn dále. Je to dobré především proti DDoS útokům, které většinou falšují IP adresu odesílatele. Také je vhodné u firewallu nastavit filtr UDP požadavků služeb z internetu. Tímto krokem lze zabránit příjmu UDP paketů, které mají nelegitimní parametry. Doporučeno je provádět pravidelně zálohování dat a systémové konfigurace. V případě, že už se subjekt stane obětí útoku, může své servery rychle obnovit a začít znovu fungovat. (Přibyl, 2006)

3.10 CORS (Cross Origin Resource Sharing)

Zde se nejedná přímo o útok, který může být namířen na webovou aplikaci, ale o mechanismus, který může být použit ke zneužití dat nebo získání citlivých informací. CORS je mechanismus, který používá hlavičky HTTP ke sdílení zdrojů dat z webové stránky pro aplikace na jiných doménách. Může ulehčovat například poskytovatelům

nějaké služby předávání informací svým zákazníkům. Aby bylo používání CORS bezpečné, je třeba chránit data proti neoprávněnému přístupu. (Gibb, 2014)

Data aplikací jsou chráněna před zneužitím opatřením, které je založeno na kontrole původu domény. Pokud je tento ochranný prvek implementován, tak je kontrolováno, z jaké domény požadavek na sdílení dat pochází. Obvykle jsou definovány domény, od kterých žádost o sdílení dat aplikace přijme. Pokud tedy o informace zažádá jiná doména, tak jí data nebudou poskytnuta. Když ale není kontrola původu domény definována, tak po zaslání jakékoliv žádosti o sdílení dat jsou tyto informace zaslány potencionálnímu útočníkovi. (Gibb, 2014)

3.11 SQL injekce

Tato hrozba se zaměřuje na útok na databázové systémy. Zneužívá chybného ošetření vstupu od uživatele při tvoření dotazů pro vstup do databáze prostřednictvím dotazů v jazyce SQL a jeho derivátů. (Ferschmann, 2008)

Důsledkem může být modifikace dat v databázi, jejich přidávání, mazání nebo poškození integrity dat. Útočník také může z databáze data ukrást a nějakým způsobem zneužít. To platí hlavně pro přihlašovací jména a hesla k uživatelským účtům na internetových stránkách. Jedná se o jeden z nejstarších a nejznámějších typů útoků, které byly prováděny na webové aplikace. (Acunetix.com, 2012)

Před tímto útokem se lze vcelku jednoduše chránit. Hlavním ochranným prvkem je ošetření parametrů na vstupech. To lze realizovat pomocí vázaných proměnných, jejich konverze nebo filtrace. Validaci vstupů lze provést také pomocí whitelistů. Whitelisty označují seznam položek, které se můžou na vstupu vyskytnout. Nelegitimní vstupy budou tak zakázány. (Špaček, 2014)

Doporučeno také je minimalizovat práva, která jsou dostupná v internetové aplikaci, která přistupuje k SQL. Je vyžadováno důsledné zabezpečení toho, co obsahuje požadavek HTTP, jelikož toho v případě nezabezpečení může útočník snadno zneužít. (Špaček, 2014)

3.12 Útoky XSS (Cross-site Scripting)

Další typ útoků je založen na podstrčení škodlivého skriptu (většinou JavaScriptu) uživateli, který o ničem takovém ani nemusí vědět. Je to velmi známý druh hrozby, avšak existuje velké množství internetových stránek, které nejsou proti XSS chráněné. (Konečný, 2015)

Všechno funguje na bázi toho, že se pomocí JavaScriptu dají obvykle zjistit informace o právě přihlášeném uživateli. Tyto soubory se nazývají cookies a útočník tak může obsah využít pro nelegitimní účely. Když se mu podaří získat cookie administrátora stránky, tak si může dělat s napadenou stránkou cokoliv. Pomocí skriptu lze praktikovat také phishing. Uživatel je přesměrován na stránku, kam zadá své přihlašovací údaje a ty se odešlou prostřednictvím falešné stránky. Lze také modifikovat obsah stránky, čehož lze využít pro vložení nevyžádaných reklam na stránku nebo přidáním odkazů na nedůvěryhodné weby a v důsledku toho může být poté stránka podle vyhledávačů klasifikována jako škodlivá. (Jecas.cz, 2014)

Útok byl proveden na některé populární webové stránky jako například internetový obchod Amazon nebo americký aukční portál eBay. (Špaček, 2014)

Základní ochranou proti XSS je správné ukončování funkcí v kódu a pečlivé ošetřování dat, které se vypisují na internetových stránkách. Takzvané escapování funkcí lze provádět manuálně nebo použitím automatického nástroje, který ošetřuje proměnné a funkce intuitivně. Mezi takové nástroje se řadí například systém Latte od Nette frameworku, který sám ošetří proměnnou podle jejího umístění v kódu. (Konečný, 2015)

Ochrana dat, která se vypisují na stránky, je realizována převodem nebezpečných znaků na prostý text. Mezi nebezpečné znaky se řadí například ostré závorky. Ty jsou pomocí funkcí převáděny na znaky entitního vyjádření. Pak jsou všechny tyto na informace na stránky vypisovány ve formě prostého textu. (Špaček, 2014)

3.13 Útoky CSRF (Cross site request forgery)

Nebezpečí útoku CRSF se skrývá v tom, že se útočník pokouší využít nezamýšlené akce v aplikaci. Většinou cílem útoku není získat přístupové údaje uživatele k aplikaci, ale dá se k tomu také použít. Hrozba zneužívá práva a akce právě přihlášeného klienta. (Pbwcz.cz, 2017)

Pro útočníka je vhodná znalost nebo přibližný odhad struktury atakovaného cíle, aby věděl, jaký požadavek má přibližně poslat. Realizace probíhá zasláním HTTP požadavku, který posléze nevědomky přihlášený člověk přijme. Pomocí tohoto uživatele se útočník může dostat do sekce internetové aplikace s právy administrátora, která mu umožňuje například editovat či mazat data na stránce. To může vést k nenahraditelné ztrátě

důležitých dat, která jsou nějakým způsobem pro majitele stránky důležitá. (Timehosting.cz, 2014)

Nejlepší opatření, které chrání webovou aplikaci před touto hrozbou je použití autentizačního tokenu k potvrzování uživatelských akcí. Tím je myšleno, že pokud chce klient webové aplikace něco potvrdit, tak musí zadat náhodně vygenerovaný kód. (Timehosting.cz, 2014)

Opatření je nejčastěji realizováno potvrzovacím kódem ve formě kódu odeslaného v textové zprávě SMS uživateli nebo zadáním libovolně dlouhého náhodně určeného kódu náhodných čísel nebo náhodných písmen. Po zadání je testováno, jestli kód souhlasí se zadaným. Pokud vše souhlasí, akce je provedena, jinak je zamítnuta. (Pbwcz.cz, 2017)

3.14 Session hijacking

Nebezpečí dalšího známého útoku spočívá v krádeži sezení, zpravidla mezi administrátorem a běžným uživatelem. Útočník má hned několik možností, kterými se dá odcizení sezení realizovat. Může ukrást identifikační číslo sezení a to nejčastěji na nezabezpečené síti Wi-Fi nebo na internetových stránkách, kde není použit SSL nebo TLS bezpečnostní protokol. Když není použit, komunikace je nešifrovaná a je velice snadno napadnutelná. (Cucu, 2017)

Dalším způsobem je takzvaná fixace na sezení uživatele. Ta je realizována tak, že uživateli je podstrčeno konstantní internetové cookie, pomocí kterého může útočník využívat po dobu, kdy bude pravý uživatel přihlášen. (Interserver.net, 2016)

Posledním způsobem je odcizení identifikátoru sezení mezi uživatelem a serverem. Tímto útokem byly v minulosti napadnuty sociální sítě Facebook, Twitter a také Google. (Špaček, 2014)

Prevence spočívá už v protokolu, který je na internetových stránkách použit. Protokol HTTPS data šifruje, takže i když se k nim hacker dostane, tak je může pouze číst a nemůže s nimi nijak operovat, protože na serveru jsou uložena jako pouhý text. Klientům je doporučováno používat spolehlivý antivirový software a udržovat ho aktuální. Také by se neměli přihlašovat k účtům na nezabezpečených Wi-Fi sítích, kde přístupy nejsou šifrovány a mohou být odposlechnuty. Nejlepší prevencí proti krádeži sezení je se pravidelně všude odhlašovat. Když klient zůstane přihlášen prostřednictvím automatického přihlášení, tak má útočník přístup k sezení nepřetržitě, protože klient se nikdy neodhlásí. (Cucu, 2017)

Z hlediska internetových stránek by se session ID mělo po přihlášení uživatele změnit a mělo by být dostatečně dlouhé a náhodné, aby se nedalo snadno odhadnout. (Špaček, 2014)

3.15 Clickjacking

Jedná se o velice nebezpečný a hlavně nenápadný druh webového útoku. Uživatel například navštěvuje své oblíbené webové stránky a najednou se na nich objeví nějaké tlačítko nebo odkaz na jinou stránku s obsahem, který by mohl běžného člověka zaujmout. Většinou je prvek umístěn tak, aby uživatel nevěděl, že pochází z úplně jiné lokality a odkazuje na nebezpečnou stránku. Uživatel pak může nevědomě na panel kliknout nebo link otevřít. (Ferschmann, 2008)

Útok je záludný v tom, že samotný internetový prohlížeč této akci nezamezí, jelikož sám klient akci opravdu potvrdil, i když o tom nevěděl. Škodlivý odkaz nebo tlačítko může být přítomné také v e-mailové zprávě, která je oběti odeslána. Tímto útokem byl napaden v minulosti Facebook nebo platební portál PayPal. (Javascript.info, 2017)

Typů ochrany proti takovému útoku je hned několik. Jeden z těch méně spolehlivých je ošetření, které zajišťuje pozici okna prohlížeče. To znamená, že když se něco zobrazí přes aktuální okno, tak se automaticky zobrazí původní obrazovka. Útočníci se ale naučili toto jednoduché nastavení obejít, tudíž není rozhodně doporučováno používat pouze takto triviální ochranu. (Javascript.info, 2017)

Efektivnější obrana je zobrazení varování uživateli, pokud se nějaký objekt nebo stránka pokusí zobrazit přes původní okno. Ukáže se varovná zpráva, která se uživatele zeptá, jestli chce zobrazit cizí objekt nad oknem svého prohlížeče. (Javascript.info, 2017)

Posledním a nejvíce spolehlivým prostředkem zabezpečení je zakázání funkčnosti cizích odkazů nebo tlačítek, které se zobrazí nad oknem prohlížeče. Všechny výše uvedená ochranná opatření lze realizovat pomocí JavaScriptu. (Ferschmann, 2008)

3.16 Útoky hrubou silou

Nejstarším typem útoku pro odhalování hesel klientů různých webových aplikací nebo stránek jsou právě útoky z anglického názvu „brute force“. Fungují na principu hádání nejčastějších kombinací přístupů k účtům uživatelů, dokud není heslo nalezeno.

Tyto hrozby si lze představit jako otevírání zámku, který je chráněn číselným kódem a útočník se snaží zadávat opakovaně různé číselné kombinace vedoucí k odhalení hesla. (Root.cz, 2017)

Příliš se ale tyto útoky už nepoužívají, protože jsou hodně časově náročné. Srovnávají se nejčastěji používaná jména a hesla klientů a zkouší je zadávat do přihlášení na webových stránkách. (Root.cz, 2017)

Zabezpečení proti tomuto útoku je vcelku primitivní. Nejdůležitější je, aby měla aplikace, do které se uživatelé přihlašují, omezený počet pokusů pro správné přihlášení. Klient má pro přihlášení limit například 5 pokusů a útočníkovi, který se snaží uhodnout uživatelské údaje, se to s nejvyšší pravděpodobností na 5 pokusů nepovede. (Špaček, 2014)

Dalším důležitým bezpečnostním bodem je, aby si klienti volili hesla dostatečně silná a neměla by být od ničeho odvoditelná (heslo by nemělo být například jméno uživatelova psa, jeho dcery nebo oblíbeného zpěváka). (Špaček, 2014)

4. Vlastní práce

Praktická část práce obsahuje analýzu vybraných aplikací českých bankovních institucí, která byla provedena na základě jejich veřejně dostupných demoverzí, analýzy jejich funkcí a uživatelského prostředí. Konkrétně se jedná o webové aplikace Komerční banky, České spořitelny, Raiffeisenbank a ČSOB. Aplikace právě těchto bank byly vybrány, protože v České republice velká část klientů spadá právě k těmto čtyřem institucím. Uživatele aplikací by mohlo zajímat, jak moc jsou webové aplikace jejich finančního ústavu bezpečné.

Dále se zabývá srovnáním těchto webových aplikací z hlediska z hlediska bezpečnosti. Srovnání aplikací bude rozděleno na dvě části. První je bude porovnávat z hlediska některých použitých protokolů a dalších informací, které budou získány pomocí programu Wireshark. Program bude použit ke sledování síťové komunikace při přihlašování k jednotlivým aplikacím.

Druhá část komparace se bude zaměřovat na testování přítomnosti nebo absence mechanismu CORS, který slouží ke sdílení dat mezi různými doménami. V případě přítomnosti bude kladen důraz na to, jestli je prováděna kontrola původu domény a tím zajištěna ochrana před zneužitím sdílených informací.

4.1 Analýza webových aplikací vybraných českých bank

Vzhledem k praktické části této práce je potřeba nejprve analyzovat jednotlivé bankovní aplikace, které budou později srovnány z hlediska jejich bezpečnosti. Byly vybrány čtyři nejznámější české bankovní instituce, jejichž aplikace budou analyzovány. Konkrétně se jedná o Komerční banku, Českou spořitelnu, Raiffeisenbank a ČSOB.

Bylo tak učiněno z důvodu, že tyto bankovní instituce pojímají vysoké procento klientů u nás, které by mohla zajímat bezpečnost aplikace používané právě jejich bankou. Analýza se bude zaměřovat především na funkce jednotlivých bankovních aplikací a na uživatelský komfort, který svým klientům aplikace nabízí. Všechny tyto údaje odpovídají veřejně dostupným demoverzím aplikací, které představují jednotlivé banky pro potencionální nové klienty.

4.1.1 Komerční banka

Na úvodní obrazovce aplikace se klient dozví svůj aktuální zůstatek na svém účtu a informaci o tom, jestli je jeho karta dostupná nebo ne. Aplikace je uzpůsobená do záložek podobně jako v internetovém prohlížeči. V části platby klient může sledovat historii jeho veškerých transakcí, zadávat dočasné nebo trvalé příkazy k úhradě, spravovat svá inkasa a sledovat jejich historii. Příkazy lze zadávat v české nebo cizí měně. V neposlední řadě klient může také dobíjet kredit na svůj mobilní telefon. V záložce účty klient sleduje všechny své účty. Může zde zpětně dohledat výpisy účtů, historii transakcí a lze také sjednat schůzku s bankovním poradcem nebo změnu banky. V záložce karty lze najít informace o kartách a úvěrů k nim připojených. Klient si může sjednat debetní nebo kreditní kartu a nastavit její limit. V kartě úvěry může klient spravovat své úvěry nebo si zřídit nové.

Dále aplikace nabízí spoření a investice, kde uživatel má k dispozici přehled produktů, do kterých může investovat. Může nakupovat nebo prodávat podílové fondy a lze si zde také sjednat stavební nebo penzijní spoření. Klient si může v aplikaci překontrolovat, jaké má k dispozici pojištění, a může si založit nové cestovní pojištění nebo pojištění majetku a odpovědnosti. Záložka finanční trhy umožňuje obchodovat s depozitními obchody a spravovat platby s individuálním kurzem. Na konec na kartě moje finance lze spravovat podnikatelské úvěry.

Aplikace Komerční banky nabízí vskutku velké množství funkcí a možností pro své klienty. Malou nevýhodou takto širokého spektra služeb je, že se uživatel musí celkem snažit, než se dostane k tomu, co skutečně chce. Každá záložka obsahuje totiž ještě klidně i dalších pět sekcí s dalšími dílčími funkcemi a to snižuje uživatelský komfort. Aplikace se může zdát pro klienta z tohoto důvodu lehce nepřehledná.

4.1.2 Česká spořitelna

Servis24 po přihlášení do aplikace klientovi zobrazí informace o jeho osobním nebo firemním účtu a přehledu plateb. Rozložení aplikace je o dost jednodušší a přehlednější než u Komerční banky. Systém záložek zůstává totožný, ale dílčí podzáložky nejsou zobrazovány po kliknutí na záložku uprostřed, ale ve sloupci vlevo.

Opět se zde nachází záložka účty, ve které je obsažena i správa karet, veškerých plateb souvisejících s účtem samotným a také mobilním telefonem v případě dobíjení kreditu. V kartě spoření získá klient přehled o svém spoření, může založit nové nebo

vybrat prostředky na účet. Dále jsou k dispozici úvěry, kde klient získá kompletní pojem o svých úvěrech, jejich zůstatcích, výši a jejich stavu. Může také o nový úvěr zažádat nebo nahlédnout na smlouvy s bankou.

Karta investice dovoluje uživateli zobrazit historii jeho investic, obsahuje aktuální přehled produktů a lze zde jednotlivé produkty nakoupit nebo prodat. V záložce pojištění je zobrazen přehled pojistných smluv, které má klient sjednané s Českou spořitelnou. Jsou zde umístěny pouze základní informace, detaily se dají zjistit po kliknutí na číslo smlouvy. V poslední sekci e-shop se nachází aktuální nabídky připravené bankou. Lze zde najít úvěry, půjčky, hypotéky, nabídky spoření nebo výhodné zřízení kreditních karet. Pro detail nabídky je třeba ji opět rozkliknout.

Aplikace České spořitelny nabízí v podstatě stejné funkce jako Komerční banka, ale je více uživatelsky pohodlná. Obsahuje méně záložek a dílčí informace jsou zobrazeny přehledně ve sloupci na levé straně nebo po zobrazení detailu základních informací. Také nápověda k jednotlivým sekcím je řešena celkem elegantně. Po kliknutí na otazník se vždy zobrazí nápověda k právě otevřené části aplikace.

4.1.3 Raiffeisenbank

Po přihlášení do aplikace této banky si klient může říci, jestli je zde vůbec správně. Zobrazí se mu totiž jen primitivní informace o zůstatku jeho účtu v korunách a v eurech. Aplikace Raiffeisenbank je asi nejjednodušší ze všech analyzovaných. Uspořádání aplikace je řešeno podobně jako u České spořitelny. Záložky jsou umístěny nahoře a jejich dílčí funkce jsou seskupeny ve sloupci vlevo.

V záložce informace o účtech klient najde zůstatek svého účtu, může sledovat toky peněz na účet a z něj pryč. Lze také dohledat výpisy z účtu a tlačítkem nový příkaz lze založit další příkazy. Na kartě jednorázové příkazy jsou zobrazeny všechny příkazy bez ohledu na to, jestli proběhly úspěšně, neúspěšně nebo jsou v procesu zpracování. Lze zde vytvořit nový příkaz a je zde možnost dobytí kreditu na mobilní telefon. Dále aplikace nabízí sekci trvalé příkazy, která funguje obdobně jako jednorázové příkazy.

Termínované vklady obsahují přehled vložených prostředků a přehled žádostí o vložení peněz. Klient zde může podávat nové žádosti o vložení svých peněz na svůj účet. Karta pošta, žádosti a informace obsahuje mnoho různorodých informací, které může klient potřebovat. Dozví se zde o zprávách, které mu v aplikaci chodí a může zde zažádat o SIPO, inkaso nebo o změnu kontaktních údajů. V této sekci lze také zrušit domácí nebo

zahraniční platební příkaz. V poslední řadě zde má uživatel dostupné informace o kurzovním lístku měn a úrokové sazbě. Poslední částí aplikace je karta nastavení, ve které lze změnit například telefonní číslo připojené k účtu, certifikát klienta, heslo k účtu nebo informace o uživateli.

Raiffeisenbank nabízí svým klientům aplikaci, která se vyznačuje nejvyšším uživatelským komfortem. Informace jsou zobrazeny přehledně a v malých informačních blocích. Pozitivem je také přehledná sekce věnující se nastavení. Daní za přehlednost a jednoduchost aplikace je absence některých specifických funkcí, které ostatní aplikace obsahují.

4.1.4 ČSOB

Když se klient přihlásí do aplikace této banky, ihned obdrží informaci o stavu jeho účtu a také spořicího účtu. Už na úvodní stránce může spatřit moderní design, který je reprezentován tzv. dlaždicovým zobrazením některých záložek aplikace. ČSOB je v koncepci aplikace revoluční. Hlavní sekce aplikace jsou totiž uspořádány vlevo ve sloupci a dílčí funkce nahoře v řádku. To je přesný opak než u ostatních analyzovaných aplikací. Po najetí myší na hlavní záložky se zobrazí nabídka dalších možností, podobně jako u Komerční banky, akorát uživatel nemusí vůbec na kartu klikat.

Platby zobrazují přehled veškerých plateb s možností zadávání platby nové, ať už trvalé nebo jednorázové. Lze zde také dobít kredit na mobilní telefon nebo převádět peníze mezi účty. V kartě přehledy má uživatel přehledně seřazeno, co se kdy na jeho účtu dělo z hlediska plateb. Sekce produkty zobrazuje svým klientům všechny služby, které mají s bankou sjednané. Uživatel má tak všeobecný přehled všech svých smlouvách. Výdaje a rozpočty nesou informaci o stavech různých rozpočtů. Mohou zde být zobrazeny například půjčky nebo hypotéky s grafikou, kolik peněz už klient splatil a kolik mu ještě zbývá.

Svět odměn reprezentuje věrnostní program, který ČSOB pro své klienty vytváří. E-shop klientům nabízí nejvýhodnější produkty, které má jejich banka současně k dispozici. Jedná se především o půjčky, spoření, pojištění a hypotéky. Poslední částí aplikace je nastavení, kde si uživatel může pohodlně změnit PIN při přihlášení, kontaktní údaje nebo názvy a pořadí účtů.

Československá obchodní banka nabízí svým klientům asi nejvyváženější aplikaci z hlediska uživatelského komfortu a dostupných funkcí. Design záložek a jejich dílčích

funkcí je na oko pohledný, v aplikaci se není složité orientovat a cokoliv rychle najít. Nechybí ani žádné důležité funkce včetně pohodlné změny nastavení.

4.2 Srovnání z hlediska protokolů pomocí programu Wireshark

V této části byl použit k realizaci srovnání program Wireshark. Program byl použit k analýze protokolů, sledování paketů v síti a ke sledování síťové komunikace při přihlášení do jednotlivých demoverzí bankovních aplikací.

Pro potřebu této komparace bylo provedeno sledování síťové komunikace při přihlašování do demoverze určité bankovní aplikace. Program tímto předal potřebná data o protokolech a jejich verzích, šifrování dat, změně klíče klienta a serveru po přihlášení. Některé parametry srovnání byly také převzaty z webových aplikací přímo bez použití programu Wireshark. Jedná se o požadavek dočasného SMS kódu pro přihlášení do aplikace a o podpoře odhlášení neaktivního klienta z aplikace.

4.2.1 Shrnutí parametrů srovnání

K posouzení bezpečnosti webových bankovních aplikací hraje roli mnoho různorodých parametrů. Pro lepší pochopení a přehlednost následuje seznam parametrů, které byly použity v tomto srovnání.

Verze protokolu TLS nebo SSL

TLS a SSL protokoly zabezpečují komunikaci na internetu pro služby, jako jsou například WWW, fax nebo elektronická pošta a další přenosy dat. Zabraňují tak odposlechnutí citlivých dat nebo falšování rozesílaných zpráv, které v aplikaci kolují. Realizují šifrování dat a změnu klíče serveru a klienta. Je vhodné používat nejnovější verzi těchto protokolů, protože právě tato verze poskytuje nejspolehlivější ochranu pro webovou aplikaci.

Verze protokolu IP

Tento protokol, který pracuje v síťové vrstvě, je jedním z nejpoužívanějších v počítačových sítích a internetu. Vyskytuje se ve dvou verzích. Verze IPv4 umí generovat pouze 32bitové adresy, což může být v dnešní době nedostatečné, vzhledem k počtu

zařízení. Podporuje také méně spolehlivý přenos dat, než druhá verze. Verze IPv6 umí generovat až 128bitové adresy, což s přehledem pokryje počet zařízení, které mohou unikátní IP adresu požadovat. Realizuje také spolehlivější přenos dat, jelikož oproti verzi IPv4 podporuje řízení kvality služby.

Protokol QUIC UDP Internet Connection

Cílem tohoto protokolu, který je postavený na UDP protokolu je nahradit protokoly HTTP nebo HTTPS, které jsou postaveny nad TCP protokolem. Výhoda spočívá v tom, že po první komunikaci se serverem už při každé další není třeba znovu sestavovat spojení mezi komunikačními body. Data tak stráví méně času v rizikových zónách a mají menší šanci na potencionální zneužití, odposlechnutí a podobně. QUIC protokol navíc data šifruje i během sestavování spojení, když prohlížeč se serverem komunikuje poprvé, na rozdíl od protokolu TCP.

Přítomnost šifrování dat v aplikaci

V dnešní době v mnoha aplikacích kolují data, která by se neměla dostat na veřejnost nebo k osobám, které by je mohly zneužít. K tomuto účelu slouží šifrování dat, které data přepíše do takové podoby, kdy nemohou být zneužita. I kdyby se útočník k těmto datům dostal, tak z nich nic nevyčte, protože jsou převedena do nečitelné formy. K jejich rozluštění by potencionální zločinec musel mít k dispozici klíč k dešifrování dat.

Změna klíče serveru a klienta po přihlášení uživatele

Tento způsob ochrany je také velmi důležitý. Změna klíče klienta a serveru po přihlášení uživatele do aplikace zajistí, že pokud byl klíč odposlechnut při přihlášení, tak se nedá použít totožný na právě přihlášeného klienta, jelikož se klíč poté změnil. Většina aplikací toto opatření podporuje právě z výše zmíněných důvodů.

Dočasný SMS kód pro přihlášení do aplikace

Běžně se klient do aplikace přihlašuje přes své přístupové jméno nebo uživatelské ID a heslo. Není ale na škodu, použít ještě další ochranný prvek v případě, že by klientské údaje byly odcizeny třetí osobou. Dá se použít kód z textové zprávy odeslané na telefonní číslo, které je k bankovnímu účtu připojeno. Zamezí se tím vniknutí třetí osoby na účet,

i když zná přihlašovací údaje uživatele. Zločinec totiž nemá přístup k telefonu, na který potvrzovací zpráva nutná k přihlášení přijde a nemůže ji do aplikace zadat.

Odhlášení neaktivního klienta z aplikace

Tento typ opatření je také hodně důležitý při zabezpečení aplikací. Přihlášený klient se může zapomenout odhlásit po dokončení veškerých operací v programu nebo se přihlásí, naléhavě musí dělat něco jiného a aplikaci se nějakou dobu nevěnuje. Na takto přihlášeného uživatele mohou být poté vedeny útoky typu CSRF nebo session hijacking, jelikož je stále k aplikaci přihlášen. Když se uživatel zapomene odhlásit, tak může být zneužito jeho sezení nebo jeho akce v aplikaci, protože je stále přihlášen.

4.2.2 Tabulky se zjištěnými daty

Tabulka 1 - Výsledná tabulka - Komerční banka

Komerční banka	
Verze protokolu TLS	TLSv1.2
Verze protokolu IP	IPv4, IPv6 jen přihlášení
Přítomnost protokolu QUIC	Ano
Šifrování dat v aplikaci	Ano
Změna klíče serveru/klienta	Ano
Dočasný SMS kód při přihlášení	Ano
Odhlášení neaktivního klienta	Ne

Tabulka 2 - Výsledná tabulka - Česká spořitelna

Česká spořitelna	
Verze protokolu TLS	TLSv1.2
Verze protokolu IP	IPv4, IPv6 jen přihlášení
Přítomnost protokolu QUIC	Ano
Šifrování dat v aplikaci	Ano
Změna klíče serveru/klienta	Ano
Dočasný SMS kód při přihlášení	Ne
Odhlášení neaktivního klienta	Ano (10 minut)

Tabulka 3 - Výsledná tabulka - Raiffeisenbank

Raiffeisenbank	
Verze protokolu TLS	TLSv1.2
Verze protokolu IP	IPv4, IPv6 jen přihlášení
Přítomnost protokolu QUIC	Ne
Šifrování dat v aplikaci	Ano
Změna klíče serveru/klienta	Ano
Dočasný SMS kód při přihlášení	Ne
Odhlášení neaktivního klienta	Ne

Tabulka 4 - Výsledná tabulka - ČSOB

ČSOB	
Verze protokolu TLS	TLSv1.2
Verze protokolu IP	IPv4, IPv6 jen přihlášení
Přítomnost protokolu QUIC	Ne
Šifrování dat v aplikaci	Ano
Změna klíče serveru/klienta	Ano
Dočasný SMS kód při přihlášení	Ne
Odhlášení neaktivního klienta	Ne

4.2.3 Výsledek srovnání na základě protokolů

Z hlediska protokolů a dalších dostupných informací vycházejících za daných podmínek z programu Wireshark a prací s demoverzemi jednotlivých aplikací se uspokojivou bezpečností prezentovaly dvě banky, a to Komerční banka s Českou spořitelnou. Obě tyto instituce mají aktuální verzi bezpečnostního protokolu TLS, podporují IPv4 a IPv6 při přihlášení, je zde také přítomný protokol QUIC UDP internet connections, aplikační data jsou šifrována a klientský i serverový klíč se po přihlášení mění. Mezi zabezpečením aplikací těchto bank lze najít ale i tak určité rozdíly.

Komerční banka po klientech vyžaduje zaslání a následného vyplnění dočasného SMS kódu při přihlášení. Takovou možnost Česká spořitelna nepodporuje. Pokud klient někomu prozradí své přihlašovací údaje nebo jsou někým odposlechnuty, tak se třetí osoba

může bez větších problémů dostat oběti na účet. Toto jednání je s žádostí o kód z textové zprávy při přihlášení pro klienty Komerční banky vyloučeno. Česká spořitelna podporuje zase odhlašování neaktivního klienta. Po deseti minutách neaktivity uživatele upozorní, že s aplikací nepracuje a pokud nezačne, tak bude automaticky odhlášen. Tato metoda chrání klienty České spořitelny před krádeží sezení tzv. session hijackingem a útoky CSRF, které zneužívají akcí a práv právě přihlášeného uživatele.

O druhé místo se dělí zbylé dvě bankovní instituce, a to Raiffeisenbank a ČSOB. Tyto bankovní domy mají zabezpečení aplikací za daných podmínek a použitých parametrů srovnání naprosto totožné. Stejně jako u výše zmíněných bank používají nejaktuálnější verzi TLS protokolu, podporují IPv4 a IPv6 při přihlášení, veškeré přenosy dat z aplikace a ven jsou šifrovány. Také klientský a serverový klíč se po přihlášení změní.

Už zde není přítomen protokol QUIC UDP internet connections, tudíž všechna data tráví více času na síti, než se dostanou ke svému cíli. To způsobuje jejich větší riziko odposlechu a zneužití, než s použitím tohoto protokolu. Ani jedna z těchto bank nevyžaduje zadání dočasného SMS kódu při přihlášení uživatele. Tím vzniká větší riziko zneužití jejich účtu při vynesení přihlašovacích údajů. Totéž platí pro odhlášení neaktivního klienta. Ani jedna z bank neaktivního klienta neodhlašuje, takže zde existuje větší riziko zneužití uživatelského sezení nebo akcí a práv právě přihlášeného klienta.

4.3 Srovnání aplikací z hlediska mechanismu CORS

Druhá část srovnání se bude zabývat tím, jestli v bankovních aplikacích je nebo není přítomen mechanismus CORS (Cross-Origin Resource Sharing). V případě, že přítomen byl, zkoumalo se, jestli je realizováno bezpečnostní opatření ošetřující kontrolu původu domény, ze které požadavek přichází. Realizace této části komparace byla provedena pomocí internetového nástroje pro testování, jestli je CORS v aplikaci implementován a zda je zde ošetřen původ domény. Pro upřesnění je níže uvedeno, co to vlastně Cross-Origin Resource Sharing je.

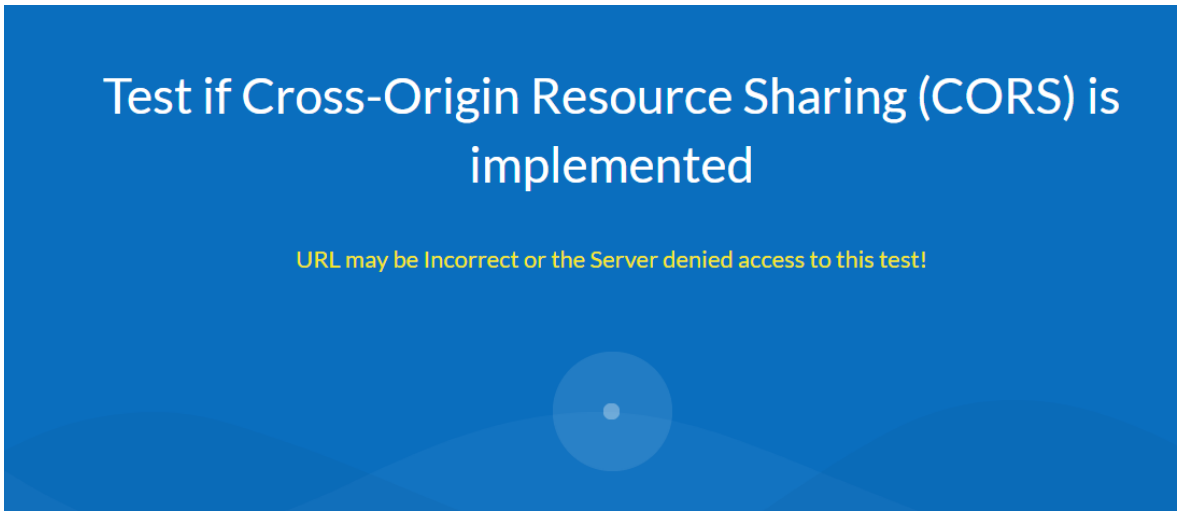
4.3.1 CORS (Cross-Origin Resource Sharing)

Je to mechanismus, který dovoluje sdílet zdroje dat webové stránky pro aplikaci na jiné doméně. Volání mezi různými doménami je zakázáno internetovým prohlížečem, kvůli omezení požadavků na stejnou doménu. Tato metoda umožňuje, že se server

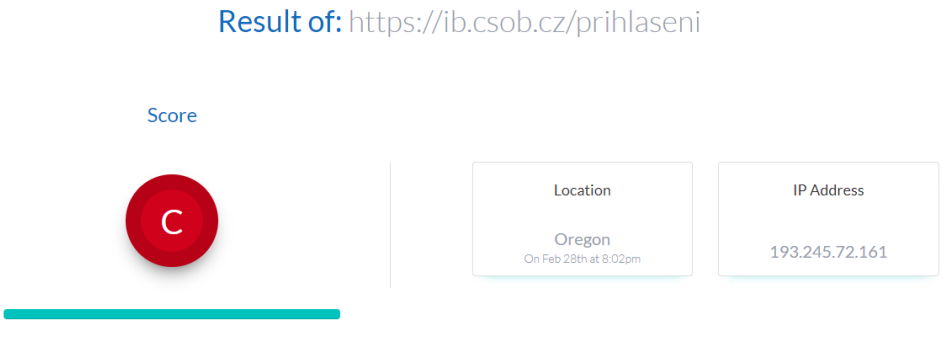
a prohlížeč mohou dohodnout na tom, jestli se volání mezi různými doménami povolí nebo nepovolí.

Obvykle jsou definovány domény, od kterých žádost o sdílení dat aplikace přijme. Pokud tedy o informace zažádá jiná doména, tak jí data nebudou poskytnuta. Když ale není kontrola původu domény definována, tak po zaslání jakékoliv žádosti o sdílení dat jsou tyto informace zaslány potencionálnímu útočníkovi.

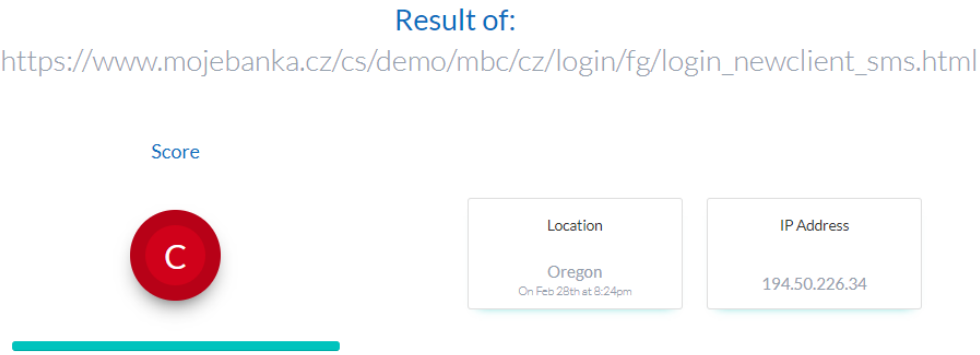
4.3.2 Obrázky s výsledky CORS testů



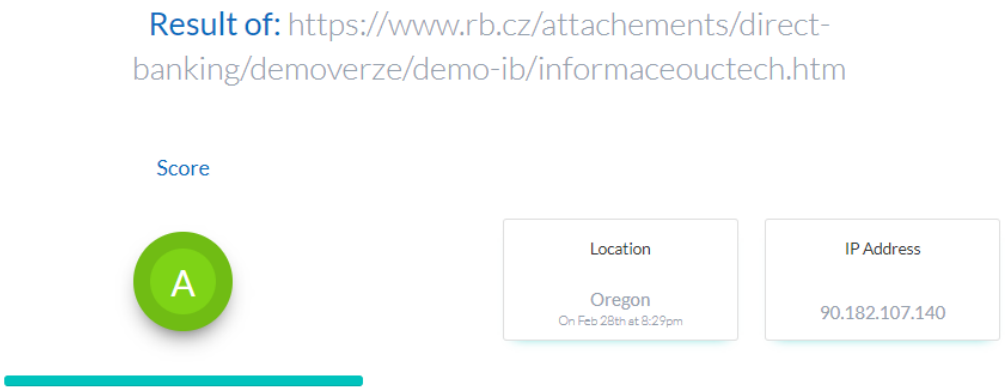
Obrázek 5 - CORS test - Česká spořitelna



Obrázek 6 - CORS test – ČSOB



Obrázek 7 - CORS test - Komerční banka



Obrázek 8 - CORS test – Raiffeisenbank

4.3.3 Výsledek srovnání na základě CORS testů

V případě CORS testu si nejlépe vedla za daných podmínek testování webová aplikace České spořitelny. Její server totiž úplně odmítl přijmout žádost tohoto typu, přístup byl zamítnut. To znamená, že volání mezi různými doménami nemůže být v aplikaci této bankovní instituce zneužito, protože server požadavek ani neprovede, natož aby vrátil nějakou odpověď.

Na druhém místě skončila instituce Raiffeisenbank. CORS mechanismus je v této aplikaci implementován, ale je zde kontrolována doména, ze které požadavek pochází. Jsou povoleny pouze ty požadavky, které pochází z domény www.rb.cz. Po zaslání se zkontroluje jeho původ a žádosti, které nepochází z výše zmíněné domény, nebudou

provedeny. Aplikace tak CORS podporuje, ale ošetřením původu domény zamezuje zneužití dat.

Nejhůře dopadly za daných podmínek testování aplikace Komerční banky a ČSOB. Webové aplikace těchto institucí mají CORS mechanismus implementován, ale nijak nekontrolují původ požadavku, který je aplikaci zaslán. Může se tak stát, že aplikace zašle data člověku, který je bude moci nějakým způsobem zneužít. Mohou také vyjít na povrch některá citlivá data.

5. Vyhodnocení výsledků

5.1 Teoretická část

Teoretická část práce se zabývá elektronickým bankovnictvím, jeho druhy, dalšími možnostmi plateb, zabezpečením společně s různými jeho druhy a bezpečnostními riziky spojených s používáním této služby. Dále pojednává o internetových protokolech, jejich funkcích a úlohách. Také se zaměřuje na různé druhy webových útoků a na to, jakými způsoby se lze před těmito hrozbami nejlépe chránit.

5.2 Praktická část

Jejím obsahem je analýza webových aplikací vybraných českých bankovních institucí. Jmenovitě se jednalo o Komerční banku, Českou spořitelnu, Raiffeisenbank a ČSOB, které byly vybrány na základě jejich největšího počtu klientů v naší zemi. V analýze aplikací za daných podmínek nejlépe obstála ČSOB, jejíž aplikace reprezentuje dobrou rovnováhu mezi uživatelským komfortem a dostupnými funkcemi. Následuje aplikace České spořitelny, která také obsahuje velké množství funkcí, ale moderní grafické prvky a vylepšení zde nejsou dostupné v tak hojné míře. Poté aplikace Komerční banky disponuje velkým množstvím funkcí, které jsou uspořádány tak, že uživatelský komfort aplikace není na dobré úrovni. Aplikace je nepřehledná, a když klient chce něco najít, většinou to dlouho trvá. Nakonec program Raiffeisenbank svým klientům nabízí největší uživatelský komfort, ale v aplikaci chybí některé funkce, které jsou v ostatních aplikacích dostupné.

Dále byla praktická část práce rozdělena do dvou částí. První část byla zaměřena na zkoumání internetových protokolů a dalších dostupných informacích o bezpečnosti webových aplikací vybraných bankovních institucí. K analýze použitých protokolů a informací o síťové komunikaci byl využit program Wireshark. Tímto programem byly sledovány jednotlivý demoverze bankovních aplikací při přihlašování a z těchto dat byly zpracovány výsledky. Některé informace, které se týkají například způsobu přihlašování nebo odhlašování neaktivního klienta, byly převzaty přímo z veřejně dostupných demoverzí webových aplikací určitých institucí. Za daných podmínek na základě použitých parametrů se o první místo dělí Komerční banka s Českou spořitelnou. Jediný rozdíl v zabezpečení těchto dvou bank je ten, že Komerční banka požaduje po klientech při

přihlašování dočasný SMS kód a Česká spořitelna podporuje odhlášení neaktivního klienta po deseti minutách neaktivity. Následuje společně Raiffeisenbank s ČSOB, které mají aplikace chráněné na základě parametrů srovnání naprosto totožné.

V druhé části bylo provedeno testování přítomnosti nebo absence mechanismu CORS v jednotlivých aplikacích a v případě přítomnosti bylo zkoumáno, jestli je k dispozici bezpečnostní opatření kontroly původy požadavku z domény. Pro realizaci tohoto testu byl použit internetový nástroj, který testuje, jestli má aplikace CORS implementován nebo ne a zjistí i to, zda je dostupná kontrola původu domény. Po provedení těchto testů za daných podmínek bylo zjištěno, že asi nejlépe chráněná proti zneužití dat pomocí požadavků zaslaných z jiných domén je Česká spořitelna, hned po ní Raiffeisenbank a za nimi Komerční banka společně s ČSOB.

5.3 Diskuze

5.3.1. Analýza vybraných bankovních aplikací

Začneme s analýzou webových aplikací vybraných českých bankovních institucí. Bylo zjištěno, že za daných podmínek nejvyváženější aplikaci z hlediska poměru uživatelské přívětivosti a dostupných funkcí nabízí banka ČSOB. Posouzeno bylo hlavně uspořádání funkcí v aplikaci, její design, přehlednost a dostupné funkce, které banka nabízí. Další v pořadí se nacházela aplikace České spořitelny. Neobsahovala tolik moderních grafických prvků, jako předchozí, ale stále zde lze najít relativní rovnováhu mezi přehledností, přívětivostí a funkcemi. Dílčí funkce jsou zde implementovány v levém sloupci a systém záložek je řešen podobně jako v internetovém prohlížeči. Také nápověda k jednotlivým sekcím aplikace je řešena vcelku sympaticky. V každé části je k dispozici ikonka otazníku, která dává uživateli možnost se dozvědět více o aktuálně otevřené sekci. Aplikace Komerční banky je pro klienta z hlediska uživatelského komfortu méně pohodlnou. Nabízí velké množství funkcí a vymožeností, ale implementaci vedlejších funkcí, které se zobrazují po kliknutí na základní funkce, nemá řešenou příliš dobře. Klient stráví v aplikaci mnoho času, protože něco v aplikaci nalézt trvá relativně dlouho. Kdyby byly funkcionality aplikace lépe implementovány, dalo by se docílit většího uživatelského komfortu společně se zachováním veškerých funkcí. Aplikace Raiffeisenbank nabízí svým uživatelům asi největší uživatelský komfort. Po otevření aplikace se zobrazí pouze základní přehled a i další záložky jsou realizovány malými informačními bloky.

Uspořádání se podobá jiným aplikacím, záložky jsou umístěny nahoře a dílčí funkce ve sloupci vlevo. Daní za uživatelskou pohodlnost je absence některých funkcí, které jiné aplikace obsahují. Rozdílné výsledky analýzy aplikací mohlo způsobit to, že data byla brána z demoverzí jednotlivých aplikací, které jsou veřejně dostupné. Je možné, že pokud by bylo čerpáno z plných verzí konkrétních aplikací, tak by se dospělo k jiným výsledkům. Hodnocení aplikací může být subjektivní, jelikož každý člověk má jiné uživatelské preference a vyhovuje mu něco jiného. Někdo má raději uživatelsky pohodlnou aplikaci a jiná osoba dává přednost velkému množství funkcí bez ohledu na komfort.

5.3.2 Testování na základě protokolů

Proběhlo také porovnání analyzovaných aplikací na bázi použitých protokolů a dalších informací o bezpečnosti jednotlivých bankovních programů. Pro sledování protokolů a síťové komunikace při přihlašování byl použit program Wireshark. Při použití jiného programu pro monitorování zkoumaných parametrů by bylo možné dospět k jiným výsledkům. Srovnání dospělo k výsledku, že za daných podmínek a použitých parametrů komparace se nejlepší ochranou prezentovaly dvě bankovní instituce. Byla to Česká spořitelna a Komerční banka, ale i mezi nimi byly nalezeny rozdíly. Komerční banka vyžadovala SMS kód při přihlášení do aplikace a Česká spořitelna zase odhlašovala po deseti minutách neaktivního klienta. Dále byly shodně zabezpečeny Raiffeisenbank a ČSOB. Z hlediska použitých parametrů se ochrana těchto bankovních domů v ničem nelišila. Používají nejaktuálnější verzi protokolu TLS, protokol IPv4 a IPv6 používají při přihlášení, stejně jako obě předchozí banky. Data v obou aplikacích jsou chráněna šifrováním a klientský i serverový klíč se po přihlášení změní. Na rozdíl od programů České spořitelny a Komerční banky tyto dvě instituce nepoužívají protokol QUIC. Tyto aplikace pak mohou být náchylnější k zneužití dat z důvodu jejich delšího pobytu na síti. Pro srovnání byly vybrány parametry verze TLS protokolu, verze IP protokolu, QUIC protokol, šifrování dat v aplikaci, změna klíče serveru a klienta po přihlášení, podpora dočasného SMS kódu při přihlášení a odhlášení neaktivního klienta. Pokud by byly vybrány odlišné parametry, výsledky by se mohli lišit od výše zmíněných.

5.3.3 Testování mechanismu CORS

Poslední částí výzkumu bylo porovnání bankovních aplikací dle přítomnosti mechanismu CORS. Když byl mechanismus v aplikaci implementován, bylo zkoumáno, jestli je kontrolován původ domény, ze které požadavek na sdílení dat do aplikace přišel. Byl využit internetový nástroj, který výše zmíněné testy realizuje. Nejlépe se prezentovala v této oblasti webová aplikace České spořitelny. Server totiž úplně odmítl provést test tohoto typu. Z toho vyplynulo, že tato aplikace nemůže být zneužita z hlediska sdílení dat napříč doménami. Dále následovala Raiffeisenbak, která mechanismus CORS implementován měla, ale byl zde kontrolován původ domény, ze které požadavek pocházel. Aplikace tak mohla bezpečně sdílet data, jelikož bylo realizováno opatření proti případnému zneužití dat. Aplikace Komerční banky a ČSOB měly mechanismus CORS implementován také, avšak opatření ke kontrole domény, ze které požadavek pocházel, už realizováno nebylo. Data tak teoreticky mohla být zneužita potencionálním útočníkem. Zabezpečení těchto dvou bankovních programů bylo v tomto směru na stejné úrovni.

6. Závěr

Dokonale ochránit aplikaci před všemi hrozbami, které dnes existují, může být dost pracné. Je třeba ošetřit všechny vstupy a výstupy s daty a nenechat žádnou část systému nezabezpečenou.

Mohlo by se zdát, že banky mají vše dokonale zabezpečeno a neměly by být v zabezpečení bankovních aplikací v podstatě žádné rozdíly. Nemusí to být ale úplně pravda. Dočasný SMS kód při přihlášení do aplikace vyžaduje pouze Komerční banka a Česká spořitelna jako jediná ze čtyř srovnávaných bank po určité době odhlašuje neaktivního klienta. QUIC protokol, který umožňuje datům, se co nejrychleji dostat k jejich adresátovi používá jen Komerční banka a Česká spořitelna. Raiffeisenbank a ČSOB tento protokol nevyužívají. Při srovnání kontroly původu požadavku v mechanismu CORS nejlépe obstála Česká spořitelna, hned po ní následovala Raiffeisenbank a na posledním místě se umístila Komerční banka společně s ČSOB.

Ze zpracovaných dat v praktické části práce za daných podmínek plyne, že obstojně chráněnou bankovní aplikaci má Česká spořitelna. Druhá v pořadí následuje Komerční banka, která má nedostatek pouze v absenci kontroly původu požadavku v mechanismu CORS. Třetí v ochraně své aplikace následuje Raiffeisenbank, která má na rozdíl od ostatních bank, vyjma České spořitelny, dobře ošetřenou kontrolu původu požadavku o sdílení dat v mechanismu CORS. Ostatní bezpečnostní aspekty nejsou na takové úrovni jako u České spořitelny nebo Komerční banky. Skupinu uzavírá banka ČSOB, která nevyniká v žádné části srovnání. Základní bezpečnostní prvky jako ostatní banky sice splňuje, ale v porovnání s ostatními bankovními institucemi lehce zaostává. V poměru uživatelského komfortu a dostupných funkcí v aplikaci ostatní banky ale převyšuje.

Jak lze vidět, i přes moderní informační technologie, bezpečnostní prvky a doporučení se zabezpečení webových aplikací českých bank v jistých směrech liší.

Jedním z přínosů této práce je, že se noví klienti na základě srovnání bezpečnosti aplikací čtyřech českých nejrozšířenějších bankovních institucí (konkrétně České spořitelny, Komerční banky, Raiffeisenbank a ČSOB) mohou rozhodnout, které z nich dají přednost při výběru banky.

7. Seznam použitých zdrojů

ACUNETIX.COM, 2012. *What is SQL injection (SQLi) and How to fix it.* [online]. [cit. 2018-01-09]. Dostupné z WWW: https://www.acunetix.com/websitesecurity/sql-injection/

ADAPTIC.CZ, 2011. *Co je to DNS.* [online]. [cit. 2018-01-02]. Dostupné z WWW: http://www.adaptic.cz/znalosti/slovnicek/dns/

BANKY.CZ. *Co je to bankomat?* [online]. [cit. 2017-11-28]. Dostupné z WWW: https://www.banky.cz/bankovni-slovnik/bankomat/

BEZPEČNÝ INTERNET, 2016. *Bezpečnost internetového bankovnictví obecně.* [online]. [cit. 2017-12-28]. Dostupné z WWW: http://www.bezpecnyinternet.cz/pokrocily/internetove-bankovnictvi/bezpecnost.aspx

BOUŠKA, Petr, 2014. *Protokoly SSL/TLS.* [online]. [cit. 2018-03-06]. Dostupné z WWW: https://www.youtube.com/watch?v=eACohWVwTOc

BOUŠOVÁ, Kateřina, 2006. *Internetové bankovnictví: Jsou vaše peníze v bezpečí?.* [online]. [cit. 2017-12-28]. Dostupné z WWW: https://www.penize.cz/bezne-ucty/18366-internetove-bankovnictvi-jsou-vase-penize-v-bezpeci

CEED.CZ, 2006. *Elektronické bankovnictví.* [online]. [cit. 2017-12-30]. Dostupné z WWW: http://www.ceed.cz/bankovnictvi/778elektronicke_bankovnictvi.htm

CNB.CZ, 2014. *Upozornění České národní banky na rizika spojená s využíváním elektronického bankovnictví.* [online]. [cit. 2017-12-30] Dostupné z WWW: https://www.cnb.cz/cs/dohled_financni_trh/vykon_dohledu/upozorneni_pro_verejnost/upozorneni_el_bankovnictvi.html

CUCU, Paul, 2017. *Session Hijacking Takes Control of Your Account. Here's how.* [online]. [cit. 2018-01-09]. Dostupné z WWW: https://heimdalsecurity.com/blog/session-hijacking/

FERSCHMANN, Petr, 2008. *Bezpečnost na webu - přehled útoků na webové aplikace - Zdroják.* [online]. [cit. 2018-01-09] Dostupné z WWW: https://www.zdrojak.cz/clanky/prehled-utoku-na-webove-aplikace/

FINANCE.CZ, 2012. *Přímé bankovnictví.* [online]. [cit. 2017-11-27]. Dostupné z WWW: https://www.finance.cz/ucty-a-sporeni/bezne-ucty/abeceda-beznych-uctu/prime-bankovnictvi/

GENIAR, Mattias. 2016. *Google's QUIC protocol: moving the web from TCP to UDP.* [online]. [cit. 2018-03-06]. Dostupné z WWW: https://ma.ttias.be/googles-quic-protocol-moving-web-tcp-udp/

GIBB, Robert, 2014. *What is CORS?* [online]. [cit. 2018-03-06]. Dostupné z WWW: https://www.maxcdn.com/one/visual-glossary/cors/

CHIP.CZ, 2015. *Jak nejlépe ochránit svůj počítač?* [online]. [cit. 2017-12-30] Dostupné z WWW: http://ppk.chip.cz/cs/poradna/bezpecnost/firewally/jak-nejlepe-ochranit-svuj-pocitac.html

INTERSERVER.NET, 2016. *What is session hijacking and how to prevent it? - Interserver tips.* [online]. [cit. 2018-01-09] Dostupné z WWW: https://www.interserver.net/tips/kb/session-hijacking-prevent/

IT-SLOVNÍK.CZ, 2012. *Co je to paket?* [online]. [cit. 2018-01-02] Dostupné z WWW: https://it-slovnik.cz/pojem/paket

JAVASCRIPT.INFO, 2017. *The clickjacking attack.* [online]. [cit. 2018-01-09]. Dostupné z WWW: https://javascript.info/clickjacking

JECAS.CZ, 2014. *Využití XSS díry.* [online]. [cit. 2018-01-09]. Dostupné z WWW: http://jecas.cz/xss

KABELOVÁ, Alena, DOSTÁLEK, Libor, 2012. *Velký průvodce protokoly TCP/IP a systémem DNS.* Brno: Computer Press, 488 s. 5. aktualiz. vyd. ISBN: 978-80-251-2236-5.

KAFKA, Jaroslav, 2006. *Přímé bankovnictví v Česku.* [online]. [cit. 2017-12-30]. Dostupné z WWW: https://finexpert.e15.cz/prime-bankovnictvi-v-cesku

KEJDUŠ, Radek, 2012. *Technologie počítačové sítě: Jak pracuje TCP/IP a ISO/OSI.* [online]. [cit. 2018-01-02]. Dostupné z WWW: https://www.cnews.cz/technologie-pocitacove-site-jak-pracuje-tcpip-a-isoosi/

KONEČNÝ, Martin, 2015. *Obrana proti útoku XSS v PHP.* [online]. [cit. 2018-01-09] Dostupné z WWW: https://www.itnetwork.cz/php/bezpecnost/tutorial-bezpecnost-v-php--utoku-xss-a-obrana

MANAGEMENTMANIA.COM, 2015. *Pharming.* [online]. [cit. 2017-12-30]. Dostupné z WWW: https://managementmania.com/cs/pharming

MINISTERSTVO FINANCÍ, 2014. *Slovník pojmů.* [online]. [cit. 2017-12-28] Dostupné z WWW: https://www.psfv.cz/cs/slovnik-pojmu#tab-slovnik-pojmu-p

MITCHELL, Bradley, 2017. *HTTP: The Protocol That Makes the Internet Work.* [online]. [cit. 2018-02-12]. Dostupné z WWW: https://www.lifewire.com/hypertext-transfer-protocol-817944

NIC.CZ, 2007. *CZ.NIC - O doménách a DNS.* [online] [cit. 2018-02-12] Dostupné z WWW: https://www.nic.cz/page/312/o-domenach-a-dns/

NYKODÝMOVÁ, Helena, 2006. *Jak je to s bezpečností internetového bankovnictví.* [online]. [cit. 2017-12-28]. Dostupné z WWW: https://www.lupa.cz/clanky/jak-je-to-s-bezpecnosti-internetoveho-bankovnictvi/ ISSN: 1213-0702.

PBWCZ.CZ, 2017. *Cross-site request forgery Cross.* [online]. [cit. 2018-01-09] Dostupné z WWW: http://www.pbwcz.cz/Pocitacovy%20utok/Databaze/crosssite_request_forgery_cross.html

POSTSIGNUM.CZ. *Kvalifikované certifikáty.* [online]. [cit. 2017-12-28]. Dostupné z WWW: http://www.postsignum.cz/kvalifikovane_certifikaty.html

PŘIBYL, Tomáš. 2006. *Zákeřný útok jménem DoS*. [online]. [cit. 2018-01-09] Dostupné z WWW: https://www.systemonline.cz/it-security/zakerny-utok-jmenem-dos.htm ISSN: 1802-615X

ROOT.CZ, 2017. *Útoky hrubou silou stále fungují, z redakčních systémů dělají botnety - Root.cz.* [online]. [cit. 2018-01-09] Dostupné z WWW: https://www.root.cz/clanky/utoky-hrubou-silou-stale-funguji-z-redakcnich-systemu-delaji-botnety/. 1212-8309. ISSN: 1212-8309

ROUSE, Margaret, 2008. *What is internet protocol?* [online]. [cit. 2018-01-02]. Dostupné z WWW: http://searchunifiedcommunications.techtarget.com/definition/Internet-Protocol

SATRAPA, Pavel. 2011. *Internetový protokol verze 6.* Praha: CZ.NIC. 409 s. aktualiz. a dopl. vyd. ISBN: 978-80-904248-4-5.

SECURITY-PORTAL.CZ, 2013. *Seznamte se - DoS a DDoS útoky*. [online]. [cit. 2018-01-09]. Dostupné z WWW: http://www.security-portal.cz/clanky/seznamte-se-%E2%80%93-dos-ddos-%C3%BAtoky

SLÍŽEK, David, 2006. *Co je to phishing?* [online]. [cit. 2017-12-30]. Dostupné z WWW: https://zpravy.aktualne.cz/ekonomika/ceska-ekonomika/co-je-to-phishing/r~i:article:221550/

ŠPAČEK, Michal, 2014. *5 typů kyber-útoků na e-shopy a jak se jim bránit.* [online]. [cit. 2018-01-09]. Dostupné z WWW: https://www.shopsys.cz/clanky/5-typu-kyber-utoku-na-eshopy-a-jak-se-jim-branit/

TIMEHOSTING.CZ. 2014. *Cross-Site Request Forgery - Jak na webové stránky.* [online]. [cit. 2018-01-09]. Dostupné z WWW: http://timehosting.cz/cross-site-request-forgery/

TŮMOVÁ, Věra, 2008. *Odkud kam míří český internetbanking.* [online]. [cit. 2017-11-27]. Dostupné z WWW: https://www.penize.cz/prime-bankovnictvi/42614-odkud-kam-miri-cesky-internetbanking

ZÁMEČNÍK, Petr, KRČMÁŘ, Petr, 2005. *Analýza zabezpečení internetového bankovnictví v České republice.* [online]. [cit. 2017-12-28]. Dostupné z WWW: http://i.iinfo.cz/urs-att/Mesec.cz-studie_int.bankovnictvi-112002647608700.pdf

ZLATAKORUNA.CZ, 2003. *Co byste měli vědět o elektronickém bankovnictví.* [online]. [cit. 2017-12-30] Dostupné z WWW: http://www.zlatakoruna.info/zpravy/e-bankovnictvi/co-byste-meli-vedet-o-elektronickem-bankovnictvi

8. Přílohy

8.1 Seznam obrázků

8.2 Seznam tabulek

8.3 Obrázky získaných dat z CORS testů

CORS Information

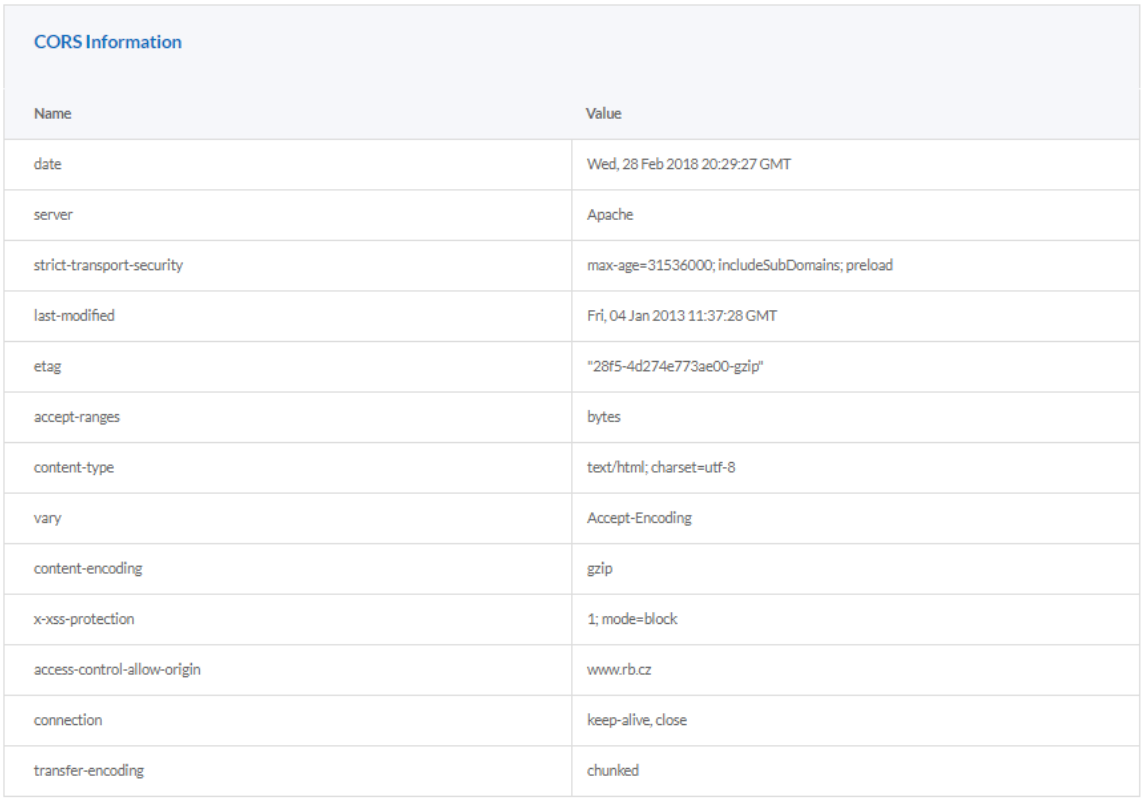
Name	Value
date	Wed, 28 Feb 2018 20:02:31 GMT
strict-transport-security	max-age=16070400; includeSubDomains
x-frame-options	SAMEORIGIN, SAMEORIGIN
x-powered-by	Servlet/3.0
x-content-type-options	nosniff
x-xss-protection	1
expires	Thu, 01 Jan 1970 00:00:00 GMT
cache-control	private, no-cache, no-store, must-revalidate
pragma	no-cache
pdp-current-url	/prihlaseni
content-security-policy	default-src 'none'; img-src 'self' tracking-secure.csob.cz b2bpr.vaservices.eu statistics.csob.cz data:; connect-src 'self' ocim.csob.cz; script-src 'self' 'unsafe-inline' 'unsafe-eval' statistics.csob.cz; style-src 'self' 'unsafe-inline'; font-src 'self' data:; object-src 'self'; frame-ancestors 'none'
content-type	text/html; charset=UTF-8
content-language	en-US
connection	close
set-cookie	GUEST_LANGUAGE_ID=cs_CZ; Expires=Thu, 28-Feb-19 20:02:30 GMT; Path=/; Secure; HttpOnlysrv=1IB_BLUE_03;path=/;Secure;HttpOnlyONE_Ibcsob_SESSION=554a76f82173d036e855ec56068625264ec01feabd5657d498081a87c08601ad;Path=/;Domain=ib.csob.cz;Version=1;Secure;HttponlyTS015763f0=0154fb53f2422697399831ebb81188e12a1fac10cc93bc720d7aee3c6a2cb1f9725c19f4a44c60a0acb7aff62d8e3e88c6cb4e66b063b48d9a056afbd371b2b34ee0f81f6aa3f6a22ac7d4a68c45f21edd7adad139;Path=/TS013467b1=0154fb53f22b5bd522cd59923c7537fd11556fa31393bc720d7ae3c6a2cb1f9725c19f4a41b573c76e2fdade8593afa72eb3eb9aa79323f981b714a36b9efa82e14803a9c; path=/; domain=ib.csob.cz
vary	Accept-Encoding
content-encoding	gzip
transfer-encoding	chunked

Obrázek 9 - CORS data - ČSOB

CORS Information

Name	Value
date	Wed, 28 Feb 2018 20:24:27 GMT
x-frame-options	SAMEORIGIN
last-modified	Tue, 19 Dec 2017 12:35:28 GMT
accept-ranges	bytes
vary	Accept-Encoding
content-encoding	gzip
cache-control	max-age=0, no-cache, no-store, must-revalidate
pragma	no-cache
note	CACHING IS DISABLED ON LOCALHOST
expires	Wed, 11 Jan 1984 05:00:00 GMT
x-xss-protection	1; mode=block
x-content-type-options	nosniff
content-length	7861
content-type	text/html
connection	close
strict-transport-security	max-age=16070400; includeSubDomains

Obrázek 10 - CORS data - Komerční banka



CORS Information

Name	Value
date	Wed, 28 Feb 2018 20:29:27 GMT
server	Apache
strict-transport-security	max-age=31536000; includeSubDomains; preload
last-modified	Fri, 04 Jan 2013 11:37:28 GMT
etag	"28f5-4d274e773ae00-gzip"
accept-ranges	bytes
content-type	text/html; charset=utf-8
vary	Accept-Encoding
content-encoding	gzip
x-xss-protection	1; mode=block
access-control-allow-origin	www.rb.cz
connection	keep-alive, close
transfer-encoding	chunked

Obrázek 11 - CORS data - Raiffeisenbank